DEFEATING COERCIVE INFORMATION OPERATIONS IN FUTURE CRISES

National Security Perspective

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

DEFEATING COERCIVE INFORMATION OPERATIONS IN FUTURE CRISES

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

This National Security Perspective contains the best opinion of the author(s) at time of issue. It does not necessarily represent the opinion of JHU/APL sponsors.

NSAD-R-21-002

Contents

Figures

Image credits:

Figure 1. Conflict Continuum. Adapted from US Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: JCS, January 17, 2017; incorporating Change 1, October 22, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

Figure 2. Percentage of US Adults Who Get News Often from Each Platform. Reproduced from "Social Media Outpaces Print Newspapers in the U.S. as a News Source," Pew Research Center, Washington, DC, December 18, 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

Figure 3. Public Trust in the Federal Government, 1958–2019. Reproduced from "Public Trust in Government: 1958–2019, "Pew Research Center, Washington, DC, April 11, 2019, https://www.people-press.org/2019/04/11/public-trust-in-government-1958-2019/.

Summary

For thousands of years, combatants have spread falsehoods to help achieve victory. Many of their efforts failed or backfired. However, with the rise of social media and sophisticated technologies to exploit it, attackers have potent new means of conducting information operations (IOs) to shape their victims' perceptions and coerce them to yield in future crises.

The IO campaigns that Beijing and Moscow are conducting today against the United States provide a starting point for assessing potential US vulnerabilities to coercion. Deepfake technologies, techniques for manipulating social media algorithms, and other tools used to influence our elections can all be repurposed to shape American perceptions in regional crises. Ongoing Chinese and Russian efforts to weaken public confidence in the integrity of US leaders and institutions (including IOs to exploit the COVID-19 pandemic) also help prepare the cognitive battlefield for future coercive campaigns.

But today's IOs differ from the coercive pressures that the United States could face in an edge-of-war confrontation in the South China Sea, the Baltics, or other potential conflict zones. Coercion relies on threats of punishment to convince an adversary to yield in a crisis. In particular, by threatening to inflict suffering on an opponent, coercive campaigns seek to convince opposing leaders that the costs of continuing to resist outweigh the benefits of doing so. If IOs alone fail to achieve capitulation, attackers can make good on their punitive threats and pair destructive attacks with warnings that further suffering will follow unless the opponent capitulates.

This study examines how China and Russia can convey vivid, exquisitely targeted messaging during regional crises, crafted to convince the US public and senior officials that unless the US backs down, Americans will suffer costs far beyond what they are willing to pay for the sake of regional allies. The study also analyzes how Beijing and Moscow can fuel mutually reinforcing doubts between US leaders and their foreign counterparts as to whether they will live up to their defense commitments as war looms. Based on these threat assessments, the study identifies specific gaps in US preparedness against coercive IOs and identifies options for building resilience against them—including new forms of emergency coordination between social media companies and federal agencies.

US policymakers should also prepare for the risk that adversaries will carry out their threats to inflict suffering on the American population. If the president stands firm against coercive IOs, China and Russia may strike the power grid or other US targets to (1) magnify public fears and raise the perceived costs of defending US allies and (2) reinforce the cognitive impact of those attacks with warnings that more devastation will follow unless the president caves in.

Of course, the US could respond to any such attack by inflicting costs on China and Russia that their leaders would find unacceptable. Striking US targets could also launch a spiral of uncontrolled escalation. These escalatory dangers help make combined attacks (which employ both IOs and cyber or kinetic weapons) much less likely than IO-only operations.

Yet, it would be shortsighted to ignore the risk that in a confrontation over the very highest of stakes, Beijing or Moscow might resort to combined attacks if IOs alone fail to drive a US retreat. The doctrines of both nations envision the combined use of information and destructive cyber operations at the outset of armed conflict, tailored to convince the opposing leaders that they cannot hope to win at an acceptable price. Chinese and Russian doctrines also offer precepts for managing escalatory risks and for manipulating the enemy's fears of escalation for coercive leverage. This study examines how Beijing and Moscow may use IOs to achieve such manipulation and suggests possible countermeasures.

Alexander George and other theorists of coercion highlight an additional opportunity for attackers to manage escalation. Rather than conduct massive strikes that could provoke an equivalent response, attackers can launch small-scale, "exemplary" strikes to illustrate the suffering that they can inflict while also warning of worse horrors to follow. IOs delivered via social media are ideally suited to magnify the coercive effects of such exemplary attacks.

The Kremlin has already tested the use of IOs to incite public alarm over (faked) infrastructure disruptions. In 2014, Russia's Internet Research Agency launched a social media attack on St. Mary Parish, Louisiana, to convince residents that an explosion at a chemical plant threatened their safety. Although no such explosion had occurred, seemingly realistic reports of toxic fume releases metastasized in minutes via text messages, Twitter, Facebook, YouTube, and other platforms.[1] Parish officials moved quickly to persuade area residents that they were safe. But calming US citizens will be vastly more difficult if China or Russia pairs IOs with exemplary cyberattacks that actually do release toxic clouds, cripple regional hospitals, or create other disruptions that reinforce the population's dread of further punishment. Adversaries could also supplement coercive strikes with IOs to convince American families that they are suffering on behalf of worthless, unreliable allies.

Beijing and Moscow can seek to drive US crisis decision-making in three distinct but mutually supportive ways. All three are suitable for use with IOs alone rather than in combination with cyber or kinetic attacks. Indeed, because "IO-only" campaigns offer US adversaries the lowest-risk opportunity to prevail in an intensifying political confrontation, they will almost certainly pursue that option if they think it may succeed. Yet, all three pathways for coercing US behavior are equally well suited for combined attacks and take advantage of major gaps in US strategies, defensive capabilities, and coordination mechanisms.

Social media lends unprecedented effectiveness to the first and most familiar means of coercion: the threatened or actual punishment of an opponent's population. The American public is much more vulnerable to manipulation through social media than via other means of communication and is especially prone to believing (and to persisting in believing) disinformation conveyed during disasters or other stressful events.[2] Beijing and Moscow have gained enormous expertise in exploiting social media algorithms that could help them conduct such messaging. They can also tailor their threats to specific population segments and "influencers" and—with the help of artificial intelligence (AI) programs—convey microtargeted IOs on a massive scale.[3] Together with improvements in deepfake capabilities and other technological advances, as well as the personal data that China and Russia have amassed on US citizens, these nations can deliver coercive messaging in extraordinarily effective ways.

US opponents can also use a less studied but increasingly prominent coercive strategy. Rather than threatening to punish an enemy's population to exert pressure on leadership decision-making, an attacker can target IOs against opposing leaders to directly shape their perceptions and behavior. The *National*

[1] Chen, "The Agency."

[2] Vosoughi, Roy, and Aral, "Spread of True and False News Online," 1146; and Bongar et al., *Psychology of Terrorism*, 122.

[3] NSCAI, *Final Report*, 22.

Counterintelligence Strategy of the United States of America 2020–2022 (January 2020) warns that adversaries are already conducting campaigns to "influence and deceive key decision makers" in the United States.[4] We should expect Chinese operatives to use the personal data they have stolen on US security clearance holders from the Office of Personnel Management and other hacks. We should also prepare for Moscow to apply lessons learned from its past operations against US legislators and others who may influence the administration's decision-making in future crises. In addition, building on current Chinese and Russian influence campaigns against US military personnel, these nations may target IOs against senior US military leaders who develop the operational plans for regional contingencies, the military units assigned to execute those plans, and their families.

A third coercive strategy will be especially useful in regional conflicts: employing IOs against the leadership and population of US allies. China and Russia are already conducting disinformation campaigns to weaken the cohesion of NATO and other alliances. Those nations are also using IOs to cast doubt on the willingness and ability of the US to live up to its defense commitments. In future crises, Beijing and Moscow are likely to sharpen the focus of such messaging to undermine allied support for specific coalition operations. For example, if an intense crisis emerges in the Baltics, Russia may use IOs to delay and confuse NATO decision-making and (via threats of punishment) convince one or more members to block military operations under Article 5. More broadly, Beijing and Moscow may warn US security partners that they will incur terrible consequences if they request American military assistance or permit the use of their ports and other infrastructure to support coalition warfighting.

These three means of coercing US and alliance behavior are not mutually exclusive. Quite the contrary: adversaries may simultaneously employ all of them to achieve synergistic, multi-layered influence over US decision-making. US strategies against coercion will need to account for such "all of the above" operations. Our strategy should also integrate measures against both threatened and actual cyberattacks. As the United States strengthens its resilience against IO-only campaigns and reduces their chances of success, adversaries may turn to exemplary strikes as a more effective (though also more dangerous) alternative. This study examines opportunities to build playbooks that encompass both IO and infrastructure defense operations in ways that barely exist today. The study also explores how we can shift the adversary's own calculus of the costs and benefits of conducting combined attacks against the United States. Specific options to tilt adversary assessments and develop overarching strategies against coercion follow below, initially for IO-only campaigns and then for combined information-cyberattacks.

Pair Attack Suppression Abroad with Defensive Operations at Home

The US may be able to block coercive IOs by disrupting the infrastructure and operations used to launch them from Shanghai, St. Petersburg, or other locations abroad. The Department of Defense (DoD) has demonstrated its ability to conduct such operations. The US Cyber Command successfully prevented the Internet Research Agency from targeting the United States with IOs just before the 2018 midterm elections. The command followed up in November 2020 by countering Iranian efforts to influence the presidential election.[5] Equivalent operations could help defeat campaigns to shape US perceptions and behavior in

[4] NCSC, *National Counterintelligence Strategy*, 9.

[5] Nakashima, "U.S. Undertook Cyber Operation."

future crises. DoD components and their intelligence community partners should continue to strengthen (and, as necessary, use) their plans and capabilities to disrupt IO campaigns conducted by facilities abroad.

However, the United States cannot solely rely on suppressing attacks from foreign territory. China and Russia are almost certainly hardening their attack infrastructure and taking other measures to ensure their IOs reach American audiences. Most importantly, Russia is increasingly employing US-based servers, virtual private networks, and unwitting US citizens to deliver disinformation. That shift is no coincidence. The National Security Agency and other DoD components have extensive capabilities to detect and disrupt IO campaigns. Yet, they have very limited authorities to monitor US infrastructure and conduct domestic operations to defend it. Adversaries are taking advantage of these legal constraints to maneuver around our stoutest defenses. They are sure to do the same in future coercive campaigns.

The limits on DoD's ability to operate at home are sensible and should stay in place. Rather than expand DoD's authorities to monitor and defend infrastructure within the United States, the Department of Homeland Security and other non-DoD agencies should partner with the private sector to help defeat coercive campaigns conducted on or against American territory. The United States should also develop plans and coordination mechanisms to integrate operations at home and abroad to maximize the effectiveness of both and achieve *defense in depth*.

Develop a Defensive Strategy for IOs in the Dark-Gray Zone

US policymakers and analysts are intensifying their focus on threats in the gray zone—that is, operations in the space "beyond diplomacy and short of conventional war."[6] IOs constitute a primary tool for Chinese and Russian gray-zone campaigns against the United States. Before Kathleen Hicks became deputy secretary of defense, she co-led a study detailing how US competitors are using IOs to break down the authority and legitimacy of US institutions. Hicks and her coauthors also found that the "United States has yet to formulate a synchronized and coherent approach to counter information operations targeting US interests at home and abroad," reflecting a "lack of serious strategy devoted to this gray zone activity."[7]

That strategic vacuum applies to coercive IOs as well. IO-only campaigns to drive US decision-making are a subset of the broader gray-zone challenge. However, they occupy the darkest portion of that realm. Chinese and Russian measures to weaken the legitimacy of US institutions and democratic governance constitute a long-term strategic campaign that—unless effectively countered—will help those nations strengthen their power relative to the United States on their periphery and around the globe. IOs to shape US crisis decision-making represent a very different challenge. Such operations are most likely to occur in deepening, high-stakes disputes involving American security partners, where risks of war are vastly greater than those posed during the day-to-day corrosive information campaigns that the US currently confronts.

It is very likely that the White House situation room will also be operating in an entirely different mode. Every person in that room, along with their advisors and families, may be faced with deeply personalized messaging intended to shape their views of the crisis. Adversaries may simultaneously subject tens of millions of Americans to frightful threats and imagery, promising that their families will suffer if the president continues to defend an ally that many of them could not even find on a map.

[6] Dalton et al., *By Other Means*.

[7] Dalton et al., *By Other Means*, 6 and 8.

Chinese and Russian operations to implant malware on US infrastructure lay the groundwork for such coercive IOs. The *National Counterintelligence Strategy* cautions that adversaries are developing the capacity to degrade critical infrastructure and that "their efforts likely are aimed at influencing or coercing U.S. decision-makers in a time of crisis by holding critical infrastructure at risk of disruption."[8] Infrastructure operators and government agencies should accelerate their development of specialized resilience initiatives to counter such threats. For example, just as electric utilities take extensive emergency measures when hurricanes approach, they are also developing plans to "raise the cyber gates" in an intensifying crisis, and take well-publicized (as well as covert) pre-attack measures to protect their systems and prepare for accelerated restoration of power to water systems, military bases, and other critical customers. Countering coercive threats should be a key feature of playbooks for such emergency operations.

Focus on Protecting the Constitution

Defensive strategies should do more than respond to adversary threats. They should also uphold American values and principles of democratic governance. Coercive threats pose major challenges for charting such a way forward. The United States confronts an asymmetric information environment vis-à-vis China and Russia. China's Great Firewall (and Russia's declared ability to erect a similar barrier in future crises) can cut citizens off from all but state-approved sources of information. At the same time, Beijing and Moscow enjoy unfettered access to the US public and can exploit the First Amendment for a one-sided advantage in information warfare.

The worst option for fixing this asymmetry would be for the United States to mimic its adversaries. Blocking citizens' access to coercive enemy messaging or prohibiting them from spreading that messaging from their own social media accounts would risk compromising their rights to free speech. For decades, Supreme Court rulings have given increasing substance and scope to First Amendment rights to receive information and ideas. These decisions cast doubt on the constitutionality of restricting citizen access to foreign speech, even if that speech promotes falsehoods or conveys enemy propaganda. Adversaries would like nothing better than to have the US government jettison the First Amendment in future crises and emulate their techniques of censorship and repression. Developing strategies to defeat coercive campaigns without trampling on the Constitution is of core importance.

Moreover, based on Chaplinsky v. New Hampshire and other Supreme Court rulings, opportunities may exist within the Constitution to constrain enemy messaging that conveys threats of punishment and seeks to incite public disorder.[9] Specific options for further analysis include the following:

- build consensus with social media companies on developing and applying specialized filters to block coercive messaging during crises, focusing on content that threatens cyberattacks and other means of inflicting punishment on the US population;
- amend Section 230 of the Communications Decency Act to enable new regulatory initiatives, ideally developed in consultation with the private sector, to help counter emerging adversary tactics, techniques, and procedures to exploit social media; and

[8] NCSC, *National Counterintelligence Strategy*, 6.

[9] Blitz, "Lies, Line Drawing, and (Deep) Fakes," 76.

- leverage the extensive presidential authorities under Section 706 of the Communications Act to create new emergency plans and capabilities to counter coercive campaigns in regional confrontations.

Bolster In Extremis Industry–Government Collaboration

Forging government–industry agreement on how to block coercive IOs will be as difficult as it is important. Google, Facebook, and other companies are ramping up their efforts to detect and filter disinformation from China and Russia, most recently with respect to COVID-19. Yet, efforts to expand on this progress to help defeat coercive campaigns will confront deep-seated problems. For example, the data sets and algorithms that help platform advertisers target their ads are ripe for Chinese and Russian exploitation in future crises. Accounting for the global business models of major platforms and their techniques for maximizing revenue will also present complex challenges for collaborative operations.

Developing criteria to block Chinese- and Russian-generated content will present additional problems. Many existing platform policies for content assessment and filtering are fairly straightforward, including those for child pornography and snuff videos. Coercive messaging will have entirely different content. Yet, those differences could also provide the basis for narrowly targeted standards for filtering. Beijing and Moscow will seek to coerce US behavior by threatening to inflict suffering on the US public. It should be possible to agree on the nature of that distinctive content. And because adversaries will likely conduct coercive campaigns only in severe crises, it may also be possible for the United States and social media platforms to agree on specialized, "just break glass" emergency coordination and information-sharing mechanisms to use in predefined circumstances.

Reaching agreement on such issues will only begin to build genuine capacity to defeat coercive IOs. Industry and government will need to develop and exercise playbooks for response operations. These partners will also need to account for the near-certainty that when defensive measures begin, China and Russia will tell Americans that the president is violating their constitutional freedoms, while also seeking to intensify partisan conflict over defending US allies in a crisis.

Identify Gaps in Counter-messaging and Other Critical Requirements

In the current fiscal environment, it will be essential to prioritize IO defense initiatives that offer the greatest benefits relative to the investments they require. The development of counter-messaging plans and capabilities exemplifies such high-payoff opportunities. To reduce the vulnerability of the US public to coercive IOs, the United States should develop programs that help the public discern and discount adversary messaging. However, such efforts will take years to succeed, especially given the Chinese and Russian advances in deceptive technologies and persuasive techniques analyzed in this study. We should assume that early in a crisis, adversaries will successfully reach US social media users with their coercive threats. The president and other senior officials must be ready and able to counter such messaging and limit the fears that promised or actual cyberattacks will create.

Doing so will entail novel defensive requirements. Research has found that once social media users adopt a belief, they tend to stick with it even in the face of evidence to the contrary.[10] The result: China and Russia can gain a first-mover advantage by launching IOs early in an emerging crisis. Rapid and nimble counter-messaging will be crucial to limit their ability to exploit this advantage. Indeed, US and allied governments should be prepared to preempt enemy IOs and blunt in advance the coercive threats and crisis-oriented disinformation that Beijing and Russia are likely to convey. Since these nations will rely on social media to launch such IOs, building coordination mechanisms and playbooks for counter-messaging should become a top priority for federal agencies and their social media partners.

An additional challenge lies in the propensity of many Americans to disbelieve their leaders. In decades past, presidents could benefit from a "rally round the flag" effect that often occurred during crises and generated public support for standing firm against US opponents. But public confidence in US leaders has been declining. A September 2020 poll by the Pew Research Center found that only 20 percent of Americans trust the federal government.[11] That decline has occurred over many years. Ongoing Russian (and more recently, Chinese) IOs seek to deepen and accelerate the public's loss of faith in US leaders. It would be foolish to rely on a rally-round-the-flag effect in the emerging, and highly contested, information environment. Instead, the president's messaging will need to account for the decline of public trust and for Chinese and Russian IOs to exploit it in a crisis.

Prepare against Combined Information-Cyberattacks

The recommendations offered thus far focus on IO campaigns that Beijing and Moscow will employ in the dark-gray zone, when they approach the edge of war. The United States must also be prepared for them go over the edge and reinforce their coercive messaging with cyber or kinetic attacks. Intensive efforts are underway to counter improving Chinese and Russian capabilities to defeat US forces in regional contingencies. Policymakers should align those efforts with measures to defeat combined attacks against the United States itself, and deny adversaries any hope of coercing their way to an early, low-cost victory.

The prerequisite to do so is to clarify how IOs can intensify the cognitive impact of cyber-induced damage to US infrastructure and other targets. A number of studies contend that cyberattacks offer little value for coercion.[12] They argue that cyberattacks are poorly suited to communicate coercive threats and may not be able to incite sufficient fear to drive government decision-making. However, none of these studies account for the danger that adversaries will supplement cyberattacks with IOs to overcome these limitations. China and Russia can tailor messaging in combined attacks to explicitly convey their demands for settling a crisis. As noted above, they can also use IOs to magnify the fear created by even limited, exemplary attacks and issue graphic warnings of wider destruction to follow.

[10] Nemr and Gangware, *Weapons of Mass Distraction*, 9–12; and Wadley, "Why People Are Resistant to Correcting Misinformation."

[11] Pew Research Center, *Americans' Views of Government*.

[12] Borghard and Lonergan, "Coercion in Cyberspace," 480; Valeriano, Jensen, and Maness, *Cyber Strategy*, 51–52 and 89–90; and Lindsay and Gartzke, "Coercion through Cyberspace," 3–4 and 9.

It would be a mistake to develop separate US strategies against coercion for peacetime and war. Chinese and Russian doctrines envision the use of IOs from the outset of a crisis through full-scale combat.[13] The United States and its security partners need equivalent strategies for defense across the continuum of conflict. Those strategies also need to include special measures to deal with the transition from peace to war. Drawing on lessons learned from Russia's invasion of Crimea in 2014, adversaries may seek to delay and confuse allied decision-making regarding their initial attacks and establish local military dominance early in a regional conflict that might be costly to overcome. Defensive strategies should put a premium on countering such deceptive tactics and the IOs that enable them.

Prepare for the Synergistic Effects of IOs and Cyberattacks

Coercive messaging can do more than exacerbate the psychological impact of strikes against US infrastructure. To develop a strategy against combined operations, US policymakers need to draw on recent conflicts—and their imaginations—to anticipate how the combination of cyberattacks with IOs can create novel US defensive challenges. The selective disruption of US communications systems offers a prime example. To support Russia's invasion of Crimea, the Kremlin cut off systems that Ukraine's government could use to communicate with its own citizens while simultaneously using Russian-controlled television stations to flood the region with disinformation about the nature and scale of the attack.[14] China and Russia may use similar tactics against the United States. That is, they will seek to disrupt the systems on which the president will rely to communicate with the US public while exploiting the social media platforms they "own" to control and dominate information about the crisis.

The federal government has networks for classified communications that are hardened against cyberattacks and other types of disruption. Telecommunications companies are strengthening the resilience of their own systems, including against Chinese and Russian efforts to corrupt the supply chains on which those companies rely. Using the National Security Telecommunications Advisory Committee as a forum for discussion and bringing in greater representation from social media companies, industry and government should develop plans and capabilities to counter strategies of selective disruption.

Policymakers should also overcome the current stovepiping of IO and cybersecurity initiatives, and integrate them into a unified strategy against coercion. US infrastructure owners and operators are aggressively improving the cyber resilience of their systems and (in partnership with government agencies) are building increasingly detailed playbooks to restore service to critical customers if disruptive attacks occur. But those industry and government plans have only begun to address the risk that adversaries will employ IOs to impede cyber mutual-assistance programs and disrupt the situational awareness on which response operations depend.

On a completely separate path, government agencies and social media companies are taking aggressive steps to counter foreign influence campaigns in today's "blue sky" environment. Yet, they are ill-prepared to do so in the face of attacks on the voice or internet communications they use for information sharing, much less attacks on water, power, and other services vital to the well-being of their employees. We are

[13] Beauchamp-Mustafaga, "Cognitive Domain Operations," 24; and *Hearing on Disinformation in the Gray Zone*, Maier statement.

[14] White, *Lessons from the Russia-Georgia War*.

creating independent cylinders of excellence for IOs and cybersecurity. Integrating them should become key strategic goal.

Bolster Alliances against Hybrid Warfare and Coercion by Denial

Rather than conduct combined attacks against the United States alone, China and Russia are likely to also target US security partners and use specialized tactics to weaken alliance cohesion and defensive operations. Russia's hybrid warfare operations have illuminated some of the IOs that might be used for this purpose. While neither Russia nor China uses the term hybrid warfare to refer to their own military doctrines and operations, NATO employs it to encompass the unconventional warfare operations conducted by Russia against Ukraine and other nations in eastern Europe. Russia used IOs to delay and confuse decisions by Western nations as to whether and how to assist Ukraine as "little green men" poured across its borders. NATO's North Atlantic Council needs to strengthen its mechanisms for crisis decision-making against such hybrid tactics.

NATO members should also continue to examine lessons from Russia's first-ever pairing of IOs with cyberattacks on Ukraine's power grid. The brief blackouts that Russia created failed to weaken the resolve of Ukrainian leaders to resist the invasion.[15] But given advances in Russian and Chinese cyberattack capabilities, US and allied strategies against coercion must anticipate much more devastating outages, paired with IOs to intensify pressure on alliance members to peel off and yield to the adversary's demands.

Adversaries may also strike US and allied military assets and supporting civilian infrastructure to achieve "coercion by denial." In a comprehensive analysis of past coercive campaigns, Robert Pape finds that they are most likely to succeed by using denial strategies rather than by inflicting punishment on an opponent's population. Coercion by denial seeks to thwart an adversary's military strategy for achieving its goals. By selectively degrading the adversary's military capabilities and dooming its strategy to failure, the coercer seeks to convince the enemy to back down and—ideally—enable themselves to win at a lower cost than would be required to obliterate the opposing force.[16] Put in the broader calculus of coercion, denial functions by reducing the benefits that the enemy expects to gain through further resistance relative to the costs of continuing to fight. Pape's analysis preceded the rise of sophisticated IO capabilities. Almost certainly, however, future efforts at coercion by denial will include messaging to reinforce the cognitive impact of cyber and kinetic attacks and further convince opposing leaders that they have no hope of prevailing at an acceptable cost.

DoD should conduct a self-assessment of its regional warfighting plans to identify potential vulnerabilities to coercion by denial. This study provides a case study of how to do so. To achieve victory in East Asia, the Baltics, or other conflict zones, DoD will need to surge forces from installations in the United States to those regions. US defense officials warn that adversaries may seek to disrupt and delay such deployments by striking US ports and transportation systems while also sending more of their own forces into the contested region and consolidating their gains. Attacks on allied ports slated to receive US forces and support their onward movement could put the US at a further disadvantage. If sufficiently disruptive, such

[15] Resnikov, "Russia Remains Unwilling."

[16] This characterization of denial draws on the analysis provided by Pape, *Bombing to Win*, 10, 13, and 17–20; and Art and Greenhill, "Coercion," 20–22.

operations might indeed reduce US chances of victory, raise the costs of retaking the region, and (paired with IOs) help convince the president to sue for peace.

If Chinese and Russian leaders launched such large-scale attacks on US infrastructure, they would face the prospect of suffering unacceptable costs in response. That danger minimizes the chances that they will employ coercion by denial. Yet, DoD is already developing new weapons and tactics to prevent China and Russia from denying US access to conflict zones on their periphery. As those efforts go forward, DoD should account for both the physical and cognitive realms of regional conflicts and (with the help of domestic agencies and infrastructure owners) reduce the potential vulnerability of the United States to coercion by denial.

Deterrence as the Top Priority for Further Analysis

While this study focuses on assessing coercive threats and implications for developing US and allied strategies to defeat them, other topics also merit analysis by scholars and policymakers. Three issues are particularly important. The first is how to organize the federal government for defensive planning and operations. Congress and the administration should consider options to kick-start progress by assigning those missions to the organizations that are already responsible for countering election interference and ongoing corrosive campaigns against democratic governance. The Department of Homeland Security's Countering Foreign Influence Task Force and the Federal Bureau of Investigation's Foreign Influence Task Force offer especially promising opportunities for such progress. The same is true of the State Department's Global Engagement Center and programs by the Federal Emergency Management Agency and Department of Homeland Security to counter disinformation during disasters. Most recently, the Office of the Director of National Intelligence is creating the Foreign Malign Influence Center to serve as a clearinghouse for intelligence related to malign influence from multiple government agencies and provide assessments and warning of such activities.[17]

But it would be miraculous if these legacy programs somehow coalesced into a coherent whole to meet coercive threats the United States has never before faced. Rather than wait for a miracle, policymakers should create a strategy to integrate existing building blocks for progress, fill the gaps between them, and uphold the very constitutional liberties that adversaries seek to exploit. Policymakers can also facilitate integrated, government-wide progress by expanding DoD's support to other agencies in ways that utilize the department's unique IO expertise and capabilities. This study explores options for focusing such defense support to provide the greatest and most immediate benefits.

A second priority for follow-on analysis lies in looking beyond Chinese and Russian threats and accounting for the strategies that other potential adversaries may employ. Syria, Iran, and North Korea, for example, may be more willing to target coercive operations against the US financial system because of their lack of interdependence with the US economy. The Department of the Treasury and the financial services sector are already taking aggressive measures to protect financial systems from cyberattacks. This study briefly examines how they can make equivalent progress against combined attacks that use sophisticated IOs to incite panic behavior in US stock markets, runs on banks, and other psychological effects to intensify

[17] Matishak, "Intelligence Community Creating Hub."

coercive pressure on US leaders. Analyzing these global threats will become all the more important as AI enables additional nations to develop and use sophisticated IOs and cyber weapons.

Third, and most important, researchers and policymakers should explore how to deter coercive IOs and combined information-cyberattacks. One approach is to strengthen deterrence by denial. As formulated during the Cold War, this form of deterrence functions by increasing the costs that attackers will bear relative the gains they hope to achieve.[18] Against coercive IO campaigns, the US may be able to increase the costs China and Russia expect to incur by strengthening DoD's ability to disrupt or destroy their infrastructure for conducting such operations. But such efforts alone will never achieve deterrence by denial. Beijing and Moscow have cheap and plentiful means of conducting coercive attacks, including by exploiting servers and social media networks in the United States. The United States should focus on working the other end of the denial equation: strengthen our domestic defenses against attack to reduce the gains that adversaries can expect to achieve. The defensive initiatives recommended in this study will help do so.

Deterrence through threats of cost imposition offers another option and one that deserves careful analysis of using IOs against those who attack us. The United States needs to convince Chinese and Russian leaders that if they launch a coercive campaign, they will suffer costs that they deem unacceptable. The president does not need to inflict such costs by retaliating in kind to IOs or combined attacks. The United States can use a broad array of forces and nonmilitary means to conduct response operations.

Nevertheless, policymakers should explore whether and how the United States might develop information tools to strengthen deterrence and challenge the asymmetric advantages that Beijing and Moscow currently enjoy. The leaders of those countries hide their citizens from the truth because those leaders fear it. They should also fear that if they launch coercive attacks on the United States, their firewalls will collapse, giving their own populations unfiltered access to information about their regimes. But using IOs to help impose costs on Chinese and Russian leaders could carry immense escalatory risks, especially if such IOs threatened their grip on power. Assessing these risks, and placing them within the larger context of Chinese, Russian, and American doctrines for managing escalation, constitutes a formidable yet essential task for future analysis.

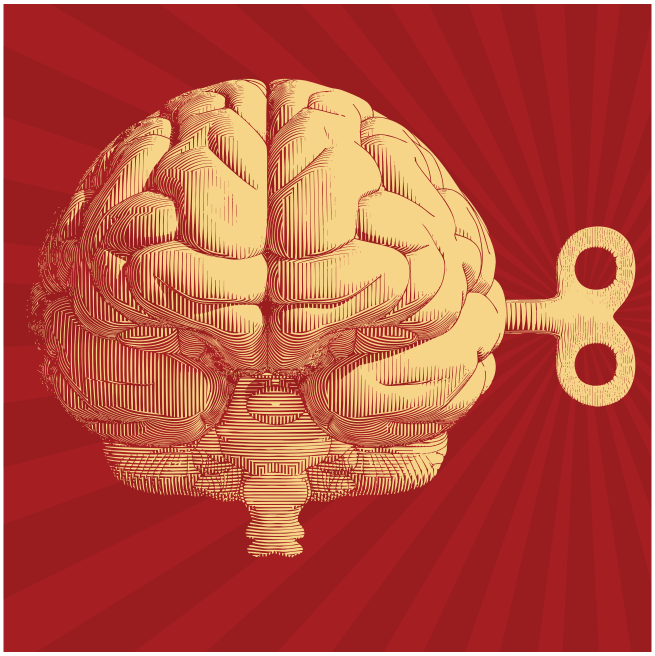
[18] Adapted from Snyder, *Deterrence and Defense*, 14–15; and Davis, "Toward Theory for Dissuasion."

Scoping the Challenge

The United States is pursuing a dangerously one-sided approach to coercion. The Department of Defense (DoD) is developing new plans, capabilities, and techniques to prevail in future conflicts by shaping adversary perceptions and behavior rather than by annihilating the adversary's forces. Yet, US policymakers have barely begun to deal with the risk that America's adversaries will conduct equivalent operations to coerce US behavior. This inattention to domestic preparedness is even more remarkable given the focus of Beijing and Moscow on using sophisticated information operations (IOs) to help convince their adversaries to capitulate in future confrontations.

We lack even a shared terminology to assess such information-based threats and ground the development of strategies against them. US policymakers, military officers, and social media companies disagree over how IOs should be defined and continue to invent new terms for such operations. The US Advisory Commission on Public Diplomacy found in 2020 that there are "hundreds of ways to describe aspects of malign influence operations: misinformation, disinformation, propaganda, information operations, and psychological operations, to name just a few." The resulting definitional confusion has significant policy consequences. The Advisory Committee notes that "without agreed-upon definitions, it is hard to come to a shared understanding of the threat, to define a set of common strategic objectives, or to concur on desired outcomes."[1] This section of the study defines IOs to provide a shared foundation for defensive initiatives by US and allied governments and with the private sector.

We also suffer from a near-exclusive focus on the need to defeat IOs in peacetime. It is vital to counter ongoing Chinese and Russian campaigns to widen divisions in US society and corrode faith in democratic governance as well as other measures



to weaken the domestic political foundations of our global power. But the US military does not view IOs as an exclusively peacetime phenomenon. Neither do Chinese and Russian leaders. The analysis that follows examines how adversaries can employ coercive IOs across the conflict continuum, from the outset of a crisis to increasingly intense warfare, and then analyzes the implications for US defensive requirements. This analysis also examines how adversaries can seek to manage the escalatory risks of moving from IO-only campaigns to combined information-cyberattacks and manipulate US fears of escalation as a coercive tool.

The Sound of One Hand Clapping

US military doctrine is undergoing a fundamental shift in emphasis. The US Joint Chiefs of Staff has declared that "instead of relying primarily on physical power" to destroy enemy targets, "the Joint Force must transition to an approach that builds information into operations that deliberately leverage information and the informational

[1] ACPD, *Public Diplomacy*, 6.

aspects of military activities to affect the perceptions, attitudes, and other elements to drive desired behaviors."[2]

To deepen and accelerate this transformation, the Joint Staff is bringing IOs into the heart of military planning and official statements of doctrine. In 2017, General Joseph Dunford, chairman of the Joint Chiefs of Staff, approved "information" as a new joint function of the military—that is, part of the capabilities and activities that are essential for the US armed forces to conduct joint operations. This addition, the first since the Joint Staff codified the original six functions (including command and control) over twenty years ago, encompasses the application of information "to influence relevant-actor perceptions, behavior, action or inaction, and human and automated decision making."[3]

At the most basic level, this shift further aligns the US military with Clausewitz's dictum that war is a "political instrument"; IOs are simply another means of achieving the policy goals for which the United States is fighting.[4] DoD has long prioritized the disruption of enemy information and command and control networks in combat while defending those of the United States.[5] During the Cold War and World War II, the United States also developed capabilities for "political warfare" that integrated psychological and clandestine military operations.[6] More recently, Russian leaders have claimed that overt and covert US operations fueled Ukraine's Orange Revolution in 2004–2005 and now threaten to spark additional "color revolutions" in Moldova, Belarus, and other nations.[7]

DoD's new approach to warfare builds on the foundations established in past decades but also puts a stronger and more explicit emphasis on shaping enemy perceptions. The US armed forces now seek to drive desired behaviors through IOs and selective kinetic attacks rather than annihilating the enemy's order of battle.[8] Ideally, such coercive operations can achieve US goals at costs far lower than those that would be incurred in open warfare—and with far fewer escalatory risks. And more broadly, according to General John Hyten (now vice chairman of the Joint Chiefs of Staff), the "military that figures out how to control information will be the most powerful military on the planet."[9]

The commanders of US regional and functional combatant commands are leading the shift from kinetic to information-oriented warfighting in current operations and plans for future conflicts. The commander of US Special Operations Command (USSOCOM), General Richard Clarke, exemplifies this transition. When Clarke served in Afghanistan from 2002 through 2011, he "spent about 90% of [his] time thinking about the kinetic fight—the raid, the mission, the kill-capture mission." In contrast, "the commander there on the ground now spends 60% of his working [hours] in the information space . . . thinking about how he is influencing the Taliban thought process" and civilian perceptions. Clarke also argues that IOs will be "critical" for the United States to prevail in future conflicts.[10] Consistent with that focus, USSOCOM's psychological operations (PSYOPS) components continue to develop new means of driving adversary

[2] JCS, *JCOIE*, 19. For a description of the refocusing of US doctrine on influencing adversary behavior by exploiting new information, cyberattack, and precision-strike technologies, see also DoD, *Strategy for Operations*; JCS, *Information Operations*; and JCS, *Military Information Support Operations*.

[3] JCS, *Doctrine for the Armed Forces*, I-19.

[4] Clausewitz, *On War*, 23.

[5] DoD's current shift toward IOs was rooted in initiatives from the 1990s, including the rise of network destruction and precision strike as military priorities. See Feaver, "Blowback," 88–90; and Valeriano, Jensen, and Maness, *Cyber Strategy*, 176.

[6] Jensen, "Cyber Character of Political Warfare," 160–165; and Robinson et al., *Growing Need to Focus*.

[7] Necsutu, "Russia Accuses US"; and Reuters, "Russia Accuses US."

[8] JCS, *JCOIE*, ix.

[9] Gertz, "Stratcom Worried," quoted in Thompson and Paul, "Paradigm Change," 9.

[10] Cox, "Less Door-Kicking, More Influencing."

behavior, including standing up new organizations to better conduct IOs abroad.[11]

The US armed services are also integrating their capabilities to conduct cyberattacks, electronic warfare, IOs, and other types of operations to disrupt and coerce enemy decision-making under the rubric of "information warfare." The services are establishing new information warfare commands to advance this functional integration. The US Navy has established an Information Warfare Enterprise to include both cyber and IOs.[12] The US Air Force merged its cyber, IO, electronic warfare, and other functions into the 16th Air Force (also known as the Information Warfare Numbered Air Force).[13] The US Marine Corps and US Army are also consolidating their cyber and information warfare capabilities in new organizations, with the Army doing so by transforming the Army Cyber Command into the Army Information Warfare Command.[14] According to the leader of that command, General Stephen G. Fogarty, it will "build information capabilities into combined arms teams with converged cyber, influence, and electromagnetic capabilities that deploy to bring immediate, turn-key informational combat power to maneuver commanders."[15] All such transformations reflect the US military's ongoing efforts to "reimagine what 'combined arms' means in 21st-century warfare" and to capitalize on the mutually reinforcing effects of cyber and IOs on enemy behavior.[16]

The armed services are also beginning to embed IO and broader information warfare teams in their forces and operations abroad. The Navy now assigns an information warfare commander to every carrier strike group on par with the air, undersea, surface, and strike warfare commanders historically included in such groups.[17] US Central Command and US Cyber Command (USCYBERCOM) have pioneered the use of IOs as part of broader DoD operations against ISIS. These operations include Joint Task Force-ARES, USCYBERCOM's online offensive against the Islamic State group, and its Operation Glowing Symphony, the command's largest and most complex operation. The latter operation targeted ISIS media and online operations, disrupting ISIS's IO infrastructure and preventing ISIS members from communicating and posting propaganda.[18]

To strengthen the coercive impact of IOs and combined cyber-IOs, the armed services are using sophisticated new approaches to shape leadership perceptions and exploit specific features of the enemy's decision-making process. The US Joint Staff calls for relying on subject-matter experts and advanced automated-analysis systems to identify relevant targets for IOs, "including, but not limited to key influencers, centers of influence, and power brokers; and their patterns of behavior, enduring motivations, and collective strengths and weaknesses."[19] The armed forces are also developing artificial intelligence (AI) tools to sharpen and accelerate influence operations abroad. General Clarke, not-

[11] Cook and Collins, "PSYOP, Cyber, and InfoWar"; 1st Special Forces Command, Airborne, *Vision for 2021 and Beyond*; and Tucker, "Key Official."

[12] This new command is also responsible for cryptology, signals intelligence, and electronic warfare (jamming of radar, etc.). See USN, *Community Vision*; USNA, "Information Warfare Community"; Braswell, "Information Warfare Commander"; and Shutka, "NAVIFOR."

[13] The Air Force merged the 24th and 25th Numbered Air Forces to create this new Information Warfare Numbered Air Force. See USAF, "Sixteenth Air Force"; Air Combat Command Public Affairs, "24 and 25 AF Merger"; and Cohen, "16th Air Force."

[14] Pomerleau, "How the Marines Are Mobilizing"; and Pomerleau, "A New Name?"

[15] Fogarty and Sparling, "Enabling the Army," 20.

[16] Grynkewich, "Information as a Joint Function," 6; Pomerleau, "Marine Information Warfare Unit"; and Cohen, "16th Air Force." On the broader ways in which IOs may be transforming warfare, see Singer and Brooking, *LikeWar*.

[17] Burgess, "Information Warfare."

[18] Graff, "Man Who Speaks Softly"; and Pomerleau, "What Cyber Command's ISIS Operations Means."

[19] JCS, *JCOIE*, 32.

ing the importance of these tools, stated that "we're going to have to understand how the adversary is thinking, how the population is thinking, and work in these spaces in time of relevance. If you're not at speed, you won't be relevant."[20]

Contractors are following suit (or, to put a finer point on it, following the money). The Office of the Secretary of Defense has established an industry consortium, the Information Warfare Research Project, to develop tools for 5G network-related IOs and pursue other initiatives.[21] More broadly, contractors are seeking to follow DoD's lead in shifting from the physical destruction of opposing forces to shaping adversary behavior. As noted by the lead IO business developer for Lockheed Martin, "It's not tank on tank anymore. You're trying to affect people's perception."[22]

DoD's transition to this new concept of warfare is far from complete. A central component of the department's emerging Joint Warfighting Concept will be that of maintaining an "information advantage" over China and Russia in future conflicts.[23] Yet, General Hyten admits, "I'm not exactly sure how we're going to document what information advantage really is."[24] Shifting from previous strategies for driving adversary decision-making to modern, microtargeted campaigns presents internal challenges for the armed services. Lieutenant General Timothy Haugh notes that for the 16th Air Force, seeking to achieve "precision effects" will present "somewhat of a cultural shift in military operations, which has often focused on messaging aimed at more generalized populations."[25] Building a coherent and integrated approach to DoD's new concept of warfare will also require the department to overcome what Herbert Lin calls the "tangled and confused" history of IOs, cyber operations, and PSYOPS within the department.[26] Bureaucratic infighting and conflicts over IO-related roles and missions create an additional impediment to progress: the difficulties of coordinating the intelligence community with IO components in DoD.[27]

Yet, delays and difficulties in adopting new forms of warfare are commonplace for the US military. The US Army clung to the horse cavalry well into the twentieth century despite vivid evidence from World War I that cavalry charges against machine guns and tanks were not exactly a prescription for success.[28] DoD's shift to shaping adversary behavior, as opposed to annihilating adversary forces, will be bumpy as well. That transition will also take many years to complete. US Army Cyber Command, for example, has laid out a ten-year plan to build information capabilities into combined arms teams and "cultivate a new, 21st century Operational Art that leverages the ever-growing force of information and communication to amplify and empower the timeless, coercive power of violence."[29]

Intelligence support for IOs constitutes a crucial gap that also highlights the military's "demand pull" for improved coercive tools and data. In January 2020, nine combatant commanders signed a memorandum known as the "36-star memo"—a reference to the almost unprecedented decision by nine of DoD's eleven four-star combatant commanders to sign the statement.[30] US defense officials describe the memo as asking for "increased support from the Intelligence Community for messaging and countering disinformation operations as part of great power

[20] Pomerleau, "Pentagon's AI Center."

[21] DoD, "DOD, USAF Warfare Center."

[22] Pomerleau, "What Is Industry's Role?"

[23] JCS, *JCOIE*, 20.

[24] Hitchens, "JROC Struggles."

[25] Haugh, Hall, and Fan, "16th Air Force," 40.

[26] Lin, "Doctrinal Confusion and Cultural Dysfunction," 89.

[27] Schwille et al., *Intelligence Support*.

[28] Katzenbach, "Horse Cavalry," 120–150.

[29] Fogarty and Sparling, "Enabling the Army," 20.

[30] Woodruff Swan and Bender, "Spy Chiefs Look to Declassify Intel," 4.

competition."[31] These officials note that measures are underway to meet the memo's requests and that the new Defense Intelligence Strategy prioritizes countering Russian and Chinese disinformation and will provide more timely information to combatant commanders to support their efforts.[32] Years of additional efforts will be necessary to close the gap between the aspirational goals of the US military and the capabilities in hand to achieve them. But the military's shift toward coercion, and the use of emerging IO and cyber technologies to prevail in future crises, is well underway.

Congress is reinforcing that shift. The *2018 National Defense Strategy*, *2017 National Security Strategy*, and the National Defense Authorization Act for Fiscal Year 2018 all contained language calling on DoD to bolster its capability to produce effects in the information environment.[33] Congress also has required DoD to establish a new "principal information operations adviser" to strengthen those capabilities by integrating and overseeing policy, strategy, planning, and resourcing for IOs.[34] Leading cybersecurity analysts are also urging the US military to shift toward coercive strategies, with James Andrew Lewis calling for "using cyber actions against opponents to reshape their calculations."[35]

It is too soon to know how the Biden administration will shape the trajectory of IO initiatives in the department. Secretary of Defense Lloyd Austin is overseeing the IOs posture review Congress required in the 2020 National Defense Authorization Act and the update of the 2016 *Strategy for Operations in the Information Environment*.[36] It is certain, however, that such operations will be crucial for DoD's ability to both prevail in conflicts before full-scale conventional warfare breaks out and (ideally) convince US adversaries to yield without firing a shot.

Defending the United States against Coercion: The Nature of the Challenge

No remotely equivalent effort is underway to prepare against Chinese or Russian operations to coerce US crisis decision-making. Even as DoD develops new doctrine and capabilities to drive adversary behavior, the Department of Homeland Security (DHS) and other agencies responsible for domestic security have barely begun to address the risk that US opponents will seek to do the same against American leaders.

Developing strategies to defeat (and, ideally, deter) coercive campaigns against the United States will require an understanding of how adversaries will seek to drive US crisis decision-making. Extensive literature exists on the psychological and political dynamics that coercive operations seek to harness. In particular, Alexander George and Thomas Schelling have examined how nations can use threatened or actual punishment, paired with warnings of more suffering to follow, to help convince their victims that the costs of continuing to resist are greater than the benefits of doing so.[37] Herman Kahn and other analysts have also analyzed how attackers can leverage the dangers of nuclear escalation to enhance rather than inhibit their coercive campaigns.[38] More recently, Robert Pape has examined how adversaries can achieve "coercion by denial" by thwarting their opponents' military strategy and convincing them that they have no hope of prevailing in a confrontation.[39]

[31] *Hearing on Disinformation in the Gray Zone*, Maier, Tipton, and Sullivan statement.

[32] Hitchens, "New Strategy."

[33] Schwille et al., *Intelligence Support*, ix.

[34] Pomerleau, "Top Information Operations Adviser."

[35] Lewis, *Toward a More Coercive Cyber Strategy*, 8.

[36] Pomerleau, "SecDef Nominee Pledges."

[37] George, *Forceful Persuasion*; and Schelling, *Arms and Influence*.

[38] Kahn, *On Escalation*.

[39] Pape, *Bombing to Win*.

Yet, these theoretical works provide only a starting point for assessing how China or Russia may pressure US leaders to back down in crises involving Taiwan, Estonia, or other US security partners. Beijing and Moscow will tailor their coercive campaigns to exploit specific vulnerabilities of the US crisis decision-making process and drive wedges between the United States and its allies. They will also employ advanced IO capabilities, tailored to exploit US public and leadership dependence on social media, in ways that George and other theorists of coercion never anticipated.

A growing number of nations are acquiring advanced cyber and IO tools that they could use in such campaigns. However, this study focuses on China and Russia. Doing so aligns with DoD's determination that these nations pose the most significant challenges to US security.[40] China and Russia have especially well-developed doctrines and capabilities to conduct coercive IOs and combined information-cyberattacks. They can also threaten the use of nuclear weapons to pressure US leaders into backing down in a crisis, just as the Kremlin did to discourage Western assistance to Ukraine during Russia's invasion of Crimea.[41] These factors make China and Russia benchmarks for assessing the adequacy of US preparedness against coercion.

Nevertheless, it would be a mistake to assume that "if we can take care of the cat, we can take care of the kittens." Iran, North Korea, and other potential adversaries are exploiting advances in deepfake technologies and other means of conducting sophisticated information attacks.[42] Their capabilities to conduct cyberattacks against US infrastructure are improving as well. Accordingly, the United States must not only scale its defensive requirements to defeat Russia and China but also develop strategies to counter the specialized threats (exemplified by Syria's attacks on the financial services sector) posed by lesser but increasingly capable powers.[43]

China and Russia have other means besides cyber weapons to disrupt US civilian infrastructure and military targets. For example, both nations are developing hypersonic deep-strike weapons to conduct kinetic attacks in the United States. Adversaries might also use biological weapons to create extraordinary public fears in a coercive campaign. However, the 2020 *National Counterintelligence Strategy of the United States of America 2020–2022* warns that cyber weapons offer adversaries an especially useful means of holding US infrastructure at risk to shape crisis decision-making.[44] This study focuses accordingly on the threatened or actual use of cyberattacks to coerce US behavior.

In particular, the study examines the possibility that early in an emerging crisis, China or Russia will use IOs to convince US decision-makers that the United States will incur devastating cyberattacks if it defends regional allies. If IOs alone fail to convince the president to yield, Beijing and Moscow may act on their threats and pair strikes on infrastructure with IOs designed to inflame fears of further punishment. Escalating the crisis in this manner would be extraordinarily dangerous. The United States could respond to even limited cyberattacks by inflicting costs on China and Russia that their leaders would find unacceptable. Nevertheless, both of those nations have developed strategies to manage such risks and manipulate US fears of escalation as a coercive tool. We should also expect China and Russia to conduct coercive operations against US security partners involved in the crisis and discourage American allies from authorizing or participating in coalition operations.

[40] Secretary of Defense Lloyd Austin cites China as the department's "pacing challenge." Austin, "Message to the Force." Similarly, Avril Haines, director of national intelligence, assesses that "China is an unparalleled priority for the Intelligence Community." *Hearing on Worldwide Threats*, Haines statement.

[41] Keck, "Russia Threatens Nuclear Strikes."

[42] Bradshaw and Howard, *Challenging Truth and Trust*, 3; and Friedman, "Foreign Interference."

[43] Fisher, "Syrian Hackers Claim AP Hack."

[44] NCSC, *National Counterintelligence Strategy*.

Signposts already exist to help guide assessments of these threats and their implications for US defensive requirements. DoD warns that in future confrontations, China's People's Liberation Army (PLA) will seek to shape US perceptions and behavior to prevail in future confrontations and has demonstrated increasingly sophisticated capabilities for IOs.[45] In particular, DoD warns that "the PLA considers information operations (IO) as a means of achieving information dominance early in a conflict," including those involving regional confrontations with the United States.[46]

China has not yet combined IOs with destructive cyberattacks against its victims' infrastructure. However, China is building its preparedness for such combined attacks and is consolidating space, cyber, electronic, and psychological warfare capabilities under the new Strategic Support Force to help make IOs "decisive in future wars."[47] Continuing private sector and government efforts to strengthen the resilience of US infrastructure can help counter such combined attacks. But that infrastructure remains vulnerable to increasingly sophisticated Chinese malware. The US director of national intelligence testified in April 2021 that China has "substantial cyber capabilities that if deployed, at a minimum, can cause localized, temporary disruptions to critical infrastructure inside the United States."[48] Combined with IOs to maximize the fear generated by localized attacks and threaten additional, widespread punishment unless the president caves into Chinese demands, these capabilities will provide powerful coercive tools in future crises.

The Kremlin also has formidable tools and expertise to shape US crisis decision-making. Russian IOs build on an extensive legacy of such operations from the czarist and Soviet eras. Over the past decade, General Valery Vasilyevich Gerasimov, chief of the General Staff of the Russian Armed Forces, has led a sustained effort to update and strengthen the military's preparedness to use coercive IOs in future confrontations. These preparations include the development of plans and capabilities for combined attacks. The director of national intelligence notes that Russia will employ "new weapons and cyber capabilities to threaten the United States and its allies" and will use IOs to "influence U.S. decision-making."[49]

Threats to power grids and other critical systems will play a key role in such coercive operations. The US Intelligence Community's 2021 Annual Threat Assessment finds that "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis."[50] If threats alone prove inadequate to convince the president to back down, General Terrence O'Shaughnessy, former commander of US Northern Command, warns that "in a crisis or conflict, we would expect Russia to conduct cyber operations against critical infrastructure in an attempt to compel de-escalation."[51]

The SolarWinds hack exemplifies the need to intensify US efforts to prepare against future coercive IOs and combined information-cyberattacks. Initial assessments of the hack suggested that Russian operatives were seeking to gather access codes and intelligence across scores of government and private sector networks. However, Anne Neuberger, deputy national security advisor for cyber

[45] OSD, *Annual Report to Congress*, 112; and Rosenberger and Cooper, "Time for U.S. to Start Pushing Back."

[46] OSD, *Annual Report to Congress*, 63.

[47] Costello and McReynolds, *China's Strategic Support Force*, 1.

[48] *Hearing on Worldwide Threats*, Haines statement, 3.

[49] *Hearing on Worldwide Threats*, Haines statement, 3.

[50] ODNI, *Annual Threat Assessment*, 10.

[51] *Hearing on Defense Authorization Request for Fiscal Year 2020*, O'Shaughnessy statement. See also Flynn, "Russia's Evolving Approach to Deterrence," 37 and 40–41; and US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault*.

and emerging technology, has determined that the SolarWinds hackers have more ambitious goals. “When there is a compromise of this scope and scale, both across government and across the U.S. technology sector, to lead to follow-on intrusions, it is more than a single incident of espionage,” Neuberger emphasizes. “It’s fundamentally of concern for the ability for this to become disruptive.”[52] The value of SolarWinds for enabling disruptive attacks in future crises gets a more pointed assessment from Suzanne Spaulding, who served as director of DHS’s Cybersecurity and Infrastructure Security Agency (CISA) during the Obama administration. Spaulding warns that Russia’s goal “may be to put themselves in a position to have leverage over the new administration, like holding a gun to our head to deter us from acting to counter Putin.”[53]

Yet, current Chinese and Russian capabilities for coercion will pale in comparison with future threats. Both nations are devoting immense resources to AI and technologies that will help them create far more advanced tools for IOs and combined attacks than they possess today. In a comprehensive assessment of such trends, the National Security Commission on Artificial Intelligence concluded that “AI is deepening the threat posed by cyber attacks and disinformation campaigns that Russia, China, and others are using to infiltrate our society, steal our data, and interfere in our democracy. The limited uses of AI-enabled attacks to date represent the tip of the iceberg.”[54] Looking below the iceberg’s waterline and anticipating how adversaries will use future AI-enabled weapons and tactics to shape US crisis decision-making will be essential for developing US strategies against coercion.

Part of the Solution: Develop Plan and Capabilities to Suppress Coercive Attacks

DoD can make significant, near-term contributions to strengthening US defense against coercive IOs and combined attacks. The most important of these is to build plans and capabilities to blunt or disable attacks at their origins abroad. Operation Glowing Symphony is only one example of how USCYBERCOM has disrupted an opponent’s infrastructure and online operations. Policymakers should scale up these capabilities and develop options to employ them when coercive attacks are imminent or underway.

USCYBERCOM is already committed to “defending forward” and to imposing costs on cyber adversaries. The command’s 2018 vision statement, *Achieve and Maintain Cyberspace Superiority*, notes that DoD “is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems.”[55] The command is also persistently engaging cyber adversaries to “create friction for adversaries, and cause them to shift resources to defense.” In particular, USCYBERCOM “imposes tailored, non-kinetic costs on adversaries.”[56]

The command’s defense of the 2018 midterm elections exemplifies the benefits of such cost imposition. General Paul Nakasone, commander of USCYBERCOM, notes that in advance of the elections, the command “executed offensive cyber and information operations.” Those actions “imposed costs by disrupting those planning to undermine the integrity of the 2018 midterm elections.”[57] The Internet Research Agency (IRA) in St. Petersburg, Russia, bore the brunt of that disruption. USCYBERCOM blocked the IRA’s internet access

[52] Riley, “Cybersecurity 202.”

[53] Sanger, Perlroth, and Barnes, “Russian Hacking.”

[54] NSCAI, *Final Report*, 7.

[55] USCYBERCOM, *Achieve and Maintain Cyberspace Superiority*, 5.

[56] *Hearing on Fiscal Year 2021 Budget Request*, Nakasone statement, 2.

[57] *Hearing on Fiscal Year 2021 Budget Request*, Nakasone statement, 5.

and prevented Russia from launching the interference IOs that the agency had prepared.[58] And shortly before the election began, USCYBERCOM conducted a series of attacks on infrastructure used by Russian hackers and sought to sabotage their hacking tools.[59]

Michael Fischerkeller and Richard Harknett draw a distinction between such cost-imposition activities and coercion. In disrupting the Russian IRA's efforts to interfere with the 2018 elections, USCYBERCOM was not seeking to "change the strategic decision calculus of the attacker" or conduct coercive signaling. Rather, "any IRA plans to launch cyber-enabled disinformation were thrown off balance as Cyber Command captured the initiative in setting security conditions" and imposed costs on Russia.[60]

However, for *defense* against coercion, USCYBERCOM's capabilities to disrupt the adversary's infrastructure and operations could be enormously valuable if reoriented and scaled up for that mission. Operations to suppress coercive attacks would constitute a cyberspace version of counterbattery fire. Instead of using kinetic weapons to destroy the enemy's artillery, mortars, and other "indirect fire" assets in traditional counterbattery operations, DoD can now use cyber weapons to disable the cyber infrastructure that adversaries are using to strike the United States. Nakasone states that "cyber effects operations allow Cyber Command to disrupt and degrade the capabilities our adversaries use to conduct attacks."[61] As part of a broader strategy to defend the United States from coercion, US policymakers should develop plans to disrupt and degrade the capabilities that China and Russia could employ in future crisis-oriented campaigns.[62]

Policymakers should also explore how other agencies and the private sector might partner with USCYBERCOM to suppress attacks. On October 7, 2020, the US Justice Department announced that it had seized nearly one hundred websites linked to Iran's Islamic Revolutionary Guard Corps. These sites had been conducting a global disinformation campaign, targeting audiences from the United States to Southeast Asia with pro-Iranian propaganda. One day later, Facebook and Twitter revealed that they had taken down more than a dozen disinformation networks used by political and state-backed groups in Iran, Russia, Cuba, and other nations.[63] To help counter the use of such networks and other assets in future coercive campaigns, the United States should develop integrated, multiagency plans for attack suppression and—as will be discussed later—coordinate such operations at home with social media companies.

But it would be foolish for the United States to rely on attack suppression alone. The analogy with counterbattery fire is useful in this regard as well. Artillery units can limit the effectiveness of counterbattery fire by hardening their position, adopting "scoot and shoot" and other maneuver tactics, and countering enemy efforts to pinpoint their location. China and Russia will almost certainly adopt equivalent measures to protect the IO and cyberattack infrastructure on their territory from US disruption.

These nations will also seek to evade suppression operations by using infrastructure within the United States. Chinese and Russian operatives are already conducting IOs and cyber operations from

[58] Nakashima, "Trump Confirms Cyberattack"; and Nakashima, "Operation Disrupted Internet Access."

[59] Nakashima, "Fewer Opportunities."

[60] Fischerkeller and Harknett, "Persistent Engagement and Cost Imposition."

[61] Nakasone and Sulmeyer, "How to Compete in Cyberspace."

[62] The 16th Air Force is already exploring such options to suppress IOs and combined information-cyberattacks. Cohen, "16th Air Force."

[63] Raymond, "Forget Counterterrorism."

infrastructure located on American territory.[64] When China's state-sponsored "Hafnium" group struck Microsoft's widely used Exchange software in 2020, it used leased virtual private servers in the United States as well as US-based computers from at least four service providers to mount their attack.[65] Suspected Russian operatives also used US-based cloud services to support key stages of their attack against SolarWinds.[66] In addition, Russia's IRA—recently renamed the Lakhta Internet Research (LIR)—appears to be hiring citizens in target countries to open social media accounts on its behalf, a practice known as "franchising," to add a layer of camouflage to Russian disinformation campaigns.[67]

Russia has developed new techniques as well to amplify content created within the United States.[68] As in the Trickbot campaign, Russians are infecting and networking computers inside the United States to spread ransomware.[69] DHS reports that Russian operatives are also likely to use other US-based infrastructure "to mask their location, obscure login activity, and prevent account banning."[70] We should expect adversaries to exploit all such domestic threat vectors in future coercive campaigns, especially as the United States bolsters its capabilities to disrupt infrastructure on adversary territory.

China and Russia will also rely on US-based infrastructure to evade the ability of our most capable government agencies to detect and disrupt their attacks. General Nakasone gave the following testimony to Congress in March 2021:

> We as U.S. Cyber Command or the National Security Agency may see what is occurring outside of the United States, but when it comes into the United States, our adversaries are moving very quickly. They understand the laws and the policies that we have within our nation, and so they're utilizing our own infrastructure, our own internet service providers, to create these intrusions.[71]

US strategies against coercion must account for these Chinese and Russian maneuver operations and for their efforts to turn our domestic legal constraints against us. Domestic initiatives will also be necessary to make the US public less credulous and vulnerable to disinformation and coercive messaging. In tandem with developing plans and capabilities to suppress attacks abroad, the United States should strengthen its domestic capabilities to counter such attacks and create a strategy of "defense in depth" against coercion that integrates both sets of initiatives.

Strengthening Domestic Defenses: Foundations for Progress and Key Strategic Gaps

DoD should never be (and has shown no interest in becoming) the lead department for domestic operations to defeat Chinese and Russian corrosion of US democracy. The same is true for domestic defenses against coercion. Statutory constraints on the armed forces preclude them from performing domestic functions that could be essential against coercive IOs and combined attacks. For example, as adversaries conduct IOs to incite fear and mobilize opposition to defending US allies, the federal government must be ready to provide counter-messaging to the public. US law prohibits DoD from conducing "publicity" activities within the United States.[72]

[64] Goldman et al., "Lawmakers Warned."

[65] Uberti, "Microsoft Warns of Chinese Hackers."

[66] Volz and McMillan, "Massive Hacks Linked to Russia."

[67] Alba, "Russia's Troll Farm." On the recent renaming of the IRA, see NIC, *Foreign Threats to the 2020 US Federal Elections*, 4.

[68] Rosenbach et al., *Election Influence Operations Playbook*, 7.

[69] Greene and Nakashima, "Microsoft Seeks to Disrupt Russian Criminal Botnet."

[70] DHS, *Homeland Threat Assessment*, 12.

[71] Tucker, "General Says Attacks."

[72] The Duncan Hunter NDAA for FY2009 specifies that "no part of any funds authorized to be appropriated in this or any

The United States might conceivably meet these requirements for domestic missions by rewriting US law and tasking DoD to perform them. But DoD seems unlikely to request any such expansion of its authorities. Nakasone told Congress in April 2021 that despite the exploitation of existing US legal constraints by Beijing and Moscow, "I'm not seeking legal authorities either for NSA or for U.S. Cyber Command" to help defeat their operations.[73] There are compelling operational reasons to maintain these limits on DoD's roles at home. Making DoD responsible for domestic defense against coercive campaigns would divert the department from its existing missions and ignore the comparative advantages offered by nondefense agencies. These advantages are especially significant for building preparedness against combined information-cyberattacks. The Department of Energy and other departments already serve as Sector Specific Agencies (SSAs) to help their respective infrastructure sectors strengthen their resilience. In particular, with support from DHS, these SSAs are responsible for helping infrastructure owners and operators strengthen the cybersecurity of their systems and for coordinating with them to restore electricity, water service, and other vital functions when disruptive events occur.[74] A number of these agencies also have emergency authorities that could be enormously valuable in defeating coercive campaigns. For example, if adversaries strike the grid to jeopardize public health and safety or disrupt the flow of forces to a regional crisis, the secretary of energy can order electric utilities to protect and restore grid service in ways that directly counter such attacks.[75]

It would be difficult and time consuming for DoD to acquire the sector-specific expertise, industry ties, and authorities that SSAs already possess. SSAs should continue to have primary responsibility for helping infrastructure owners in their sectors strengthen the cyber resilience of their systems, including against attacks intended to coerce US crisis decision-making. DoD and the broader intelligence community should continue to support such efforts and help SSAs and their industry partners keep pace with (and, ideally, get ahead of) growing Chinese and Russia capabilities to disrupt US infrastructure.

However, SSAs are far less capable of countering the information component of combined attacks or the IO-only campaigns that China and Russia may initially conduct in a crisis. A number of government programs exist to counter election interference and strategic corrosion. Policymakers should consider assigning some of these programs the additional responsibility of countering coercive IOs. Yet, without a threat-informed strategy to guide and align such mission assignments, domestic defenses will remain inadequate.

A growing array of government initiatives might be integrated within an overarching strategy for defense against coercion. The following are prime candidates for inclusion:

- The Foreign Malign Influence Center. The Office of the Director of National Intelligence is creating this congressionally mandated center to provide a clearinghouse for intelligence related to malign influence from multiple government agencies and provide assessments and warning of such activities. In describing the center's mission, director of national intelligence Avril Haines told legislators that stemming foreign influence operations constitutes an "incredibly important issue."[76] The Center's threat assessment and warning missions might

other Act shall be used by the Department of Defense for publicity or propaganda purposes within the United States not otherwise specifically authorized by law."

[73] Katz, "Nakasone Deflects Senators' Invitations."

[74] CISA, "Sector Specific Agencies."

[75] For an analysis of grid security emergency authorities over the bulk power system, see Stockton, *Resilience for Grid Security Emergencies*.

[76] Matishak, "Intelligence Community Creating Hub."

be expanded to include Chinese and Russian coercive campaigns as well.

- CISA's Countering Foreign Influence Task Force (CFITF). This organization is responsible for helping the American people understand the risks of foreign influence operations and how they can play a role in reducing the impact of foreign influence on their organizations and communities.[77] The task force and other CISA components have also developed significant expertise in defending US elections that might be refined for use against coercive IOs. For example, during the 2020 election, CISA maintained a "rumor control" website to debunk common misinformation and disinformation narratives and themes that relate broadly to the security of election infrastructure and related processes.[78] Going forward, those programs and capabilities provide a starting point for debunking Chinese or Russian messaging on the perfidy of US allies or other IOs intended to corrode support for standing firm in a crisis.
- The Federal Bureau of Investigation's Foreign Influence Task Force. The task force focuses on identifying and counteracting malign foreign influence operations targeting the United States and serves as the lead federal agency responsible for investigating foreign influence operations.[79]
- The State Department's Global Engagement Center (GEC). The center's mission is to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations."[80]
- The Federal Emergency Management Agency (FEMA). This agency has developed extensive programs to counter disinformation during natural disasters and is currently operating a coronavirus rumor-control website to help defeat false data and narratives generated and distributed over social media by China, Russia, and other disinformation sources.[81] As with the initiatives above, opportunities exist to repurpose FEMA's emergency communications programs to help counter Chinese and Russian IOs.

Yet, many of these organizations are not fully equipped to execute their current missions, much less the additional task of defeating coercive campaigns. For example, the CFITF lacks sufficient legislative authority to counter the full range of existing IO threats to US institutions and the public and build adequate collaboration with the private sector. The CFITF is also hampered by fluctuations in staffing and inadequate resources.[82] Furthermore, while at least some of these organizations are beginning to gain additional funds and augmented workforces, no government-wide strategy guides their efforts or helps integrate their operations against foreign disinformation campaigns. The US Advisory Commission on Public Diplomacy found in September 2020 that "as new workflows and authorities are established to support existing resources, actors (offices, bureaus or agencies, field posts, etc.) with equities in countering the disinformation threat are increasingly siloed, reporting on their activities through narrow bureaucratic channels. This atomization of effort not only mitigates against a coordinated response but limits a broader understanding" of federal efforts at countering disinformation.[83]

[77] CISA, "Countering Foreign Influence Task Force."

[78] CISA, "#Protect2020 Rumor vs. Reality."

[79] FBI, "Combating Foreign Influence."

[80] DOS, "Global Engagement Center."

[81] FEMA, "Coronavirus Rumor Control."

[82] Dalton et al., *By Other Means*, 10.

[83] ACPD, *Public Diplomacy*, 4.

The government's failure to achieve better coordination is especially notable since the problem has received so much high-level attention for so many years. The *2017 National Security Strategy* found that US efforts to counter adversary disinformation and influence campaigns were "tepid and fragmented" and "lacked a sustained focus."[84] The 2018 Senate Committee on Foreign Relations report examined these shortfalls in greater detail. The report noted that the US government "still lacks a coherent, public strategy to counter the Kremlin's disinformation operations abroad and at home" and instead has a "patchwork of offices and programs tasked with mitigating the effects of Kremlin disinformation operations."[85] The Homeland Security Advisory Council Countering Foreign Influence Subcommittee's May 2019 report found that even against familiar, ongoing types of campaigns, coordination between federal agencies is weak. Although "some federal agencies think they are leading the work on countering foreign influence, no single entity has officially been provided with a mandate to do so." Moreover, "the United States has no national strategy to counter foreign influence."[86] Academic researchers have reached similar conclusions. In particular, they warn that the federal government has failed to "articulate a coherent doctrine for American counter-propaganda," in part because of the overly broad range of actors and institutions attempting to solve the problem and insufficient coordination between them.[87]

Creating an integrative strategy will be vital to strengthening coordination against both disinformation and campaigns to drive US crisis decision-making. Before assigning coercive defense missions to the CFITF and other existing organizations, policymakers will first need to clarify the additional challenges that coercive threats will entail and develop an overarching vision of how government organizations (in partnership with the private sector) will meet these challenges.

As part of that process, legislators and executive branch officials should consider reallocating current agency roles and responsibilities. That effort could start with a reassessment of the leadership functions assigned to the State Department's GEC. Congress gave the GEC the responsibility to lead and coordinate federal efforts to counter foreign disinformation against the United States and its allies. The GEC has not been adequately resourced to perform this function. As of 2020, the center was composed of just over one hundred people.[88] Moreover, as a State Department organization, it is poorly positioned to lead US domestic defense initiatives. Current regulations restrict the department's ability to monitor activity inside the United States and provide counter-messaging against Chinese and Russian IOs.[89] If those nations escalate from IOs to combined attacks in a crisis, the GEC lacks the authorities and expertise of SSAs and DHS to support infrastructure-protection measures.

In contrast, the GEC is ideally positioned to coordinate US and allied countermeasures against coercive campaigns that seek to discourage and disrupt coalition defense operations. Policymakers should allocate federal roles and responsibilities based on the comparative advantages that agencies possess for countering specific coercive threats. The prerequisite for doing so is to anticipate how China and Russia may seek to drive US crisis decision-making and exploit the vulnerabilities of the US public,

[84] White House, *National Security Strategy*, 35.

[85] US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault*, 149.

[86] HSAC, *Interim Report*, 10.

[87] Vilmer et al., *Information Manipulation*, 125–126. Similarly, former director of the Cybersecurity and Infrastructure Security Agency Christopher Krebs noted in 2018 that when government officials first discovered Russian efforts to influence the 2016 elections, they "didn't know who to call" and suggested that insufficient coordination and information sharing existed between them. See Wemer, "Here's How to Fight Disinformation."

[88] Kent, *Striking Back*, 31.

[89] Kent, *Striking Back*, 31.

senior leaders, and allies with increasingly sophisticated means of shaping their perceptions.

Threat assessments will also be crucial for identifying and filling gaps in emergency coordination plans and capabilities. DHS leads two federal Emergency Support Functions (ESFs) that will be crucial for countering coercive IOs: ESF #2, Communications, and ESF #15, External Affairs, which coordinates efforts to provide accurate and timely information to the media and public during a disaster or other incident.[90] Neither ESF recognizes the risks posed by coercive campaigns or the capabilities that will be needed to counter them. Nor do they account for the danger that the very coordination mechanism they encompass will be targeted for manipulation.

Federal plans to coordinate cyber response operations suffer from equally significant shortfalls in preparedness against combined information-cyberattacks. The National Cyber Incident Response Plan (NCIRP) is designed to facilitate information sharing and incident management. Under the plan—and consistent with Presidential Policy Directive 41, *United States Cyber Incident Coordination*—a Cyber Unified Coordination Group can establish shared objectives for threat response, asset response, and intelligence support to guide cyber incident response and recovery efforts in the short to midterm.[91] None of these plans account for the Chinese and Russian military doctrines to supplement cyberattacks with IOs and magnify the coercive pressure that such attacks will create. Policymakers should begin integrating cyber and IO emergency response plans and coordination mechanisms to meet combined threats. Such integration will require new partnerships and capabilities not only across federal agencies but across the private sector as well.

Expanded Public–Private Partnerships

China and Russia already use Facebook, Twitter, and other social media networks to conduct election interference and corrosive IO campaigns and have become adept at exploiting platform algorithms to maximize the reach and impact of their messaging. Beijing and Moscow will use these same tactics and techniques in future crises to shape the perceptions of the US public, senior officials, and American allies. Building government–industry partnerships to block and counteract coercive messaging will be essential for domestic defense.

Existing partnerships highlight both the promise of such collaboration and the impediments that lie ahead. As the 2020 presidential election approached, Google and other major social media firms deepened their collaboration with federal agencies to share intelligence on disinformation and refine countermeasures against it.[92] That collaboration continues to improve in terms of countering COVID-19 disinformation, with social media companies taking unprecedented steps to remove, hide, and restrict such messaging.[93]

Nevertheless, a growing number of legislators are dissatisfied with the self-created policies that social media companies employ to designate and filter objectionable content, including foreign disinformation and domestic political messaging. This dissatisfaction is driving efforts to amend the laws and regulations that currently apply to social platforms and limit government control over their content. Proposed legislation focuses on Section 230 of the Communications Act of 1934 (47 U.S.C. §230, hereinafter termed Section 230), which Congress enacted as part of the Communications Decency Act of 1996. Section 230 broadly protects interactive computer service providers, including social media operators, and their users from liability for

[90] FEMA, *Emergency Support Function #2*; and FEMA, *Emergency Support Function #15*.

[91] DHS, *National Cyber Incident Response Plan*, 31; and White House, *Presidential Policy Directive*.

[92] Isaac and Conger, "Google, Facebook and Others."

[93] Butcher, "COVID-19 as a Turning Point."

publishing, and in some instances removing or restricting access to, another user's content.[94]

Congress might consider amending Section 230 to require operators to block coercive messaging when directed to by the Federal Communications Commission (FCC) or another federal entity.[95] To be effective, however, the government and social media companies would first need to define what constitutes coercive content. Facebook is now calling for broader rules "to help deter foreign actors" from conducting electoral interference and disinformation campaigns.[96] Industry–government collaboration against coercive IOs will require anticipating the messaging tactics and microtargeted content that China and Russia are likely to employ and the technologies they will use to evade filtering measures.

Government agencies and social media companies will also need to resolve deeper problems. Jonathan Reiber, DoD's former chief strategy officer for cyber policy, has found that it is far more difficult to develop industry–government plans and coordination mechanisms to defeat cyberattacks than to engage in peacetime, day-to-day collaboration. The lack of trust between these partners and disagreements over the defensive roles that private companies should play constitute especially significant impediments to progress. Disagreements over the cyber threats confronting the United States reinforce these problems.[97] Social media companies and government agencies will need to overcome similar challenges to defeat coercive IO campaigns and combined attacks.

This study provides a threat assessment to guide the development of strategies, programs, and partnerships to counter Chinese and Russian efforts at driving US crisis decision-making. To establish a foundation for that assessment, it will first be helpful to resolve two initial issues: how to define IOs and how to determine where they fit on the spectrum of conflict between peacetime and war.

Untangling the Spaghetti Pile

The United States currently lacks a widely accepted definition of IOs that can help ground the development of a defense strategy against them. Disagreements over how to define IOs are sharp and deeply rooted.[98] Moreover, analysts frequently use other terms to categorize similar information-related activities, including PSYOPS, "influence operations," "political warfare," and "hostile social manipulation." They are also coining new combinations of these terms, such as "information warfare and influence operations" and "influence cyber operations."[99]

Policymakers exacerbate this definitional confusion by shifting the meaning of IO-related terminology.

[94] Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. §230. While this provision is often referred to as Section 230 of the Communications Decency Act of 1996 (Pub. L. No. 104-104), it was enacted as Section 509 of the Telecommunications Act of 1996, which amended Section 230 of the Communications Act of 1934.

[95] The FCC classifies broadband-internet access services as an information service. This classification could subject these service providers to greater regulation. However, the FCC does not currently regulate internet content. Gallo and Cho, *Social Media*.

[96] Facebook, "Updated Internet Regulations."

[97] Reiber, *Public, Private War*, 12–13.

[98] Theohary, *Information Warfare*; and Brangetto and Veenendaal, "Influence Cyber Operations," 113. Given this confusion, one analyst goes so far as to recommend that the US government entirely abandon the term. See Paul, "Is It Time to Abandon?"

[99] Theohary, *Information Warfare*, 1; Robinson et al., *Growing Need to Focus*; and Mazarr et al., *Hostile Social Manipulation*, 33–49. *Hostile Social Manipulation* provides an excellent overview of these and other related definitions on pages 12–14. For more on the rationale for coining the term information warfare and influence operations, see Lin and Kerr, "Cyber-Enabled Information/Influence Warfare," 4; see Lin, "Developing Responses" for an updated work on cyber-enabled information warfare and influence operations. For more on influence cyber operations, see Brangetto and Veenendaal, "Influence Cyber Operations," 113.

PSYOPS provides a case in point. In 2010, DoD leaders directed the Army to stop employing the term PSYOPS to describe its IO activities and instead use the less menacing "military information support operations." Facing sustained Army resistance, DoD reversed that change in 2017.[100]

One way to escape from this definitional tangle is to adopt a definition used by social media companies and other key government partners since their collaboration will be essential for strengthening domestic defenses against coercion. Facebook, for example, defines IOs as:

> actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion (we refer to these as "false amplifiers").[101]

This definition has the benefit of highlighting the means by which Russia and other rivals are warping US public opinion for strategic gains. However, Facebook's usage also has a critical limitation: it focuses on offensive operations and excludes defensive measures to block or otherwise defeat false narratives put forward by opponents.

Domestic resilience will require the president's readiness and ability to counter enemy disinformation and provide US citizens with factual, government-vetted data. As noted above, the US State Department and other federal agencies are already developing programs to "support the development and dissemination of fact-based narratives and analysis to counter propaganda and disinformation directed at the United States" and its allies.[102] The United States will need equivalent capabilities to counter coercive messaging.

Rather than define IOs exclusively in terms of offensive operations and coin a separate term for counternarratives and other defensive measures, the United States should establish a single definition that includes both realms of activity. The DoD's definition of IOs provides a starting point for doing so.

DoD defines IOs as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[103] This definition has the advantage of including both offensive and defensive components. However, DoD's definition includes a constraint that precludes its adoption by other federal agencies and private companies. In DoD's usage, IOs are "conducted during military operations." Such operations do not necessarily constitute open warfare. Military operations include a wide range of peacetime influence activities, including Navy port visits and training/confidence-building engagements with foreign militaries, all of which DoD can support with IOs. But DHS and other civilian agencies critical for IO defense do not conduct military operations. Neither does Facebook, Twitter, or any other digital media company that can help block enemy disinformation during a crisis. These partners for preparedness need a less defense-specific definition of IOs.

This study proposes to establish a more broadly usable term by "demilitarizing" DoD's definition.

[100] Cowan and Cook, "What's in a Name?"; and Theohary, *Defense Primer*, 1.

[101] Weedon, Nuland, and Stamos, *Information Operations and Facebook*.

[102] National Defense Authorization Act for Fiscal Year 2017. The Tactics, Techniques, and Procedures section of this paper also examines other federal initiatives, including programs developed by FEMA, to provide counternarratives and "debunk" false information.

[103] JCS, *Information Operations*, ix.

To enable nondefense usage, IOs should constitute "*the employment of information-related capabilities to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.*"

IOs defined in this way are not limited to the dissemination of "false" or "fake" information. IOs are "vast in scale, varied in target and numerous in strategies and tactics," and many disinformation campaigns do not leverage fabricated, falsified, or deceptive information to achieve their goal.[104] Focusing exclusively on fake information would overlook the other types of coercive messaging that China and Russia can use and hobble the development of countermeasures against more sophisticated means of shaping US public and leadership behavior.

Information Warfare as a Broader Category of Operations

Policymakers and researchers will also find it helpful to distinguish IOs from the more inclusive category of information warfare. While the US government does not define information warfare, practitioners conceptualize it as "a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations."[105] Russian military doctrine and analysis of security issues often uses the term information warfare instead of IOs. The Main Intelligence Directorate of the Russian Armed Forces (commonly referred to as the GRU) uses the term information warfare to describe its efforts to subvert the 2016 US elections by "spread[ing] distrust towards candidates for political office and the political system in general."[106] Many US analysts have adopted this definition of information warfare to characterize Russia's drive to influence the US electoral process and—more broadly—its long-term campaigns to shape public opinion and perceptions in opposing nations.[107] But as the Tactics, Techniques, and Procedures section will examine, Russia is also prepared to conduct short-term information warfare campaigns in peacetime crises and across the conflict continuum.

Information warfare most clearly differs from IOs in the diversity of military missions that information warfare encompasses. Russia has a holistic concept of information warfare that seeks to impact both the physical (i.e., information networks and command and control systems) and cognitive dimensions of the information environment. Russia's definitions of information warfare and "information conflict" include computer network operations, psychological operations, influence activities, electronic warfare, and communications disruption.[108] The Chinese PLA's term "informationalized warfare" similarly comprises the use of electronic warfare, computer network attacks, deception, and IOs to achieve information superiority and degrade the adversary's battle networks.[109] The US armed services treat information warfare still more expansively. For example, the US Navy's Information Warfare Enterprise includes not only IOs but also cryptology, signals intelligence, electronic warfare, cyber operations,

[104] Krasodomski-Jones et al., *Warring Songs*.

[105] Theohary, *Defense Primer*, 1.

[106] *Khusyaynova v. United States*. A 2011 Russian Ministry of Defense report on future information operations defined information warfare (информационная война) as "the ability to . . . undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a State in order to destabilize society and the government; and force a State to make decisions in the interest of their opponents." Ministry of Defence of the Russian Federation, *Conceptual Views*, quoted in Thomas, "Russia's 21st Century Information War," 12.

[107] Jones, *Going on the Offensive*.

[108] Giles, *Handbook of Russian Information Warfare*, 6; and Tashev, Purcell, and McLaughlin, "Russia's Information Warfare," 139.

[109] Work and Grant, *Beating the Americans*, 8.

and even meteorology.[110] Integrating all such missions can offer synergistic benefits in combat. For the sake of brevity, this study focuses on IOs and combined information-cyberattacks.

Aligning IOs along the Conflict Continuum

In a 2019 study, Kathleen Hicks (who now serves as the deputy secretary of defense) and her coauthors argued that ongoing Chinese and Russian IO campaigns fall in the gray zone "beyond diplomacy and short of conventional war."[111] They also found that the United States lacked a strategy to counter those operations.[112] Filling that gap should be a key priority for US policymakers. As they develop such a strategy, they should also account for the risk that China or Russia will conduct coercive IOs at the dark end of the gray zone, where a high-stakes crisis puts those nations on the brink of armed conflict with the United States. An integrated strategy of this sort will need to help the US counter a broad range of messaging, from familiar operations to corrode public confidence in government to novel (and vivid) threats of punishment. The strategy should also account for the unique challenges of US decision-making in the dark-gray zone and for adversary efforts to magnify and exploit the challenges of allied coordination at the edge of war.

A comprehensive approach to IO defense should not stop at that edge. Policymakers need a framework to assess how China and Russia can employ IOs across what the Pentagon calls the conflict continuum, from peacetime engagements through war. In addition, policymakers should anticipate how Beijing and Moscow could tailor combined attacks to intensify pressure on US leaders to back down in a crisis and manipulate US fears of escalation as an integral part of their coercive campaigns.

Beyond the Gray Zone: The Conflict Continuum for Domestic Defense

US doctrine calls for conducting IOs and other military operations across the "conflict continuum that spans from peace to war."[113] A US strategy against coercion should apply that spectrum in revised form to the domestic realm. Different portions of the continuum will require particular types of defensive plans, capabilities, and coordination mechanisms, including between government agencies and social media owners. A US strategy should clarify those lines of effort and help integrate them so that countermeasures against corrosive campaigns can be efficiently applied against coercive IOs. The strategy should also enable the alignment of operational plans so that adversaries cannot gain coercive advantages by making unexpected escalatory jumps across the continuum of conflict.

Using the gray zone to characterize various types of coercive campaigns fails to capture the full range of adversary options. Figure 1 illustrates the broader conflict continuum over which China and Russia can conduct such operations. At the far left, in the peacetime, precrisis environment, China and Russia will continue their ongoing corrosive IO campaigns to weaken US security alliances and undermine public confidence in US leaders and government institutions. These nations will also sustain their efforts to embed advanced persistent threats (APTs) in US infrastructure networks, including malware designed to disable or disrupt US infrastructure in future conflicts.

The outbreak of a regional crisis would fall in the center of the continuum. As the crisis begins, Beijing and Moscow would shift their messaging to

[110] USN, *Community Vision*; USNA, "Information Warfare Community"; Braswell, "Information Warfare Commander"; Shutka, "NAVIFOR"; and Ackerman, "Naval Warfighting Embraces the Full Spectrum."

[111] Dalton et al., *By Other Means*, 2. For other definitions of the gray zone, see Popp and Canna, *Characterization and Conditions*, 2; and Morris et al., *Gaining Competitive Advantage*.

[112] Dalton et al., *By Other Means*, 6 and 8.

[113] JCS, *Joint Operations*, V-1 and V-4.

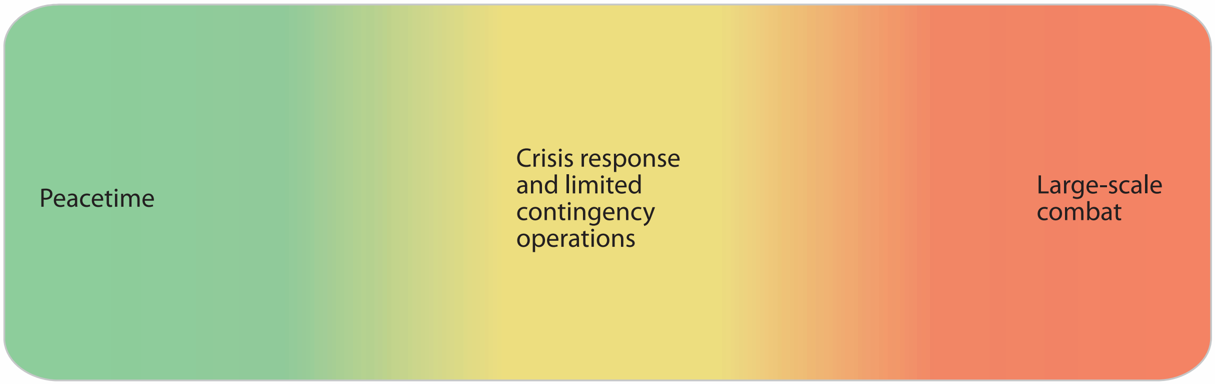


Figure 1. Conflict Continuum

prevail in the crisis without initiating cyber or kinetic warfare. They could tailor their IOs to (1) convince the public and senior officials that the United States will suffer unacceptable punishment if the United States persists in defending its security partners; (2) intensify doubts about the benefits that the United States can achieve by protecting those partners; and (3) persuade alliance members to block or weaken preparations for mutual defense.

Beijing and Moscow may accompany this shift toward coercive messaging with further cyber intrusions into US infrastructure. They may seek to install in US infrastructure more capable and difficult-to-detect APTs that they are holding in reserve for such contingencies and take other measures to help prepare the cyber battlefield. They may also conduct "noisy" penetration efforts. While serving as commander of US Northern Command, General Terrence O'Shaughnessy noted that Beijing can seek twofold benefits from installing malware. Chinese leaders view cyber intrusions as a "low-cost deterrent that demonstrates capabilities and resolve to an adversary" and enables them to target US critical infrastructure if the crisis further escalates.[114] In an intensifying crisis, Beijing and Moscow could accompany these penetration campaigns with IOs to highlight their ability to hold US infrastructure at risk and to weaken the public's confidence that US leaders can protect them.

The portion of the continuum on the right would encompass the transition to war. That transition will not mark the end of coercive operations and the shift to total warfare. On the contrary: rather than bear the costs of physically annihilating US and allied forces, Beijing and Moscow may combine IOs with the selective use of force to convince the US to back down, and thereby prevail at the lowest possible level of violence. A comprehensive US strategy against coercion must encompass this end of the conflict continuum together with its more peaceful realms.

Accounting for combined information-cyberattacks (as well as combined attacks using kinetic weapons, electronic warfare, and other means of disruption) is consistent with broader US defense strategy. DoD's highest priority is deterring and, if necessary, defeating China or Russia in a major conflict.[115] Developing strategies to counter coercive uses of force fits squarely within this defensive focus. Indeed, given the emphasis that Chinese and Russian doctrines place on achieving coercion if war occurs, it would be dangerous to leave the US unprepared for combined information-cyberattacks.

[114] *Hearing on Defense Authorization Request for Fiscal Year 2020*, O'Shaughnessy statement.

[115] On this focus and its implications for US cyber initiatives and investments in other technologies, see *Hearing on Innovation Opportunities and Vision*, Fox statement.

Policymakers should account for the possibility that Beijing and Moscow may design their initial attacks to inflict carefully limited effects. In particular, they may conduct exemplary attacks that highlight their ability to jeopardize US public safety and pair those attacks with IOs that both magnify the fear the attacks generate and threaten widespread devastation unless US leaders abandon their allies. China and Russia could conduct similar combined attacks against US security partners to encourage them to back down and deny American use of their ports and military bases necessary for regional defense. If exemplary strikes proved inadequate, Beijing and Moscow could increase their disruption of US and allied infrastructure and their warnings of still greater suffering to follow.

These nations may also adopt less gradual approaches to coercion.[116] US defense officials have warned that Russia may inflict large-scale cyber or kinetic attacks on American territory very early in a conflict and seek to "escalate to de-escalate" the confrontation.[117] As General O'Shaughnessy framed this option, Russian and Chinese leaders may use attacks against critical military and civilian infrastructure to limit US decision-makers' options in a crisis and "compel de-escalation" by the United States.[118] In particular, they may strike water systems, the power grid, and other infrastructure that FEMA designates as "community lifelines"—that is, any system that enables "the continuous operation of critical government and business functions and is essential to human health and safety or economic security."[119] Adversaries may also supplement the coercive effects of those attacks by delivering horrific imagery over social media and threatening to inflict further devastation unless the United States meets their demands.

Attacks on lifeline systems would carry immense escalatory dangers. While Beijing and Moscow might intend their attacks to compel US de-escalation in a crisis, disruptive strikes could have the opposite effect. James Andrew Lewis and other analysts note that destructive strikes on critical infrastructure or other military assets could incur devastating retaliation. Accordingly, "coercive acts that stay below a level that is likely to trigger retaliation will be more attractive to opponents."[120] Those incentives are all the stronger because of the risk that disruptive cyberattacks (including those against critical infrastructure) could lead to accidental or inadvertent escalation and spark wars far more destructive than either opponent intended.[121] These dangers will continue to reduce the likelihood that China or Russia will cross the threshold to combined attacks and reinforce their incentives to seek victory through IOs alone.

Yet, modern IO tactics and technologies also give these nations new options to reduce the escalatory risks they face and manipulate US fears of escalation to influence crisis decision-making in the White House. Anticipating these options and building countermeasures against them should be a cornerstone of US strategies against coercion.

[116] On the risks of sudden escalation in cyber events, see Libicki, *Crisis and Escalation in Cyberspace*, 120.

[117] In June 2015, then deputy secretary of defense Robert Work and the vice chairman of the Joint Chiefs of Staff Admiral James Winnefeld testified that "Russian military doctrine includes what some have called an 'escalate to deescalate' strategy—a strategy that purportedly seeks to deescalate a conventional conflict through coercive threats, including limited nuclear use." Ryan, "Russia's Nuclear Toolbox?" See also US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault*.

[118] *Hearing on Defense Authorization Request for Fiscal Year 2020*, O'Shaughnessy statement, 4; and *Hearing on Defense Authorization Request for Fiscal Year 2021*, O'Shaughnessy statement, 3 and 6.

[119] FEMA, "Community Lifelines."

[120] Lewis, *Rethinking Cybersecurity*, 26.

[121] Morgan et al., *Dangerous Thresholds*, 18–27; Lin, "Escalation Dynamics," 46–70; Libicki, *Crisis and Escalation in Cyberspace*, 2–3 and 81; Cavaiola, Gompert, and Libicki, "Cyber House Rules," 81–104; and Gray, *Making Strategic Sense of Cyber Power*, 45–48.

Managing the Risks of Cyber Escalation in a Contested Information Environment

Studies of cybersecurity typically—and accurately—conclude that cyber warfare would carry immense escalatory dangers.[122] While cyber operations are common in today's peacetime, precrisis realm of the conflict continuum, the great powers have not yet used disruptive cyberattacks against each other in a regional conflict. Joseph S. Nye Jr. notes that "there remains much that analysts do not know about cyberattacks in wartime, including cyber crisis stability, escalation in war, and intra-war deterrence (efforts to restore stability). There are many hypotheses; unlike peacetime, however, there is little empirical evidence because no full-scale cyberwar has occurred."[123] Empirical data is similarly lacking for combined information-cyberattacks, in which false and manipulative messaging between combatants will create novel escalatory risks. Our sheer inexperience with this new form of warfare will increase the likelihood of missteps and misunderstandings as combatants intensify pressure on each other to sue for peace.

The transition from IO-only campaigns to combined attacks would itself be fraught. Jim Miller, former undersecretary of defense for policy, argues that adversaries in a crisis will have strong incentives to employ cyberattacks before their opponents do. He notes that both Russian and US military forces are vulnerable to cyberattacks that could significantly reduce the effectiveness of these forces. Their mutual vulnerability creates classic "first use" pressures. "In the event of a crisis," Miller writes, "knowing how vulnerable it is to a potential impending cyber attack, each side is incentivized to use its cyber-vulnerable capabilities first or lose them." Going first may still result in severe retaliation. But adversaries will perceive going second as "notably worse," creating severe instabilities in an intensifying crisis.[124] Coercive IOs would exacerbate these instabilities. As an aggressor threatens its opponent with catastrophic cyberattacks and promises that more punishment will follow unless the opponent yields, that messaging will create all the more incentive for the opponent to strike first (and for the aggressor to anticipate and preempt the strike).

Once combined attacks are underway, no agreed-upon ladder of escalation exists to help combatants manage the conflict and avert all-out war. During the Cold War, Herman Kahn suggested that "rungs in the escalation ladder" could serve as a metaphor for how adversaries might seek to use nuclear weapons without spiraling into uncontrolled exchanges. Kahn identified forty-four specific rungs between subcrisis maneuvering and "spasm or insensate war."[125] Policymakers in the United States, China, and Russia might conceivably develop and seek consensus on an equivalent ladder to manage the escalatory pressures unleashed by combined cyber-information attacks.

Doing so would be incredibly difficult and not worth the effort. Thankfully, we have no idea whether the rungs in Kahn's ladder would help guide and constrain nuclear exchanges. Nor is it clear whether or how his escalatory rungs might usefully translate to the cyber realm. Kahn identified defects in his ladder that would almost certainly apply to the development and use of a cyber equivalent, including sharp discontinuities between rungs and broader escalatory dynamics.[126] Jason Healey and Robert Jervis critique the entire notion that escalatory ladders and existing models of conflict management apply to cyberspace and recommend that those

[122] Libicki, *Crisis and Escalation in Cyberspace*, 81–95; and Lin, "Escalation Dynamics," 52–53.

[123] Nye, "Deterrence and Dissuasion," 70.

[124] Miller and Fontaine, *New Era in U.S.-Russian Strategic Stability*, 30 and 34. See also Healey and Jervis, "Escalation Inversion," 13–15.

[125] Kahn, *On Escalation*, 52 and 194.

[126] Kahn, *On Escalation*, 214–220.

models be "avoided, treated cautiously, or reconceptualized altogether."[127]

Reconceptualization of the escalatory dangers of cyberwarfare is especially needed in the cognitive and behavioral realms. In all types of conflicts, misperceptions of the adversary's goals and beliefs, distortions and ingrained biases in decision-making by senior officials, and other psychological factors can produce failures of deterrence and crisis management.[128] Cyberwarfare will be no different. The same is true of the decision-making failures that stem from the human tendency to rely on intuitive, reflexive, and emotionally driven modes of thought in crises and other stressful situations, as opposed to slower, more deliberate and analytic modes in normal circumstances.[129]

Danielle Jablanski, Herbert Lin, and Harold Trinkunas argue that in the nuclear realm, the massive flow of information over social media will exacerbate these cognitive problems and make crisis management far more difficult:

> Against a backdrop of multiplatform communication suffused with a mix of information—true and false, official and unofficial, from friend and from foe, emotionally charged and serenely rational—the dynamics of the modern information ecosystem suggest unprecedented pressures on government decision makers during crisis. The timelines for decision making will be far more constrained, a fact likely to lead to a greater reliance on fast thinking by decision makers just at a time—during a crisis—when slow, deliberate, analytical thinking is most important.[130]

Going a step further, a study by Heather Williams and Alexi Drew finds that messaging over Twitter and other social media platforms is especially prone to create misunderstandings between parties to a crisis and exacerbate tensions between them. Their recommendation: "To manage escalation during crises, stop tweeting."[131]

China and Russia are unlikely to heed that advice. Quite the opposite: they will use Twitter and other platforms to intensify pressure on the United States to settle on their terms and warn that further resistance will expose Americans to suffering far greater than they believe their allies are worth.

"Turning the Screw:" Adversary Options to Manage and Exploit Dangers of Escalation

Beijing and Moscow may seek to reduce the escalatory risks by conducting combined attacks that inflict very little (but vividly portrayed) damage rather than by conducting nationwide strikes that would be sure to incur a devastating response. Infrastructure disruptions on a nationwide scale would cross existing US thresholds of attack severity in a clear and unambiguous manner and trigger well-defined federal response operations. Presidential Decision Directive (PDD) 41, *United States Cyber Incident Coordination*, establishes criteria for assessing the severity of cyber incidents and guiding federal responses to them. PDD-41 divides incidents into two categories.

A. Cyber incident. An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal

[127] Healey and Jervis, "Escalation Inversion," 20.

[128] Jervis, *Perceptions and Misperceptions*.

[129] Lin, "Existential Threat," 8–11. Subsequent portions of this study address cognitive issues and decision-making failures associated with the use of coercive messaging.

[130] Jablanski, Lin, and Trinkunas, "Retweets to Midnight."

[131] Williams and Drew, *Escalation by Tweet*.

controls, or implementation that could be exploited by a threat source.

B. Significant cyber incident. A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.[132]

A comprehensive attack on US infrastructure would clearly constitute a significant cyber incident. The 2016 NCIRP Cyber Incident Severity Schema provides additional guidance that would help policymakers categorize the severity of such an attack and trigger US response operations. The schema establishes five levels of emergencies, with level 5 (the most severe) constituting those that pose "an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens."[133]

None of these documents mention the threat that adversaries will combine IOs with cyberattacks and, potentially, achieve powerful coercive effects at very low levels of disruption. PPD-41 and the NCIRP focus on cyber threats alone. That limited focus was both understandable and much needed: both documents clarified major uncertainties concerning incident thresholds and response protocols. Now, policymakers should resolve the equivalent uncertainties that surround combined information-cyberattacks. As noted above, their efforts should account for the possibility that China and Russia will combine very low levels of disruption with massive, microtargeted IOs to exacerbate public and leadership fears of escalation. But within that general attack strategy, US defensive strategies will also need to anticipate specific, and innovative, designs for combined attacks.

Policymakers should pay special attention to a coercive technique examined by Alexander George: the "gradual turning of the screw" to drive an opponent's behavior.[134] By employing IO-heavy exemplary attacks and threatening that more punishment will follow, China and Russia may seek to prevail without crossing the thresholds that a massive attack would clearly exceed. The US should expand or supplement the Cyber Incident Severity Schema to account for such coercive techniques. The schema should include low-disruption, high-psychological-impact attacks in emergency level 5, which includes the most severe events that should guide US investments in preparedness. In addition, the schema's category of "public confidence" (currently used to help define less-severe level 3 emergencies) should be refined to account for coercive threats and included in higher emergency levels to reflect their potential consequences for national security.

These revised thresholds should avoid drawing "bright lines." Preserving wide presidential latitude for responding to combined attacks will be essential to dealing with unexpected attack vectors and to preventing US crisis managers from being locked into rigid positions that adversaries might exploit. In particular, it would be risky to publicize explicit red lines that would trigger specific kinds of US countermeasures. Chinese and Russian leaders might be tempted to conduct operations just below those levels if they believed doing so would reduce the likelihood of US defensive operations.[135] Policymakers will also need to strike a balance between ensuring that adversaries know we have plans and capabilities for effectively responding to exemplary attacks and maintaining the secrecy necessary to prevent adversaries from developing effective countermeasures against US response options.

Updates to the PPD-41 coordination mechanisms that would be triggered by severe cyber incidents

[132] White House, *Presidential Decision Directive*.

[133] DHS, *National Cyber Incident Response Plan*, 8. The Cyber Incident Severity Schema is on p. 38.

[134] George, *Forceful Persuasion*, 8.

[135] Stockton, *Resilience for Grid Security Emergencies*, 18.

are also necessary. The only mention that the directive makes of public communications is that "the Departments of Homeland Security and Justice shall maintain and update as necessary a fact sheet outlining how private individuals and organizations can contact relevant Federal agencies about a cyber incident."[136] Such fact sheets were never intended to deal with the impact that IOs could achieve in combination with cyberattacks and are totally inadequate for doing so. The NCIRP provides a more detailed description of the information-sharing mechanisms to be used for incident response, but they fall short of what will be necessary against coercive messaging campaigns.[137]

One gap will be especially significant yet difficult to fill: the risk that adversaries will conduct specialized IOs to manipulate public and leadership fears of escalation in regional conflicts. Escalation is not just a danger for China and Russia to manage through the use of exemplary attacks and other tactics. They can also use escalation as a tool of coercion. George notes that "the impact of coercive diplomacy is enhanced if the initial steps taken against the adversary arouse his fear of escalation to levels of warfare that he would regard as unacceptable and would be strongly motivated to avoid."[138] Fostering such fears can comprise a key component of the adversary's strategy for prevailing in a confrontation. As Herman Kahn states, adversaries can intentionally manipulate the risks of escalation or "eruption" from the (not necessarily explicit) agreed levels of conflict to which opponents had previously limited themselves.[139]

Building preparedness against such manipulation (and being seen in Beijing and Moscow as having done so) is all the more important given the US response to Russia's interference in the 2016 election. In the Obama administration, senior leaders were reluctant to respond more harshly to Russia's campaign in part because of concerns that doing so would prompt Russia to escalate and conduct even more disruptive actions. Former CIA Director John Brennan shared these worries and noted their impact in curtailing US countermeasures:

> I was concerned about what the Russians might have up their sleeve and what they could do, because it's not just dealing in a foreign theater, where we make a chess move and they make a chess move. . . . I didn't know what the Russians might stoop to and so I did not have great ideas at all about if we do this it's really going to have that salutary effect.[140]

Russia and China could be excused for imagining that they will be able to manipulate and exploit such escalatory concerns to discourage US military action and drive American capitulation in future confrontations.

Of course, in the aftermath of the 2016 election, the United States has adopted a more forward-leaning posture in responding to Russia's election interference and corrosive campaigns. USCYBERCOM's doctrine of persistent engagement and its execution of defend-forward missions exemplify that shift. Persistent engagement may create new options to manage escalation in the conflict continuum short of war. Michael Fischerkeller and Richard Harknett argue that in the ongoing competition in cyberspace, "Operations that intensify or escalate but are designed to allow for the metering of effects and/or reversible damage, for example, take account of the uncertainty the target state may have regarding another's intentions and, therefore, facilitate de-intensification or de-escalation." Over time, persistent engagement may also clarify "what

[136] White House, *Presidential Decision Directive*, 6.

[137] DHS, *National Cyber Incident Response Plan*, 34.

[138] George, *Forceful Persuasion*, 79.

[139] Kahn identifies a number of means by which combatants can execute coercive escalation strategies and erupt beyond the "limited conflict or 'agreed battle' going on." Kahn, *On Escalation*, 4–7.

[140] Quoted in SSCI, *Russian Active Measures, Vol. 3*, 20.

can be regarded within the rules of an increasingly stabilizing *agreed competition*."[141] Imposing costs on Russia and China in response to their continuing gray-zone campaigns (including SolarWinds and the 2021 Microsoft hack) will be essential to achieving such goals.

But managing escalation during cyber warfare will entail problems for escalation management and public messaging far beyond those for persistent engagement. For example, as destructive cyberattacks begin, senior US officials may need to strike a balance between the desire to defend American allies and interests and the fear that doing so will lead to escalating exchanges that inflict far more punishment on US citizens than they (and the officials themselves) believe is worth the cause. We should count on Beijing and Moscow to use IOs aimed at tilting that calculus to their advantage.

Chinese and Russian military doctrines provide indications as to how those nations may seek to manage escalation and employ it as a coercive tool. The analysis that follows examines these doctrinal clues. However, to develop a strategy against coercion, we also need to understand (1) the mechanisms and causal linkages by which threatened or actual punishment can drive US and allied decision-making; (2) how the rise of social media creates unprecedented vulnerabilities of the US public to coercive messaging; (3) Chinese and Russian tactics, techniques, and procedures (TTPs) to exploit those vulnerabilities; and (4) how Beijing and Moscow may apply customized IOs and combined attacks to take advantage of specific US and allied weaknesses.

Organization of the Study

The study is structured to help meet each of the analytic requirements identified above and examines their implications for developing US defensive strategies. The study also proposes options to reduce US vulnerabilities to coercion and suggests priorities for further research.

The How Coercion (Sometimes) Works section analyzes the underlying dynamics of coercion and examines why past coercive campaigns have so often failed. These failures have been especially common when attackers have used mass conventional bombings to punish civilian populations. Recent studies contend that coercive cyberattacks are even *less* likely to succeed. However, none of those studies account for the possibility that adversaries will pair cyberattacks with sophisticated IOs to intensify public fears and magnify the coercive effects generated by such campaigns. Nor do those studies explore two other coercive strategies that Beijing and Moscow might use. During Operation Allied Force in 1999, NATO sought to coerce Yugoslavia by directly targeting IOs against that nation's leadership as well as bombing its infrastructure. We should expect China and Russia to target US leaders in the same manner but with vastly more sophisticated technologies. We should also expect those nations to conduct campaigns to sow mistrust between the US and its security partners and (seeking coercion by denial) convince alliance members that further defensive operations are doomed to fail. This section provides an overview of all three pathways of coercion and their potential uses in cyberspace.

The Underlying US Vulnerabilities section examines the US public's vulnerability to coercive messaging, especially through the use of social media. US strategies against IOs and combined attacks will need to account for the public's exceptional dependence on these networks during periods of stress, its tendency to believe and share sensational reporting (regardless of its veracity), and the difficulty of

[141] Fischerkeller and Harknett, *Persistent Engagement, Agreed Competition*, 21 and 23. For a more skeptical assessment of the prospects for escalation management during persistent engagement, see Healey, "Persistent (and Permanent) Engagement."

altering false beliefs once the public has adopted them. This section examines how China and Russia can design coercive campaigns to leverage the ongoing corrosion of faith in US democratic institutions and governance and take advantage of the broader "truth decay" underway in the United States. This analysis also examines the new forms of partnerships between social media companies and government that will be required to counter such campaigns and options to overcome the impediments to building such collaboration.

The Tactics, Techniques, and Procedures section explores how adversaries can exploit America's vulnerabilities to IOs. To provide a threat-based foundation for defensive initiatives, US policymakers will need to anticipate emerging Chinese and Russian TTPs to manipulate the perceptions of US policymakers and the public. This section examines technologies that can enhance the effectiveness of future coercive campaigns, including deepfakes, AI, and (most recently) techniques to impersonate US and allied officials. This analysis also assesses Chinese and Russian tools and tactics to conduct microtargeted IO campaigns at scale, manipulate social media algorithms, and evade disinformation-blocking policies and procedures.

The Combined Information-Cyberattacks section moves beyond the challenges posed by IO-only campaigns, and examines how these nations can combine information and cyberattacks to shape US crisis decision-making. Their precepts for managing and manipulating escalation form only one component of their broader focus on achieving victory early in a confrontation by shaping enemy perceptions and beliefs.

The Defeating Customized Attacks section identifies potential US defensive requirements against specific adversary threat vectors, including efforts to create mass panic and target US military personnel to discourage and disrupt crisis zone operations. This analysis also proposes how to develop sector-specific measures to defeat coercive operations against the US financial system and other infrastructure components. In addition, the section examines options to counter the coercion of NATO decision-making and coalition operations in Asia and defeat combined attacks designed to achieve coercion by denial.

The Conclusions and Priorities for Future Analysis section summarizes key findings and recommendations of the study. This section also recommends priorities for further analysis, including options to strengthen deterrence of coercive campaigns and integrate defensive measures at home with operations to suppress attacks abroad.

How Coercion (Sometimes) Works

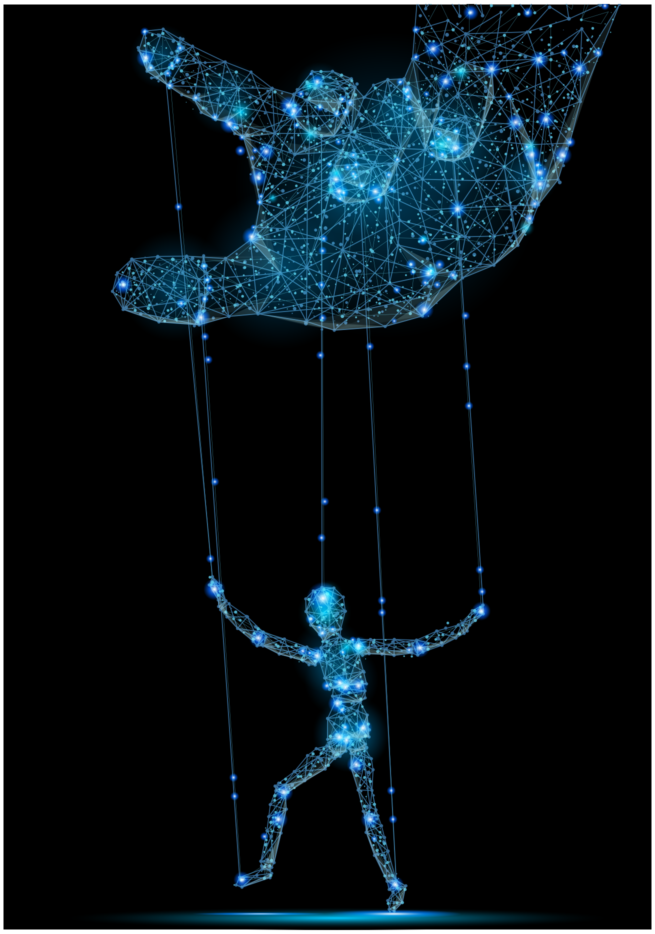
From a historical perspective, defeating coercive attacks should be as easy as falling off a log. Robert Pape's study *Bombing to Win* provides a comprehensive assessment of past campaigns to alter enemy decision-making—in particular, by inflicting so much harm on civilians that their leaders comply with the attacker's demands.[142] Pape finds that bombing campaigns that punish civilians and destroy critical infrastructure almost always fail to achieve their coercive goals. Analyzing these repeated failures, Pape concludes that "coercion is extremely hard."[143] Other studies reach the same conclusion.[144]

[142] Pape, *Bombing to Win*, 1.

[143] Pape, *Bombing to Win*, 316. Pape notes that instead of punishing civilians, attackers can also attempt to coerce adversaries by exploiting their military vulnerabilities and using military means to prevent adversaries from achieving their political objectives or territorial goals. As noted on p. 17 of this study, the Department of Defense and its partners are conducting mission assurance programs to defeat such "coercion by denial" strategies. Pape, *Bombing to Win*, 316.

[144] A survey of these studies and the data sets on which they rely can be found in Art and Greenhill, "Coercion," 16–17. For additional surveys that reach similar conclusions about the frequent failures of coercive campaigns, see Borghard and Lonergan, "Coercion in Cyberspace," 454; and Valeriano, "How Rival States Employ Cyber Strategy."

Pape argues that these failures stem in part from the attackers' inability to inflict sufficient devastation. Reviewing a large number of case studies, he finds that conventional munitions rarely inflict enough punishment on civilians to drive shifts in enemy behavior, even when attacks are designed to cause massive casualties.[145] Pape also argues that aerial attacks against power grids, water utilities, and other infrastructure systems provide still weaker coercive effects because they have less impact on civilians than direct attacks.[146]



Cyber weapons provide China and Russia with new means of striking the infrastructure on which US public health and safety depend. Yet, many analysts conclude that cyberattacks will be less effective for coercive campaigns than conventional bombings. Those assessments overlook how Beijing and Moscow can use modern information operations (IO) technologies to magnify public fears and generate pressure on US leaders to back down in regional crises. Existing studies also ignore the danger that adversaries will pair those attacks with curated, intelligence-supported messaging targeted against the US decision-makers. This section uses NATO's Operation Allied Force (OAF; 1999) as a case study to analyze how attackers can integrate public and leadership-level campaigns and explores the implications of such operations for developing US strategies against coercion.

In regional conflict, China and Russia will probably conduct such operations against US security partners as well. Secretary of Defense Lloyd Austin notes that "our allies and partners are a force multiplier and one of the greatest strategic assets we have in protecting our Nation."[147] Alliance cohesion will be essential to coordinate policies in edge-of-war situations and, if attacks occur, authorize and coordinate collective defense operations. We should expect Beijing and Moscow to target those alliances with IOs and combined information-cyberattacks accordingly.

Two shortfalls in alliance preparedness against coercion deserve particular attention. First, the United States should better anticipate (and build defensive strategies against) the use of hybrid warfare techniques to disrupt and delay alliance decision-making. General John Hyten, vice chairman of the Joint Chiefs of Staff, states that the United States has not "done a good job of understanding the hybrid threat, and therefore we haven't done a good job of responding." He urges the United States and its allies to focus analysis on adversary hybrid warfare strategies "just like we study conventional warfare" and other forms of conflict.[148] The analysis that follows examines the coercive components of Russia's hybrid warfare operations in eastern

[145] Pape, *Bombing to Win*, 22–23.

[146] Pape, *Bombing to Win*, 69.

[147] Austin, "Message to the Force," 3.

[148] Tirpak, "U.S. Poorly Integrates CCMDs."

Europe and how Moscow and Beijing may (drastically) update and realign those techniques to delay and confuse allied decision-making.

The second shortfall lies in examining coercion by denial, a less familiar strategy but one that Pape has found historically to be more effective than traditional punishment campaigns. Under coercion by denial, an attacker seeks to degrade the opponent's military forces and counter its strategy to prevail in the conflict, and thereby convince opposing leaders that they have no hope of prevailing.[149] Put in the broader calculus of coercion, denial strategies function by reducing the benefits that the enemy expects to gain through further resistance compared with the military losses and other costs the enemy will incur by continuing to fight. Combined information-cyberattacks provide new means to achieve coercion by denial. US policymakers should assess how China and Russia could customize such attacks to counter specific Department of Defense (DoD) plans and "surge" deployment operations and pair those customized attacks with IOs to convince the president and allied leaders to abandon a hopeless fight before hostilities escalate.

Coercion through Punishment in the Cyber Era

Alexander George explains the underlying dynamics of punishment-based coercion in *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (1991). Coercive diplomacy constitutes the threatened or limited actual use of force to convince the opponent to stop or undo an aggressive action:

> [Coercive diplomacy] seeks to persuade an opponent to cease his aggression rather than bludgeon him into stopping. In contrast to the blunt use of force to repel an adversary, coercive diplomacy emphasizes the use of threats to punish the adversary if he does not comply with what is demanded of him. If force is used in coercive diplomacy, it consists of an exemplary use of quite limited force to persuade the opponent to back down. By "exemplary" I mean the use of just enough force of an appropriate kind to demonstrate resolution to protect one's interests and to establish the credibility of one's determination to use more force if necessary.[150]

At the most basic level, coercion functions by altering decision-makers' perceptions of the costs and benefits of alternative courses of action.[151] Coercion also operates by exploiting fears of future punishment or other costs. Thomas Schelling notes that "it is the threat of damage, or of more damage to come, that can make someone yield or comply."[152] George himself notes that coercive campaigns can falter for a variety of reasons, including from asymmetries in the stakes that the attacker and the victim see in a conflict.[153] Misperceptions, miscalculations, and failures to account for victim's values and

[149] This characterization of denial draws on the analysis provided by Pape, *Bombing to Win*, 10, 13, and 17–20; and Art and Greenhill, "Coercion," 20–22.

[150] George, *Forceful Persuasion*, 5. The DoD dictionary of terms does not have a definition of coercion. However, the US Air Force defines coercion as "convincing an adversary to behave differently than it otherwise would through the threat or use of force." See USAF, *Practical Design*, 1. For a similar definition of coercion, see Byman, Waxman, and Larson, *Air Power as a Coercive Instrument*, 10. Coercion is also similar to compellence, which Thomas C. Shelling defined as "initiating an action . . . that can cease, or become harmless, only if the opponent responds." Schelling, *Arms and Influence*, 72. For a discussion of how compellence differs from deterrence and other uses of military power, see Art, "To What Ends Military Power?," 7–10. On the difference between deterrence and coercion, see Art and Greenhill, "Coercion," 5. Art and Greenhill provide an updated definition of coercion in "Coercion," 4. On the use of nuclear weapons for coercive diplomacy, see Fuhrmann and Seschser, *Nuclear Weapons and Coercive Diplomacy*.

[151] Schelling, *Arms and Influence*, 2–6; Pape, *Bombing to Win*, 12; and Borghard and Lonergan, "Coercion in Cyberspace," 453 and 460.

[152] Schelling, *Arms and Influence*, 3. See also Art and Greenhill, "Coercion," 4 and 13–14.

[153] George and Simons, *Limits of Coercive Diplomacy*.

culture can further impede coercive operations.[154] These problems will persist regardless of the types of forces and information technologies that attackers employ.

In addition to the endemic impediments to coercion, attackers may face special difficulties in using cyber weapons to shape their victims' behavior. Recent studies contend that cyberattacks will be even less effective for coercion than conventional bombing.[155] A survey of cyber-supported campaigns bears out this finding. Analyzing repeated uses of cyber-induced disruptions and other coercive uses of cyber capabilities, Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness conclude that only 5.7 percent of 192 episodes of cyber exchanges between rivals achieved observable concessions.[156] Moreover, despite continued improvements in malware sophistication and critical infrastructure systems' increased dependence on industrial control systems and devices tied to the internet, Jon Lindsay and Eric Gartzke conclude "the coercive utility of cyberspace is actually somewhat limited."[157]

These and other researchers identify fundamental constraints on the effectiveness of cyberattacks to achieve coercion through punishment. Taken together, those constraints would seem to limit the ability of China or Russia to successfully conduct such operations against the United States and minimize (if not eliminate) the need for new defensive strategies and programs to counter them. Key limitations include the following:

Inability to inflict sufficient suffering. Erica Borghard and Shawn Lonergan contend that "governments cannot kill a lot of people in a very short period of time using cyber weapons," especially when compared with strategic bombing. They argue that "access requirements and the customized nature of cyber capabilities render it nearly impossible to launch a time-dependent, highly coordinated cyber campaign of the scale required to inflict severe costs on enemy populations."[158]

Poorly suited to communicating coercive threats and influencing perceptions. For coercion to succeed, the victim of the campaign must know who is attacking, understand what must be done for the punishment to stop, and be convinced that further suffering will follow unless they yield. Cyberattack-based coercive campaigns may face special difficulties in meeting these messaging requirements. In past cyberattacks, perpetrators have often tried to hide their identities and used sophisticated means to prevent victims from attributing the attacks to them. Such impediments to attribution weaken the utility of cyberattacks for coercion.[159]

Furthermore, to be effective, many types of attacks must be conducted in secrecy. Otherwise, the victim will patch the vulnerability that the attacker is exploiting, disconnect from the internet, or otherwise sever the access the adversary needs to disrupt or disable its targets.[160] Victims are more likely to misunderstand an attacker's intent in cyber operations than in conventional bombing campaigns, especially because policymakers lack a shared understanding of cyberspace to help them divine the meaning behind a cyber signal.[161] These and

[154] George, *Forceful Persuasion*, 4.

[155] Borghard and Lonergan, "Coercion in Cyberspace," 480; Valeriano, Jensen, and Maness, *Cyber Strategy*, 51–52 and 89–90; and Lindsay and Gartzke, "Coercion through Cyberspace," 3–4 and 9.

[156] Valeriano, Jensen, and Maness, *Cyber Strategy*, 79.

[157] Lindsay and Gartzke, "Coercion through Cyberspace," 203.

[158] Borghard and Lonergan, "Coercion in Cyberspace," 477. However, as will be discussed later in the section, these scholars qualify their argument by noting that improving cyberattack technologies and increasing infrastructure vulnerabilities could make punishment via cyberattacks more viable. Borghard and Lonergan, "Coercion in Cyberspace," 480.

[159] Borghard and Lonergan, "Coercion in Cyberspace," 457.

[160] Lindsay and Gartzke, "Coercion through Cyberspace," 17, 25, and 31.

[161] For a review of the literature on the problems of using cyber operations to convey the coercing state's intentions, see Borghard and Lonergan, "Coercion in Cyberspace," 456.

other problems make cyber weapons ill-suited for conveying coercive messaging.[162]

Weak linkages between civilian punishment and leadership decision-making. In explaining why bombings of civilian populations so often fail to coerce state behavior, Pape cites a fundamental problem for all such punishment strategies: inflicting suffering will not necessarily drive the public to rise up and apply pressure on government leaders to yield (or throw them out of office if they fail to do so). On the contrary, "the citizenry of the target state is not likely to turn against its government." Pape adds that "the supposed causal chain—civilian hardship produces public anger which forms political opposition against the government—does not stand up" upon review of the record of multiple coercive campaigns.[163]

The use of coercion to shape crisis decision-making can even produce results that harm the attacker's cause. Pape finds that "punishment generates more public anger against the attacker than against the target government." These boomerang effects are especially likely when attackers seek to drive states to yield in a crisis. The record of such campaigns indicates that "serious international disputes tend to produce a 'rally around the flag effect' which increases support for the government even among groups who tend to oppose government policies in peacetime."[164]

Rather than attempt to generate public pressure on the government to yield, punishment strategies could seek to drive leadership decision-making by creating mass panic and disorder. Again, however, past coercive campaigns have failed to validate this causal mechanism. Lewis argues that the assumption that power blackouts or other service disruptions will produce chaos is "very doubtful." In fact, "Nothing of the kind happened in the aerial attacks of the 1940s or afterwards. Instead, the result was a stiffening of resistance."[165]

IOs as a Supplement for Coercive Cyberattacks

The rise of social media and technologies to exploit it enable China and Russia to greatly enhance the effectiveness of cyber weapons for coercion. Martin Libicki argues that the United States should expect adversaries to combine IOs and cyberattacks "because almost all situations where cyber attacks are useful are also those which offer no good reason not to use other elements of IW [information warfare]."[166] The value proposition for combined information-cyberattacks goes still further. IOs can help adversaries remedy each of the constraints on cyber-driven coercion that would otherwise hobble their effectiveness. Some of these benefits are readily apparent. Others set the analytic agenda of the remainder of the study.

Inflicting Sufficient Suffering

While Borghard and Lonergan (writing in 2017) cast doubt on whether cyber weapons can cause damage to critical infrastructure to drive a victim's behavior, they also caution that as technology evolves, states may come to view coercive cyber operations as more viable. That day has arrived. Although US infrastructure owners and operators are intensifying their efforts to strengthen the resilience of their systems, cyber threats to these systems are increasing as well and may be overtaking US defensive efforts.

The energy sector exemplifies both trends. While serving as the acting director of the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response, Alexander Gates noted in 2020 that electric utilities and their government

[162] Valeriano, "Introduction," 13.

[163] Pape, *Bombing to Win*, 24.

[164] Pape, *Bombing to Win*, 25.

[165] Lewis, *Rethinking Cybersecurity*, 26.

[166] Libicki, "Convergence of Information Warfare," 62.

partners are making great strides in protecting the grid from attack. Yet, "despite all the progress made today, the cyberthreats to the sector are real and outpacing our collective solutions."[167] US Secretary of Energy Jennifer Granholm provided a more dire assessment of the threat in June 2021. When asked whether the nation's adversaries have the capability to shut down the US grid, Granholm replied "Yeah, they do."[168] Defeating coercion will require sustained efforts to reduce the risk of catastrophic attacks, along with measures to maintain the credibility of US response forces and deterrence policies.

But large-scale attacks should not be our only (or even our primary) concern. China and Russia can design IOs to greatly magnify the fear that even limited infrastructure disruptions create. For example, videos delivered via social media to one hundred million Americans, vividly displaying the effects of striking a single city's infrastructure and warning of wider devastation to follow, could enable adversaries to conduct George-style "exemplary" attacks with unprecedented effectiveness. US urban water systems are ideal for such limited attacks because (unlike the grid) those systems are almost never interconnected with others; cyber-induced disruptions of them cannot cause cascading, multicity failures. Using AI, however, China and Russia can plan and conduct narrowly targeted strikes against any infrastructure systems they choose. The National Security Commission on Artificial Intelligence finds that "the expanding application of existing AI cyber capabilities will make cyber attacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyberweapons, and make cyber campaigns more effective on a larger scale."[169]

US opponents may also find exemplary attacks advantageous for reducing the escalatory dangers they face. James Andrew Lewis notes that "truly crippling" attacks on infrastructure would provoke a powerful response from the victim and are therefore unlikely to occur.[170] Subsequent portions of this study examine how China and Russia might use, in combination with their existing doctrines to exploit adversary fears of escalation as a coercive tool, carefully limited attacks to manage those escalatory risks. The study also examines how they can pair exemplary attacks with IOs that maximize their coercive leverage over the American public and White House decision-makers.

Communicating Threats

Attributing attacks will be dead easy in regional crises with China and Russia. While the United States needs to account for the risk of false-flag or covert third-party attacks in such confrontations, the least of our problems will be figuring out who is seeking to coerce US behavior. Arguments that requirements for secrecy impede coercion are similarly misplaced. Information technology (IT) networks are tightly connected to the internet. In the face of adversary threats of attack, many network operators can temporarily sever those connections as a defensive measure. However, adversaries seeking to create blackouts or other disruptive effects will attack operational technology (OT) systems: that is, systems used to manage infrastructure operations, including industrial control systems.

A growing number of infrastructure owners and their software vendors are linking IT and OT networks and thereby creating potential internet-based pathways for attack. Adversaries may worry that if they announce they are on the brink of attacking, network operators will sever IT–OT connections. But temporarily disconnecting from the internet during a crisis will not make OT systems invulnerable. China and Russia are developing a wide array of tactics, techniques, and procedures (TTPs)

[167] Vasquez, "More Money, Power Needed."

[168] Duster, "Adversaries Have Capability of Shutting Down US Power Grid."

[169] NSCAI, *Final Report*, 50–51.

[170] Lewis, *Toward a More Coercive Cyber Strategy*, 12.

to disrupt operational controls that do not depend on delivering malware just before an attack. Both nations conduct operations in peacetime to hide within infrastructure systems advanced persistent threats (APTs) that are extremely difficult to detect, analyze, and eradicate.[171] Adversaries are also seeking to corrupt the supply chains that produce critical US infrastructure components and software. Most notably, the Biden administration has determined that China is "actively planning to undermine the electric power system in the United States" through supply-chain attacks.[172] All such means of attack are ideal for conducting coercive operations.

The assumption that cyberattacks must stay covert also misses a deeper transformation in their uses for coercion. General Edward Cardon, former commander of the US Army Cyber Command, recalls that intelligence professionals have long wanted to keep US cyber capabilities secret. However, as battlefield operators began using cyber weapons in ARES to disrupt ISIS capabilities and shape the organization's behavior, they concluded that the desire for secrecy was misplaced. Intelligence personnel "would say, 'If you do it like that, they'll know it's you!' " Cardon remembers. "I'd just look at them and say, 'Who cares? When I'm using artillery, attack aviation, jets—you think they don't know it's the United States of America?' "[173] The same will be true of attacks to drive US decision-making in a crisis. Beijing and Moscow will eagerly claim credit for the disruptions they create and ensure that the senior officials and the public know what will be required to stave off further punishment.

Credit claiming can also magnify the effectiveness of such operations. US Cyber Command's operations to defend the 2018 midterm elections highlight the potential advantages of openly attacking. Fischerkeller and Harknett (drawing on open-source reporting) note that:

> the United States could have opted to covertly persist in this infrastructure, in a limited intelligence gain posture, to learn about IRA capabilities or intentions and feed that information back to improve U.S. cyber defenses (and perhaps it did so for a period). Instead, it chose to make its presence known. When Russia became aware of a change in security conditions, cost imposition effects created organizational friction within the IRA, and Russia shifted focus and efforts toward defense, both of which served a U.S. objective of taking Russia's focus off of cyber-enabled information operations directed at U.S. elections. Once aware of a U.S. presence, IRA operators likely and hastily sought to reexamine security practices, discern where else the United States might be in IRA infrastructure, and determine what information or capabilities the United States might have ascertained or exfiltrated by leveraging its exploitation.[174]

In addition, IOs can supplement the cognitive impact of infrastructure disruptions and convey explicit warnings that more punishment will follow unless the victim yields. The US armed forces have long combined IOs with conventional bombing to drive adversary behavior. In Operation Desert Storm (1991) and Operation Iraqi Freedom (2003), for example, the United States used leafleting and radio broadcasts to reinforce the impact of kinetic attacks on enemy perceptions.[175] China and Russia can now use drastically updated means to shape US public perceptions in future crises and overcome

[171] CISA, "Alert (AA20-352A)."

[172] DOE, *Notice of Request for Information*, 6; and Trump, *Executive Order on Securing Bulk-Power System*.

[173] Graff, "Man Who Speaks Softly."

[174] Fischerkeller and Harknett, "Persistent Engagement and Cost Imposition."

[175] Jones and Summe, "Psychological Operations," 2–5; DoD, *Conduct of the Persian Gulf War*, 537–538; and Lamb, *Psychological Operations*, 48–51.

the impediments cited by previous studies to using cyberattacks for coercion.

The Causal Links between Punishment and State Behavior

Advances in IO technologies make it essential to reassess how threatened or actual cyberattacks could shape public perceptions and dampen the "rally round the flag" effects that have impeded past coercive campaigns. Chinese and Russian campaigns to corrode the US public's faith in government institutions and in the credibility and competence of US leaders lay the groundwork for such dampening efforts. So can their operations to widen divisions in the United States and fuel partisan hostility. All such efforts can create opportunities for microtargeted IOs to raise doubts about the need to defend US allies, undermine confidence in US leaders (including through the use of deepfake technologies), and inflame fears that US families will soon be deprived of water and power for the sake of Taiwan, Estonia, or some other security partner that many Americans know little about and care for even less.

In addition to understanding how adversaries are preparing the cognitive battlefield for future coercive campaigns, it is also essential to clarify the specific causal mechanisms that Russia and China may seek to exploit to drive US behavior. The *National Counterintelligence Strategy* notes that adversary campaigns are currently underway to "sway public opinion against U.S. Government policies" and build support for adversary agendas.[176] Adversaries can harness those efforts as a means of mobilizing opposition to defending US allies. However, that is only one of multiple pathways of influence that China and Russia can use.

Integrating Direct and Indirect Pathways of Influence: Lessons from OAF

Punishment strategies offer an indirect means of achieving coercive effects. By inflicting sufficient punishment on the opponent's population, attackers hope that suffering will generate public pressure on their leaders to yield in a confrontation. In addition, those leaders may fear that unless they accede to public demands to back down, their ability to effectively govern (or maintain their grip on power) will be increasingly at risk.

Adversaries can pair these indirect means of coercion with another pathway of influence: direct, curated messaging to individual decision-makers and those on whom they rely for advice and political support. The *National Counterintelligence Strategy* emphasizes that adversaries are already conducting campaigns to "influence and deceive key decision makers" in the United States.[177] As in China's hack of security clearance forms maintained by the Office of Personnel Management, ongoing adversary efforts to gather sensitive data on US leaders, military officers, and senior government officials will facilitate personalized IOs to exert leverage over those officials and their families.[178]

OAF provides a case study of how attackers can combine direct and indirect strategies for coercion and seek to achieve synergies between them. In 1999, the United States and its NATO allies paired infrastructure bombings with intensive IOs to coerce Slobodan Milosevic, president of the Federal Republic of Yugoslavia, into pulling Yugoslav forces out of Kosovo. NATO reinforced its campaign by disabling or destroying Yugoslav television infrastructure and other government-controlled sources of public information while also intensively broadcasting the alliance's coercive messaging from a

[176] NCSC, *National Counterintelligence Strategy*, 9; and Herrmann, "Weaponized Narrative and Disinformation."

[177] NCSC, *National Counterintelligence Strategy*, 9.

[178] For more about the OPM hack, see Barrett, "Chinese National Arrested."

"ring around Serbia." US policymakers should prepare for China and Russia to conduct equivalent tactics of selective media disruptions in future crises.

While Milosevic did ultimately withdraw Yugoslav forces from Kosovo, it is impossible to know the extent to which NATO's combined IOs and bombing attacks drove his decision. Other factors may have influenced his retreat, including the loss of Russian political backing for his occupation of Kosovo and NATO's threat of attacking with ground forces if bombing and IOs proved insufficient.[179] Milosevic never said which sources of pressure were most compelling. While a small cottage industry has emerged to sort out these factors, it would require a leap of faith to conclude that OAF's coercive operations were solely responsible for Yugoslavia's retreat from Kosovo.[180] As noted by Samuel Berger, the US national security advisor at the time, "we will never know exactly why Milosevic ultimately capitulated."[181]

Moreover, OAF's value for shaping US defenses against coercion is limited by the starkly different structure of the US policymaking process vis-à-vis that of Yugoslavia. The United States and its NATO partners tailored their combined operations in OAF to reflect and exploit the centralized authority exercised by Milosevic and convince him to withdraw Yugoslav forces from Kosovo. Adversaries seeking to drive US behavior will design their operations to leverage the distinctive features of the US policymaking process. To defeat such tailored campaigns, US analysts will need to "red team" US mechanisms for crisis decision-making, anticipate how adversaries are likely to exploit the vulnerabilities of those mechanisms, and derive US-specific defensive options accordingly.

One further limitation of OAF as a case study lies in the primitive level of coercive technologies that NATO employed compared with those that Beijing and Moscow can wield. Assessments of the coercive threats now confronting the US must account for these technological increases—above all, the ability of social media to give adversaries direct access to US officials, their families, and influencers who shape public perceptions. Nevertheless, OAF highlights how adversaries can use both direct and indirect means of shaping adversary behavior and employ selective media cutoffs to strengthen the impact of coercive messaging.

Operations to Directly Influence Leadership Behavior

Gregory Schulte, who helped design and execute OAF while serving on the National Security Council, notes that coercive campaigns such as OAF seek to redirect enemy decision-making rather than rout the enemy's military through brute force. The prerequisite for doing so requires an "in-depth understanding of the enemy leadership and its worldview and interests." Success so requires "a sound understanding of how the enemy makes and carries out its decisions and which individuals and factors play in that process."[182]

OAF carefully focused its combined operations to shape Milosevic's perceptions of the conflict. Berger recalls that "we knew the power to change Serbia's course was concentrated in Milosevic's hands. And we knew he was not immune to pressure from within."[183] OAF personnel conducted IOs directly

[179] For more on the importance of NATO's threat of a ground forces attack in driving Milosevic's withdrawal from Kosovo, see Byman and Waxman, "Kosovo and the Great Air Power Debate," 7; Pape, "True Worth of Air Power"; Cordesman, *Lessons and Non-Lessons*, 78–79; and Daalder and O'Hanlon, *Winning Ugly*, 214. For more on the importance of the loss of Soviet support for the occupation of Kosovo, see Lambeth, *NATO's Air War for Kosovo*, 69; and Berger, "Winning the Peace in Kosovo."

[180] For the most detailed and compelling assessment of the relative impact of these various sources of coercion, see (especially pp. 68 and 80) Lambeth, *NATO's Air War for Kosovo*, chap. 4; and Berger, "Winning the Peace in Kosovo."

[181] Berger, "Winning the Peace in Kosovo."

[182] Schulte, "Revisiting NATO's Kosovo Air War," 18.

[183] Berger, "Winning the Peace in Kosovo."

against Milosevic. For example, via a "friendly intermediary," the United States shipped him a videotape showing what fuel-air explosives could do to his forces.[184] NATO also bombed his presidential villa and socialist party offices. Most notable: a precision strike against Milosevic's residence left a hole in his bedroom wall.[185] Reports at the time indicated that Milosevic's wife became "increasingly hysterical" as the bombing intensified.[186]

While Milosevic exercised enormous personal control over Yugoslav decision-making, his grip on power depended on the backing of Yugoslavia's economic and political elite, both within the Serbian Socialist Party and beyond. OAF targeted these elites with specialized kinetic/IOs to corrode their support for Milosevic and to help convince him to capitulate. As one senior NATO officer framed this influence effort: Milosevic "doesn't care if his soldiers die in Kosovo, as long as he stays in power. But if you blow up some things near and dear to him—or somebody close to him—then that could have an effect."[187]

Successful efforts to "influence the influencers" outside of the top leadership team depend on careful mapping of a nation's power structure. The most comprehensive assessment of NATO's campaign against Milosevic's "cronies," a report published by the US Air Force's Air University, found that the campaign appeared to be based on detailed intelligence work that resulted in an influence diagram of Milosevic's power structure. Planners then used that analysis to guide influence operations.[188]

These operations combined IOs with bombings of the factories and other assets owned by Milosevic's closest allies within the regime. In Yugoslavia's state-run economy, virtually every industry and economic activity was tied to Milosevic's government. Milosevic also used funds from crony-owned businesses and factories to finance the security forces that helped him maintain control of the country.[189] OAF systematically bombed these factories to exert pressure on Milosevic. The night before specific facilities were attacked, factory owners were reportedly contacted via cell phone with a warning that their assets would be destroyed within twenty-four hours and that further destruction of such businesses in Yugoslavia would follow unless Milosevic capitulated.[190]

Current and future US presidents will rely on entirely different mechanisms to guide their decision-making and maintain domestic political support. Moreover, it is difficult (though not impossible) to imagine how China and Russia could conduct effective coercive attacks against the president's major campaign donors or other "crony equivalents." In the IO realm, however, it seems likely that these nations will seek to target the social media feeds of the president's advisors and those who support them to shape crisis policy options. US defensive strategies against coercion should include counterinfluence measures to protect the US decision-making process. Such measures should be akin to (and borrowing best practices from) threat-informed counterintelligence strategies and operations.

Indirect Influence and Strategies of Selective Cutoff of Communications

OAF illuminates an additional pathway of coercion: the use of bombings and IOs to convince an adversary's population that it faces intolerable suffering so that it will then pressure its leaders to back down in a confrontation and, perhaps, even throw

[184] Lambeth, *NATO's Air War for Kosovo*, 71.

[185] Schulte, "Deterring Attack," 85.

[186] Lambeth, *NATO's Air War for Kosovo*, 71.

[187] Schmitt and Myers, "Crisis in the Balkans."

[188] Tolbert, "Crony Attack," 32. For more on the focus and structure of IOs against Milosevic's cronies, see also Lambeth, *NATO's Air War for Kosovo*, 71.

[189] Schmitt and Myers, "Crisis in the Balkans."

[190] Barry, "NATO's Game of Chicken"; Tolbert, "Crony Attack," 31–36; and Arkin, "Ask Not for Whom the Phone Rings."

its leaders out of power if they fail to capitulate. Other nations have long employed such indirect strategies of coercion. However, OAF applied some novel communications tactics to shape the Yugoslav public's beliefs and perceptions—tactics that are ripe for updating in the information age.

Previous efforts at using IOs to drive an opposing population's behavior have often failed. The Vietnam War offers a case in point. The United States dropped billions of propaganda leaflets in North Vietnam to supplement its bombing of infrastructure and other targets. The leaflets urged the Vietcong to desert, defect, or surrender and sought to intensify pressure on North Vietnamese leaders to sign a cease-fire that would halt US bombings as part of a broader effort to achieve US negotiating objectives.[191] After-action reviews by the Air Force found that these IOs were ineffective.[192] Indeed, while air-dropped leaflets saturated North Vietnam, many of them "were promptly used as toilet paper."[193]

Operation Desert Storm provides a more recent example of failure. In 1991, US military planners designed their bombing campaign against Iraqi infrastructure to incite Iraqi public opinion against the occupation of Kuwait and—ideally—incite Iraqi citizens to rise up against President Saddam Hussein. Planners viewed blacking out the Iraqi power grid as an especially important means to influence Iraqi public perceptions as well as to disrupt electricity-dependent military infrastructure. Lieutenant General Charles Horner (US Air Force), who had overall command of the air campaign, said that destroying the grid would give the US extraordinary leverage over the Iraqi government and would provide the psychological "side benefit" of having the lights go out on ordinary Iraqi citizens.[194] The United States also used intensive IOs against Iraqi citizens and troops to magnify the bombing campaign's psychological effects and strengthen opposition to Hussein.[195] But no popular uprising occurred until after US forces annihilated the Iraqi military and—temporarily—weakened Hussein's ability to clamp down on Kurds, Shia Arabs, and other ethnic and religious minorities that had long opposed his rule. The preceding US bombing campaign had failed to generate such a revolt or create sufficient domestic pressure on Hussein to withdraw from Kuwait.[196]

OAF *may* offer a more successful case study of indirect influence. As with OAF efforts to directly shape Milosevic's behavior, it impossible to know how much (if at all) he cared about the Yugoslav public's shift in perspectives on the occupation of Kosovo. His centralized control over Yugoslavia was well defended by the State Security Service, the Interior Ministry, and other agencies that protected him against domestic opposition or popular uprisings.[197]

[191] Thompson, *To Hanoi and Back*; and Hosmer, "Information Revolution," 221–222.

[192] Barger, "Psychological Operations Supporting Counterinsurgency," 4; and Thompson, *To Hanoi and Back*, 251.

[193] Singer and Brooking, *LikeWar*, 18.

[194] The long-term leverage the United States sought in striking twenty-eight grid targets included not only the weakening of the Iraqi economy and the disruption of the flow of power to Iraqi military facilities and infrastructure, but also the implicit bargain that if Hussein withdrew from Kuwait, the United States would help repair the grid. Gellman, "Allied War Struck Broadly in Iraq."

[195] Jones and Summe, "Psychological Operations," 2–5; and DoD, *Conduct of the Persian Gulf War*, 537–538.

[196] Pape, *Bombing to Win*, 27. The bombing campaign also failed in its goal of encouraging Iraqi generals to abandon the fight against the United States before ground operations commenced. The Iraqi army withstood a six-week bombing campaign by US-led coalition forces. Yet, when the coalition ground offensive began, the Iraqi army effectively folded within a day, and the coalition liberated Kuwait in four days. See History.com Editors, "Gulf War Ground Offensive Begins." However, as will be discussed later in this section, US psychological operations against Iraqi forces achieved significant success in terms of encouraging desertions and surrender.

[197] Milosevic controlled one hundred thousand internal police and paramilitary troops affiliated with the Interior Ministry (MUP) and the State Security Service (RDB). See Loeb, "Yugo-

But public perceptions did indeed change. When OAF bombings began, citizens in Belgrade responded by attending outdoor rock concerts and wearing T-shirts featuring bull's-eyes and the word "target."[198] Influence operations targeted those citizens via other means. OAF planners specifically crafted their messaging to the Yugoslav public to magnify the psychological effects of infrastructure bombings. Attacks on the power grid exemplify this combined strategy. As Benjamin Lambeth notes in his comprehensive history of OAF, NATO forces began striking the Yugoslav electric systems with carbon/graphite thread-dispensing munitions. While those attacks produced only short-term blackouts, they "brought the war, for the first time, directly to the Serbian people."[199]

NATO then ramped up its disruption of the grid and combined those attacks with IOs warning of further punishment to come. An OAF follow-up strike cut electric service to 70 percent of the population. Conventional bombing also intensified against other civilian infrastructure systems and major factories, confronting the public with widespread hardships and job losses.[200] OAF paired this punishing bombardment with leafleting that asked, "How long will you suffer for Milosevic?"[201] The outdoor rock concerts in support of Milosevic ceased. Instead, as Berger recalls, "the initial public mood in Serbia—defiant support for Milosevic's stance—turned sour as the impact of our efforts came home."[202]

One contributor to that success could also bolster coercive campaigns against the United States. OAF strengthened the effectiveness of its IOs by surrounding the Yugoslav public with NATO-provided messaging to generate pressure against Milosevic's polices while also selectively cutting off the public's access to the media he controlled. The first component of this one-two punch was provided by the "ring around Serbia." NATO established multiple radio transmitters in neighboring countries that transmitted OAF-approved messaging. Combined with leafleting by B-52 bombers, broadcasts by Command Solo aircraft, and other IO measures, NATO planners structured the ring to "break Milosevic's monopoly of the airwaves."[203]

The second component entailed disrupting Milosevic's own means of communicating to his public and countering NATO's messaging. Most important, NATO struck TV stations owned by Milosevic's daughter and political cronies in the Serbian Socialist Party, entirely cutting off citizens' access to government-controlled transmissions in some cities. At the same time, NATO leafleted Yugoslavia to advertise the radio and TV stations on which the public could hear NATO-supplied information and tailored alliance messaging to support OAF's broader influence campaign.[204]

Such efforts to control the messaging available to the enemy's population constitute a strategy of the *selective cutoff* of information to the public: attackers disable the mass media and other communications systems that the government relies on to communicate with its citizens, while leveraging communications systems the attacker owns, to corrode the public's support of their government and its policies.

OAF also used selective media cutoffs to enhance the effectiveness of direct influence operations against Milosevic and the core supporters of his

slav Military Is Formidable Foe"; and Watson, "Yugoslav Opposition Works to Gain Support."

[198] Tolbert, "Crony Attack," 33.

[199] Lambeth, *NATO's Air War for Kosovo*, 40–41.

[200] NATO's multiyear economic sanctions to pressure Milosevic inflicted further damage on the Yugoslav economy. See Lambeth, *NATO's Air War for Kosovo*, 41–42.

[201] Hosmer, *Conflict over Kosovo*, 72.

[202] Berger, "Winning the Peace in Kosovo."

[203] Schulte, "Revisiting NATO's Kosovo Air War," 16.

[204] OAF left selected government-controlled media on the air in some regions, including those served by the main state network, Radio and Television of Serbia. See Erlanger, "Crisis in the Balkans."

regime. Even as aerial attacks destroyed Yugoslavia's television transmission system, the air campaign carefully avoided damaging the country's cellular phone networks (including the main switching stations in Serbia). Doing so enabled cell-based IOs against Milosevic's cronies to go forward unimpeded.[205]

US adversaries may selectively cut off communications systems to help achieve their coercive goals in future crises. In particular, attackers could allow the survival of those US social media platforms or other systems they were using to convey disinformation or IO efforts while disrupting other systems that they do not "own." Doing so could help them flood the systems that survive with coercive messaging while denying access to government-provided information. The Defeating Customized Attacks section examines these risks of selective interruption in greater detail, both for "hardened" leadership networks and for systems to communicate with the public, and suggests possible US countermeasures.

Coercing US Security Partners

Secretary Austin's characterization of US allies and security partners as "force multipliers" only begins to capture their importance for defeating China and Russia in regional confrontations. The US *National Defense Strategy* notes that the partners "provide complementary capabilities and forces along with unique perspectives, regional relationships, and information that improve our understanding of the environment and expand our options. Allies and partners also provide access to critical regions, supporting a widespread basing and logistics system that underpins the Department's global reach."[206] During regional crises, US dependence on these partners will make them prime targets for coercion designed to weaken allied cohesion against Chinese or Russian demands and discourage support for coalition defense operations.

Beijing and Moscow can employ the same coercive strategies against US partners that they will employ against the United States itself, including the threatened or actual punishment of allied populations and direct, leadership-focused messaging. But these counter-alliance campaigns may also pose distinctive challenges and will require specialized defensive countermeasures. Beijing and Moscow can focus their messaging to exploit the inherent tensions surrounding collective defense. In particular, they may use modern IO technology to reinforce decades-old doubts over whether the president will sacrifice US cities to defend those of America's allies.

Adversaries may also use hybrid warfare techniques to delay and disrupt alliance decision-making. Russia's attacks on Ukraine illuminate how hybrid techniques might be used (in significantly modified forms) against NATO in future crises. China may revamp some of these techniques against US partnerships in Asia as well.

In addition, using much more destructive combined attacks, adversaries could seek to achieve coercion by denial by convincing US and allied leaders that their regional war plans are doomed to fail. Managing the escalatory risks of such attacks would be enormously difficult. Nevertheless, understanding how coercion by denial is supposed to function and how China and Russia might employ it should become part of overall US regional contingency planning.

Punishment Strategies for Alliance Disruption

Austin and Secretary of State Antony Blinken note that "as countries in the region and beyond know, China in particular is all too willing to use coercion to get its way."[207] Russian pressure on Ukraine and

[205] Arkin, "Ask Not for Whom the Phone Rings."

[206] DoD, *National Defense Strategy*, 9.

[207] Blinken and Austin, "America's Partnerships Are 'Force Multipliers.' "

other nations on its periphery is similarly unrelenting. Longer-term IO campaigns are also underway to undermine the foundations of US defense partnerships and weaken the credibility of US regional security commitments. At the broadest level of global messaging, the Department of Homeland Security (DHS) assesses that Moscow is using IOs to "increase its global standing and influence by weakening America—domestically and abroad—through efforts to sow discord, distract, shape public sentiment, and undermine trust in Western democratic institutions and processes."[208]

NATO is an especially prominent focus of such messaging. A study team appointed by NATO's secretary general reported in November 2020 that "the last ten years have been characterised by questions about the commitment of the United States to the defence of the European continent" and other threats to alliance cohesion.[209] Disinformation campaigns aimed at NATO and individual allies have intensified these concerns.[210] Russia also customizes IOs against NATO members to promote specific narratives that undermine defensive preparations.[211] Most recently, for example, Moscow has been conducting deceptive messaging to disrupt planning and force realignments for the Enhanced Forward Presence initiative along NATO's eastern flank, launched in part in response to Russia's invasion of Ukraine and its continuing threats against other central European countries.[212]

Adversaries can also use IOs to widen and exploit differences between US and allied interests. In Southeast Asia, for example, US security priorities go far beyond the protection of specific US partners. Indeed, building defense relationships with those partners serves US global objectives. US Pacific Command notes that "Sea lanes though the region carry the life's blood of world prosperity and must remain open."[213] But IOs could test the willingness of Southeast Asian leaders to put their own citizens at risk to defend Washington's global objectives—and, more generally, to align with the United States against China in an emerging confrontation. Singapore Prime Minister Lee Hsien Loong states that the US–China competition in Asia presents regional nations with "profound" questions. "Asian countries see the United States as a resident power that has vital interests in the region. At the same time, China is a reality on the doorstep. Asian countries do not want to be forced to choose between the two."[214] In future regional crises, China is likely to conduct IOs against Lee Hsien Loong, his influential allies in the container shipping business, and other targets that exploit China's doorstep position and threaten Singapore with punishment for aligning with the United States.

Such crisis-focused IOs will not only take advantage of ongoing Chinese and Russian campaigns to widen divisions between the United States and its partners but also exploit inherent dilemmas for collective defense. Since early in the Cold War, Russia has sought to convince European nations that they cannot rely on the United States to come to their aid in future conflicts. That argument capitalizes on a fundamental problem for extended deterrence and many other security guarantees: American leaders will never "trade" New York for London or Paris and incur massive devastation on US territory for the sake of allied defense. Rebecca Friedman Lissner argues that "in the present climate, a similar question could be asked about the costs the United States is willing to incur for Tallinn or Riga."[215] That question will be especially pertinent if Russian IOs intensify US fears of being punished for protecting security partners and reinforce partner doubts

[208] DHS, *Homeland Threat Assessment*, 10.

[209] Reflection Group, *NATO 2030*.

[210] Reflection Group, *NATO 2030*, 20 and 46.

[211] Giles, *Handbook of Russian Information Warfare*, 22.

[212] Bugajski, *Why Does Moscow?*

[213] Garamone, "Free, Open Indo-Pacific."

[214] Loong, "Endangered Asian Century."

[215] Friedman Lissner, "Preventing a Credibility Crisis."

that US leaders will invite such punishment on their behalf.

Equivalent problems exist in Asia. Admiral Lee Hsi-ming, former chief of the General Staff of Taiwan's armed forces, has stated that Taiwanese defense against Chinese attack depends on the United States intervening on Taiwan's behalf. But he asks: "What reason is there to believe that the United States will sacrifice the lives of its own children to defend Taiwan?"[216] In future crises, Beijing can customize IOs against the Taiwanese public, elected officials, and senior military officers to reinforce their doubts as to whether they can count on US assistance.

IOs can foster uncertainties in the other direction as well and raise US officials' suspicions that their foreign partners will bail when crunch time comes. Given the dependence of the United States on regional partners for military basing, logistic support, and combat forces, China and Russia may use threats of punishment to discourage those partners from making good on their own defense commitments. US strategies against coercion must prevent such IOs from creating a spiral of mutually reinforcing suspicions between US and allied leaders and account for the risk that adversaries will use sophisticated impersonation and deepfake technologies to confuse alliance decision-making. Russia and China may also design their IOs to exploit specific vulnerabilities in alliance coordination mechanisms, including those employed by NATO to authorize collective defense under Article 5 of the alliance's founding treaty. The Defeating Customized Attacks section of this report provides a detailed assessment of these threats and options to counter them.

Russian Hybrid Warfare: A Proving Ground for New Coercive Tactics and Technologies

If China and Russia cannot disrupt US–allied defense cooperation through IOs alone, they may (at much greater risk to themselves) escalate to combined information-cyberattacks. Russia's hybrid warfare campaigns against Georgia in 2008 and Ukraine in 2014 and 2016 help illuminate how Moscow, and perhaps Beijing, may conduct such combined operations in future confrontations. The use of cyber weapons to inflict blackouts on Ukraine exemplifies how US adversaries can move beyond IO-only campaigns to punishment. However, from an alliance perspective, the most valuable lessons lie in Russia's use of deceptive IOs and specialized hybrid tactics to delay and confuse decision-making by Ukraine's leaders and their potential supporters in the West.

As with OAF, a few qualifiers are in order before using the attacks on Ukraine to help guide the development of defensive strategies against combined information-cyberattacks. One problem lies in defining hybrid warfare. Russia does not use the term hybrid warfare to refer to its own operations against Ukraine. Drawing on the most comprehensive US military study on Russian hybrid tactics, *Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014*, this study defines hybrid warfare as the integrated use of irregular forces, cyberattacks, IOs, and other unconventional warfare tactics.[217] Such operations have deep historical roots. In the IO realm, hybrid warfare draws on long-standing Soviet and Russian practices of *maskirovka* and emphasizes the value of ambiguity for confusing and delaying decision-making by Russia's opponents.[218] But

[216] Lee, Lague, and Blanchard, "China Launches 'Gray-Zone' Warfare," 13.

[217] On the definitions and characteristics of hybrid warfare and Russian "unconventional operations," see USASOC, *Little Green Men*, 2–6. In Russian writing, this term is more frequently used to describe *US* military doctrine, rather than Russia's own. See Adamsky, *Cross-Domain Coercion*, 9.

[218] Johnson, *Russia's Approach to Conflict*, 1–2 and 6–8. This study's section on Chinese and Russian doctrine examines the

pairing these IOs with disruptive cyberattacks constitutes the new frontier of coercion.

A key limitation in using Ukraine as a case study is that many of Russia's hybrid tactics could never be effectively employed against the US or many of its security partners. For example, in conducting IOs against Ukraine, the Kremlin targeted Russian-speaking populations in that country and exploited their reliance on Russian-owned media, including propaganda outlets such as Sputnik and RT and the social media platform VK (VKontakte).[219] The Baltic states may be vulnerable to such tactics. Native Chinese speakers in East Asia could provide equivalent IO targets for Beijing. However, no equivalent linguistic and ethnic opportunities for exploitation exist in the United States or many of its other security partners.

Chances are equally remote that Russia or China will flood the United States with irregular forces. In hybrid operations against Ukraine, little green men played a critical role in seizing Crimean territory and critical infrastructure nodes while still enabling Russia to deny responsibility for the attacks. No equivalent threat exists to the United States or its partners that are geographically removed from Russia and China.

On a more limited and selectively targeted basis, however, adversaries might seek to use irregular forces and kinetic weapons to disrupt US and allied infrastructure. Operators of American nuclear power plants, electric utilities, and other infrastructure take very seriously the risk that spetsnaz-style units could strike their critical facilities with kinetic weapons in selective, targeted ways. Spurred by the attack against California's Metcalf electricity substation in 2013, regulators now require bulk power system entities to meet mandatory standards for physical protection of their critical assets (as do nuclear power plants).[220] Utilities and their government partners have also developed and regularly exercise plans to defend their systems against integrated physical and cyberattacks.[221]

Future plans and exercises should account for the risk that cyber and kinetic attacks will include IOs as well. For example, to discourage utility CEOs from sending cyber response personnel to assist stricken systems in other regions, adversaries could warn those utilities that they will be attacked next. The electric industry's Cyber Mutual Assistance system should begin to build preparedness against such coercive messaging. [222]

More immediately applicable lessons from hybrid operations against Ukraine can also help shape US and allied preparedness initiatives. The measures Russia took to delay and confuse decision-making in Kiev and the West go beyond strategies of coercion through punishment. Nevertheless, as part of broader allied efforts to protect allied cohesion as adversaries transition to combined information-cyberattacks, strengthening preparedness against those hybrid tactics will be vital. And while cyber-induced blackouts failed to weaken Ukraine's resolve to defend its territory, the way Russia designed its cyberattacks to achieve psychological effects can help policymakers anticipate much more sophisticated and disruptive operations to come.

place of hybrid warfare in the broader context of Russian military thinking.

[219] US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault*, 65.

[220] Unknown assailants opened fire on the Metcalf electric substation in San Jose, California, in 2013. The attack knocked seventeen of Metcalf's twenty-three transformers out of operation. See Onishi and Wald, "Sniper Attack Still a Mystery." To mitigate such risks, the electric industry has developed mandatory physical security standards and a design basis threat for utilities to use when designing physical protections and mitigations. See NERC, *CIP-014-2—Physical Security*; and E-ISAC, *E-ISAC End of the Year Report 2016*, 7.

[221] See, e.g., NERC, *GridEx V*.

[222] ESCC, "ESCC's Cyber Mutual Assistance Program."

Disrupting Allied Decision-Making

Many of the techniques that Russia used to impede Ukraine's ability to establish situational awareness, as well as the other deceptive measures the Russians employed, reflected Moscow's efforts to improve on previous operations. In the 1991 Lithuanian conflict, for example, Russian operatives used propaganda and organized protests in that country to turn public sentiment against the government, and they seized communications infrastructure once they finally invaded.[223] As the Russians moved from covert to overt military tactics in Lithuania, they learned another important lesson that further influenced Russian military thinking: "large-scale conventional operations against sovereign states would invite unwanted scrutiny, international pressure, and domestic protest within Russia. To maintain their control over states on the periphery, they would have to employ power in a more clandestine, deniable fashion."[224]

Subsequent Russian attacks have drawn on these lessons and have continued to refine hybrid TTPs for delaying and disrupting response operations. Indeed, a recent US Senate report concluded that Russia is using eastern Europe as a "laboratory" to develop, test, and refine new ways of using IOs and force below the level of open warfare.[225]

These experiments began in earnest in Russia's hybrid war on Georgia. Russia conducted IOs with cyberattacks on communications systems and other targets to impede the Georgian government's ability to react, respond, and communicate.[226] The Kremlin also designed these operations to shape Western responses to the invasion. Russia used IOs on an unprecedented scale to convince the region and international community (including nations that might come to Georgia's assistance) that Georgia and Mikheil Saakashvili, its president, were the aggressors; that Russia was compelled to defend its citizens; and that neither the United States nor its Western allies had any basis for criticizing Russia because of similar actions these nations had taken in other areas of the world, most notably in Kosovo.[227] Moscow also used television broadcasts at home and in the region to highlight the alleged atrocities the Georgians were committing.[228]

Russia's combined cyber operations and IOs ultimately failed to achieve their intended effects on Georgia's leadership. Based on interviews with Georgian military officers and defense officials, US Army captain (now major) Sarah White found that while cyberattacks added a layer of chaos to Georgia's response to the invasion, they did not affect military decision-making about the crisis in any significant way.[229] This limited impact reflected the relatively weak capabilities that Russia brought to bear. Russia's cyberattacks were executed primarily by its "patriotic hacker community" and other government-inspired third parties rather than by more capable cyber forces within the military.[230] Had the Kremlin chosen to employ those forces, it could have inflicted much longer and more pervasive disruptions of Georgian infrastructure and—potentially—exerted greater coercive pressure on Georgia's leaders.[231]

Russian IOs were also ineffective in achieving their goals in NATO and beyond. While the international community did little to assist Georgia during the conflict apart from diplomatic efforts and humanitarian aid, other factors beyond Russia's

[223] USASOC, *Little Green Men*, 9.

[224] USASOC, *Little Green Men*, 10.

[225] Ukraine, in particular, "seems to have emerged as Russia's favorite laboratory for all forms of hybrid war." See US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault*, 62.

[226] White, *Lessons from the Russia-Georgia War*, 1–2.

[227] Iasiello, "Russia's Improved Information Operations," 53.

[228] USASOC, *Little Green Men*, 14.

[229] White, *Lessons from the Russia-Georgia War*, 1.

[230] White, *Lessons from the Russia-Georgia War*, 6–7.

[231] Bumgarner and Borg, *Cyber Campaign against Georgia*.

IOs contributed to that inaction.[232] However, as the Russian military assessed the shortfalls of its IO campaign and the implications for future conflicts, it adopted changes in planning and capabilities that proved enormously effective when Russia seized Crimea in 2014.[233]

Russia's occupation of Crimea and support for separatists in the Donbass region of eastern Ukraine marked significant steps forward in the sophistication of combined attacks. One improvement was in the sequencing of cyber operations. In contrast to the attack on Georgia, in which cyberwarfare began when Russian military forces moved in, cyberattacks against Crimea shut down telecommunications infrastructure, disabled major Ukrainian websites, and jammed the mobile phones of key Ukrainian officials before Russian forces entered the peninsula on March 2, 2014, thereby delaying and disrupting government officials' ability to respond to the invasion.[234]

Russia also conducted more sophisticated IOs to disrupt Ukraine's decision-making and discourage Western assistance. NATO's analysis of Russia's Crimea operations notes that "Russia was prepared to conduct a new form of warfare in Ukraine where an information campaign played a central role."[235] Throughout the campaigns in Crimea and the Donbass region, Russian IOs sought to convince Ukraine and its potential allies that no Russian troops were engaged in the conflict while also highlighting their military capabilities (including for conducting nuclear strikes) if the West pushed too far in resisting the operations. The *Little Green Men* study captures the goals and design of these IOs:

> The coordinated information warfare campaign was carefully crafted to modify the messaging to the West. In Russian media outlets aimed at American and European audiences, the themes were changed slightly to tout the essential "democracy" of Russia's actions in Ukraine. Everything came about because of the "people's choice," and Russia simply acted in accordance with local wishes. Other messaging targeted the pacifist sectors of the West by both threatening war and simultaneously assuring the world that Russia wanted peace. If Moscow fell short of convincing the more cynical critical thinkers in the West, it nevertheless persisted in reiterating its themes of justifiable intervention.[236]

These efforts to generate uncertainty and ambiguity in Ukraine, "which were aimed at blocking the counteraction," were critical to Russia's territorial gains.[237] They helped soften the response to Russian involvement in eastern Ukraine by portraying the conflict as a grassroots separatist movement vying for freedom.[238] The IO campaign also helped conceal Russia's actual objectives, allowed Russia to deny its involvement, and created new opportunities to shape the conflict in ways that enabled Russia to achieve its strategic objectives.[239]

More broadly, the invasion of Crimea provided a real-world, "proof of concept" operation to

[232] One notable exception: the governments of Poland and Estonia provided assistance to help the Georgian government get back online, with the Estonians sharing experiences form the attack on their cyber infrastructure the year before. US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault*, 74; and Pruitt, "Five-Day War."

[233] Iasiello, "Russia's Improved Information Operations," 54.

[234] Iasiello, "Russia's Improved Information Operations," 54.

[235] Lange-Ionatamišvili, *Russia's Information Campaign against Ukraine*, 4.

[236] USASOC, *Little Green Men*, 48. Russia also conducted IOs to indoctrinate ethnic Russians in Ukraine and garner domestic support for the operation within Russia. The section on customizing coercion against America examines US opportunities to disrupt such domestic messaging and provide a counternarrative to the adversary's population.

[237] Botye, "Social-Media Technology, Tactics, and Narratives," 93, quoting Pocheptsov, "First Cognitive War."

[238] USASOC, *Little Green Men*, 58.

[239] Snegovaya, *Putin's Information Warfare in Ukraine*, 8.

apply and reinforce Russia's ongoing shift toward information-centric warfare. As Keir Giles concludes, the Russian military places IOs at the core of that operation "not just to give them a strategic narrative to try to justify what they did, but [also] to use information to deceive, delay and disrupt, like a smokescreen."[240] The Crimean invasion also demonstrated how adversaries can pair IOs with cyberattacks on communications infrastructure to further disrupt their victim's coordination of response operations and shape the data available to potential allies.[241]

These disruptive measures could give Russia or China significant tactical advantages in transitioning from peacetime crises to (ambiguous) conflict and help them tilt alliance calculations of the costs and benefits of intervening. US Army Lieutenant General Eric Wesley notes that creating "ambiguity in the battlefield" can help prevent the West from acting until its adversaries have seized their objectives, deployed additional defenses, and dug in. Wesley also states that such a "fait accompli attack" can greatly increase the costs of Western intervention. He urges that rather than having to retake the contested territory by "mobilizing from the continental United States . . . to engage in protracted conflict," the United States and its allies need the ability to deter and defeat such tactics.[242] Overcoming deceptive IOs and other measures to deepen the ambiguities of the battlefield (including cyberattacks on allied communications infrastructure, surveillance and reconnaissance systems as well as command and control networks) will be essential for such progress.

Inflicting Punishment: Ukraine as a Test Drive

If threats of punishment fail to discourage the United States and its allies from coming to the defense of a stricken partner, Beijing and Moscow may follow through by combining IOs with exemplary cyberattacks against allied infrastructure or (taking an even more dangerous escalatory jump) may conduct large-scale strikes against those targets to maximize civilian suffering.

Developing allied strategies against such coercive campaigns will depend in part on conjecture. While Chinese and Russian military doctrine provides indications of how those nations will conduct combined information-cyberattacks, the US government has yet to officially attribute such an operation to Beijing.[243] Russia has done so, most extensively in its hybrid wars against Ukraine. Those wars illustrate threat vectors that adversaries can use to conduct both exemplary and larger-scale coercive strikes but also fall short of providing a road map sufficient to guide US and allied preparedness efforts.

Russia's use of cyberattacks to inflict outages on Ukraine's electric distribution system in 2015 was a watershed in the cyber era. For the first time, cyber weapons caused large-scale disruptions of civilian infrastructure. Russia's follow-up attack in 2016 created blackouts by striking Ukraine's high-voltage transmission grid, which delivers power to distribution systems.

The 2015 blackout lasted only four hours. Nevertheless, Russia employed TTPs that could create much greater disruption in future coercive campaigns. First, attackers used the grid's own automation and operator tools and technologies to disrupt electric service. After gaining remote access to the utility control networks, attackers hijacked

[240] Giles, *Handbook of Russian Information Warfare*, 46, quoting Defence Committee, "Oral Evidence: Russia."

[241] Johnson, *Russia's Approach to Conflict*, 10.

[242] Freedberg, "Fog of Information War."

[243] Press accounts have indicated that China inflicted blackouts on Mumbai, India's power grid in October 2020 but that evidence is inconclusive. Cunningham, "Was China behind Last October's Power Outage?"

human–machine interfaces to operate over fifty distribution substations, halting electric service to more than 225,000 customers.[244]

In addition, attackers used destructive malware and malicious firmware updates to wipe hard drives of operator workstations and servers. They also disrupted critical field communications devices, operating system components, and communications devices.[245] Utility personnel used manual operations to restore power in less than four hours. However, some of the stricken utilities needed a year to fully recover from these attacks and restore their ability to operate the grid with supervisory control and data acquisition (SCADA) systems. As they battled to regain the integrity of the operational cyber assets compromised by the attack, they also needed to employ conservative operations and relied on cross-region manual control to maintain the grid's reliability.[246] American utilities are developing "spare tire" fallback OT systems to help them sustain operations when SCADA systems are degraded. However, as digitization of the grid accelerates and personnel familiar with manual operations retire, the United States may not be able to rely on manual restoration in the way that limited the impact of Russia's attacks on Ukraine.[247]

The Kremlin designed the follow-on attack in 2016 to physically damage Ukraine's transmission system and test TTPs that could create long-duration, wide-area blackouts in future conflicts. Russia used CRASHOVERRIDE malware to map and mis-operate a transmission-level substation in Kiev.[248] In addition, the CRASHOVERRIDE attack was designed to secretly deny the ability of grid protection systems to effectively function and thus allow power surges to potentially damage transformers and other critical grid equipment.[249] Taken together, the disabling of protection systems and the mis-operation of the grid could create equipment damage that would require many weeks of repair and replacement operations and—potentially—produce catastrophic effects on electricity-dependent water systems, hospitals, and other lifeline infrastructure.

The 2016 attack also revealed a further challenge for defense against future attacks. Instead of requiring the attackers to retain covert access to their victims' systems and use remote operators to disrupt the grid, the malware in the 2016 event interfaced with the substation equipment via specific protocols and was capable of directly issuing commands to grid devices. These TTPs maneuvered around the difficulties that attackers would otherwise face in creating outages.[250]

The Russian operatives made technical mistakes in launching the 2016 attack, and, as a result, the outage lasted a little over an hour (though the temporary loss of load from striking a single transmission substation was greater than the total load impact from the disruption of fifty distribution systems in 2015).[251] Russia no doubt learned from its mistake. As with the malware and threat vectors used in the 2015 blackout, we can expect Russia to continue to upgrade its ability to employ the TTPs used in 2016

[244] SANS ICS and E-ISAC, *Attack on the Ukrainian Power Grid*, 2. This analysis of the 2015 and 2016 attacks and their implications for the United States greatly benefited from insights shared by Tim Conway and Rob Lee.

[245] Bochman and Freeman, *Countering Cyber Sabotage*, 200–201.

[246] SANS ICS and E-ISAC, *Attack on the Ukrainian Power Grid*, 2.

[247] King, "Automation May Hamper Grid Recovery."

[248] ICS-CERT, "Alert (ICS-ALERT-17-206-01): CRASHOVERRIDE Malware"; ICS-CERT, "Alert (TA17-163A): CrashOverride Malware"; Dragos, Inc., *CRASHOVERRIDE*, 8; and DSB, *Task Force on Cyber Deterrence*, 4. On Russia's additional use of BlackEnergy and NotPetya against Ukraine, see Cerulus, "How Ukraine Became a Test Bed."

[249] Dragos, Inc., *CRASHOVERRIDE*.

[250] Bochman and Freeman, *Countering Cyber Sabotage*.

[251] Data provided by Rob Lee, Dragos.

and develop new and increasingly effective means of attacking OT systems.

Adversaries may target both distribution and transmission systems in future coercive campaigns as well. For exemplary attacks, strikes targeted against specific power feeds and substations that distribute electricity to a city's water system or other critical facilities could offer narrow-focused opportunities to seek coercive leverage. Strikes on transmission systems are better suited to creating wide-era outages aimed at jeopardizing US and allied public safety on a greater scale or for longer durations if equipment damage is pursued.

The most immediate requirement for preparedness against such attacks is to ensure that power grids and other infrastructure (including natural gas systems) are secured against the threat vectors Russia used in 2015 and 2016. Many system operators have been doing so while also undertaking broader resilience efforts to meet future threats. Such efforts include measures to improve visibility over OT networks and remedy other security shortfalls revealed by the SolarWinds compromise and other recent attacks.[252]

These forward-looking initiatives are essential. Russia and China are almost certainly holding their most potent cyber weapons in reserve for use in a conflict involving the United States. These nations may also exploit threat vectors entirely different from those used against Ukraine. For example, adversaries may seek to access large numbers of smart meters and cause a widespread blackout by switching smart meter loads on and off repeatedly.[253] They may also seek to corrupt various stages of critical equipment supply chains for the electric sector and interdependent sectors (including telecommunications and natural gas systems) and then use that equipment to create outages for either a carefully targeted or large-scale impact.[254]

Rather than reveal those weapons and enable the United States and its allies to develop countermeasures against them, we will likely see at least some malware for the very first time when an attack occurs. Preparing against the unknown will require far-reaching intelligence operations to identify emerging or potential threats. Dedicated OT strategies to integrate prevention, detection, and response operations will also be essential. In addition, we need to ensure that if infrastructure disruptions occur, alliances can counter IOs aimed at magnifying public fears and discouraging collective defense operations.

Ukraine's experience offers useful insights to help guide such efforts. A NATO study—*Hybrid Warfare against Critical Energy Infrastructure: The Case of Ukraine*—stresses that the destruction of grid infrastructure "was not the final goal" of Russia's attacks. Their purpose "was to achieve the larger goals of economic and political weakening of the country and the formation of a predisposition to surrender to the aggressor."[255]

The Kremlin failed to achieve that objective. Ukraine's leadership continues to resist Russian-supported insurgencies in the Donbass and other contested regions and remains politically aligned with the West.[256] Russia's attacks do, however, offer a framework for assessing how

[252] Zetter, "SolarWinds Hack Infected Critical Infrastructure."

[253] GAO, *Electricity Grid Cybersecurity*, 18–20; Gurzu, "Hackers Threaten Smart Power Grids"; DOE, *Advanced Metering Infrastructure*, 7 and 69; and Hansen, Staggs, and Shenoi, "Advanced Metering Infrastructure," 3. On broader risks of load manipulation, see Amini, Pasqualetti, and Mohsenian-Rad, "Dynamic Load Altering Attacks"; Mohan, Meskin, and Mehrjerdi, "Comprehensive Review of the Cyber-Attacks."

[254] The Trump administration issued Executive Order 1992 to counter supply-chain threats. The Biden administration is revising those defensive measures. Trump, *Executive Order on Securing Bulk-Power System*. For more on the threat that China and Russia will use compromised equipment for coercive campaigns, see Stockton, *Securing the Grid*.

[255] Butrimas et al., *Hybrid Warfare against Critical Energy Infrastructure*, 24. See also Dupuy et al., "Energy Security."

[256] Resnikov, "Russia Remains Unwilling."

adversaries can design cyberattacks to achieve psychological effects and influence alliance decision-making. According to the NATO energy security report, the Kremlin sought to intimidate Ukraine's leadership and public by demonstrating that (in the authors' words) "we can turn your lights off any time we wish." Russia also sought to apply psychological pressure by showing that even brief power interruptions could halt water service in major cities by disrupting electricity-dependent pumping operations. All such disruptions were designed to convince Ukraine's citizens that their government was incompetent and unable to protect their well-being.[257] Russia and China will seek to achieve equivalent psychological effects to discourage security partners from coming to each other's assistance.

Russian leaders took a further step to underline how costly it would be for the West to come to Kiev's defense: they threatened to use nuclear weapons to protect their gains. In a documentary aired on Russian television in March 2015, Vladimir Putin acknowledged that he was ready to signal Russia's readiness to use nuclear weapons during the Crimea annexation.[258] Russian Foreign Minister Sergey Lavrov noted that Moscow saw Crimea as an integral part of Russian territory. He then emphasized that Moscow has a military doctrine that outlines how Moscow would respond to threats to its territorial integrity. The military doctrine "very clearly" states that the "Russian Federation reserves the right to utilize nuclear weapons" in these situations.[259]

In a study titled *Nuclear-Backed "Little Green Men,"* Jacek Durkalec argues that such nuclear threats are fully consistent with Russian nuclear doctrine. He also found, however, that the Kremlin's nuclear-related actions during the Ukraine crisis were "unprecedented in frequency, scale and complexity, and provocative in nature."[260] As with hybrid techniques to disrupt allied decision-making, US strategies against coercive campaigns should also prepare for Russia (and, potentially, China) to discourage allied defense operations by making them appear unbearably dangerous and destructive to defense partners.

Coercion by Denial

While the most prominent means to coerce allies and disrupt coalition defense lies in threatening to punish them, adversaries may also use a quite different strategy: coercion by denial. Under this strategy, Beijing or Moscow will seek to thwart the US military's plans for prevailing in a regional conflict and convince the president that further fighting would be costly and futile.

Coercion by denial does not rely on the physical annihilation of opposing forces. Instead, by degrading the enemy's military capabilities and countering its strategy to prevail in the conflict, the attacker may convince the enemy to back down and—ideally—enable themselves to win at a lower cost than would be required to obliterate the opposing force.[261] Put in the broader calculus of coercion, denial functions by reducing the benefits that the enemy expects to gain through further resistance when compared with the military losses and other costs of continuing to fight.

The successful use of coercion by denial requires more than a generalized focus on convincing adversaries that they are likely to lose. Assessing past examples of denial campaigns, Pape and other analysts found that while they tend to be more successful than punishment-oriented operations, their outcomes varied with relative levels of resolve

[257] Butrimas et al., *Hybrid Warfare against Critical Energy Infrastructure*, 24.

[258] Weaver, "Putin Was Ready."

[259] Keck, "Russia Threatens Nuclear Strikes."

[260] Durkalec, *Nuclear-Backed "Little Green Men,"* 15.

[261] This characterization of denial draws on the analysis provided by Pape, *Bombing to Win*, 10, 13, and 17–20; and Art and Greenhill, "Coercion," 20–22.

between the attacker and the victim, the types of forces and other coercive tools being used, and other factors.[262] Especially critical for success is the ability of the coercer to exploit particular vulnerabilities in the opponent's military strategy.[263]

Analyzing Chinese and Russian strategies for regional conflicts with the United States can help identify vulnerabilities for the DoD to exploit and, ideally, use to convince decision-makers in Beijing and Moscow to settle such conflicts before they escalate to larger-scale warfare. Reversing that analysis offers similar benefits for protecting the United States from coercion by denial. Using Chinese and Russian strategies for victory as a starting point, we can then analyze how those nations may seek to shape US behavior in a regional crisis and apply their broader military doctrines for IOs and cyber warfare to exploit specific US strategic vulnerabilities.

DoD's *2018 National Defense Strategy* and assessments that supported its development offer a foundation for both lines of analysis. Elbridge A. Colby, who served as deputy assistant secretary of defense for strategy and force development in 2017–2018, helped lead the development of the 2018 strategy. Colby testified to Congress that Russia and China have "plausible *theories of victory*" for regional conflicts involving US allies and "established security partners like Taiwan."[264] Under these theories, Beijing or Moscow would try first to overpower US allies and establish local military superiority while holding off US and other allied forces. Then, by extending and reinforcing a defensive umbrella over the area, China and Russia would "render the prospect of ejecting their occupying forces too difficult, dangerous, and politically demanding for Washington and its allies to undertake, or to undertake successfully."[265]

Colby testified that this fait accompli theory of victory is not the only one that China and Russia might employ in regional confrontations. However, he stressed that the fait accompli strategy is the "most severely challenging" one that China or Russia could employ, "especially against Taiwan in the Pacific or the Baltics and Eastern Poland in Europe."[266] Of particular concern to Pentagon officials are cyberattacks on US ports and other transportation infrastructure that could delay and disrupt the flow of US forces to those regions until adversaries have consolidated control over them.

Cyberattacks on that scale would inflict massive levels of disruption and would almost certainly prompt the US to launch a proportionately devastating response (and not necessarily with cyber weapons). They are therefore much less likely to occur than other types of coercive campaigns. Cyberattacks on such a destructive scale might not even seem to constitute coercion but rather the de facto elimination of America's order of battle for a regional conflict.

Nevertheless, disrupting the flow of US forces can contribute to coercion in a way that is fundamentally cognitive and ripe for manipulation. Such operations, especially if paired with IOs, may undercut the hopes of the president and the public that the United States can prevail at an acceptable cost and prompt the White House to settle on the attacker's terms before more extensive and needless damage occurs. Hobbling US delivery of forces can also shape allied perceptions. To have any chance of prevailing against China or Russia, US security partners will need timely, large-scale reinforcements from the United States. Their

[262] Art and Greenhill, "Coercion," 22. One such variable: Pape finds that the use of tactical airpower for denial tends to be more successful than strategic airpower and that the rise of precision-guided munitions is likely to increase this differential. See Pape, *Bombing to Win*, 15, 316–318, and 326.

[263] Pape, *Bombing to Win*, 30.

[264] Emphasis in original. See *Hearing on China and Russia*, Colby statement, 3.

[265] *Hearing on China and Russia*, Colby statement, 4.

[266] *Hearing on China and Russia*, Colby statement, 4.

own ports and supporting infrastructure also need to keep functioning to receive and support the onward movement of US forces. Combined information-cyberattacks against those partners may dash their faith that coalition operations can succeed and convince them that suing for peace is the least bad option.

A comprehensive strategy against coercion should account for these decision-making effects and include targeted measures to defeat coercion by denial. The Defeating Customized Attacks section of this report offers a starting point to do so by providing a more detailed assessment of how Beijing and Moscow may conduct denial-oriented campaigns and proposes options to counter them.

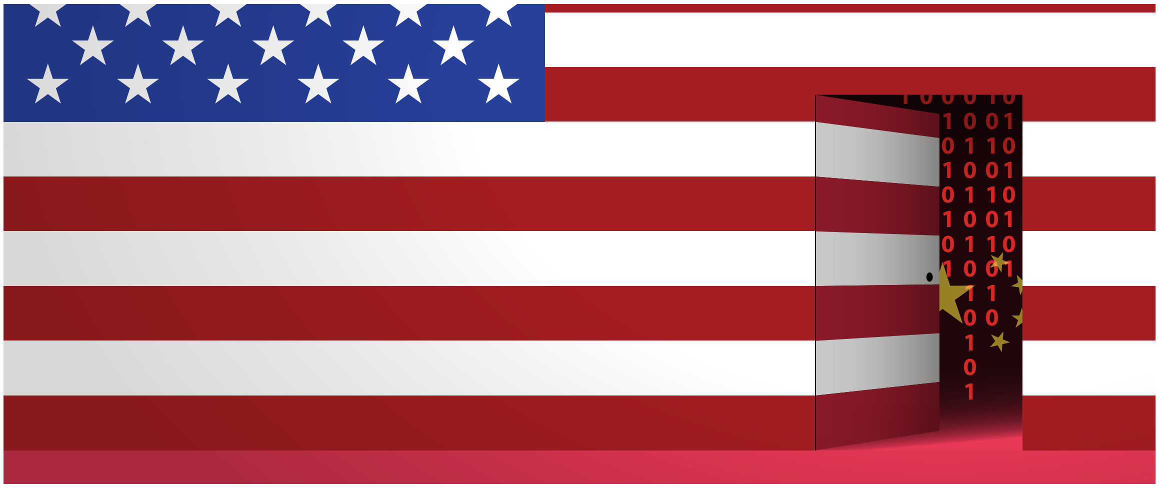
Preparing for "All of the Above" Campaigns

Denial, punishment, and leadership-focused strategies for coercion have distinctive characteristics and rely on separate pathways of influence. But they are not mutually exclusive. China and Russia may integrate them to achieve especially powerful cognitive effects and complicate US defensive measures. US strategies against coercion must achieve similar integration across the multiple lines of attack that adversaries can employ, and do so in ways that strengthen US and allied preparedness across the full conflict continuum. A prerequisite for developing such a strategy lies in understanding how the dependence of the American people on social media has made them so extraordinarily susceptible to enemy messaging.

Underlying US Vulnerabilities to Coercion and Implications for Defense

The rising use of social media by the US public and senior decision-makers creates novel opportunities for adversaries to customize and directly convey disinformation. Yet, that rise *understates* the United States' growing vulnerability to coercive information operations (IOs). The public is far more reliant on social media during disasters and other crises than in normal conditions. Moreover, Americans are especially receptive to disinformation during such events and will be slow to abandon false beliefs once adversaries inculcate them.

Ongoing efforts to combat foreign influence over US elections and disinformation during disasters can help strengthen preparedness against future coercive IO campaigns. However, defeating such IOs will also pose additional policy challenges—including the exercise of federal emergency authorities over media and the defense of the First Amendment during intense, fear-inducing crises. The federal government will also need to take emergency actions beyond those necessary against



election influence. Especially problematic: speedy and effective US counter-messaging will be essential against coercive IOs. Yet, in an era of plummeting public confidence in government and "truth decay," many Americans will be quicker to believe enemy disinformation than statements by the president.

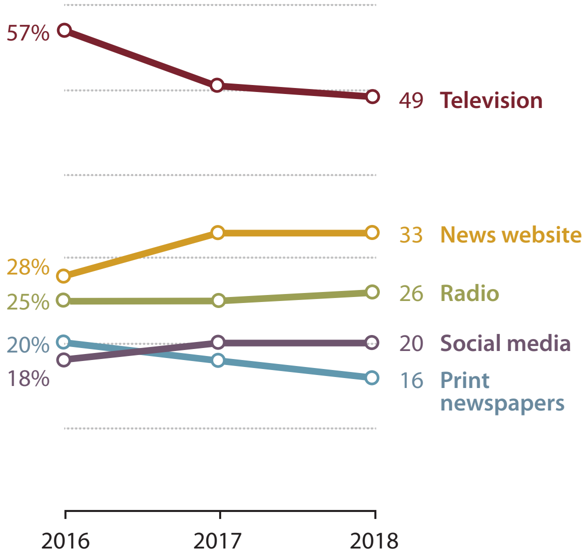
Modern Communications Networks as a Vehicle to Shape Public Perceptions

Russia's use of Facebook, Twitter, and other social media platforms to influence US elections and corrode confidence in democratic institutions highlights why social media can offer a uniquely effective tool for coercing US behavior. These platforms are the primary source of news and information for a large and growing percentage of the US population and are particularly vulnerable to exploitation.[267] Social media platforms serve as a "force multiplier" for IO activities.[268] Compared with broadcast television, print newspapers, and other "legacy" news providers, they offer adversaries major advantages in spreading lies rapidly and on a massive scale. US resilience measures against coercion need to account for these advantages and whittle them down.

Social media's dominance of the communications landscape is far from complete. Figure 2 depicts the leading sources of news for the US public—specifically, those sources that respondents said they used "often." 2018 marked an important turning point: for the first time, social media outpaced print newspapers as a news source in the United States. But broadcast television remains by far the most heavily used platform for receiving news.[269] News websites and even radio broadcasts are also well ahead of social media as frequently used news sources. Moreover, the share of US adults using Facebook and other social media platforms has stayed largely flat for the past few years.[270] The diversity of news sources available to US citizens will complicate adversary efforts to control and shape the flow of information in a crisis.

More Americans get news often from social media than print newspapers

% of US adults who get news often on each platform



Note: The difference between social media and print newspapers in 2017 was not statistically significant.

Source: Survey conducted July 30–Aug. 12, 2018.

PEW RESEARCH CENTER

Figure 2. Percentage of US Adults Who Get News Often from Each Platform

However, the value of social media as a vehicle for IOs will grow because of demographic change in the United States. Millennials and other younger Americans are far more likely than older age cohorts to rely on social media as a news source.

[267] SSCI, *Russian Active Measures, Vol. 2*, 9; and Rosenbach et al., *Election Influence Operations Playbook*, 7.

[268] Theohary, *Defense Primer*, 1.

[269] From a methodological standpoint, is unclear whether "social media" as a news source consists exclusively of written content online, or whether this includes links to online news sources posted on social media platforms. Careful observers will also note that the sources are not mutually exclusive: the figures add up to 144%, meaning some respondents get news "often" from multiple different sources. See Shearer, "Social Media Outpaces Print Newspapers."

[270] Perrin and Anderson, "Share of U.S. Adults Using Social Media."

Indeed, that 49 percent of US adults get news "often" from TV reflects a striking concentration in ages fifty and up. Respondents aged eighteen to twenty-nine use social media most often, followed by news websites. Online news also edged out TV as a primary source among respondents aged thirty to forty-nine, and their social media figures were slightly above the national average.[271]

These factors suggest that public dependence on social media will rise as older cohorts age out. Moreover, the use of social media among older Americans has grown significantly since 2012, further reinforcing the growing reach of such platforms and their potential value for conducting IOs.[272]

One source of information that this analysis does not examine is text messaging. While basic text messaging applications are not considered social media, text messaging is the most frequently and most widely used function on mobile phones in the United States.[273] Industry estimates suggest Americans send 5.5 billion text messages each day.[274] While text messages have a smaller audience than social media posts (typically just a single recipient), people may be more likely to believe information delivered via text message from friends and family.[275] If a social media user comes across convincing disinformation online, they may unwittingly spread it to people in their immediate social circles. One recent example: when misleading text messages began suggesting that former president Trump was going to implement a national lockdown to curb the spread of COVID-19, those messages circulated so quickly that the National Security Council felt compelled to address the rumor directly online over fears that it might affect the stock market.[276] Moreover, because text messages are considered private conversations, they are much more difficult for researchers or anti-disinformation technology to trace. Disinformation based on text messages is outside the scope of this paper and deserves further study, especially since adversaries may leverage this means of conducting IOs to evade the systems that major platforms have implemented to thwart disinformation.[277]

Beyond the Numbers: Dependence on Social Media during Crises

While many Americans turn to broadcast television and other "legacy" outlets for news more frequently than social media on a day-to-day basis, the public is much more likely to rely on social media when disasters or other crises strike. That reliance has grown both during terrorist attacks (such as the bombing at the 2013 Boston Marathon) as well as during hurricanes and other natural disasters. Affected members of the public, emergency managers, and first responders increasingly utilize social media platforms as a rapid, large-scale means of seeking and sharing information and of offering comfort and support to survivors.[278] Media usage during Superstorm Sandy in 2012 exemplifies this growing reliance. Before, during, and after Sandy made landfall, government agencies throughout the Northeast used social media to communicate with the public and response partners, share information, maintain awareness of community actions and needs, and more.[279]

Social media platforms have also become a crucial source of crisis updates for the general public. In

[271] Shearer, "Social Media Outpaces Print Newspapers."

[272] The "baby boomers" (born between 1946 and 1964) increased from 40 percent to 59 percent while the "silent generation" (born 1945 and earlier) increased from 15 percent to 28 percent. See Vogels, "Millennials Stand Out for Their Technology Use."

[273] Smith, *U.S. Smartphone Use*.

[274] CTIA, *2019 Annual Survey Highlights*, 3.

[275] Timberg, Nakashima, and Tony, "Falsehoods Spread."

[276] Timberg, Nakashima, and Romm, "Falsehoods Spread."

[277] Timberg, Nakashima, and Romm, "Falsehoods Spread."

[278] For a survey of this literature and a summary of its findings, see Huang et al., "Connected through Crisis," 1.

[279] Estes Cohen, "Sandy Marked a Shift."

modern crises, society depends on social media for a process of "collective sensemaking"—with both helpful and harmful effects.[280] A study of individuals who used social media in the aftermath of the 2013 Boston Marathon bombing found that social media sites were used as primary sources of real-time news, that many of the participants believed social media sources were better than mainstream media ones, and that users sometimes shared information from social media in attempt to help others stay informed without checking whether it was true (and sometimes it was not).[281]

Purveyors of disinformation are already capitalizing on this dependence. A study of IO campaigns found that such efforts are often "concentrated in bursts around particular events," including terrorist attacks or major political events.[282] In the hours after the Boston Marathon bombing, for example, false reporting about the identity of the bombers reached hundreds of thousands of Twitter, Reddit, and other platform users.[283] Social media sites during Superstorm Sandy were also filled with fake photos and misinformation, including forged photos of the New York Stock Exchange under three feet of water.[284] Subsequent hurricanes have spurred waves of false reports that, through rapid retweeting and other sharing mechanisms, highlighted opportunities to exploit the virality of disinformation on social media.[285]

The spread of false reports from social media to broadcast news constitutes an additional means to broaden the reach of IOs. As noted by Senator Mark R. Warner, "what happens on social media doesn't stay isolated to social media."[286] Indeed, content generated on social media platforms provides a cheap, simple, and speedy way of acquiring stories, especially for local television stations and newspapers. As a result of staff reductions driven by declining revenues, fewer newspapers and local outlets have the resources to fact-check stories that they pick up from social media.[287] Moreover, as newspapers increasingly focus on their online versions, even companies as traditional as the *New York Times* value page views, "most emailed" articles, and trending topics. The net result: mainstream news organizations frequently source their stories directly from Twitter and other social media platforms and use more inflammatory headlines to drive engagement.[288]

Given the advertising-based online revenue model, there is value in being the first to publish a story, especially if other outlets credit and link to the initial report. However, in the race to be first, even legitimate news outlets may rush to publish stories that contain disinformation. And once outlets publish false stories, efforts to debunk them can also have the unintended effect of amplifying them.[289]

[280] Starbird, "Crisis Researcher Makes Sense."

[281] Huang et al., "Connected through Crisis," 1.

[282] Krasodomski-Jones et al., *Warring Songs*, 30.

[283] Madrigal, "#BostonBombing."

[284] Hill, "Hurricane Sandy"; and Estes Cohen, "Sandy Marked a Shift."

[285] Bonazzo, "Fake News about Hurricane Florence." DHS's Social Media Working Group also warns of opportunistic disinformation in crises, including malicious, politically motivated attempts to "cause harm and disrupt the standard flow of truthful information during a specific event or incident." See SMWGESDM, *Countering False Information*, 8. DHS also warns that adversaries could "game" social media networks to impede or delay access to response services, propagate misinformation, or misrepresent event details. See VSMWG, *Using Social Media*, 35.

[286] Timberg, "Russians Struggled to Spread DNC Files."

[287] Of course, this decline in revenue is itself a partial result of the rise of digital and social media, and especially the shift in advertising income to online sources. Marwick and Lewis, *Media Manipulation*, 41–42. On the broader economic pressures that competition from social media has created for traditional news sources, see Pritchard, "Readers' Editor"; Chu, "Clickbait"; and Tracy, "Google Made $4.7 Billion."

[288] Indeed, some outlets have begun to publish content "before they are finished, let alone fact-checked." See Marwick and Lewis, *Media Manipulation*, 42–43; and Chu, "Clickbait."

[289] Warzel, "Epstein Suicide Conspiracies."

Adversaries will tailor their social media content to exploit these problems. They will also craft their messaging to provoke an emotional response and then amplify it with bot networks to maximize the likelihood that newspapers, television, and their online versions pick up and spread the content. Media manipulators deliberately plant false content on social media platforms for local TV and news outlets by generating viewer-attractive hoaxes.[290] They exploit the inability of these resource-constrained news outlets to debunk false stories.[291] If that local coverage generates sufficient attention and engagement online, larger outlets may pick up the story and increase its coverage and reach. Press coverage of Hurricane Harvey exemplifies how purveyors of disinformation can exploit such tactics in a crisis. As flooding intensified and posed growing threats to public safety, a tweet purporting to show a shark swimming up a flooded Houston freeway went viral. Even a modicum of fact-checking with local emergency managers would have debunked the tweet. Yet, Fox News host Jesse Watters picked up and spread the false information on his nationally televised show, claiming that he "saw a shark on a highway swimming in the water."[292]

That incident is laughable but also offers a cautionary lesson. Given the speed with which legacy media outlets can spread even dubious social media information, the United States should expect adversaries to achieve similar effects in future crises, thereby reaching a wider audience and diminishing the problems that media diversity would otherwise create.

Russian "Proof of Concept" IOs against the United States

Russia has already tested its ability to exploit the public's dependence on social media in crises and the virality of false but frightening content. On September 11, 2014, the Internet Research Agency (IRA) used social media platforms and widespread text messaging to convince residents and local officials in St. Mary Parish, Louisiana, that they faced a dangerous threat to their safety. Hundreds of Twitter accounts began documenting a (non-existent) disaster at a local chemical plant. Supposed eyewitnesses provided false images of flames engulfing the plant with explosions and thick and potentially toxic smoke pouring from the facility. Dozens of media outlets and public officials found their Twitter accounts inundated with such messages, including a realistic-appearing screenshot of CNN's homepage showing that the disaster had already made the national news.[293]

This coordinated effort involved dozens of fake accounts that posted hundreds of tweets for hours, targeting a list of figures precisely chosen to generate maximum attention. In addition to the false screenshot from CNN, the campaign created fully functional clones of the websites of Louisiana TV stations and newspapers as well as a Wikipedia page citing false YouTube videos of the disaster.[294]

The chemical sector is not alone in being vulnerable to such disinformation operations. The Federal Emergency Management Agency (FEMA) has identified a set of "community lifelines," including energy, health and medical services, and food and water, that are "essential to human health and safety or economic security."[295] Cyberattacks that disrupt these lifelines—or simply IOs that convince the public of a false disruptive attack—could have coercive value for an attacker. The IRA has conducted a proof-of-concept operation against the US food-distribution system designed to test how effectively Russia can spread false information to

[290] DiResta, "Computational Propaganda."

[291] Marwick and Lewis, *Media Manipulation*, 38–39.

[292] Eberhardt, "Fake Shark Photo."

[293] Chen, "The Agency."

[294] Chen, "The Agency."

[295] FEMA, *National Response Framework*, 8.

incite fear and panic.[296] During the 2015 Thanksgiving holidays, the agency launched a coordinated information campaign in which users posing as US citizens claimed that a batch of poisoned turkeys had sent two hundred people to the hospital in "critical condition." The attackers spread this disinformation on multiple social media platforms (including over ten thousand tweets), posted on online forums, established a Wikipedia page, and created a blog post that claimed to cite the NYPD (New York Police Department).[297]

Of course, these IOs employed primitive technologies and tactics compared to those that Russia and China are currently developing. Moreover, the operations occurred in the absence of an international confrontation that would already have citizens on edge and that would magnify the believability (and virality) of false social media reporting. Adversaries may tailor crisis IOs to exploit that virality to incite fear and bring home the risks of standing up for US allies. Efforts to strengthen domestic resilience must be structured accordingly.

Psychological Vulnerabilities of the US Public to Manipulation via Social Media

Efforts to strengthen domestic resilience against coercive IOs must account for an additional problem: the innate psychological vulnerability of the US public to false information conveyed on social media networks. Studies have found that falsehoods diffuse over Twitter and other platforms much more rapidly and broadly than truthful news.[298] One study found that false news stories are 70 percent more likely to be retweeted than true ones and that it takes true stories six times as long to reach 1,500 people compared with false reports.[299] False news stories are more likely to elicit strong emotions and thereby intensify user engagement. In addition, people often share information that they see as "new" (regardless of whether it is true or not) to gain attention or to be seen as "being in the know."[300]

Social media users are especially prone to deem negative information as "more informative and influential" than positive information. Adversaries can leverage that tendency to magnify public fears and apprehension during stressful events, promote misinformation, and instigate rumors.[301] The fact that adversary messaging is false does not automatically make it less attractive to users. In the three months leading up to the 2016 US election, the twenty top-performing intentionally false stories about the election on Facebook outperformed the top twenty legitimate stories from major news outlets.[302] The public's proclivity to spread falsehoods versus the truth will be ideal for exploitation in IO campaigns designed to incite fear and discourage support for US allies.

Once people believe a false report, convincing them to abandon that belief is difficult. When individuals are presented with information that conflicts with the beliefs they have already acquired, they will double down on their original views rather than revising them.[303] Moreover, simply exposing people to false information makes people more

[296] SSCI, *Russian Active Measures, Vol. 2*, 53; Foster, "Russian Trolls Are Using American Businesses"; and Kranz, "Thanksgiving Food Poisoning Hoax."

[297] Berry, "Russian Trolls Tweeted Disinformation"; and Kranz, "Thanksgiving Food Poisoning Hoax."

[298] Vosoughi, Roy, and Aral, "Spread of True and False News Online," 1146.

[299] Vosoughi, Roy, and Aral, "Spread of True and False News Online," 1150.

[300] AEP, *Targeted Disinformation Campaigns*, 9; and Dizikes, "On Twitter, False News Travels Faster."

[301] Bongar et al., *Psychology of Terrorism*, 122.

[302] Silverman, "Fake Election News Stories Outperformed Real News."

[303] Nemr and Gangware, *Weapons of Mass Distraction*, 9–12; and Wadley, "Why People Are Resistant to Correcting Misinformation."

likely to believe it later on. If people have already seen something, they subconsciously use that as an indication that the information is true.[304] Indeed, no matter the veracity of a given piece of information, the more an individual sees that information online, the more they become familiar with it, and the more they are willing to accept it as true.[305] This "illusory truth effect" is shown to increase the perceived accuracy of fake information, and it compounds with repetition.[306]

This tendency suggests that adversaries will enjoy a significant *first-move advantage*; by striking first with IOs in a regional crisis, and establishing a false narrative regarding why and how US leaders are assisting an ally, opponents can shape public perceptions in ways that will be difficult for those leaders to undo.[307] If adversary disinformation goes viral, that content will dominate many users' social media feeds. Popular content is, by nature, more likely to generate the engagement that increases its "value" to the algorithms that curate social media feeds. This self-reinforcing effect is particularly powerful for shaping public opinion.

Adversaries can also amplify and spread disinformation by manipulating social media algorithms that determine what is "trending." All major platforms have some variation of this trending function, which uses proprietary (and closely held) algorithms to determine, based on user-posted content, that something important or interesting is happening that other users will want to know about.[308] These algorithms operate without regard for the accuracy or quality of the trending topic or story—they can determine whether content is being shared but not whether it *should* be shared. As a result, trending functions are "eminently gameable."[309] Malicious actors manipulate these algorithms by conducting coordinated campaigns, often using bots and other technological amplifiers, to create volume around a preselected message.[310]

Twitter is often exploited in this way. Because of the platform's focus on short messages, which are broadcast instantly to followers and the public more broadly, Twitter exerts a "magnetic" attraction during breaking news stories.[311] Reliance on Twitter is especially heavy in the immediate aftermath of a disaster or other major event, before other (and more reliable) sources of information can catch up. Users are inclined to believe any information that trends as a result of this increased usage, in part because so many people are sharing it.[312] Journalists and other media figures often pick up on trending information as well.[313] The net result: "If you make it trend, you make it true."[314] Adversaries can leverage this dynamic in a crisis to magnify public fear and achieve other goals with greater speed and reach than would otherwise be possible.

The public's poor ability to detect disinformation will reinforce the effectiveness of such operations. Multiple studies have found that it can be difficult for people to identify false stories and that even digitally savvy citizens fail to ask important questions about content they encounter on a browser. An Ipsos Public Affairs survey determined that fake headlines fool US adults about 75 percent of

[304] Steinmetz, "How Your Brain Tricks You."

[305] Yates, "Dissecting Disinformation."

[306] Wholly implausible statements (e.g., "the earth is a perfect square") stand as a notable exception. See Pennycook, Cannon, and Rand, "Prior Exposure Increases Perceived Accuracy," 31.

[307] On the first-move advantage, see Paul and Matthews, *Russian "Firehose of Falsehood*," 4. Subsequent portions of this section examine the consequences of this first-move advantage for crisis stability and escalation management.

[308] Feldman, "Time to End 'Trending.' "

[309] Feldman, "Time to End 'Trending.' "

[310] Another common tactic is to co-opt an already trending topic or hashtag by flooding those conversations with disinformation. See DiResta, "Computational Propaganda."

[311] Warzel, "Epstein Suicide Conspiracies."

[312] AEP, *Targeted Disinformation Campaigns*, 9.

[313] Warzel, "Epstein Suicide Conspiracies."

[314] DiResta, "Computational Propaganda."

the time.[315] Other studies have shown that 59 percent of people retweet links without clicking on them and rely too much on search engines.[316] Massachusetts Institute of Technology (MIT) cognitive scientist David Rand has found that, on average, participants in his studies are inclined to believe false news at least 20 percent of the time. Stanford University psychologist Sam Wineburg notes that when it comes to consuming information online, "we are all driving cars, but none of us have licenses."[317]

Training programs to make US citizens more discerning consumers of online content could potentially provide the equivalent of "driver's ed." However, underlying psychological factors will limit the effectiveness of educational campaigns and skill development initiatives. For many people, emotional responses to social media content tend to prevail over objective, fact-based assessments of news credibility. Stories (true or false) that instill a sense of fear, uncertainty, and/or anger are the most likely to go viral.[318] Social media IOs to magnify public fears in a crisis will be perfectly positioned to capitalize on such emotionally driven behavior.

Individuals are also poorly prepared to deal with the high volume of information that social media platforms are designed to convey, especially when anxious and dealing with uncertainties. Human cognitive biases lead people to discard information they consider "unwanted" and confine their attention to a limited set of social media accounts or pages that produce information that already aligns with their views.[319] Disinformation that invokes feelings of anger, fear, or disorientation also spreads across vast networks at high speeds, leaving users more vulnerable to future manipulation via disinformation.[320]

Taken together, these factors lead some researchers to conclude that humans are simply "not rational consumers of information."[321] Of course, driven by the imperative to increase clicks and the associated ad revenue they help produce, social media algorithms tend to promote content that appears to be generating significant engagement, which leads to greater circulation of stories with provocative headlines regardless of whether the content is reliable.[322] As will be discussed in the next section of this study, Russia has proven particularly adept at exploiting these algorithms and platform functions, combining the use of multiple social media platforms and leveraging their respective strengths to maximize their reach.

Social media companies are taking steps to make their algorithms less vulnerable to attention-grabbing disinformation.[323] But psychological factors will give China and Russia an inherent advantage in shaping public perceptions versus efforts to dislodge those perceptions. Moreover, artificial intelligence (AI) and other technological advances will likely be able to "exploit the weaknesses inherent in human nature at a scale, speed, and level of effectiveness previously unseen."[324] Strategies to strengthen resilience must account for this uphill terrain.

Declining Public Trust in US Leaders and Democratic Governance

The public's growing vulnerability to IOs reflects an additional trend—one that Russia is striving to deepen and accelerate. Over the past two decades,

[315] Silverman and Singer-Vine, "Most Americans Who See Fake News Believe It."

[316] Martineau, "Power of Crowd."

[317] Quoted in Steinmetz, "How Your Brain Tricks You."

[318] Meyer, "Grim Conclusions."

[319] Nemr and Gangware, *Weapons of Mass Distraction*, 7–9.

[320] Jackson, "Issue Brief."

[321] Nemr and Gangware, *Weapons of Mass Distraction*, 3.

[322] Oremus, "Facebook's Most-Shared Story."

[323] See, e.g., Barrett, *Tackling Domestic Disinformation*, 16.

[324] Paul and Posard, "Artificial Intelligence."

the US public's trust in government has fallen to historic lows. Russian efforts to influence US elections and corrode faith in democratic institutions are designed to accelerate this decline (as well as to achieve other goals). However, those efforts are not the only source of diminishing trust of government. Deeply rooted domestic factors are also driving that decline, including the increasing polarization of US politics, society, and the economy. The resulting loss of confidence in government will create far-reaching opportunities for adversaries to exploit in future IOs, create fertile ground for conspiracy theories to flourish, and provide a head start for efforts to convince the public that their leaders are lying to them in a crisis.[325]

Russia's current efforts to discredit and subvert democratic governance in the United States build on a century of IOs by the Soviet Union and its czarist predecessors.[326] In assessing Russian activities and intentions in recent US elections, the US Office of the Director of National Intelligence (ODNI) found that "Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order." That report also found that Russia's purpose was not only to damage Hillary Clinton's electability vis-à-vis former president Donald Trump but also to "undermine public faith in the US democratic process," and that Russia will leverage lessons learned from this operation to conduct expanded influence campaigns in the future.[327] Indeed, the Senate Intelligence Committee found that Russian disinformation surrounding the 2016 election "was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society," and represented "only the latest installment in an increasingly brazen interference by the Kremlin on the citizens and democratic institutions of the United States."[328]

Efforts to defeat such influence campaigns have twin benefits for strengthening resilience against coercive IOs in a crisis. By cataloging the means by which Russia used social media and other methods to shape voter perceptions and incite conflict within and between political factions in the United States, and by developing defensive measures against them, initiatives to counter electoral interference can provide valuable tools and technologies for use against crisis IOs. Blunting Russian efforts to corrode public confidence in democratic governance could also help reduce the US public's vulnerability to such operations.

However, the lack of public trust in government reflects deep domestic roots. Figure 3 charts the loss of such confidence. Only 17 percent of Americans say they can trust the federal government to do what is right "just about always" (3 percent) or "most of the time" (14 percent). These are close to the lowest levels of trust ever recorded. They also indicate a multi-decade decline, reflecting most recently the immense partisan divides over the credibility of former presidents Barack Obama and Donald Trump.[329] Dissatisfaction with the federal government's response to COVID-19 may ultimately drive levels of public trust down even further.[330]

These declines are paralleled by a loss of public belief that mass media reporting is true. Only 45 percent of Americans have a "great deal" or a "fair amount" of trust in mass media to report the news "fully, accurately and fairly." That level of confidence represents a significant rebound from the all-time low of 32 percent in 2016, although media

[325] Tavernise, "Will the Coronavirus Kill What's Left of Americans' Faith in Washington?"

[326] Mazarr et al., *Hostile Social Manipulation*, 33–49.

[327] ODNI, *Assessing Russian Activities*, ii. For a deeper analysis of Russian goals in subverting the 2016 election, see McFaul, *Securing American Elections*, 1–16.

[328] SSCI, *Russian Active Measures, Vol. 2*, 5.

[329] Pew Research Center, *Public Trust in Government*.

[330] Tavernise, "Will the Coronavirus Kill What's Left of Americans' Faith in Washington?"

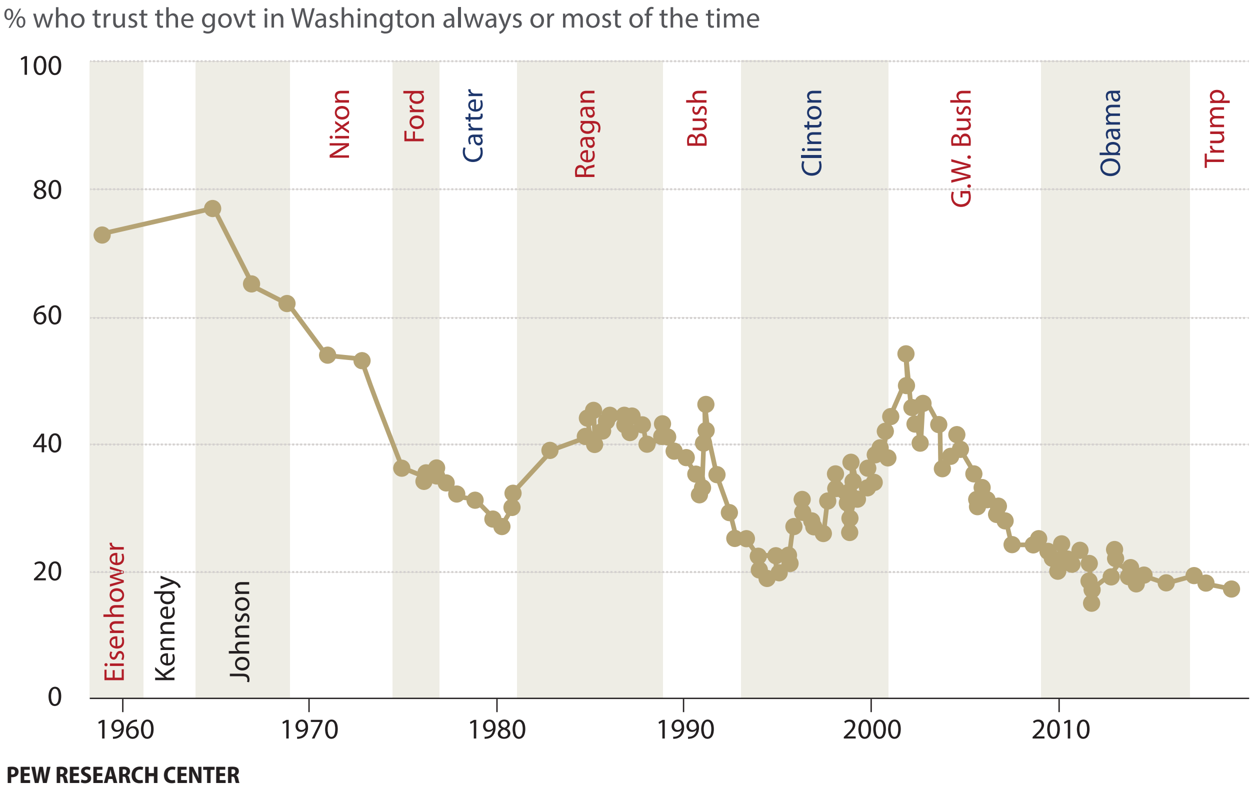


Figure 3. Public Trust in the Federal Government, 1958–2019

trust remains below what it was in the late 1990s and early 2000s.[331] The fact that less than half the public believes in the accuracy of mass media reporting will help adversaries advance their own narratives, especially if the government relies on such media to convey and seek support for its policies in a crisis. Nor is the public any more likely to believe government-endorsed content on social media platforms. On the contrary: nearly 60 percent of Americans across a number of polls believe social media content (whether provided by government agencies or other sources) contains inaccurate or false information.[332] That belief will help Russia advance its goal to cloud the truth and advance the public's perception that no narrative or news source can be trusted at all.[333]

A study published by RAND on "truth decay" identifies further domestic sources of vulnerability to crisis IOs. In addition to loss of trust in government and media as sources of factual information, the study finds that the US electorate also faces heightened disagreement about facts and the analytical interpretation of data as well as a drastic increase in the volume of opinion-driven content versus factual information.[334] The net result: facts and data play a diminishing role in American public life. The authors find that truth decay is eroding civil discourse and reinforcing political paralysis in the federal government. In addition, while this phenomenon poses deep problems for US democracy and undermines the foundations of national

[331] Jones, "U.S. Media Trust Continues to Recover."

[332] A Pew poll indicated that 57% of respondents who use social media for news purposes *expect* that news to be largely inaccurate. See Shearer and Matsa, "News Use Across Social Media Platforms 2018." In a study by NBC News and the Wall Street Journal, 55% of respondents indicated that social media "spreads lies and falsehoods." See Murray, "Americans Give Social Media Thumbs-Down."

[333] Tucker, "Russia Wants to See US 'Tear Ourselves Apart.'"

[334] Kavanagh and Rich, *Truth Decay*, x–xi.

resilience, it could also serve as a critical enabler for adversaries seeking to coerce US behavior. Absent truth decay, an opponent would find it more difficult to cast doubt on the wisdom and veracity of pronouncements by US leaders, and to mobilize unwitting agents who will spread the opponent's disinformation. With such decay and the polarization of politics that helps cause it, adversaries will have ready-made advantages to drive US decision-making.

Implications for Strengthening Domestic Resilience

The most deeply rooted sources of US vulnerability to coercion will be difficult, if not impossible, to fully mitigate. Initiatives to help US citizens become more careful consumers of online information exemplify these difficulties. Studies of Russian operations to inflame disagreements within the US electorate and corrode confidence in government propose a range of citizen-focused efforts, including public education campaigns, efforts to improve media literacy and "digital hygiene," and training on critical thinking.[335] The Cyberspace Solarium Commission (March 2020) also recommends that Congress fund research on how best to improve digital citizenship and that digital literacy curricula be included in American classrooms at the K–12 level and beyond.[336] However, such efforts will take years to implement and will need to overcome major hurdles to success.[337]

Declining public trust in government will be at least as difficult to reverse. The Cyberspace Solarium Commission proposes that digital literacy programs be coupled with civics education curricula to help restore faith in democracy, which would explain "what democracy is, how individuals can hold their leadership accountable, and why democracy must be nurtured and protected."[338] Such efforts may ultimately impede Russia's campaigns of democratic corrosion. However, public confidence in government has been falling for decades. Rather than depend on a quick turnaround of that trend, US policymakers should assume that the public will remain at least somewhat vulnerable to IOs that exploit societal divisions and distrust of US leaders and shape US domestic defenses against coercion accordingly.

Voluntary Public–Private Collaboration for IO Defense

Social media platforms could play uniquely valuable roles in helping US agencies defeat coercive campaigns. Precisely because these platforms offer adversaries a prime means of manipulating public beliefs, platform managers, algorithms, and content-monitoring staffs are exceptionally well positioned to block enemy disinformation and assist in providing timely US government counter-messaging. But their willingness and ability to perform such defensive operations is far from clear, especially given the novel problems entailed in helping US leaders prevail in foreign crises.

Platforms are now policing hate speech and other "harmful" content more aggressively than in the past. Facebook exemplifies this shift. In 2016, Facebook CEO Mark Zuckerberg stated that the company should not be responsible for identifying and eliminating disinformation, and that "we must be extremely cautious about becoming arbiters of the truth ourselves."[339] That stance has changed. In 2020, Zuckerberg noted that Facebook had

[335] Bulger and Davidson, *Media Literacy*; Huguet et al., *Exploring Media Literacy Education*; Vilmer et al., *Information Manipulation*, 177–179; Knight Commission, *Crisis in Democracy*, 9; and Fried and Polyakova, *Democratic Defense against Disinformation*, 13.

[336] CSC, *Official Report*, 69.

[337] Bulger and Davidson, *Media Literacy*, 15–17; Huguet et al., *Exploring Media Literacy Education*, 58–59; and Boyd, "You Think You Want Media Literacy?"

[338] CSC, *Official Report*, 69.

[339] Guynn and McCoy, "Zuckerberg Vows to Weed Out Facebook 'Fake News.' "

bolstered its policies and capabilities to take down harmful content and emphasized that "the last thing I want is for our products to be used to divide people or rip society apart in any kind of way."[340] However, leaked internal deliberations show that Zuckerberg and other Facebook executives are not entirely committed to mitigating the divisive effects their platforms are having.[341] Critics also suggest that the changes Facebook has made to date are insufficient, likening them to a "strategic appeasement strategy" that offers fixes that sound promising but achieve very little in practice.[342] Meanwhile, a two-year independent audit found that Facebook encountered a "seesaw of progress and setbacks" in terms of addressing disinformation, algorithm bias, content moderation, advertising practices, and other divisive issues.[343]

These policies are in flux. While Zuckerberg recently stated that he "doesn't believe private companies should regulate political speech," pushback from employees and an organized advertising boycott by several large companies appear to be softening this stance.[344] Russian interference in US elections has spurred other social media companies to make similar transitions from resisting "editorial roles" to supervising content in far-reaching new ways.[345] However, Facebook, Twitter, Google, and other companies continue to face pressure from both those who argue more action is necessary to address disinformation and harmful content and those who argue the platforms are already interfering too much with free speech in ways that reflect a political bias.[346]

These companies are also launching new initiatives to block disinformation, many of which might be repurposed to counter coercive messaging against the US public. Platforms have refined their ranking and recommendation algorithms and improved AI to identify harmful content, including from automated spammers and suspicious impersonator accounts. They have hired thousands of additional content reviewers and contracted with platoons of outside fact-checkers to identify disinformation and "coordinated inauthentic behavior"—groups of pages or people working together to mislead others and manipulate discussions on their platforms.[347] The following are examples of recent initiatives:

- *Facebook* announced the creation of an independent oversight board for content moderation and continues to be proactive in removing coordinated inauthentic behavior.[348]
- *Twitter* continues to refine its rules for manipulated media, which may be labeled as such or removed from the platform entirely.[349]
- *Google* has announced the implementation of AI-based tools to help journalists, fact-checkers,

[340] AP, "Zuckerberg Says Facebook Must Stand Up."

[341] The platform's senior leadership chose to discontinue research that found that their algorithms "exploit the human brain's attraction to divisiveness," and limited (or entirely blocked) efforts to reduce these effects among Facebook products. While their stated concern at the time was how the reforms would disproportionally impact users on one side of the political spectrum, internal documents also highlighted their concerns that reforms would hamper user engagement, which would negatively affect advertising revenue. See Horwitz and Seetharaman, "Facebook Executives Shut Down Efforts"; and Smith, "Facebook Knew."

[342] Scola, "Inside the Ad Boycott"; and Vranica and Seetharaman, "Facebook Tightens Controls."

[343] Ortutay, "Facebook Civil Rights Audit."

[344] Glazer, "Facebook Removes Trump Campaign Ads"; and Bond, "Over 400 Advertisers Hit Pause." A Facebook spokesman, however, denied that changes were spurred by "revenue pressure." See Vranica and Seetharaman, "Facebook Tightens Controls."

[345] Vilmer et al., *Information Manipulation*, 143.

[346] Glazer, "Facebook Removes Trump Campaign Ads."

[347] Barrett, *Tackling Domestic Disinformation*, 15; and Fried and Polyakova, *Democratic Defense against Disinformation 2.0*, 12.

[348] Harris, "Preparing the Way Forward"; Gleicher, "Removing Coordinated Inauthentic Behavior from China"; and Klonick, "Facebook Oversight Board." The company also posts monthly reports about coordinated behavior on their platform. See, e.g., Facebook, *Coordinated Inauthentic Behavior Report*.

[349] Roth and Achuthan, "Building Rules in Public."

and disinformation researchers detect fake media.[350]

- *YouTube* (owned by Google) announced new content moderation policies that specifically target false, misleading, or manipulated election-related content for removal.[351]

These platforms have put forth a particularly concerted effort to deal with COVID-related disinformation. In March 2020, major social media platforms and other technology partners put out a joint statement on their commitment to fighting such disinformation, elevating authoritative content from public health experts, and working with government agencies to share important updates.[352] Google, in particular, has conducted large-scale efforts to ensure that its users and YouTube users only get access to legitimate information, and has forgone potential profits by blocking advertisements attempting to capitalize on the virus.[353]

Most important, the 2016 presidential election awakened social media companies to the ease and effectiveness with which Russia (and potentially other nations) can use their platforms to manipulate the US public. Zuckerberg again exemplifies this recognition that platforms have become a vehicle for influence campaigns. Shortly after the 2016 election, he dismissed accusations that disinformation shared over Facebook affected the race, calling it a "pretty crazy idea" that such influence had occurred. Zuckerberg later expressed remorse for that statement, and Facebook disclosed that Russian entities had purchased $100,000 in ads to promote divisive political and social messages during the 2016 presidential campaign.[354]

Content filtering reemerged as a problem in the run-up to the next presidential election. In January 2020, Zuckerberg was quoted as disagreeing with "those who say that new types of communities forming on social media are dividing us." This belief undergirded Facebook's initial decision not to fact-check political content ahead of the 2020 election.[355] Yet, facing intense congressional scrutiny and public pressure, Facebook introduced additional (although still limited) measures to counter election-related disinformation in September 2020.[356]

Russia's 2020 election interference campaign spurred broader private sector initiatives as well. Social media and Big Tech companies strengthened their collaboration with federal agencies in anticipation of disinformation operations in the 2020 election. Facebook, Google, Microsoft, and Twitter met with Department of Homeland Security (DHS), ODNI, and Federal Bureau of Investigation (FBI) officials in September 2019 to discuss their preparations for that election. Cooperation is growing on threat modeling, intelligence sharing, and strengthening ties between industry and government.[357] Nathaniel Gleicher, head of cybersecurity policy at Facebook, noted that industry and government partners have discussed ways to "improve how we share information and coordinate our response to better detect and deter threats."[358]

Social media companies and federal agencies should explore opportunities to expand their collaboration for defense against coercive IOs. However, building such collaboration will encounter major obstacles. The most significant is that no

[350] Sullivan, "'Prodigious Problem.'"

[351] Miller, "How YouTube Supports Elections."

[352] Shu and Shieber, "Joint Statement."

[353] Newton, "Google Has Been Unusually Proactive."

[354] Weiss, "From 'Crazy' to 'Regret.'"

[355] Horwitz and Seetharaman, "Facebook Executives Shut Down Efforts."

[356] Facebook, "New Steps to Protect the US Elections"; and Isaac, "Facebook Moves to Limit Election Chaos."

[357] Isaac and Alba, "Big Tech Companies Meeting with U.S. Officials."

[358] Rodriguez, "FBI Visits Facebook"; and Wagner, "Facebook Meets with FBI."

crisis-driven IO campaign has yet occurred. It was only after the 2016 election that social media platforms recognized their role as a tool of foreign influence and took on new content-monitoring functions and government relationships in response. Many companies are continuing to play catch-up. A recent industry–government study found that "while some major social media platforms have taken steps to limit disinformation on their platforms, these steps, in general, have been reactive in nature" and constitute a "perpetual game of 'whack-a-mole.' "[359] Rather than wait until Russia or China has successfully coerced the United States in a future crisis, social media companies and their industry and government partners should conduct research and exercises to better anticipate such crises and examine collaborative plans and capabilities to defeat them.

Their discussions will also need to address impediments to such collaboration. One problem lies in the business model that platforms use to attract users and advertising revenue. Sensationalist content sells best;[360] adversaries seeking to instill fear in the US public during a crisis will have ample opportunities to craft their IOs for maximum viewership. Moreover, the business practices and algorithms that help platform advertisers microtarget ads are ideally suited for attackers to exploit for coercion. Platforms collect data about their users, organize them into like-minded audiences with shared preferences, and sell those groups' aggregated attention to ad purchasers. If users engage with the ad content, both the purchaser and the platform benefit, even if (as in 2016) the purchaser is spreading disinformation.[361] Foreign intelligence agencies are also becoming increasingly adept at stealing such data. In 2019, for example, millions of users downloaded the ToTok messaging application from Google and Apple app stores; the app then funneled their contacts, texts, and other sensitive data to United Arab Emirates spies.[362]

As noted above, social media companies took measures to identify and block similar influence operations ahead of the 2020 election. Twitter banned political ads entirely to reduce the potential for election-based disinformation.[363] Google also adopted new policies to counter such campaigns.[364] But the underlying problem remains: the tools social media companies have developed to maximize ad revenue, including microtargeting, rely on gathering and exploiting increasingly detailed personal data in ways that create real opportunities for disinformation campaigns.[365]

Companies will also need very different criteria for assessing "harmful" content in a regional crisis between the United States and Russia, China, or other adversaries. Industry–government collaboration against election interference reveals some of the difficulties of establishing such standards. While Mark Zuckerberg acknowledged the need for Facebook to improve its filtering of divisive and manipulative content in advance of the 2020 election, he has also emphasized that "at some point, we've got to stand up and say, 'No, we're going to stand for free expression.' Yeah, we're going to take down the content that's really harmful, but the line needs to be held at some point."[366] Twitter and other platforms have long espoused a similar

[359] AEP, *Targeted Disinformation Campaigns*, 22.

[360] Fried and Polyakova, *Democratic Defense against Disinformation 2.0*, 15. Moreover, content that evokes negative emotions tends to increase the time users spend on social media, which gives platforms more time to generate revenue from advertisements. See Nguyen, "Doomscrolling."

[361] Ghosh and Scott, "Disinformation Is Becoming Unstoppable."

[362] Roose, Frenkel, and Perlroth, "Tech Giants Prepared."

[363] Conger, "Twitter Will Ban All Political Ads"; and Twitter, "Political Content."

[364] Roose, Frenkel, and Perlroth, "Tech Giants Prepared."

[365] Fried and Polyakova, *Democratic Defense against Disinformation 2.0*, 15; AEP, *Targeted Disinformation Campaigns*, 8; and Barrett, Wadhwa, and Baumann-Pauly, *Combating Russian Disinformation*, 14.

[366] AP, "Zuckerberg Says Facebook Must Stand Up."

commitment to protecting free speech and defending the First Amendment.[367]

Determining where to draw the line on content arising from a regional crisis could be problematic. Many existing platform criteria for removing harmful content are fairly straightforward, especially for child pornography, snuff videos, and other clearly objectionable posts and discussions.[368] Yet, within the context of election security efforts, companies are at odds on defining their role in moderating false or misleading campaign messaging and establishing criteria for doing so—or whether they should allow political ads at all.[369] Both political parties in the United States were also unhappy with Facebook's proposal to limit their ability to microtarget their political advertisements based on highly specific characteristics.[370] Facebook has already come under criticism for how its algorithm treats content regarding civil unrest and has pledged to review its existing policies, including potentially strengthening rules that already allow for greater restrictions during emergencies.[371]

It will be even more problematic for social media companies to adapt their moderation and content assessment policies to counter specialized, crisis-oriented disinformation, including messaging on "foreign policy" issues that would be unthreatening in a peacetime environment. Monika Bickert, Facebook's vice president for global policy management, notes that the company is committed to removing content that poses "a threat to public safety" or is tied to ongoing violence or the threat thereof.[372] How Facebook would apply that policy amid an escalating great power confrontation is unclear.

Social media platforms and US agencies should develop use cases to explore these challenges and (ideally) begin to develop criteria for filtering coercive disinformation. Building on past Russian operations in the near abroad, for example, they might discuss how moderators would deal with video "evidence" that Estonia had begun torturing its ethnic Russians, and block Russian disinformation about its deployment of little green men to seize Estonian territory.[373] Equivalent use cases could anticipate the Chinese use of IOs to justify forcible reunification with Taiwan and convince the US public that the costs of defending that nation would far outweigh the benefits.

Another option would be to derive content-filtering criteria from the essence of coercion. As noted in the Scoping the Challenge section, coercion functions by creating and exploiting an opponent's fears of suffering future punishment and by altering the opponent's perceptions of the costs and benefits of alternative courses of action.[374] Adversaries will conduct coercive operations against the United States in a regional confrontation in an attempt to reduce the perceived benefits of defending US allies and interests, while at the same time raising the perceived costs of doing so. So, for example, Beijing might portray the leaders of Taiwan as feckless, corrupt, and not worthy of the suffering that US citizens would endure from the confrontation with China that would occur if the US military came to their aid.

[367] The First Amendment, however, precludes government censorship and would not actually constrict privately owned social media companies. See Leetaru, "History Tells Us"; and Barrett, *Tackling Domestic Disinformation*, 1.

[368] While the platforms may face challenges in implementing such policies, it is conceptually straightforward to ban such clearly objectionable material. See Watts, *Advanced Persistent Manipulators*, 11; Vilmer et al., *Information Manipulation*, 143; and *Boston Globe*, "No More Snuff Videos."

[369] Isaac and Kang, "Facebook Says It Won't Back Down."

[370] Isaac, "Why Everyone Is Angry at Facebook"; and Timberg, "Facebook's Powerful Ad Tools."

[371] Chin, "Facebook to Review Content Policies."

[372] FCW, "Can the IC Police Foreign Disinformation?"

[373] On Russia's past use of such irregular forces, often termed little green men, see USASOC, *Little Green Men*.

[374] Schelling, *Arms and Influence*, 2–6; Pape, *Bombing to Win*, 12; and Borghard and Lonergan, "Coercion in Cyberspace," 453 and 460.

IOs tailored to heighten those perceived costs may have clearly definable characteristics. Warnings that cyberattacks will soon cripple lifeline infrastructure systems, especially if paired with false but terrifying reports of infrastructure breakdowns, exemplify how adversaries might use coercive messaging to exploit the public's increased dependence on social media (and vulnerability to disinformation) in crises. Criteria to identify and block coercive content could be especially useful if IOs alone fail to produce US capitulation and adversaries thus begin combining them with exemplary cyberattacks to magnify public fear. Government agencies can identify options for such standards based on their understanding of how coercive campaigns might escalate. However, industry input will also be essential to help shape those standards so that content algorithms and monitoring teams can apply them at scale.

Government–industry discussions and supporting analysis will also be necessary to establish guidelines for collaboration in crises. It would be fatuous to expect TikTok to block Chinese messaging in a confrontation with the United States over Taiwan. And while other platforms are voluntarily collaborating with the US government to counter electoral interference, they are not subordinate components of the US national security system. They are profit-seeking companies that operate around the globe. Asking them to block coercive IOs and deliver timely presidential counter-messaging in a crisis would go far beyond their existing collaborative efforts. Quiet discussions on whether and how they might do so should begin as soon as possible.

Platforms, government agencies, and researchers should also examine how coordination mechanisms for use in crises would differ from those necessary against electoral interference. For example, given the importance of integrated, multi-platform action to defeat coercive campaigns, one promising option would be to establish an organization to coordinate cross-platform efforts and serve as a single point of contact for the government.[375] The National Security Telecommunications Advisory Committee (NSTAC) provides a model for such coordination. The NSTAC develops recommendations for the president "to assure vital telecommunications links through any event or crisis, and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture."[376] Analysis should go forward on how to borrow from the NSTAC and other models to help coordinate crisis operations by social media platforms and government agencies.

One promising opportunity to strengthen operational coordination lies in building on the Enduring Security Framework.[377] In *A Public, Private War*, a pioneering analysis of how the IT industry and government agencies can prepare for voluntary, combined operations for defense against cyberattacks, Jonathan Reiber explains that:

> The Enduring Security Framework will be a natural forum for this partnership to unfold. It is defensively focused and provides a mechanism for building relationships between the government and the private sector around a range of cybersecurity issues. It allows for a classified exchange of views; provides regular contact between the constituents through biannual senior leader meetings with companies and agencies; and builds ties between more junior employees in the public and private sectors. It also gives senior leaders an opportunity to build bonds of trust through one-on-one conversations.[378]

[375] Some major platforms such as Facebook and Twitter already share data to help each other block harmful content; this collaboration could provide a starting point for wider coordination. See Romm and Stanley-Becker, "Sprawling Inauthentic Operation."

[376] CISA, "About NSTAC."

[377] CISA, "Cross-Sector Enduring Security Framework."

[378] Reiber, *Public, Private War*.

Reiber also recommends the development of exercises and playbooks to facilitate voluntary government–industry collaboration. Electric utilities and the Department of Energy (DOE) have developed a set of such initiatives to strengthen their shared preparedness for cyberattacks on the grid. In November 2019, industry and government partnered in GridEx V to exercise their coordinated response to an especially disruptive attack. GridEx also enabled these partners to test the use of real-world response plans, explore possible additions to them, and apply their communications playbooks to deal with public fears that such an attack would create.[379] The Hamilton exercise series conducted by the financial services sector and the Department of the Treasury offers another model for strengthening industry–government coordination against cyberattacks.[380] Equivalent exercises and playbook development initiatives, designed to both build preparedness and identify gaps to remedy, could help bolster government–social media company collaboration against coercive IOs and combined cyber-information attacks.

Developing policies and protocols for emergency coordination between social media companies will be essential as well. In recent years, Russia has begun to conduct simultaneous IOs across multiple platforms. Research into such cross-platform operations has found that accounts sharing posts from one medium to another can obfuscate the source of their false or misleading claims (i.e., state-sponsored outlets) and that cross-platform analysis is necessary to understand the full extent of disinformation campaigns.[381] Greater coordination and information sharing between the companies themselves, as well as with government agencies, will be essential for defeating multi-platform operations in future crises.

Regulatory Initiatives

Even if social media companies significantly expand their collaboration with government on a voluntary basis, legislators and executive branch officials may still determine that the public remains unacceptably vulnerable to attack. Many researchers argue that stronger federal regulations are necessary to protect the American people from disinformation. Social media companies themselves are now calling for additional regulations to minimize the harmful user content they convey related to elections, terrorism propaganda, and hate speech.[382]

The regulations that currently govern social media emerged in a bygone threat environment. In 1996, when Congress amended the Communications Act of 1934, legislators did not anticipate the risks posed by sophisticated online disinformation and the possible need for regulations to help counter it. On the contrary: they believed that keeping the internet and internet-based communications systems free from government-imposed constraints would benefit democracy and the public. In adopting Section 230 of the Communications Decency Act, legislators found that the internet and other interactive computer services "have flourished, to the benefit of all Americans, with a minimum of government regulation." Accordingly, Congress made it the policy of the United States "to preserve the vibrant and competitive free market that presently exists" for such internet-based systems, "unfettered by Federal or State regulation."[383]

For countering disinformation (and, potentially, coercive IOs), Section 230 is most problematic because of its hands-off approach to internet content. With very limited exceptions, that section protects platforms from liability for the content that third parties (i.e., users) generate and spread across

[379] NERC, *GridEx V*, viii.

[380] FS-ISAC, "Exercises."

[381] Wilson and Starbird, "Cross-Platform Disinformation Campaigns."

[382] Zuckerberg, "Mark Zuckerberg: The Internet Needs New Rules"; and Bickert, *Charting a Way Forward*.

[383] Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. §230, (a)(4).

those platforms.[384] Section 230 allows platforms to voluntarily police such content and protects them from liability for doing so as long as they are acting in "good faith."[385] But nothing in the law requires them to remove foreign disinformation, no matter how disruptive in an election or regional crisis.

Section 230 has come under increased scrutiny because of an executive order on "Preventing Online Censorship" that seeks to clarify its protections. In particular, the May 2020 order states that Section 230 liability protections should not apply to platforms that "engage in deceptive or pretextual actions stifling free and open debate by censoring certain viewpoints," orders the Federal Communications Commission (FCC) to "expeditiously propose regulations" to clarify some of the Section 230 provisions, and directs the Federal Trade Commission to consider complaints about political bias and examine companies' content moderation policies.[386] However, the order has been called "unlawful and unenforceable" by a former inspector general at the Department of Justice and has been widely criticized as a threat to free speech.[387] Legal experts suggests it will "almost certainly" be challenged in court, delaying its eventual implementation.[388]

France, Germany, and other US allies have already enacted legislation that requires platforms to remove "hate speech" and other harmful content.[389] Recent studies have urged the United States to adopt other far-reaching measures. The Atlantic Council has drafted a comprehensive set of such recommendations. Options include requiring social media companies to (1) post accurate information about the sponsors of ads; (2) identify bots; and (3) disclose or remove inauthentic accounts.[390] Other studies call for further regulations to promote transparency and eliminate harmful content.[391] It might be possible to reorient many of these regulatory tools for use in crises and help the government require and guide social media operations to block coercive IOs. However, Congress has yet to consider changes in US code that could enable such drastic measures.

Legislators are instead considering far more modest and narrowly focused proposals. Two such regulatory initiatives have received significant congressional attention. The Honest Ads Act would mandate transparency for political ads online in a fashion similar to already-existing requirements for traditional broadcast and print media. Under the legislation, platforms would have to disclose who bought political ads, how much they cost, and to what audience they were targeted.[392] This proposal could help counter election interference but would be of little use against coercive campaigns.

The Deceptive Experiences To Online Users Reduction (DETOUR) Act could offer a more useful starting point to counter such threats. This act would prohibit Facebook and other major online platforms from relying on user interfaces that intentionally impair user autonomy, decision-making, or choice.[393] But this proposal

[384] 47 U.S.C. §230, (c)(1).

[385] 47 U.S.C. §230, (c)(2).

[386] Trump, *Executive Order on Preventing Online Censorship*.

[387] Thomsen, Robson, and Scarcella, "'Unlawful and Unenforceable'"; and Savage, "Trump's Order Targeting Social Media Sites."

[388] Romm and Dwoskin, "Trump Signs Order"; Human Rights Watch, "US: Trump Attacks Social Media Platforms"; and Coaston, "Trump's Social Media Executive Order."

[389] McAuley, "France Moves toward a Law"; *DW*, "Germany's Government Approves Hate Speech Bill"; and Reality Check Team, "Social Media."

[390] Fried and Polyakova, *Democratic Defense against Disinformation 2.0*, 18.

[391] See, e.g., Kornbluh and Goodman, *Safeguarding Digital Democracy*; Nye, "Protecting Democracy"; and Rosenberger and Salvo, *ASD Policy Blueprint*, 6.

[392] Honest Ads Act, H.R. 2592.

[393] Deceptive Experiences to Online Users Reduction Act, S. 1084.

focuses on deceptive practices by domestic users.[394] To defeat sophisticated IO attacks by Russia, China, or other adversaries, legislators may need to consider creating additional regulatory tools—ideally in collaboration with social media companies who might find new regulations helpful to address their own concerns.

Facebook has identified one such concern that could help build consensus on crisis-oriented regulations. Zuckerberg notes that "lawmakers often tell me that we have too much power over speech, and frankly I agree. I've come to believe that we shouldn't make so many important decisions about speech on our own."[395] Facebook is calling for regulations that would require platforms to develop and maintain systems to reduce harmful speech and set performance targets for those systems to achieve. The company also proposes that governments require platforms to "remove certain content beyond what is already illegal" and establish standards that platform content monitors can enforce "practically, at scale, with limited context about the speaker and content, without undermining the goal of promoting expression."[396]

Efforts to develop such regulations should consider including requirements to remove or block content that is part of a coercive IO campaign. A presidential declaration that such a campaign was underway might serve as a trigger for removal operations. However, in an era of truth decay, that declaration could itself prove divisive and reinforce public opposition to the president's crisis policies. Difficult work would also be required to identify the characteristics of coercive messaging and shape the filtering algorithms and monitoring rules that platforms can apply against sophisticated IO techniques and technologies. Still greater problems loom in establishing an overall US strategy to guide such regulatory efforts and structure the federal government to partner with industry in crisis operations.

Defending the Public *and* the Constitution

Blocking citizens' access to coercive enemy messages could risk compromising their rights to free speech. Rulings by the Supreme Court have given increasing substance and scope to First Amendment rights to receive information and ideas. These decisions cast doubt on the constitutionality of restricting citizen access to foreign speech, even if that speech promotes falsehoods or conveys enemy propaganda.[397]

The Supreme Court's 1965 ruling in *Lamont v. Postmaster General* helps frame the nature of this challenge. The court struck down a federal statute requiring the postmaster general to "detain communist political propaganda" that is "printed or otherwise prepared in a foreign country." The court found that restricting the flow of such propaganda violated the recipient's rights to the "'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment." More broadly, the government could not "control the flow of ideas to the public" even from hostile foreign governments advocating upheaval of the government.[398]

On the basis of Lamont and related free speech decisions, including *United States v. Alvarez* (2012), measures to block deepfakes or other types of adversary disinformation during regional crises would seem of dubious constitutionality.[399] But significant uncertainties persist as to how the First Amendment applies to internet-delivered

[394] Fried and Polyakova, *Democratic Defense against Disinformation 2.0*, 11.

[395] Zuckerberg, "Mark Zuckerberg: The Internet Needs New Rules."

[396] Bickert, *Charting a Way Forward*, 9 and 17.

[397] Thai, "Right to Receive Foreign Speech."

[398] Thai, "Right to Receive Foreign Speech," 280–282.

[399] On Alvarez, see Blitz, "Lies, Line Drawing, and (Deep) Fakes."

false speech.[400] These uncertainties could be especially great with regard to IOs designed to create mass fear and public disorder. As the court noted in *Schenck v. United States* (1919), the First Amendment would not protect a speaker "shouting fire in a theatre and causing panic."[401] And in *Chaplinsky v. New Hampshire*, the court ruled that free speech law does not protect the use of "fighting words—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace."[402] Coercive messaging designed to incite panic, either alone or in conjunction with casualty-inducing cyberattacks on US infrastructure, could become the focus of narrowly targeted policy and planning initiatives for use in escalating crises.

Analysts might also explore options for specialized, emergency-oriented authorities to defeat coercive campaigns. The prerequisite to do so is to partner with social media companies to clarify how these authorities would be employed and to develop playbooks and exercises to prepare for their execution in a crisis.

Section 706 of the Communications Act anticipates precisely the dire circumstances that could precede a coercive IO attack. "Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States," Section 706 provides powers that could be extraordinary useful against disinformation in a crisis.[403] Under the emergencies described by the act, the president may:

- "direct that such communications as in his judgment may be essential to the national defense and security shall have preference or priority with any carrier subject to this chapter;"
- "suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States as prescribed by the Commission;" and
- "authorize the use or control of any such facility or station [for wire communications] and its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners."[404]

However, Congress enacted Section 706 within a month after the attack on Pearl Harbor and could not have envisioned the evolution of communications technology that has taken place in the decades since. Before considering how the president would exercise these emergency authorities in a crisis, it will therefore be necessary to clarify whether and how they should be applied to the internet and the social media platforms that ride on it.

Congressional proceedings have documented some discussion regarding whether and how Section 706 applies to the internet. Senate hearings on protecting US cyber infrastructure in 2010 included testimony from then DHS deputy undersecretary Philip Reitinger, who concedes that Section 706 and other potential authorities are "older or not specifically designed for this case." Yet, Reitinger asserted that Section 706 and "other legal authorities" provide the federal government with the authority to direct private sector response to a cyber emergency.[405] Similarly, the Senate committee's report concluded that Section 706 "gives the President the authority

[400] Chemerinsky, "False Speech."

[401] Quoted in Thai, "Right to Receive Foreign Speech," 283.

[402] Blitz, "Lies, Line Drawing, and (Deep) Fakes," 76.

[403] The emergency provisions granted by Section 706 of the Communications Act are found in §606 of US Code Title 47, and secondary sources sometimes refer to one or the other. See War Powers of President, 47 U.S.C. §606.

[404] 47 U.S.C. §606, (a), (c), and (d).

[405] *Hearings on Protecting Cyberspace as a National Asset*, Reitinger statement.

to take over wire communications in the United States and . . . shut a network down."[406]

More recently, Jessica Rosenworcel, an FCC commissioner, determined that "if a sitting President wants to shut down the internet or selectively cut off a service, all it takes is an opinion from his Attorney General that Section 706 gives him the authority to do so."[407] Former FCC chair Tom Wheeler suggests that a president may not even need the attorney general's opinion to invoke the powers.[408] However, these assessments and interpretations of Section 706 focus on the president's authority to shut down internet networks in response to a cyberattack. They do not even begin to consider how the president's authority may apply to content online in an emergency. A better approach would be to have Congress clarify the extent to which this section should now be applied to social media platforms. As Rosenworcel suggests, "the time has come for a modern assessment of this language, what it means, and what it should mean in the digital age."[409]

Emergency authorities in other realms provide a model from which to borrow for IO defense. For example, to help counter cyberattacks and other threats to the US electric grid, Congress amended the Federal Power Act in 2015 to grant the secretary of energy new powers in emergencies. In particular, Section 215A of the act gives the secretary the authority to issue orders for "emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure during such emergency."[410]

That grant of power is vast and—for electric utility owners and operators—potentially problematic (especially if emergency orders were to inadvertently compromise safe and reliable control of the grid). Yet, Congress adopted the amendment with industry support. Legislators made the amendment more acceptable by including the provision that, "to the extent practicable," the secretary will consult with power companies and other grid stakeholders before issuing emergency orders.[411] DOE has also been collaborating with the Electricity Subsector Coordinating Council to develop "template orders" that the department can modify for use in future grid security emergencies. DOE and its industry partners have begun exercising the issuance and execution of such orders and drawing valuable lessons learned from doing so.[412] Equivalent initiatives by social media platforms and government agencies, guided by the need to uphold the First Amendment, could help provide "arrows in the quiver" for use *in extremis* against coercive campaigns.

But such initiatives must be narrow in scope and used only under the most extraordinary (and carefully predefined) circumstances. If emergency measures enable adversaries to claim that the government is abandoning the Constitution and trampling on the rights of US citizens, defeating their IO messaging will be all the more difficult. Already, disinformation campaigns surrounding the COVID-19 pandemic include allegations that the government is censoring social media. [413] China and Russia are certain to make similar claims if the government blocks access to their messaging in future crises. We need to not only account for such tactics but do so in ways that uphold our values when they are in greatest need of defense.

[406] US Senate Committee on Homeland Security and Government Affairs, *Protecting Cyberspace*.

[407] Rosenworcel, remarks to the State of the Net Conference, 4.

[408] Wheeler, "Could Donald Trump Claim a National Security Threat?"

[409] Rosenworcel, remarks to the State of the Net Conference, 5.

[410] Critical Electric Infrastructure Security, 16 U.S.C. §824o–1, (b)(1).

[411] 16 U.S.C. §824o–1, (b)(3).

[412] NERC, *GridEx V*, 3.

[413] NIC, *Foreign Threats to the 2020 US Federal Elections*, 4.

Counter-messaging

To defeat coercive IO campaigns, the government will need counter-messaging plans and capabilities that can function even in the face of declining public trust in US leaders and broader truth decay. A foundation to develop these capabilities lies in recent FEMA and DHS initiatives to counter disinformation during disasters. FEMA now sets up rumor-control pages for hurricanes in an attempt to dispel common misconceptions that could cause mass panic or social unrest. During Hurricane Florence (September 2018), for example, FEMA reassured residents that the Brunswick Nuclear Power Plant was not at risk of failure or malfunction due to nearby flooding.[414] FEMA set up similar rumor-control pages for hurricanes Michael, Harvey, Irma, and Maria, as well as the California wildfires in summer 2019. Most recently, FEMA established a rumor-control page to address misinformation surrounding COVID-19.[415] Researchers should analyze options to repurpose and scale up these initiatives to combat coercive operations.

FEMA and DHS are also developing new ways to use social media to convey government messages during disasters. While more traditional television emergency broadcast systems still offer important means of communication in such events, emergency managers at all levels of government use social media platforms to connect with and provide information for citizens during crises.[416] Other disaster response partners have also begun to incorporate social media into their public communications plans and response operations.[417]

A recent focus group–based study by RAND found that informing the American public about the foreign origins of disinformation can bolster the effectiveness of government public service announcements (PSAs) to counter them. The study found that PSAs are most likely to be effective if they concentrate on explaining general threats and avoid discussing any specific piece of online content. Maintaining a general focus can reduce the likelihood that the public will view a PSA, at least in the short term, as pushing a partisan agenda or targeting a group of Americans.[418] In a coercive campaign, however, Beijing and Moscow may offer detailed, crisis-specific threats and falsehoods about US allies, while also doing everything possible to stoke partisan divisions over US policy.

Crafting and delivering counter-messaging with sufficient speed will present additional challenges. As Beijing and Moscow seek to achieve first-mover advantages at the outset of an IO campaign and sustain those advantages with fresh messaging as the crisis evolves, rapid US responses will be vital. The damage that delays can cause was on full display during the January 2018 false alarm that Hawaii faced an imminent ballistic missile strike. In the 38 minutes it took for authorities to disavow the alert message and reassure the public, life on Oahu was thoroughly disrupted by the large-scale movement of a panicked population.[419] Delays in responding to Chinese and Russian threats of attacking in a crisis could cause equivalent problems. Crafting messages to quell the fears created by such threats will also entail far greater difficulties than in the Hawaii incident, especially if those nations are indeed poised to strike US targets unless the president yields.

[414] FEMA, "Hurricane Florence Rumor Control."

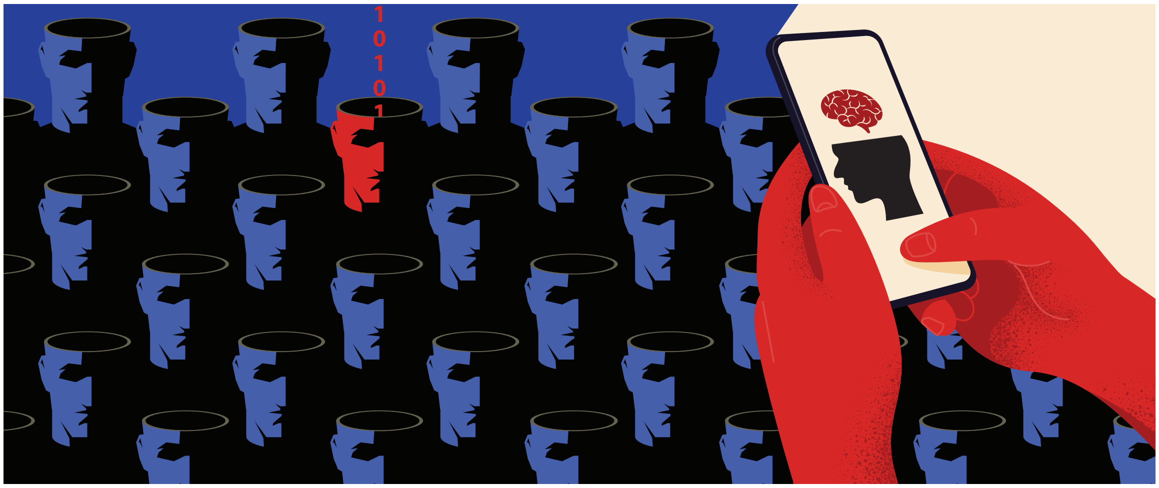
[415] FEMA, "Coronavirus Rumor Control."

[416] SMWGESDM, *Countering False Information*.

[417] See, e.g., FEMA, "Social Media and Emergency Preparedness"; and Ogrysko, "Recent Hurricanes."

[418] Posard, Reininger, and Helmus, *Countering Foreign Interference*, 36.

[419] Benjamin and Simon, "How Fake News Could Lead to Real War," 6.



Tactics, Techniques, and Procedures for Coercive Information Operations

The scale and severity of the information operations (IO) threat to the United States reflects not only underlying domestic vulnerabilities to foreign influence but also technical advances that will help opponents exploit these vulnerabilities. Ongoing Chinese and Russian campaigns to undermine US democracy are employing new tools and technologies to convey disinformation. Both nations are also developing new tactics and operational procedures to shape public perceptions. As the US builds a defensive strategy against coercion, policymakers should anticipate how China and Russia may repurpose and refine these tactics, techniques, and procedures (TTPs) to drive White House decision-making.

US defensive efforts must also account for emerging IO technologies. China is accelerating its development of artificial intelligence (AI) in ways that enable it to conduct personalized IOs against the US public and individual decision-makers and to employ deepfakes and other deceptive tools that will make today's versions seem primitive. Russia is pursuing such capabilities as well, along with new TTPs for search engine optimization (SEO), the use of botnets and other infrastructure within the United States and around the globe, and additional means to bolster the effectiveness of IO campaigns and evade defenses against them.

Chinese and Russian information doctrines place a premium on coercing adversaries without needing to employ force. The analysis that follows examines how technological advances can help them conduct IO-only campaigns against the United States, and the defensive implications for the US and its security partners. But Beijing and Moscow could use these same advances to reinforce the psychological impact of cyber-induced punishment. Subsequent portions of the study explore their doctrines for conducting combined attacks and the additional challenges for developing US and allied strategies against coercion.

Chinese IO Doctrine and Recent Campaigns

Soon after President Xi Jinping took power in 2013, he stated that "On the battlefield of the Internet, whether we can withstand and win is directly related to our country's ideological security and political security."[420] Chinese plans and capabilities for coercive campaigns fall within this broader use of IOs to advance Beijing's political and security goals. The overwhelming focus of Chinese

[420] Kinetz, "Army of Fake Fans."

operations on social media is to keep the Communist Party in power and maintain popular support for continued party rule. The Chinese government is engaged in a sustained, technically sophisticated campaign to shape the beliefs of its own populace and prevent them from receiving views, via social media or other means of communication, that run counter to the government's narrative. The "Great Firewall" plays an especially important and effective role in controlling the information that the Chinese people receive from Western sources.[421] The government also provides a constant stream of its own content to achieve these political objectives and reinforce public support for party rule. One recent study estimated that the government fabricates and posts about 448 million comments on Chinese social media platforms per year. Most of these posts espouse positive, pro-China viewpoints and narratives.[422]

Chinese IOs abroad typically focus on shaping global narratives about China that circulate outside its borders, especially among targeted communities of interest such as ethnic and religious minority groups and native Chinese speakers in the United States and other nations.[423] China views the "overseas Chinese" population as an important constituency to target for influence.[424]

Some of this outreach occurs through legacy media. For example, a 2012 article in the People's Liberation Army's (PLA) *Military Correspondent* hailed the work of a Texas-based Chinese-language newspaper that conformed to Communist Party narratives, noting that "one out of four ethnic minorities in the United States relies upon media in their mother tongue to get information and express their feelings, and the influence of these media surpasses that of the media of the country in which they reside."[425]

Social media provides a means to reach a broader US audience.[426] As noted in the section on underlying US vulnerabilities, China is increasingly using US social media platforms, which are largely banned within China itself, to manipulate foreigners' perceptions of China-related issues.[427] Chinese IOs on Western media platforms like Facebook and Twitter have traditionally been "clumsy," in large part because of their inexperience with these platforms.[428] However, this is rapidly changing. China is now "increasingly comfortable on those Western platforms, just like it is increasingly targeting a wider audience than just its diasporas, as demonstrated by the growing number of Chinese propaganda outlets published in a number of foreign languages (*Global Times*, *China Daily*, CGTN, Xinhua, etc.)."[429] Beijing is also intensifying its use of social media against Taiwan, South Korea, and other US security partners in the region to foment domestic political discord and generate support for China's policy preferences.[430]

IOs surrounding the 2019 protests in Hong Kong, in which China conducted coordinated social media campaigns to influence observers, provide a case in point.[431] Hong Kong–related content was

[421] This includes an outright ban on the use of Google, Facebook, and YouTube, among others. See Nemr and Gangware, *Weapons of Mass Distraction*, 21.

[422] King, Pan, and Roberts, "Chinese Government Fabricates Social Media Posts," 484.

[423] Mazarr et al., *Hostile Social Manipulation*, 162.

[424] Heath, "Beijing's Influence Operations."

[425] Baozhu, " 'Chinese Times' [Huaxia Shibao] Builds a Bridge," 54, quoted in Mazarr et al., *Hostile Social Manipulation*, 161.

[426] Insikt Group, *How China Exploits Social Media*.

[427] Rosenberger and Cooper, "Time for U.S. to Start Pushing Back."

[428] Vilmer and Charon, "Different Ways of Information Warfare."

[429] Vilmer and Charon, "Different Ways of Information Warfare."

[430] Corcoran, Crowley, and Davis, *Disinformation Threat Watch*.

[431] Twitter, in particular, suspended Chinese state-backed accounts that were "behaving in a coordinated manner" to amplify pro-China content regarding the protests. Similarly, Facebook removed a number of accounts and pages for "coordinated inauthentic behavior" on similar issues. See Twitter,

also censored on TikTok, a Chinese-owned app that is increasingly popular in the United States.[432] China could use similar censorship tactics to shape narratives in future conflicts involving the United States.[433]

Chinese IOs surrounding the COVID-19 pandemic also indicate a shift toward influencing US and other Western audiences. As China began reducing its COVID caseload, the country launched a "massive campaign to change the global narrative and perception of the pandemic."[434] To do so, the Chinese Communist Party used proxy accounts and bots to "disseminate false stories on numerous social media platforms around the world" and had government officials publicly participate in sharing disinformation online.[435] In particular, Chinese IOs sought to create doubts about the virus' origin and create the perception that China handled the virus well, attempting to validate its authoritarian system compared with democratic countries that were struggling to contain the virus.[436] China also pressured Western countries to report favorably on Chinese efforts to contain the virus and was able to coerce the European Union (EU) into toning down criticism of the country's COVID-related disinformation operations.[437]

A State Department report from April 2020 notes that Chinese IOs surrounding the coronavirus were in line with similar efforts from Russia and Iran, all directed against the United States. Among the common narratives, many of which overlap: the coronavirus is an American bioweapon; the United States is seeking to benefit from the crisis; the virus did not originate in China; US troops are actually responsible for spreading the virus; China's response was great while the United States' response was negligent; China, Russia, and Iran are managing the crisis well; and the US economy will fail because of the crisis.[438] According to press accounts of the State Department's report, Chinese and Russian messaging began converging in February 2020 and came from both state-run media outlets and official government sources themselves.

China has also been adapting tactics traditionally associated with Russian disinformation. Historically, both countries' approaches have been fairly distinct. Rob Joyce, the National Security Agency's (NSA) senior cybersecurity advisor, sees "Russia as the hurricane. It comes in fast and hard. China, on the other hand, is climate change: long, slow, pervasive."[439] However, China's recent IOs—especially surrounding COVID—are "a clear departure from Beijing's previous disinformation tactics," and signal its "increasingly aggressive approach to managing its image internationally."[440] In particular, China is borrowing Russian TTPs that emphasize the propagation of multiple conflicting theories to create confusion, amplification of conspiracy websites, and coordinated use of state-backed media and official government social media accounts to boost disinformation.[441]

These borrowed approaches could be useful for coercive IOs against the US public, especially for inciting fear and distrust of government. A Chinese

"Information Operations Directed at Hong Kong"; and Gleicher, "Removing Coordinated Inauthentic Behavior from China."

[432] Harwell and Romm, "TikTok's Beijing Roots."

[433] The ODNI also noted that China is capable of cyberattacks against targets in the United States to "censor or suppress viewpoints it deems politically sensitive." See *Hearing on Worldwide Threat Assessment*, Coats statement, 7.

[434] Niquet, "China's Coronavirus Information Warfare."

[435] Ha and Cho, "China's Coronavirus Disinformation Campaigns."

[436] Niquet, "China's Coronavirus Information Warfare."

[437] Ha and Cho, "China's Coronavirus Disinformation Campaigns."

[438] Woodruff Swan, "Russian, Chinese and Iranian Disinformation Narratives."

[439] Quoted in Vilmer and Charon, "Different Ways of Information Warfare."

[440] Allen-Ebrahimian, "China Takes a Page."

[441] Allen-Ebrahimian, "China Takes a Page"; and Kliman et al., *Dangerous Synergies*.

operation in March 2020 tried to induce panic by convincing the US public that the Trump administration was about to lock down the entire country. The messages appeared across multiple social media platforms, and in some cases as text messages. The US intelligence community determined that "Chinese operatives helped push the messages across platforms," and that the techniques those operatives used are novel and "alarming."[442]

Some officials believe China merely helped amplify—rather than create—these messages. To do so, it used TTPs typical of Russian operatives, such as "creating fake social media accounts to push messages to sympathetic Americans, who in turn unwittingly help spread them."[443] To rapidly spread disinformation beyond its original sources, this Chinese campaign also leveraged the trending and algorithm functions described in the section on how coercion works.

Chinese military doctrine provides insights into how the PLA might use such platforms and other means of communication to influence US decision-making in a crisis. PLA military theorists have argued that information campaigns can degrade adversary situational awareness and undermine enemy intelligence collection efforts, making it "hard for people to distinguish the true from the false and thus more easily drive [the enemy] into a trap."[444] These operations can also perplex, confound, divide, and weaken an opponent's military forces and civilian population.[445] As stated in a 2014 PLA-published article:

> Cyber media warfare is a kind of combat operations with the Internet as the platform. [. . .] Targeted information infiltration is made through the Internet media for influencing the convictions, opinions, sentiments, and attitudes of the general public so as to effectively control the public opinion condition, shape strong public opinion pressure and deterrence over the adversary, and win an overwhelming public opinion posture for one's own side.[446]

China's Three Warfares strategy lays out how the PLA will achieve such effects. Under this strategy, China will coordinate the use of three types of warfare (psychological, public opinion, and legal) to establish "discursive power" over an adversary—that is, the power to control perceptions and shape narratives that support Chinese interests and undermine those of the adversary.[447]

Psychological warfare is most closely tied to Chinese plans and capabilities to influence adversary behavior in an intensifying crisis. Psychological warfare uses propaganda, deception, and coercive threats to affect the adversary's decision-making, while also countering adversary psychological operations.[448] Chinese military writings also emphasize the value of psychological warfare to confuse enemy decision-making."[449]

The Three Warfares strategy also reflects a broader Chinese vision of what IOs encompass and their primacy in future conflicts. The PLA is developing a new psychological warfare concept called "cognitive domain operations" that reflects the crucial importance of information in modern war. These complex IOs aim to influence an adversary's cognitive functions across the entire spectrum of conflict, from public sentiment in peacetime to

[442] Wong, Rosenberg, and Barnes, "Chinese Agents Helped Spread Messages."

[443] Wong, Rosenberg, and Barnes, "Chinese Agents Helped Spread Messages."

[444] Peilin and Xue, "On 'Media Decapitation.' "

[445] Mazarr et al., *Hostile Social Manipulation*, 130.

[446] Zhengzhong, "Strengthening Cyber News Media in Wartime," trans. Mazarr et al., *Hostile Social Manipulation*, 130.

[447] Costello and McReynolds, *China's Strategic Support Force*, 28.

[448] OSD, *Military and Security Developments 2020*, 161.

[449] Engstrom, *Systems Confrontation and System Destruction Warfare*, 71–72.

decision-making in open war.[450] In particular, we should expect the PLA to conduct psychological attacks [心理进攻] to confuse US and allied decision-makers and (according to a Chinese source quoted by a 2018 RAND report) "make the enemy realize they are facing consequences that cannot be afforded so as to either prevent them from taking actions or stop actions in place."[451]

All such efforts will benefit from the application of AI technologies. China is organized, resourced, and determined to become the global leader in AI and is using it to strengthen its military capabilities and influence campaigns at home and abroad.[452] Beijing is already employing AI tools to help monitor and coerce its own citizens, including Uighur minorities.[453] Chinese companies are exporting AI tools and surveillance technologies to nations across Asia, the Middle East, and Africa, which may create opportunities for Beijing to collect intelligence on the senior officials and business leaders in those countries.[454] AI will also help China use such personal information (including data on US officials stolen in the US Office of Personnel Management [OPM] hack and subsequent operations) to target and convey messaging. It has already tested the use AI-enabled IOs to influence Taiwan's 2021 elections.[455] Those same capabilities will help China conduct coercive IOs against the US and its allies in future crises.

Russian IOs and Doctrine for Coercion

Christopher Maier, acting assistant secretary of defense for special operations and low-intensity conflict, testified to Congress in March 2016 that "Russia sees the information sphere as a key domain for modern military conflict. Russia has prioritized the development of forces and means for information confrontation in a holistic concept for ensuring information superiority since at least the 1920s . . . and wages this struggle for information dominance during peacetime and armed conflict with equal intensity," using "information-technical, information-psychological," and other means.[456]

Efforts to manipulate US elections reflect these deep historical roots. Since the early days of the Soviet Union, Soviet leaders have engaged in such manipulation.[457] The Soviets also conducted a range of other IOs to discredit the United States and weaken its alliances abroad, including a campaign alleging that US agencies created the AIDS virus.[458] However, modern technologies provide Russia with new and vastly improved means to exert such influence. The 2017 US Intelligence Community Assessment found that in the 2016 election, Russian activities demonstrated a "significant escalation in directness, level of activity, and scope of effort compared to previous operations," reflecting years of investment in IO capabilities.[459] Improvements in Russian TTPs included: (1) high volumes of disinformation across multiple channels, at high speeds; (2) the merging of overt and covert operations; (3) the use of bots, other automated accounts, and paid "trolls"; and (4) efforts to create real-life outcomes (e.g., getting people to attend events).[460]

[450] Beauchamp-Mustafaga, "Cognitive Domain Operations," 24; and Riikonen, "Decide, Disrupt, Destroy," 130.

[451] Engstrom, *Systems Confrontation and System Destruction Warfare*, 15 and 71.

[452] NSCAI, *Final Report*, 25.

[453] Harwell and Dou, "Huawei Tested AI Software."

[454] Harsono, "China's Surveillance Technology."

[455] NSCAI, *Final Report*, 48.

[456] *Hearing on Disinformation in the Gray Zone*, Maier, Tipton, and Sullivan statement.

[457] Shimer, *Rigged*.

[458] Radin, Demus, and Marcinek, *Understanding Russian Subversion*, 7.

[459] ODNI, *Assessing Russian Activities*, ii, 2. Similarly, the Senate Intelligence Committee called it "the latest and most sophisticated example of Russia's effort to undermine the nation's democracy through targeted operations." See SSCI, *Russian Active Measures, Vol. 2*, 11.

[460] SSCI, *Russian Active Measures, Vol. 2*, 6–20. For more on the results of Russia's efforts to create real-world impacts, see

This section examines still further improvements in IO tactics, techniques, and technologies.

The content of Russian messaging also represented new levels of sophistication and targeting acumen.[461] For example, Russia's Internet Research Agency (IRA) prepared for its 2016 election operations by creating fake US personas, building a large online following, and sending personnel to the United States on an "intelligence-gathering mission" to take photographs that would lend legitimacy to their online profiles.[462] US defensive plans and capabilities to counter Russian coercion in future crises should anticipate the use of all such TTPs.

US plans must also account for ongoing improvements in Russian IO capabilities and further efforts to corrode the US public's confidence in government. Federal Bureau of Investigation (FBI) Director Christopher Wray warns that Russia works "365 days a year" to "sow divisiveness and discord, and undermine Americans' faith in democracy."[463] Russian operatives began conducting spearphishing attacks immediately after the 2016 election to obtain material for follow-on, microtargeted IOs.[464] The National Intelligence Council (NIC) found that during the lead-up to the 2020 presidential election, Russia updated its interference operations to denigrate President Biden's candidacy while supporting former president Trump.[465]

The NIC report also found that throughout the 2020 election cycle, Russian online influence actors sought to advance Moscow's long-standing goals of undermining confidence in US election processes and increasing sociopolitical divisions among the American people. The Lakhta Internet Research (LIR) troll farm, which is the new name for the IRA, remains particularly active in such operations. According to the NIC, "LIR used social media personas, news websites, and US persons to deliver tailored content to subsets of the US population." LIR also "established short-lived troll farms that used unwitting third-country nationals [. . .] to propagate these US-focused narratives, probably in response to efforts by US companies and law enforcement to shut down LIR-associated personas."[466] We should expect Moscow (and, perhaps, Beijing) to use similar tactics to convey coercive messaging in future crises, especially if US agencies and social media partners strengthen their plans and capabilities to counter an adversary's use of its own IO infrastructure.

The multiplicity of Russian IO campaigns and their means of exerting influence continue to grow as well. Russia already uses a very broad range of TTPs to conduct these campaigns. As noted by the State Department's Global Engagement Center:

> Russia's disinformation and propaganda ecosystem is the collection of official, proxy, and unattributed communication channels and platforms that Russia uses to create and amplify false narratives. The ecosystem consists of five main pillars: official government communications, state-funded global messaging, cultivation of proxy

Mueller, *Investigation into Russian Interference*, Vol. I.

[461] SSCI, *Russian Active Measures, Vol. 2*, 20–22; *United States v. Internet Research Agency* (18 U.S.C. §§ 2, 371, 1349, 1028A), 14; and ODNI, *Assessing Russian Activities*, ii.

[462] By the end of the 2016 election, IRA accounts had the ability to reach millions of US citizens. See Mueller, *Investigation into Russian Interference*, Vol. I, 14–15 and 22. IRA "specialists" were focused on mimicking the behavioral patterns of the American people, including posting content based on US time zones and observing US holidays. See *United States v. Internet Research Agency*, 14.

[463] Williams, "FBI Chief Wray: Russia Works to Undermine American Democracy."

[464] ODNI, *Assessing Russian Activities*, 5; and SSCI, *Russian Active Measures, Vol. 2*, 8.

[465] NIC, *Foreign Threats to the 2020 US Federal Elections*, i.

[466] NIC, *Foreign Threats to the 2020 US Federal Elections*, 4.

> sources, weaponization of social media, and cyber-enabled disinformation.[467]

Rather than focus on a single platform or unity of messaging, Russia's ecosystem "allows for varied and overlapping approaches that reinforce each other even when individual messages within the system appear contradictory."[468] This allows the Kremlin to fine-tune false narratives to specific audiences and use proxies to provide plausible deniability, and it also allows the pillars to reinforce each other for "multiplier effect."[469]

Most recently, new data has emerged on the "Secondary Infektion" operation, which uses very different TTPs than the IRA or GRU (the Main Intelligence Directorate of the Russian Armed Forces). Secondary Infektion employs a vastly greater range of platforms to post disinformation. Indeed, researchers at Graphika have determined that no other operation from any country comes close to matching that diversity.[470] The operation specializes in impersonating Western leaders and forging documents. It has produced fake tweets, letters, and blogs from former US secretary of state Mike Pompeo, senator Marco Rubio, and senior officials of US allies.[471]

This campaign suggests two implications for developing US strategies against coercion. First, we can expect that Russia will employ a "kitchen sink" approach to using social media and other communication systems to shape US behavior and that—as in the case of Secondary Infektion—we risk being surprised after the fact by the diversity of attack vectors Russia or other adversaries could employ. *Every* means of communication on which the public and US officials will rely in a crisis must be considered a target for possible exploitation.

Second, Russia will likely impersonate US leaders and purvey fake messages from them to corrode public confidence in US crisis decision-making and weaken support for defending US allies and interests. Russia was not responsible for the 2020 seizure of the Twitter accounts for presidential candidate Joe Biden and other high-profile users.[472] But at a minimum, Russia, China, and other potential adversaries are surely studying how hackers gained control of those accounts and are developing plans to acquire and exploit equivalent access in future crises.

Acquiring control of verified accounts could greatly increase the effectiveness of coercive IOs. The Secondary Infektion campaign only created fake screenshots of tweets purporting to be from their victims' accounts. If viewers were willing and able to check the victim's actual Twitter feed, they could see that the tweets were fake. In contrast, during the Twitter hack, the attackers actually gained access to verified accounts and tweeted from them. The hackers' bitcoin scam was tactically clumsy in other respects and produced red flags that helped Twitter quickly respond. But more sophisticated operations that leverage account access could convey convincing disinformation. In future crises, we should expect adversaries to seek control of the president's Twitter account (and, potentially, leadership accounts on other platforms) to convince the public and senior officials that the president supports backing down, or convey other information designed to sow confusion and loss of confidence in US crisis management.

The content of Secondary Infektion messaging carries further implications for US defensive strategies, especially in regional crises involving US security partners. The campaign most frequently delivered fake documents and other types of disinformation to portray Ukraine as a failed state and unreliable security partner. Next most frequent were IOs depicting the United States and NATO

[467] DOS, *GEC Special Report*, 3.

[468] DOS, *GEC Special Report*, 5.

[469] DOS, *GEC Special Report*, 5.

[470] Nimmo et al., *Secondary Infektion*, 9.

[471] Nimmo et al., *Secondary Infektion*, 5–6.

[472] Frenkel et al., "Brazen Online Attack."

as aggressive, with third place going to disinformation aimed at convincing viewers that Europe is weak and divided.[473] Opponents can seek to coerce US behavior by reducing the perceived benefits of defending US allies and interests. Russia will likely seek to convince US legislators, their voters, and other target audiences that US regional partners are corrupt or otherwise not worth defending and have interests that conflict with what is best for Americans. US plans for content blocking and counter-messaging should account for these likely attack vectors, ideally in coordination with the regional partners in Russia's crosshairs.

Such defensive initiatives must go forward hand-in-hand with measures to prevent Russia from influencing US elections (and their aftermath, if contested). Just as Russia will leverage election interference TTPs for use in crises, so too should the United States apply its improved election defense capabilities for preparedness against coercion. The same is true of the Kremlin's continued efforts to weaken US society and corrode public confidence in democratic governance. In early 2020, for example, Russia launched a campaign via thousands of false media personas to provide "evidence" that US agencies created the novel coronavirus.[474] Such campaigns to discredit the US government and widen societal divisions help the Kremlin prepare the battlefield for future coercive IOs.

In addition to COVID-related disinformation, Russia is continuing its attempts to influence US elections and widen societal divisions in the country. US intelligence officials warned that Russia was attempting to stoke these divisions and even incite violence in the United States ahead of the November 2020 elections. Reports suggested they were amplifying inflammatory content to specific audiences that might take violent action in response, in hopes of fostering "a sense of chaos" in the United States.[475] Russia and other adversaries could use similar tactics in future crises to exacerbate domestic tensions and put pressure on US decision-makers to resolve the conflict.

Russian doctrine for coercing enemy behavior provides a detailed framework for incorporating such TTPs. Leading Russian military theorists note that "in the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory."[476] The Kremlin is prepared to employ IOs across all phases of a crisis, including escalation to open warfare. However, Russian military publications stress that it may be possible to achieve victory through IOs alone, thereby avoiding the costs and escalatory dangers entailed in employing destructive cyber or kinetic attacks.

The 2010 version of the *Military Doctrine of the Russian Federation* stated that modern conflicts feature "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force. . . ."[477] Subsequent military writings emphasize that the early use of IOs in a crisis can enable Russia to prevail in "new-generation warfare" well before any destructive attacks begin by demoralizing and deluding the opponent, organizing domestic political opposition to the opponent's policies, and other efforts.[478]

To achieve these disruptive effects against the United States and—ideally—prevail in a crisis

[473] Nimmo et al., *Secondary Infektion*, 5.

[474] *BBC News*, "Coronavirus: Russia Denies Spreading US Conspiracy"; and Emmott, "Russia Deploying Coronavirus Disinformation."

[475] Barnes and Goldman, "Russia Trying to Stoke U.S. Racial Tensions."

[476] Chekinov and Bogdanov, "New-Generation War," 15–16, trans. Connell and Vogler, *Russia's Approach to Cyber Warfare*, 5.

[477] Medvedev, *Military Doctrine*, trans. Carnegie Endowment.

[478] Pirumov, *Informatsionnoe Protivoborstvo*, 3, trans. Pomerantsev and Weiss, *Kremlin Weaponizes*, 3 and 12; Adamsky, *Cross-Domain Coercion*, 24 and 36–37; and Chekinov and Bogdanov, "Art of War in the Early 21st Century," trans. Connell and Vogler, *Russia's Approach to Cyber Warfare*, 4; and Connell and Vogler, *Russia's Approach to Cyber Warfare*, 3–4.

without firing a shot, Russia will use specialized cognitive techniques to "deceive the victim, discredit the leadership, and disorient and demoralize the population and the armed forces."[479] In particular, Russian IOs are designed to exercise "reflexive control" over an opponent. Reflexive control "causes a stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary's perceptions of the situation decisively."[480]

To shape US leadership and public perceptions in this manner, Russia can draw on all the TTPs it is employing and continuously refining to influence US elections and shape public perceptions. The Kremlin is also developing additional options for peacetime operations that could be useful in future crises, including false-flag operations. Russian hackers have already infiltrated Iran's cyberwarfare unit. The NSA warns that this infiltration may be designed to enable Russia to launch attacks that appear to be coming from Tehran.[481] Russia could conduct such false-flag operations to inflame US–Iranian crises in the Persian Gulf or other Middle Eastern flash points. But Russia could also employ these capabilities in its own confrontations with the United States to shift the blame for Russian IOs to third parties or seek other advantages by complicating US attribution efforts. The FBI and other US government agencies are strengthening their ability to identify the perpetrators of disruptive cyberattacks and overcome adversary efforts at deception. The United States should do the same to facilitate attribution of IOs.

Microtargeting at Scale

Chinese and Russian IOs are only beginning to exploit AI and other technological advances that are underway. US defensive strategies need to account for the emerging capabilities of both nations to conduct coercive campaigns with extraordinary precision and speed, and on an unprecedented scale, as a crisis unfolds.

Such campaigns will be fundamentally different from the ones that have so often failed in past confrontations. Mass leafleting, radio and television broadcasts, and other traditional means of conducting influence operations follow a "one size fits all" approach that precludes opportunities to exploit the personal biases and proclivities of those they reach. Most traditional IO technologies also require fairly close proximity to the target audience. With the worldwide web, and the direct but remote access to individuals it provides, adversaries can now conduct coercive campaigns against US citizens that would have been impossible in decades past.[482] China and Russia are advancing their TTPs in two realms that are especially significant for assessing (and countering) threats of coercive IOs: collection of data to exploit for tailored messaging, and specific AI tools to help plan and execute IO campaigns against the US public, crisis decision-makers, and those who influence them.

Gathering Data for Customized Manipulation of Fears and Beliefs

Cyber-based espionage is a critical enabler to customize IOs and enhance their effectiveness.[483] By capturing personal information posted by social media users, penetrating government and industry databases on US citizens, and exploiting other means of gaining personalized information, adversaries can obtain information to create targeting models and support individualized messaging.[484]

[479] Adamsky, *Cross-Domain Coercion*, 29.

[480] Snegovaya, *Putin's Information Warfare in Ukraine*, 7.

[481] Goldman et al., "Lawmakers Warned."

[482] AEP, *Targeted Disinformation Campaigns*, 15; and DiResta, "Computational Propaganda."

[483] Much of hostile social manipulation is "made possible by cyber techniques." See Mazarr et al., *Emerging Risk*, 6.

[484] Lin and Kerr, "Cyber-Enabled Information/Influence Warfare," 14. This includes the potential for insider threats, as in the case of former Twitter employees who sold access to user

Social media companies' databases constitute a treasure trove. Those companies offer free access to their platform in exchange for access to user data that allows them to tailor content and advertisements to users' preferences.[485] Adversaries can use platform advertising programs to make use of that data or employ cyber tools to obtain it for customized IOs.[486]

One way to employ such data is to conduct "malinformation" campaigns. In these operations, attackers strategically distribute genuine but privately held information to damage reputations or otherwise harm victims.[487] Russian intelligence operations to hack Democratic National Committee servers, obtain sensitive emails, and distribute them with the help of WikiLeaks demonstrated how pairing stolen documents with sophisticated social media outreach can create far-reaching effects.[488] In a similar fashion, adversaries may seek to steal and exploit government documents (including classified materials) to mobilize public opposition to US policy goals in future crises. Foreign intelligence agencies are known to be actively targeting US lawmakers and their devices to get access to sensitive or classified information.[489]

Attackers may also gather personal information on specific policymakers to target IOs against them. Adversaries have repeatedly penetrated US agencies responsible for securing sensitive personal data on government employees (including those who would play key roles in crisis decision-making). Most notoriously, China conducted the April 2015 cyberattack on the OPM in which they obtained millions of SF-86 forms containing sensitive personal information gathered in background checks for people seeking government security clearances.[490]

Such data theft campaigns continue unabated. In February 2020, for example, the Defense Information Systems Agency acknowledged that over two hundred thousand people may have had their Social Security numbers and other personally identifiable information compromised.[491] Paired with large-scale data-mining capabilities that enable adversaries to process large amounts of individuals' personal data, adversaries are increasingly well positioned to conduct microtargeted IOs against specific government officials.

Personalized IOs can also target individuals in the broader policy community. The Office of the Director of National Intelligence (ODNI) report on 2016 election interference found that "immediately

data (including names, email addresses, phone numbers, etc.) to Saudi Arabia. See Conger et al., "Former Twitter Employees Charged."

[485] AEP, *Targeted Disinformation Campaigns*, 8–9.

[486] A high-profile example of this tactic occurred in the lead-up to the 2016 US elections, when data firm Cambridge Analytica improperly obtained Facebook data on tens of millions of users that they then used to create psychological profiles that were used to tailor online content. See Meredith, "Everything You Need to Know." More broadly, the ability to specifically tailor and customize content on social media platforms makes them "especially susceptible to disinformation campaigns." See AEP, *Targeted Disinformation Campaigns*, 7.

[487] AEP, *Targeted Disinformation Campaigns*, 4.

[488] These "hack and leak" tactics are "widely used, highly effective and difficult to combat," especially in countries that respect press rights and freedoms. See Timberg, "Russians Struggled to Spread DNC Files."

[489] When House Republicans entered the Sensitive Compartmented Information Facility (SCIF) with their cell phones in October 2019, they "could have created a field day for Russian and Chinese intelligence agencies" seeking to access such information, and who could selectively leak it to inflame political tensions or misrepresent government positions. See Marks, "Biggest Cybersecurity Vulnerability."

[490] On the (belated) attribution of the OPM attack to China, see Smith, "OPM Data Breaches." On the cyber technologies and techniques China used in the attacks, see Fruhlinger, "OPM Hack Explained."

[491] Bing, "U.S. Agency That Handles Trump's Secure Communication Suffered Data Breach"; and Konkel, "DISA Confirms Breach."

after Election Day," Russian intelligence organizations "began a spearphishing campaign targeting US government employees and individuals associated with US think tanks and NGOs in national security, defense, and foreign policy fields." The goal of that campaign was to "provide material for future influence efforts" and intelligence collection focused on the incoming administration personnel.[492] In future crises, those influence efforts could include IOs to shape key policymakers' perspectives.

There are no published accounts of China using cyber espionage to help conduct influence operations against the US public or senior officials. But Beijing's espionage capabilities are vast and could be repurposed to support IOs. During the ongoing trade war, China has intensified its long-standing campaign to steal US technology and intellectual property in key economically and militarily critical realms.[493]

China is also continuing to gather personal information on US government employees and the general public for use in future coercive campaigns. Most recently, the Department of Justice has charged Chinese operatives with conducting "extremely sophisticated" cyber operations (including the use of specially tailored spearfishing emails) to seize detailed data on tens of millions of US citizens from insurance companies and other sources.[494] The US government also recently charged two Chinese citizens, allegedly working with the Chinese government, for their involvement in a global espionage campaign targeting corporate secrets and intellectual property, and for stealing data (including personally identifiable information) on US military personnel.[495] These and other cyber espionage campaigns provide China with a wealth of information for targeting IOs to influence the beliefs and behavior of US decision-makers and the general public.

China and Russia can also use social media platforms to gather data on American citizens and influence their behavior. The Trump administration warned that "the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States."[496] The TikTok mobile app—owned for the present by a Beijing-based parent company—exemplifies this threat vector. TikTok, which has been downloaded over 175 million times across the United States and over 1.5 billion times worldwide, allows users to post and share short videos.[497] Indications are growing that the Chinese government is monitoring the platform and censoring content.[498] The app also captures large amounts of data from its users, including location data, browsing history, and other network activity, which threatens to give the Chinese Communist Party access to US citizens'

[492] ODNI, *Assessing Russian Activities*, 5. The IRA also increased its social media activity after the election. See SSCI, *Russian Active Measures, Vol. 2*, 8.

[493] Sanger and Myers, "China Accelerates Cyberspying."

[494] DOJ, "China-Based Hacking Group Indicted."

[495] *United States v. Hua and Shilong*.

[496] Trump, *Executive Order on TikTok*.

[497] Trump, *Executive Order on TikTok*; Harwell and Romm, "TikTok's Beijing Roots"; and Mohsin, "10 TikTok Statistics." Russia's VKontakte (similar to Facebook) is also one of the most popular social media sites worldwide. However, its users are primarily concentrated in Russia and eastern Europe, so Russian disinformation or censorship on this platform would have limited impact on the US public. See Echosec Systems, "What is VKontakte?"

[498] TikTok has instructed content moderators to censor videos on sensitive Chinese topics (e.g., Tiananmen Square, Tibetan independence, Falun Gong). Journalists obtained internal TikTok guidance documents in September 2019 showing that content on the app that is deemed to violate its terms of service for religious, political, or other reasons may not be made visible to other users, can be deleted from the site entirely, and may even lead to a ban of the posting user. However, TikTok parent company ByteDance claims those documents are outdated and no longer guide content-related decisions. See Trump, *Executive Order on TikTok*; and Hern, "TikTok Censors Videos." On additional censorship concerns, see Biddle, Ribeiro, and Dias, "Invisible Censorship."

proprietary information—which could be used for coercion.[499] Researchers are increasingly concerned that the app could prove to be "one of China's most effective weapons in the global information war, bringing Chinese-style censorship to mainstream U.S. audiences and shaping how they understand real-world events."[500]

The United States is responding to the threat that foreign-owned social media platforms will be used to gather exploitable intelligence. Former president Trump issued an executive order to address the threat posed by TikTok in particular in August 2020. The order banned transactions with TikTok's owner, ByteDance, and its subsidiaries within forty-five days of its issuance. The former administration also sought to ban WeChat, another Chinese-owned platform. Both companies took legal action to block those actions. The Biden administration has now asked for an "abeyance"—or suspension—of proceedings while it revisits whether the apps really pose a threat. The delay means both apps can continue to operate in the United States while new staff at relevant US agencies "become familiar with the issues in this case," the legal documents state. That analysis should account for the potential coercive threats that foreign-owned platforms pose.[501]

AI Applications for Curated IO Campaigns and Deepfakes

Current Chinese and Russian efforts to leverage AI barely hint at their opportunities to exploit stolen data to conduct massive, microtargeted operations in future crises. One area of focus lies in supporting efforts to gather data and organize it for use in coercive messaging. The National Security Commission on Artificial Intelligence notes that "machine learning is a powerful tool for harvesting and analyzing data and targeting activities. Using espionage and publicly available data, adversaries will gather information and use AI to identify vulnerabilities in individuals, society, and critical infrastructure. They will model how best to manipulate behavior, and then act."[502] AI tools can also help transform raw data into usable profiles of the beliefs, behavior, and biological makeup of US individuals to "manipulate or coerce" them.[503]

Once US adversaries have assembled these profiles, AI can help them develop IO campaigns that target specific audiences with specific messages.[504] AI can also help China and Russia conduct sentiment analysis at scale, develop and deliver near-real-time messaging on that basis, and alter the content they deliver to the public and US leaders as events occur in the crisis region. In addition, AI tools may help adversaries target IOs against those most susceptible to such customized and inflammatory messaging.[505] AI tools can help attackers rapidly survey American social media posts to identify psychological vulnerabilities, allowing them to pinpoint the issues most likely to provoke inflammatory emotional responses. Adversaries will also use AI to support contingency-based decision-making processes and machine-scale testing of content to improve its effectiveness. [506]

AI can assist IO campaigns in another way: by making deepfakes and other means of conveying adversary messaging more psychologically effective and difficult to detect. The doctored video of House of Representatives Speaker Nancy Pelosi slurring her speech, which garnered over 2.5 million views on Facebook, barely hints at the sophistication and reach of false video and audio messaging that

[499] Trump, *Executive Order on TikTok*.

[500] Harwell and Romm, "TikTok's Beijing Roots." For further analysis on the risks posed by Chinese-owned apps, see Lee and Barbesino, *Challenging China's Bid*.

[501] *BBC News*, "Biden 'Pauses' TikTok and WeChat Bans."

[502] NSCAI, *Final Report*, 22.

[503] NSCAI, *Final Report*, 9 and 47.

[504] NSCAI, *Final Report*, 47–8.

[505] Lin, "Existential Threat," 190.

[506] *Hearing on Artificial Intelligence, Manipulated Media, and "Deepfakes,"* Watts statement, 1; Ghosh and Scott, *Digital Deceit*, 26; and Paul and Posard, "Artificial Intelligence."

opponents can employ to misrepresent US leadership positions in a crisis.[507] Despite evidence of video manipulation, Facebook refused to remove the content.[508] But the Pelosi video was still less sophisticated than what editing software can create today.[509] Future influence campaigns will employ deepfakes—in other words, audiovisual records "created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual."[510]

Deepfakes are a particularly valuable IO tool because people are predisposed to trust videos as credible. Audio and video recordings allow viewers to believe they have witnessed an event firsthand and to develop their own account of—and reaction to—that event accordingly.[511] Their reactions align well with the cognitive biases described in the How Coercion (Sometimes) Works section. Emotional responses to well-crafted, inflammatory videos are more likely to be shared, making deepfakes especially useful for large-scale influence operations.[512] Moreover, because even false beliefs are difficult to dislodge once established, efforts to prove that a video is a deepfake may come too late to change public perceptions in a crisis.

Russia has long used fake videos to blackmail or ruin the reputation of US officials. In 2009, for example, the Russian government produced video that first showed a surreptitious recording of a US diplomat in his hotel room and later featured a couple having sex in the same room with the lights off.[513] While Russia intended to persuade the viewer that the diplomat was involved in extramarital affairs, the individuals participating in the latter scene were not identifiable. The US ambassador to Moscow quickly dismissed it as a fake.

Now, however, AI applications can make deepfake videos vastly more difficult to identify as manufactured or manipulated.[514] New facial mapping technologies, powerful machine learning algorithms, and other AI-related advances have made it easy to fabricate videos of US leaders or other targeted individuals appearing to say or do something they didn't.[515] Academic researchers have also developed deep learning algorithms that can create synthetic audio and video that is nearly identical to the training data it seeks to replicate.[516] AI researchers at Moscow's Skolkovo Institute of Science and Technology have even developed a "few shot" AI system that can create convincing fake videos with only a few still photos of a person's face, and deepfake

[507] This video is not considered a deepfake because the creators only slightly altered real video for effect. It nevertheless exemplifies the potential for more sophisticated fakes to influence the US public. See *CBS News*, "Doctored Nancy Pelosi Video." One lighthearted deepfake that received especially wide viewership portrays former president Obama as making false statements. See BuzzFeedVideo, "You Won't Believe What Obama Says!"

[508] Facebook did downrank the video, making it appear less in algorithmically determined news feeds. Meanwhile, other popular platforms took conflicting approaches. Twitter allowed the video to remain unfettered, while YouTube removed it entirely. See Harwell, "Facebook Acknowledges Pelosi Video Is Faked."

[509] For the full spectrum of manipulated audio and video from "cheap fakes" to advanced deepfakes and the technologies they leverage, see Paris and Donavan, *Deepfakes and Cheap Fakes*, 11 and 25–38.

[510] Malicious Deep Fake Prohibition Act of 2018, S. 3805. Deepfakes have also been referred to as "images or videos that combine and superimpose different audio and visual sources to create an entirely new (and fake) video that can fool even digital forensic and image analysis experts." See Johnson and Miller, "Dangers of 'Deep Fakes.'"

[511] *Hearing on Artificial Intelligence, Manipulated Media, and "Deepfakes,"* Citron statement, 2.

[512] *Hearing on Artificial Intelligence, Manipulated Media, and "Deepfakes,"* Watts statement, 1–2; and Citron statement, 5.

[513] AP, "High-Tech Deception of 'Deepfake' Videos."

[514] Chesney and Citron, *Disinformation on Steroids*; Meserole and Polyakova, "West Is Ill-Prepared"; and SSCI, *Russian Active Measures, Vol. 2*, 74.

[515] *Hearing on Artificial Intelligence, Manipulated Media, and "Deepfakes,"* Clark statement, 1–2.

[516] Chesney and Citron, *Disinformation on Steroids*.

technologies are only continuing to improve.[517] The growing amount of tools and open-source data available online is also reducing the amount of technical expertise required to produce increasingly sophisticated deepfakes.[518]

Other AI software enables deepfake creators to edit what someone appears to be saying in a video, with the AI swapping around the person's voiced syllables and mouth movements to leave only a seamlessly altered "talking head."[519] And while previous tools for manipulating digital content may have failed to account for subtle imperfections such as lighting angles in images, or cadence in audio, deep learning and generative adversarial networks have made it possible to doctor images and video so effectively that victims will face growing difficulties in distinguishing manipulated files from genuine ones.[520]

The Defense Advanced Research Projects Agency (DARPA) has launched a number of research initiatives to help identify deepfakes, including synthetic media detection technologies.[521] Commercial technologies can also help counter deepfakes by authenticating and verifying content distributed on social media platforms and by using subtle indictors (including light and shadows, blinking, and hyper-precise facial data) to determine that a video is fake.[522] This research is critical for strengthening US resilience against crisis IOs and should be accelerated.

However, efforts to improve deepfake detection face major obstacles. A February 2020 Government Accountability Office report highlights a number of these impediments, including insufficient data to "train" detection capabilities, the lack of a reliable, automated process for deepfake detection, and methods to counter offensive adaptations to avoid detection.[523] Other researchers conclude that "automated deepfake detection is likely to become impossible in the relatively near future" as offensive capabilities improve, and they urge policymakers to seek other long-term solutions, including blockchain-based verification and reverse video search capabilities.[524]

Another obstacle reflects the technical advantages that adversaries derive from using social media platforms to deliver deepfakes. High-definition fake videos are easier to detect; the more details in the video, the more opportunities for detection systems to identify flaws. However, most social media and messaging sites and apps compress videos into formats that make them quicker and easier to share, removing vital clues.[525] Attackers can also maneuver around detection technologies by using actual footage of protests or other events but captioning it as if it happened somewhere else—including a regional crisis of concern to the US public and decision-makers.[526] Targeting the United States with frequent deepfakes may also have the perverse effect of corroding public confidence in actual messages from US leaders; even genuine content may come to be dismissed as fake in an atmosphere of pervasive, high-tech disinformation.[527]

[517] Harwell, "Race to Detect 'Deepfake' Videos"; and Cole, "New Deepfake Method."

[518] Tully and Foster, "Repurposing Neural Networks."

[519] Harwell, "Race to Detect 'Deepfake' Videos."

[520] Meserole and Polyakova, "West Is Ill-Prepared." For more on generative adversarial networks, see Rocca, "Generative Adversarial Networks."

[521] *Hearing on Artificial Intelligence, Manipulated Media, and "Deepfakes,"* Doermann statement, 2.

[522] Leading deepfake detection startup TruePic, for example, is using blockchain technology to verify press-captured images and videos. See TruePic, "Our Technology." See also Strout, "Pentagon Is Tackling Deepfakes"; and Harwell, "Race to Detect 'Deepfake' Videos."

[523] GAO, *Deepfakes*.

[524] Engler, *Fighting Deepfakes*.

[525] Harwell, "Race to Detect 'Deepfake' Videos."

[526] Harwell, "Race to Detect 'Deepfake' Videos."

[527] Chesney and Citron, *Disinformation on Steroids*.

The difficulty of detecting deepfakes will also grow in the years to come. Lieutenant General Jack Shanahan, director of the Department of Defense's (DoD) Joint Artificial Intelligence Center, notes that the growth in sophistication "appears to be exponential" and marks a critical step forward in the ability of adversaries to cause "friction and chaos" in US decision-making.[528] Adversaries can use deepfakes to sow such chaos and shape US public beliefs in almost limitless ways, ranging from public officials appearing to admit that a crisis is a "false flag" operation to videos that show catastrophic consequences of (real or yet to be launched) cyberattacks on critical infrastructure.[529] Developing an equivalently wide array of playbooks to counter deepfakes that go viral among the US public will be essential.

Of course, if the technical challenges of detecting false videos can be overcome, it would be better still to be able to lock or downrank such videos on, or speedily remove them from, social media networks. WeChat responded to user concerns over the meteoric rise of Zao-enabled deepfakes by restricting the app from its messenger platform.[530] But Facebook's refusal to delete the fake video portraying Nancy Pelosi highlights the fact that countering deepfakes is more than a technical challenge.[531] Indeed, in congressional testimony, University at Buffalo's Artificial Intelligence Institute Director David Doermann emphasized that "combating synthetic and manipulated media at scale is not just a technological issue. It is a social one as well."[532] To build plans and criteria for removing false videos in a crisis, social media companies and government agencies will need to engage in a standards development effort even more challenging than that for text-based disinformation.

Those challenges will continue to grow. AI-enabled advances in lip-syncing and manipulating physiognomic contours to match speech patterns and content will make adversary videos highly compelling, especially when viewed on the small, comparatively low-resolution displays on most smartphones and tablets.[533] AI can also help adversaries produce original text-based content and manipulate images, audio, and video, including through generative adversarial network (GAN)-enabled and reinforcement learning (RL) deepfakes that will be very difficult to distinguish from authentic messages.[534]

Using AI to Manipulate Social Media Algorithms and Enhance Botnet Attacks

Campaigns to shape US crisis decision-making will become all the more effective as China and Russia develop new, AI-enhanced means to deliver micro-targeted messaging and advanced deepfakes. The use of AI to harness large-scale botnets of increasingly complexity and resilience to conduct coercive operations will pose significant challenges for US defense.[535] Other technological advances in delivery TTPs, including AI-enabled measures to manipulate social media ranking algorithms, will also help Beijing and Moscow reach their target audiences with new power and persistence. [536]

[528] Strout, "Pentagon Is Tackling Deepfakes."

[529] Chesney and Citron, *Disinformation on Steroids*; and Lamberth, "Dangers of Manipulated Media."

[530] Damiani, "Chinese Deepfake App."

[531] Opportunities to improve collaboration between government and social media companies for the identification and removal of harmful fake content are examined in the Combined Information-Cyberattacks section.

[532] *Hearing on Artificial Intelligence, Manipulated Media, and "Deepfakes,"* Doermann statement, 3. Other researchers have similarly concluded that defeating audio-video manipulation from simple "cheap fakes" to deepfakes will require "a combination of technical and social solutions." See Paris and Donavan, *Deepfakes and Cheap Fakes*, 3.

[533] Benjamin and Simon, "How Fake News Could Lead to Real War," 6.

[534] NSCAI, *Final Report*, 47–48.

[535] Metz and Blumenthal, "How A.I. Could Be Weaponized"; and Chessen, *MADCOM Future*, 2.

[536] NSCAI, *Final Report*, 47–48.

Bots, and more specifically bot networks, allow adversaries to generate significant traffic for a topic or trend.[537] For years, relatively primitive bots have posted content at a specific time or scheduled intervals, offering basic answers to simple questions or providing content in response to triggers. Even these primitive bots can have a disproportionate impact, given how easy they are to create and the volume at which they can disseminate content.[538] These bots can also amplify the "first-mover advantage" by putting massive amounts of information out at speed, using scale to create the "majority illusion effect" that can trick people into believing a message simply because it is receiving attention.[539]

By consistently publishing content, these bots can also game the platform algorithms that curate users' feeds, improving the reach of future bot-delivered content.[540] For years, adversaries have deployed seemingly harmless bot accounts that post innocuous content, developing a following that attackers can leverage to conduct disinformation operations.[541]

Bots themselves are not inherently nefarious and have a number of legitimate uses. "Good" bots can provide value to companies by automating basic functions and prescreening or addressing customer support inquiries.[542] However, "bad" bots accounted for 20.4 percent of all internet traffic in 2018 (compared to 17.5 percent for good bots), and 73.6 percent of these bad bots are sophisticated enough to cycle through random IP addresses, use anonymous proxies, transform their identities, and mimic human behavior.[543] Other sophisticated bots have been able to generate entire phishing campaigns, doing so better than a human competitor, "composing and distributing more phishing tweets than humans, and with a substantially better conversion rate."[544]

In addition to generating high volumes of posts, comments, and other content, bots can be used to amplify existing disinformation, create the appearance of legitimacy or consensus around that disinformation, amplify follower counts, or hijack algorithms and game trending topics to push content to the top of their targets' feeds.[545] Attackers can also employ bots in distributed denial-of-service (DDoS) attacks to temporarily disable websites and other communications resources.[546]

As bot technology improves, bots will become more sophisticated and deliver messaging that increasingly mimics the behavior of human users. Adversaries may also use "cyborg" bots—bots that are periodically controlled by humans—to further heighten the difficulty of detecting and countering them.[547] In addition, integration of smarter AI tools into bot networks will provide adversaries with radically enhanced capabilities to manipulate their victims' perceptions and beliefs.[548]

New social media management software can help attackers control these modernized bot networks with greater speed and effectiveness. Developed for legitimate commercial purposes, this management software can allow adversaries to preconfigure entire campaigns to reach different audiences across multiple social media platforms. The software can

[537] Russians, in particular, are "prolific users" of bots. See SSCI, *Russian Active Measures, Vol. 2*, 18.

[538] Chessen, *MADCOM Future*, 5.

[539] Bondy, *Bad Bots*, 3; and Paul and Matthews, *Russian "Firehose of Falsehood,"* 4.

[540] Hoffmann, Taylor, and Bradshaw, *Market of Disinformation*, 18.

[541] DiResta et al., *Tactics & Tropes*, 63.

[542] Biran, "How Bots Can Generate Value."

[543] Distil Networks, *2019 Bad Bot Report*.

[544] Dvorsky, "Hackers Weaponize Artificial Intelligence."

[545] Chessen, *MADCOM Future*, 6; and SSCI, *Russian Active Measures*, *Vol. 2*, 18.

[546] Osborne, "Bad Bots"; and Woolley, "We're Fighting Fake News."

[547] Klepper, "Cyborgs, Trolls and Bots."

[548] Chessen, *MADCOM Future*, 2.

also utilize sophisticated behavioral data analytics, employ real-time, reactive social media "listening" to place the right message at the right time, and coordinate IOs across multiple communications systems simultaneously and automatically.[549]

These increasingly automated software packages, which require little human expertise, make it particularly easy to run an elaborate disinformation campaign, and their contingency-based nature will make them especially valuable for disinformation operations linked to an unfolding crisis that provides near real-time opportunities to confuse the public as to adversary activities and the rationale for US engagement in the region.[550]

All these advances come at time when the costs of creating bots and bot-generated content are plummeting. Rather than using human workers to formulate and distribute disinformation, future adversaries will be able to leverage machines to compose and deliver convincing, diverse, and tailored content on a massive scale.[551] The net result: larger numbers of more advanced bots will be available and affordable to an increasingly broad array of future adversaries.[552]

Additional Threat Vectors

The overview of Chinese and Russian IOs earlier in this section briefly referenced Secondary Infektion, Twitter-based impersonation tactics, and other TTPs in recent influence campaigns. US defenses against coercion need to scale up for improved versions of these means of attack, as well as the expanded use of infrastructure in the United States and around the globe.

Fake Accounts, Impersonation, and Exploitation of Popularity-Based Algorithms

Since late 2020, China has been creating a growing array of false Twitter accounts that convey disinformation without identifying it as government-produced. This campaign produced tens of thousands of retweets, covertly amplifying propaganda that can reach hundreds of millions of people. An additional cluster of fake accounts, many of them impersonating UK citizens, also pushed Chinese government content, racking up over 1,600 retweets and replies before Twitter kicked them off in May 2021. Moreover, this fiction of popularity distorts and takes advantage of platform algorithms, which are designed to boost the distribution of popular posts.[553]

A separate attack on Twitter highlights an additional opportunity for adversaries to scale up coercive campaigns and complicate defenses against them. In July 2020, a small handful of (mostly US-based) hackers gained access to over one hundred Twitter accounts, including those of very high-profile users, to carry out an amateurish cryptocurrency scam.[554] They did so not by stealing passwords for individual accounts but by gaining access to Twitter's internal tools and systems. The hackers gained access to Twitter's customer service portal by using personalized, "social engineering"–based messages to convince a Twitter employee that they were coworkers in the company's IT department. They then persuaded the employee to provide credentials to access Twitter's customer service portal.[555] Using these tools, the hackers were able to access the Twitter accounts of users such as former

[549] Ghosh and Scott, *Digital Deceit*, 21.

[550] Ghosh and Scott, *Digital Deceit*, 24.

[551] Metz and Blumenthal, "How A.I. Could Be Weaponized."

[552] Bondy, *Bad Bots*, 4.

[553] Kinetz, "Army of Fake Fans"

[554] DOJ, "Individuals Charged for Twitter Hack."

[555] Hollister, "Three People Charged." According to Twitter, not all employees who the hackers initially targeted had sufficient access. However, with their initial foothold, they were able to access Twitter's internal systems and gain information that "enabled them to target additional employees who did have access to our account support tools." See Twitter, "Update on Our Security Incident."

president Barack Obama, presidential candidate Joe Biden, tech CEOs Jeff Bezos and Elon Musk, among many others.

The hackers' only goal was to scam Twitter users out of bitcoin. However, Moscow and Beijing may seek to use similar TTPs in future coercive campaigns. Twitter is heavily used by senior US leaders and their foreign counterparts and is frequently a source for breaking news.[556] If an opponent can gain access to their accounts during a regional crisis, the opponent could use those accounts to send apparently authentic policy statements designed to sow divisions with US allies and confuse the US public. This risk has prompted bipartisan concern in Congress. Senator Roger Wicker (R-MS) warns that "it is not difficult to imagine future attacks being used to spread disinformation or otherwise sow discord through high-profile accounts, particularly through those of world leaders."[557] Similarly, Senator Mark Warner (D-VA) cautioned that "the ability of bad actors to take over prominent accounts, even fleetingly, signals a worrisome vulnerability in this media environment—exploitable not just for scams, but for more impactful efforts to cause confusion, havoc, and political mischief."[558]

Their concerns should be front and center as the United States develops defensive strategies against coercive IOs. So, too, should be the implications of backdoor access into major platforms used by world leaders and the material this may provide to the attacker for coercive IOs. Twitter is tightening its internal controls to avoid similar attacks in the future.[559] However, this attack was successful because of social engineering—a tactic that focuses on the human element of cybersecurity and can defeat sophisticated technical defenses. To avoid similar attacks in the future, Twitter and other social media companies will need to bolster their defenses against socially engineered attacks and insider threats.

Made in the USA (and around the Globe)

Adversaries are developing new TTPs to better evade detection. While social media companies are cracking down on inauthentic accounts and "coordinated inauthentic behavior," they face greater problems in countering the amplification of foreign disinformation by US citizens and content providers. The Kremlin is already exploiting these difficulties. Russian operatives are shifting away from the fake social media accounts and bots used by the IRA and other groups in their campaign against the 2016 election. Now, these operatives are increasingly relying on English-language news sites to push out disinformation that is then amplified by Americans, many of whom are as eager as foreign powers to widen partisan divisions inside the United States.[560] Such tactics could complicate efforts by social media platforms to block coercive content during a crisis. The majority of traffic conveying the disinformation will come from legitimate US accounts, versus the coordinated inauthentic behavior that platforms focus on countering.

A recent incident exemplifies what adversaries hope to achieve by leveraging US partisan divisions to encourage Americans to share foreign disinformation. Among the thousands of Americans who took to the streets to protest racial injustice across the country, a few individuals in Portland, Oregon, in August 2020 used a Bible as kindling for a fire. The incident received nearly no local news coverage and appears to have been largely isolated from the main protests. However, a Russian news agency released and amplified a deceptively edited video of the protests with the Bible burning as the focus of its coverage in an attempt to characterize all protesters as "Bible-burning zealots" and

[556] Lerman, "Twitter Hack Triggers Investigations"; and Frenkel et al., "Brazen Online Attack."

[557] Wicker, Letter to Jack Dorsey, 1.

[558] Bond and Allyn, " 'Get Ready for Copycats.' "

[559] Twitter, "Update on Our Security Incident."

[560] Rosenberg and Barnes, "Bible Burning."

further inflame tensions. High-profile Americans including Senator Ted Cruz (R-TX) and Donald Trump Jr. and US news outlets including the *New York Post* and the *Federalist* helped spread that false narrative.[561] Adversaries conducting crisis IOs may adopt similar tactics: if even small public protests (or counterprotests) break out concerning US crisis polices, adversaries can magnify their apparent scale and divisiveness.

Adversaries can also simply amplify US-generated content that advances their coercive goals. While disinformation operations surrounding the 2016 election created and perpetuated a lot of false content, an analysis of tactics for 2020 suggested that adversaries instead sought to amplify domestically created content.[562] This strategy, again, leverages deep partisan divides within the United States that adversaries continue to foment. Social media users are likely to share these stories because they fit with their own preconceptions, and disinformation strategies are counting on them to do so.[563] If a US media outlet or influential individuals side with an opponent during a crisis (i.e., make the case for not defending an ally), adversaries can put their disinformation networks and capabilities to use to amplify that content. In some cases, Russia is even attempting to pay US-based writers to publish stories that fit the Kremlin's IO agenda.[564]

Intelligence officials also told Congress that Russians are conducting IOs from servers located on American territory, knowing that US intelligence agencies are prohibited from operating inside the country except for very narrow and tightly constrained purposes.[565] In addition, adversaries can exploit infrastructure far beyond the United States (and thousands of miles from their own territories) to conduct information campaigns. The Kremlin-linked influence organization Project Lakhta and its Lakhta Internet Research (LIR) troll farm (previously known as the IRA) has begun establishing short-lived troll farms that employ unwitting third-country nationals in Ghana, Mexico, and Nigeria to propagate the US-focused narratives. The NIC assesses that Russia has developed these capabilities for remote operations "in response to efforts by US companies and law enforcement to shut down LIR-associated personas."[566] As those efforts intensify, we should expect Russia (and, potentially, China) to expand their use of global infrastructure to conduct coercive campaigns.

Another way in which adversaries are encouraging unwitting Americans to spread disinformation is through use of smaller social media platforms. The social media ecosystem is much larger than Facebook, Twitter, YouTube, and Google. Adversaries are sowing the seeds of disinformation on these smaller platforms—often with fewer resources to moderate content and less transparency into their moderation policies—so that Americans bring it to larger platforms themselves.[567] Russia's Secondary Infektion campaign, for example, ran in "stark contrast" to previous social media campaigns by focusing on the use of a massive collection of forums known as Reddit.[568] One additional way that adversaries could deceive Americans is by creating "local" sites to leverage in a crisis. Researchers have exposed entirely fake news outlets such as *Denton Daily*, *Livingston Ledger*, *East Michigan News*, *Grand Canyon Times*, and hundreds of others that have appeared online in recent years.[569] These sites use algorithms to copy stories from reputable outlets and republish them as their own—sometimes for profit, sometimes for domestic political goals.

[561] Rosenberg and Barnes, "Bible Burning."

[562] Rosenbach et al., *Election Influence Operations Playbook*, 7.

[563] Biasini, McKay, and Valites, *Building Blocks*, 8.

[564] Collier and Dilanian, "Russian Internet Trolls."

[565] Goldman et al., "Lawmakers Warned."

[566] NIC, *Foreign Threats to the 2020 US Federal Elections*.

[567] Rosenberg and Barnes, "Bible Burning."

[568] Biasini, McKay, and Valites, *Building Blocks*, 7.

[569] Silverman, "Fake Local News Sites"; and Bengani, "'Pink Slime' Local News Outlets."

They have achieved significant user engagement, including posts by major company executives, political activists, and scientists.[570] While these specific sites have not been connected to disinformation operations, they exemplify how easy it would be for adversaries to create realistic-seeming local news sites to leverage for IOs in a future crisis.

Search Engine Optimization and Exploitation of "Data Voids"

Adversaries are increasingly effective at manipulating search results during crises, thereby deepening the penetration of coercive campaigns. Search engines play a vital role in how internet users navigate the modern information environment and directly impact what people consume as news and information. More than 89 percent of internet users worldwide use Google Search to find information online and answer questions, giving Google a powerful role as an "information gatekeeper."[571]

Unlike social media platforms, where users follow a largely self-curated set of accounts and pages, people use Google Search to seek out specific information. Google Search results are determined by its PageRank algorithm, which prioritizes content based on over two hundred proprietary factors—including a website's reputation and popularity, its domain name, and associated keywords—to determine relevance and importance.[572] Placement in that ranking is key: studies suggest that most users do not look past the top ten results of a search and that page ranking matters more than the abstract text the results provide.[573] Google is constantly tweaking the relative weight of these categories to improve search quality, and an entire legitimate SEO industry has emerged to help companies stay abreast of these changes and maintain visibility in searches. SEO offers companies a widely used means of increasing the quantity and quality of traffic to their websites.[574]

Of course, SEO is ripe for exploitation by US adversaries in a crisis. By manipulating SEO algorithms, adversaries can trick search engines into displaying certain content for specific search words, tricking viewers into believing and spreading disinformation, or achieve other goals.[575] Adversaries can also use other cyber tools (e.g., hacking) to help game search engine algorithms.[576] Few studies have examined the potential uses of SEO in IO campaigns.[577] However, for nearly Google's entire history, malicious actors have used a variety of tactics to artificially improve their position in search results in an attempt to harm or deceive search users.[578]

Studies of other search engines such as Microsoft's Bing have offered similar results. While Google has an extremely large market share, Bing's prevalence is increasing. Bing is the default search engine for Microsoft web browsers and has partnerships with Yahoo, Apple, and other companies that might use search results from Bing without the user knowing it.[579] Compared to Google, Bing results are much more likely to feature disinformation, conspiracy

[570] Silverman, "Fake Local News Sites."

[571] Bradshaw, "Disinformation Optimised," 2 and 16.

[572] Hoffmann, Taylor, and Bradshaw, *Market of Disinformation*, 10; and Dean, "Google's 200 Ranking Factors."

[573] Metaxas, "Web Spam"; and Bradshaw, "Disinformation Optimised," 6–7. Some actors may also buy Google advertisements to appear, blatantly, as an advertisement above the true search results, as Russia did in its 2016 election interference operations, but that tactic has been shown to be much less effective than SEO manipulation. See Bradshaw, "Disinformation Optimised," 10; and SSCI, *Russian Active Measures, Vol. 2*, 57.

[574] Moz, "What Is SEO?"; Google, *How Google Fights Disinformation*, 10 and 14; and Bradshaw, "Disinformation Optimised," 15–16.

[575] Google can correct the distortion once detected, but it may take hours or days for these manipulations to be identified. See Ghosh and Scott, *Digital Deceit*, 17; and SSCI, *Russian Active Measures, Vol. 2*, 57–58.

[576] Silverman and Jones, "Hackers Are Breaking into Websites."

[577] Bradshaw, "Disinformation Optimised," 2 and 9.

[578] Google, *How Google Fights Disinformation*, 11 and 14; and Hoffmann, Taylor, and Bradshaw, *Market of Disinformation*, 11.

[579] Bush and Zaheer, "Bing's Top Search Results."

theories, extremist content, and information from sources known to be purveyors of disinformation (e.g., RT and Sputnik) and do so higher in content rankings.[580] And while Bing and Google have different proprietary ranking algorithms, efforts to game their respective algorithms may offer significant basis for subsequent customization.

Not surprisingly, preliminary research suggests that Google Search and other search engines may constitute "fertile ground for media manipulation."[581] We should expect adversaries to exploit SEO vulnerabilities to amplify coercive messaging and exploit the US public's underlying vulnerabilities to social media-delivered disinformation in crises.

Adversaries may also exploit what researchers have termed "data voids" in online information to manipulate search engines. Data voids exist when the information available online for a given (often, very specific) search term is "limited, non-existent, or deeply problematic."[582] While search engines rely on machine learning algorithms to identify and prioritize content to display in the results, in the case of data voids, these algorithms have very limited data on which to "train" and therefore to properly contextualize the search. Google acknowledges this challenge, noting that they often occur around niche conspiracy theories, and that when users enter search terms that specifically refer to these theories, ranking algorithms can only elevate links to the content that is actually available on the open web—potentially including disinformation.[583]

Some users come across these data voids naturally when using overly specific search terms. However, adversaries can use a combination of IO TTPs to exploit these data voids. In particular, they can generate a large volume of content (blog posts, comments on popular sites, social media posts, etc.) that encourages people to search for a very specific term that yields intentionally manipulated or skewed results.[584] Unlike gaming SEO algorithms to improve a specific site's rank, it is much more difficult to combat data voids because they operate precisely where there is little-to-no high-quality information to fill the void.

Known cases of data void exploitation to date have often occurred immediately after breaking news events—particularly those that involve the names of locations or suspects in violent attacks.[585] One example of this phenomenon occurred around the 2017 mass shooting in Sutherland Springs, Texas. In the immediate aftermath of the event, members of the far-right political community initiated a campaign to create online content that associated the name of the town and of the shooter with far-left extremists known as "Antifa." Recognizing that there was little content online that SEO algorithms would consider "high quality" about the town and the shooting suspect, they (accurately) assumed it would be easy to game those algorithms and fill the data void. Their ensuing disinformation campaign quickly prompted legitimate news publications to run headlines featuring the alleged Antifa ties.[586] The October 2017 mass shooting in Las Vegas offers a similar example of "data void" SEO manipulation. The morning after the shooting, the top (and entirely false) story produced by Google searches for the perpetrator's name was a conspiracy blog claiming that he was an "anti-Trump liberal," that he had recently converted to Islam, and that the FBI had linked him to ISIS.[587]

Russia has already demonstrated its ability to manipulate search engine algorithms to shape US public perceptions. Shortly after the Intelligence Community Assessment acknowledged Russia's role in

[580] Bush and Zaheer, "Bing's Top Search Results."

[581] Bradshaw, "Disinformation Optimised," 2.

[582] Golebiewski and Boyd, *Data Voids*, 1.

[583] Google, *How Google Fights Disinformation*, 16.

[584] Golebiewski and Boyd, *Data Voids*, 3.

[585] Golebiewski and Boyd, *Data Voids*, 6.

[586] Golebiewski and Boyd, *Data Voids*, 5.

[587] Roose, "Fake News Regains Its Megaphone."

interfering in the 2016 election, the top results of a search for "ODNI hacking report" were links to Russian propaganda outlet RT denying the report's allegations.[588] By using similar tactics, adversaries can help coercive content and messaging go viral and remain prominently featured in the news cycle as a crisis intensifies.

Implications for Strengthening Domestic Resilience

Even as Beijing refines its plans and capabilities to wage psychological warfare at the outset of future crises, and convince the enemy that the costs of resisting China's demands outweigh the benefits of doing so, federal agencies have yet to explain to the public how they will defeat such IO campaigns. That strategic gap applies to Russia as well. As policymakers consider options to bolster US resilience against coercion, trends in adversary TTPs will necessitate countervailing measures along each of the principal pathways of shaping US and allied crisis decision-making.

AI is creating novel challenges for defeating coercive campaigns that threaten to punish the US public. To counter massive, microtargeted messaging that adversaries can rapidly modify as a crisis evolves, the US will need the ability to block and counter-message against such operations with equivalent speed and precision. Humans alone may not be up to the job. The National Security Commission on Artificial Intelligence found that "defending against AI-capable adversaries operating at machine speeds without employing AI is an invitation to disaster. Human operators will not be able to keep up with or defend against AI-enabled cyber or disinformation attacks" or other threats "without the assistance of AI-enabled machines."[589] Developing AI capabilities that keep pace with the threat will require intensive effort. The United States is not currently prepared "to defend against AI-enabled threats and rapidly adopt AI applications for national security purposes."[590] Russia is making especially notable progress in developing and testing capabilities to conduct customized IOs en masse.[591] Russia pioneered many of those techniques in operations against its own citizens.[592] China has declared its intention to become the world leader in AI and is committed to applying its expertise to "leapfrog" US defense capabilities.[593] Policymakers should ensure that US AI research and development activities advance defensive capabilities in the psychological realm, as well as against more traditional threats.

But technical advances to conduct automated IOs constitute only part of the defensive challenge. Assuming that US machines are able to detect advanced deepfakes and track personalized messaging against millions of Americans, federal agencies and their social media partners will still need to agree on policies and protocols to filter those operations. US officials will also need to shape the policy statements (and fear-dampening messages) that platforms would deliver to the public. Overcoming the technological challenges of AI-enabled defense may be the easiest part of the problem.

Countering IOs to directly influence US decision-makers will entail requirements that are more familiar. As China and Russia use cyber means to steal sensitive personal data on these officials and their families, and package that material into IOs to drive their behavior, those efforts will constitute a high-tech version of familiar blackmail operations. The United States can adapt well-established counterintelligence programs and procedures to

[588] Waddell, "Kremlin-Sponsored News."

[589] NSCAI, *Final Report*, 9.

[590] NSCAI, *Final Report*, 8.

[591] Giles, *Handbook of Russian Information Warfare*, 71.

[592] Popescu, "Russian Cyber Sins."

[593] O'Meara, "Will China Overtake the U.S.?"

help protect White House officials, agency leaders, and senior military officers from direct influence campaigns. Defensive efforts should also anticipate the Russian use of reflexive control and other specialized TTPs that exploit personal data in ways entirely different from blackmail. Subsequent portions of this study offer detailed recommendations on how to do so, including for decision-making during the transition from IO-only campaigns to the onset of disruptive cyberattacks.

Recent Chinese and Russian technical advances will also heighten the importance and complicate the development of allied initiatives against coercion. Capabilities to impersonate US and foreign leaders could introduce new uncertainties into crisis management and mobilization of public support for alliance defense. Ongoing efforts to use foreign infrastructure in coercive campaigns will also require new forms of collaboration between the federal government and its security partners. As Russia (and, potentially, China) increasingly relies on servers and other information infrastructure within the United States, the Department of Homeland Security (DHS) and other nondefense agencies will need to not only assume the burden of domestic defense but also coordinate with their counterparts abroad. DHS and the FBI have already forged deep relationships with those counterparts on other issues. Now, with the State Department playing a leadership role, those agencies should extend their collaboration to building defensive plans and capabilities against coercion.

As with US domestic initiatives, assessments of the threats to come should guide international collaboration. China and Russia can combine all of the emerging TTPs analyzed above to create and deliver "computational propaganda": that is, the use of algorithms, automation, and human curation to strengthen the effectiveness of their messaging via social media networks.[594] China and Russia may also begin applying developments in quantum computing to create "information disorder machines" capable of real-time microtargeting on an even larger scale than possible with AI alone.[595] The US should structure coordination with its security partners (including through collaborative research and development) to meet these emerging threats as well as prepare for near-term coercive operations.

Combined Information-Cyberattacks

While China and Russia would almost certainly prefer to prevail in crises through information operations (IOs) alone, both nations are prepared to combine IOs with cyberattacks and kinetic attacks to intensify pressure on their adversaries to yield. One option to do so is to make good on the threats of punishment they have issued during initial phases of a crisis and begin disrupting infrastructure critical to the US economy and population. The US intelligence community assesses that adversaries are embedding malware in America's grid and other critical systems to gain just such coercive leverage.[596]

Chinese and Russian military writings call for the use of an additional approach: attacking military targets to heighten the opponent's perceptions of the costs and difficulties of seeking victory. We should expect those nations to strike Department of Defense (DoD) command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) assets to disrupt US decision-making and weaken of US leaders' confidence that they can prevail. Beijing and Moscow will also attempt to destroy US forces in the crisis zone and conduct anti-access/area denial (A2/AD) operations to prevent reinforcements from arriving. In addition, they can launch cyberattacks against US civilian ports and domestic transportation systems

[594] DiResta, "Computational Propaganda."

[595] Johnson, *Information Disorder Machines*, 12.

[596] NCSC, *National Counterintelligence Strategy*, 3 and 6.

essential for deploying troops and munitions to the region, and strike the allied ports that will receive American forces and enable their onward movement. The cognitive goal of all such attacks: persuade US leaders that victory has become too costly and difficult to achieve relative to the benefits they can hope to gain by continuing to fight.

China and Russia will conduct IOs to reinforce the coercive effects of strikes against US military assets and civilian infrastructure. The doctrines of both nations call for the integrated use of IOs with cyberattacks and kinetic attacks, aimed at driving adversaries to yield as early as possible in a conflict and thereby achieve their goals without incurring the costs and escalatory risks of full-scale combat. Coercive messaging will be especially important for seeking low-cost victories during what Russian military publications term the "initial period of war," including sudden and potentially deceptive transitions from the dark-gray zone to cyberwarfare.

The United States should reinforce its ability to deter combined attacks. It must also develop defensive capabilities against coercion in case deterrence fails. DoD is developing countermeasures against Chinese and Russian A2/AD capabilities and is securing its C4ISR networks. US infrastructure operators are hardening their systems as well. Entirely absent are efforts to defeat the IOs that will accompany enemy attacks. The United States needs a strategy to counter Beijing and Moscow messaging that US crisis operations are doomed to fail. Federal agencies and their social media partners should also prepare for the shift from threatened to actual punishment, and be able to block and counter messages against graphic, fear-inducing portrayals of public suffering and threats that greater pain will follow unless the president sues for peace.

China

China's concept of "system destruction" warfare [体系破击战] highlights how the People's Liberation Army (PLA) will attack US C4ISR networks and other targets to not only degrade US combat power but also achieve psychological effects. The PLA's shift toward "informatized warfare" suggests additional implications for US defensive requirements against combined operations. So do Chinese capabilities to disrupt US critical infrastructure—most notably, the natural gas pipeline systems on which power generation and home heating depend across much of the United States.

System Destruction, A2/AD, and Informatized Warfare

Beijing has closely studied the rise of network-centric warfare in the United States military.

System destruction warfare is designed to disrupt the C4ISR assets that provide the "nervous system" for US-networked operations.[597] System destruction attacks seek to paralyze the functions of the enemy's operational systems.[598] In particular, by disabling C4ISR networks and other systems essential for coordinating US naval and air operations, China could significantly impede US power projection in the South China Sea or adjacent regions.[599]

China will employ cyber weapons along with electronic warfare and other means of attack to disrupt US C4ISR networks and assets and achieve "information dominance" [制信息权] as early as possible in a conflict.[600] Attacks on US military satellites exemplify this threat. PLA leaders see counterspace operations as a means to deter and counter possible US military interventions during regional conflicts. Chinese military documents also suggest that reconnaissance, communications, navigation, and early-warning satellites could be among the targets of attacks designed to "blind and deafen the enemy."[601] All such attacks would be part of a broader cyber-enabled campaign to disrupt US decision-making and operational control over American forces. China will also structure such attacks to gain the advantage from the moment that combat begins. The US Defense Intelligence Agency (DIA) warns that the PLA could conduct cyberattacks to "establish information dominance in the early stages of a conflict to constrain an adversary's actions, or slow its mobilization and deployment" of forces to the region.[602]

Other types of weaponry can help China seek initial military dominance in the crisis zone and then disrupt the flow of US reinforcements. Beijing is rapidly upgrading the PLA forces necessary to defeat US naval and air forces in the South China Sea or elsewhere in East Asia. The PLA is bolstering its capabilities for A2/AD operations, including advanced conventional land-based ballistic missiles, cruise missiles, and integrated air defenses. The most comprehensive DoD assessment of the PLA (the 2020 *Military and Security Developments Involving the People's Republic of China*) states that China has already matched or exceeded the United States in modernizing all three types of forces. China will combine the use of all such weaponry in system destruction warfare with efforts to paralyze the functions of the enemy's operational systems.[603]

This form of warfare seeks to achieve both physical and behavioral effects. By destroying US military assets, disrupting the flow of reinforcements, and weakening US command and control, Beijing will seek to diminish US hopes of prevailing and undermine US leaders' resolve to continue fighting.[604] Attacks on C4ISR systems will go hand-in-hand with psychological operations aimed at "dampening the morale" of opposing forces and weakening the enemy's will to resist. Such operations will also seek to confuse adversary decision-making and exacerbate the enemy's concerns over facing an unfavorable situation if the war continues.[605]

China's 2019 Defense White Paper and other statements of PLA doctrine stress that such efforts to shape adversary behavior also reflect an overall shift toward "informatized wars"—conflicts where dominance over the information domain is decisive to victory.[606] Informatized wars and efforts to achieve

[597] Engstrom, *Systems Confrontation and System Destruction Warfare*, 15; Flournoy, "How to Prevent a War in Asia"; and *Defense One*, "C4ISR."

[598] Engstrom, *Systems Confrontation and System Destruction Warfare*.

[599] Flournoy, "How to Prevent a War in Asia."

[600] Kania and Costello, "Strategic Support Force," 117; and DIA, *China Military Power*, 45.

[601] OSD, *Military and Security Developments 2018*, 40.

[602] DIA, *Challenges to Security in Space*, 20–21.

[603] Engstrom, *Systems Confrontation and System Destruction Warfare*.

[604] Flournoy, "How to Prevent a War in Asia."

[605] Engstrom, *Systems Confrontation and System Destruction Warfare*, 71–72.

[606] USCESRC, *2019 Report to Congress*, 291.

information dominance include not only psychological attacks and propaganda but also electronic warfare, cyber operations, and other actions to disrupt enemy decision-making and operational command and control.[607]

China has also been reorganizing the PLA to facilitate this transition and integrate disparate capabilities for informatized warfare and system destruction. In 2015, the PLA established the Strategic Support Force (SSF) with the explicit goal of improving the PLA's ability to execute both warfighting concepts.[608] The SSF is responsible for the coordinated employment of space, cyber, and electronic warfare to "paralyze the enemy's operational system-of-systems" and "sabotage the enemy's war command system-of-systems" in the initial stages of conflict.[609] The PLA created the Network Systems Department within the SSF to remove organizational silos that once separated these capabilities and integrate them with psychological warfare missions and operations.[610] DoD has determined that the SSF's "current major target is the United States."[611]

To counter China's integrated strategy to disrupt and influence US decision-making, it will be essential to not only account for system destruction and informatized warfare but also keep pace with future changes in doctrine and technologies to implement them. One such change is already underway. The Office of the Secretary of Defense's 2020 *Annual Report to Congress* notes that by incorporating the use of artificial intelligence and enabling technologies such as cloud computing and big data analytics, China is transitioning from informatized warfare to "intelligentized" warfare.[612] US defensive initiatives will need to ramp up accordingly.

Coercion through Punishment

In addition to degrading US military capabilities to shape US leadership assessments of the costs of continuing to fight and the difficulty of prevailing, Beijing can use combined attacks to inflict suffering on the US public and warn that additional pain will follow unless the president yields. The PLA is rapidly improving its ability to attack the infrastructure on which US public health and safety depend. The US natural gas system offers a case in point. In the 2019 worldwide threat assessment hearing, Dan Coats, then director of national intelligence, warned that Chinese cyberattacks could cause the "disruption of a natural gas pipeline for days to weeks" in the United States.[613] In New England and other US regions that rely on a tiny number of interstate gas transmission pipelines, a multi-week cutoff of a such a pipeline would create cascading infrastructure failures of growing severity.

Homes that depend on gas for heating would face immediate effects, especially if the crisis coincided with a polar vortex or other severe cold-weather event that increased demand for heating while also disrupting gas supplies.[614] Electric power generation would be the next to go. In many portions of the United States, generation heavily depends on the flow of natural gas. The reliability coordinator for New England's power system has warned that even a very limited disruption to natural gas infrastructure "would result in frequent energy shortages that would require frequent and long periods of rolling blackouts."[615] China cutting off a major

[607] OSD, *Military and Security Developments 2020*, 74.

[608] Ni and Gill, "Strategic Support Force,"6.

[609] Lectures on the Command of Joint Campaigns [联合战役指挥教程], 164, trans. Costello and McReynolds, *China's Strategic Support Force*, 40. The creation of the SSF, in part, reflects efforts to operationalize new concepts in Chinese military doctrine that call for this coordinated employment of offensive capabilities to achieve information dominance. See Kania and Costello, "Strategic Support Force," 5, 10, 108, and 117.

[610] OSD, *Military and Security Developments 2019*, 48.

[611] OSD, *Military and Security Developments 2020*, viii.

[612] OSD, *Military and Security Developments 2020*, 161.

[613] *Hearing on Worldwide Threat Assessment*, Coats statement, 5.

[614] EIS Council, *EPRO® Handbook II: Volume 1—Fuel*, 213.

[615] ISO-NE, *Operational Fuel-Security Analysis*, 50.

transmission pipeline for multiple weeks would produce still more extensive power outages.

Such blackouts would have effects far beyond the grid. Hospitals, water and wastewater systems, and other lifeline infrastructure sectors all depend on grid-provided electricity to function. A growing number of these facilities have backup power generators. But in a multi-week event, these generators will soon begin to break down, and refueling them will become increasingly difficult—especially given the disruptive effects of power outages on transportation systems essential for fuel resupply.[616] Electricity-dependent infrastructure will break down accordingly, with water and wastewater system failures posing especially urgent challenges for saving and sustaining lives.[617]

These disruptions will not only cascade across multiple sectors but also reinforce each other in complex ways. Gas–electric interdependencies provide a case in point. As noted above, gas-fueled power generators are a predominant source of power in many US regions.[618] At the same time, natural gas systems increasingly rely on electricity for pipeline compressors that keep gas flowing to power generators.[619] These gas–electric interdependencies create efficiencies but also shared vulnerabilities. If adversary cyberattacks can inflict long-duration, multistate blackouts, the loss of power will disrupt electric-powered compressors and other gas system components. In turn, disrupted gas systems will be unable to provide fuel to power generators, including those essential for reenergizing the electric grid and restoring power to gas systems.[620]

Attacks that would create such devastating effects would be sure to incur a proportional US response. Rather than immediately escalate to such costly exchanges as the crisis transitions to combat operations, Beijing may attempt to coerce the president to back down with small-scale, exemplary attacks. PLA studies note that warning or demonstration strikes against select military, political, and economic targets can achieve "awing effects" to help deter adversaries intervening in a crisis.[621] As US decision-makers assess the costs and benefits of coming to the aid of their regional allies, achieving such awing effects could be useful indeed from the Chinese perspective.

Many US infrastructure systems are better suited for exemplary attacks than the grid's high-voltage transmission systems and natural gas transmission pipelines. The interconnected structure of the grid could, in theory, enable attacks to target their strikes to create cascading outages across wide areas. But electric utilities are making significant investments

[616] ISO-NE notes that fuel delivery logistics in the face of a "delivery supply chain [that has] withered" is considered an "unquantifiable X factor" for resupply operations. See ISO-NE, *Operational Fuel-Security Analysis*, 16 and 14.

[617] While many utilities are working on acquiring backup generators and expanding other emergency power capabilities, sustaining water and wastewater systems in long-term power outages will be impossible without prioritized restoration to these facilities. Trucking in bottled water supplies will also prove inadequate to maintain public health and safety in extended durations. See EIS Council, *EPRO® Handbook II: Volume 2—Water*, 114 and 183–188.

[618] This reliance on natural gas for power generation is particularly acute in New England, California, the mid-Atlantic, and a handful of other US regions. The North American Electric Reliability Corporation (NERC) notes that some areas within North America depend natural gas to meet over 60 percent of peak demand generation. See NERC, *2018 Long-Term Reliability Assessment*, 7; and NERC, *Potential Bulk Power System Impacts*, vii.

[619] DOE, *Quadrennial Energy Review*, 4–32.

[620] Many critical gas compression stations have backup generators and a limited storage of fuel for them. However, in an extended, long-duration outage, diesel distributors' ability to resupply these facilities would be at major risk—especially given the severe disruption to transportation networks that such a blackout would create. ISO-NE has noted that fuel delivery logistics in the face of a "delivery supply chain [that has] withered" is considered an "unquantifiable X factor" for resupply operations. See ISO-NE, *Operational Fuel-Security Analysis*, 16 and 14; and EIS Council, *EPRO® Handbook II: Volume 1—Fuel*, 35.

[621] OSD, *Military and Security Developments 2020*, 83.

to prevent cascading effects. Furthermore, as noted above, if adversaries overcome the immense difficulties of creating wide-area blackouts, they would face devastating US retaliation for doing so.

Electric distribution systems offer more appropriate targets for exemplary attacks. Distribution systems carry electricity from transmission systems to consumers and are increasingly at risk from cyberattacks.[622] China can target specific distribution substations and feeders to create blackouts that would create severe but localized effects. Water systems offer similar opportunities for exemplary strikes. Water utilities are almost always "stand-alone" systems that are not interconnected with their neighbors. The cutoff of water service in one city (by disrupting the industrial control systems that are increasingly vital to its operations) would not spread to other cities.[623] The same is true of cyberattacks on major chemical plants and other infrastructure facilities. Yet, while all such attacks would remain limited in geographic scope, they could have quick and potentially catastrophic effects on public safety. That makes these types of targets ideal for exemplary attacks, paired with nationwide messaging to magnify public fears and pressure US leaders to capitulate before additional attacks occur.

China may also conduct exemplary attacks earlier than US decision-makers expect in an intensifying crisis and (together with preemptive system destruction attacks) seek to gain the psychological and physical upper hand in the initial phase of war. PLA doctrine stresses that cyber and network attack operations can be an "indispensable method of deterring powerful enemies" as conflicts emerge.[624] Chinese military writings emphasize that seizing the initiative is the "single most decisive factor in controlling and winning a war."[625] US policymakers and their private sector partners (including infrastructure owners and social media companies) should develop operational playbooks for defense against early, demonstrative attacks, as well as the higher levels of physical damage and psychological pressure that may follow.

Russia

Former director of national intelligence Dan Coats stated in 2019 that Moscow is "staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis" along with posing "a significant cyber influence threat" to shape US behavior.[626] Russia's capabilities to conduct combined cyber-information attacks continue to grow. That growth reflects the crucial role that President Putin and his advisors believe IOs will play in future conflicts—a belief reinforced by the lessons they drew from the color revolutions and the implications for Putin's own grip on power.

A New Form of Warfare?

In 2013, the chief of the general staff of the Russian Armed Forces, General Valery Gerasimov, noted that a fundamental change was underway in his military's understanding of how to prevail in future conflicts. Gerasimov wrote:

> In the twenty-first century we have seen a tendency toward blurring the lines between the states of war and peace. . . .
>
> The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, the [rules of war] have exceeded the power of force of weapons in their effectiveness.

[622] GAO, *Electric Grid Cybersecurity*.

[623] DHS I&A, *Malicious Cyber Actors.*

[624] Huxley and Choong, *Asia Pacific Regional Security Assessment 2019*, 77–90.

[625] Jacobson, "Sino-Russian Convergence."

[626] *Hearing on Worldwide Threat Assessment*, Coats statement, 5.

> The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population.
>
> All this is supplemented by the military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces.[627]

Gerasimov's official pronouncements on the primacy of informational conflict and other "nonmilitary measures" prompted Western analysts to characterize Russia's new approach to conflict as "the Gerasimov Doctrine."[628] However, more recent analysis suggests that Russian IOs and related doctrinal innovations reflect diverse organizing principles and deep historical roots.[629] The Soviet-era military placed a strong emphasis on using IOs in conjunction with destructive attacks on enemy infrastructure and other targets.[630] This emphasis continued in post-Soviet army doctrine. In 1996, Acting Chief of the Russian General Staff Viktor Samsonov stated that "the high effectiveness of information warfare systems, in combination with highly accurate weapons and non-military means of influence, make it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population."[631]

This conception of warfare became still more prominent with the publication of the 2003 *Armeyskiy Sbornik* (Russian army journal) article "If There Were War Tomorrow" by Makhmut Gareyev, the president of the Russian Academy of Military Sciences. Gareyev argued:

> In recent decades we have become witnesses to how entire nations and coalitions of nations have come to be destroyed in the course of confrontation in the international arena without the direct use of armed force. . . . The correlation of political, diplomatic, economic, information, psychological, and military means of fighting in the international arena have changed markedly in contemporary times. The significance and proportionate share of nonmilitary means have increased significantly.[632]

Other pre-Gerasimov senior military officers voiced similar perspectives and called for Russia to prepare for "New-Generation War" in which IOs would be combined with precision kinetic attacks to shape adversary behavior.[633] Russian military theorists continue to use the term *new-generation warfare*, though Western writing on Russian combined operations often refers to *the Gerasimov doctrine*, *hybrid warfare*, *unconventional warfare*, or other alternatives.[634]

[627] Gerasimov, "Value of Science Is in the Foresight," originally published in *Military-Industrial Kurier* in 2013 and trans. Coalson (2014) and republished in *Military Review*.

[628] Galeotti, "'Gerasimov Doctrine.'"

[629] Rumer, *Primakov (Not Gerasimov) Doctrine in Action*; Galeotti, "Sorry for Creating the 'Gerasimov Doctrine'"; and Galeotti, *Russia's Intelligence Services*.

[630] Snegovaya, *Putin's Information Warfare in Ukraine*, 7 and 12–13. The Soviet military's focus on "reflexive control" was especially significant. Reflexive control entails the use of IOs to manipulate an adversary's perception of the world in order to predetermine its decision-making in a way that supports Russian interests. See Giles, *Handbook of Russian Information Warfare*, 19.

[631] Joyal, "Cyber Threats and Russian Information Warfare."

[632] Gareyev, "If There Were War Tomorrow," *Armeyskiy Sbornik*, April 1, 2003, trans. Robinson et al., *Modern Political Warfare*, 43. For a detailed review of Russian schools of thought on information warfare, see USASOC, *Little Green Men*, 14–20.

[633] Robinson et al., *Modern Political Warfare*, 44–45. This report includes key translated quotes from Chekinov and Bogdanov, "New-Generation War," 12–23.

[634] As noted in this study's section *How Coercion Is Supposed to Work*, the use of *hybrid warfare* is especially common in US and NATO studies of recent Russian operations in eastern Europe. In Russian writing, this term is more frequently used

The "color revolutions" in Russia's near abroad also drove a broader reassessment of the offensive and defensive implications of IOs for Russian security. Former Russian chief of general staff Yuriy Baluyevsky emphasized that in the regime changes in Georgia, Ukraine, Kyrgyzstan, and other eastern European nations, the West coerced change "primarily by covert and overt methods of political and diplomatic, economic, and information influence, various subversive actions and interference in the internal affairs of other countries."[635] The Arab Spring provided further lessons learned for the Russian military on the importance of IOs versus traditional instruments of military power. In Russia's view, these popular uprisings were driven by the use of sophisticated new types of IOs by the United States and its allies.[636]

Risks of IO-driven regime change also hit Russian leaders closer to home. In Russian president Vladimir Putin's assessment, Western IOs were responsible for mobilizing over ten thousand protesters across several Russian cities during Russia's December 2011 legislative elections.[637] The *Military Doctrine of the Russian Federation* (issued in December 2014 and still in effect) featured the broader risks that such IOs could pose to the Kremlin's rule. Noting that "there is a tendency towards shifting the military risks and military threats to the information space and the internal sphere of the Russian Federation," the doctrine warned that the main internal military risks to Russia included activities aimed at "destabilizing [the] domestic political and social situation in the country," and "subversive information activities against the population. . . ."[638]

This assessment of the potency of information-based attacks spurred two major changes in Russian security plans and capabilities. First, Putin's government launched defensive initiatives to prepare against future IOs by the West, including those that the United States might employ in a confrontation with Russia. The *Doctrine of Information Security of the Russian Federation* (2016) specifies the measures Russia would take to strengthen "the protection of the critical information infrastructure" and the protection of the Russian people "from the effects of emergencies caused by information." In particular, the strategy called for Russia to develop plans and capabilities for "Russian Internet segment management."[639]

Those defensive efforts are accelerating.[640] Their prospects for success, however, are not yet clear. Over the past few years, Russian opposition leader Alexei A. Navalny has made expert use of YouTube, Instagram, and other platforms to convey anti-government messaging to his fellow citizens. The Kremlin has been either unwilling or unable to block access to that messaging.[641] But Russia's primary goal in developing options to segment its internet may be for crisis situations. Kremlin officials claim that they are prepared stand up a "sovereign RuNet"—a network that would continue to give Russians access to Russian websites even if the Kremlin cut off the country from the World Wide Web. According to Dmitry A. Medvedev, the vice chairman of Mr. Putin's Security Council and a former prime minister, "In principle, it will be possible to restore or enable the autonomous functioning of

to describe *US* military doctrine, rather than Russia's own. See Adamsky, *Cross-Domain Coercion*, 9.

[635] Giles, *Handbook of Russian Information Warfare*, 41; Vilmer et al., *Information Manipulation*, 54; and Adamsky, *Cross-Domain Coercion*, 21–22.

[636] Vilmer et al., *Information Manipulation*, 54 and 56; Adamsky, *Cross-Domain Coercion*, 20 and 23; Giles, *Handbook of Russian Information Warfare*, 41–42; and USASOC, *Little Green Men*, 3.

[637] Vilmer et al., *Information Manipulation*, 54.

[638] Putin, *Military Doctrine*, trans. Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, "Military Doctrine."

[639] Putin, *Doctrine of Information Security*.

[640] Wakefield, "Russia 'Successfully Tests' Its Unplugged Internet"; and Taylor, "Russia Could Disconnect Itself."

[641] Troianovski, "China Censors the Internet."

the Russian segment of the web," and that "technologically, everything is ready for this."[642] US policymakers should assume that Russia will move to cut its population off from Western messaging in future confrontations, while doing everything possible to maintain access to the US public to generate fear and support for settling on the Kremlin's terms.

The second change that Putin demanded was that the Russian military bolster its offensive IO capabilities. Russia's military doctrine requires its armed forces "to enhance capacity and means of information warfare."[643] These advances are going forward in tandem with Russian efforts to protect its own citizens against possible US IOs. As the US DIA notes, "Moscow perceives the information domain as strategically decisive and critically important to control its domestic populace and influence adversary states."[644] US crisis planning should include preparedness for Russia to conduct simultaneous, integrated offensive and defensive IOs.

US strategies should also account for the specific features of Russian doctrine for combined information-cyberattacks. The United States should prepare for Russian efforts to exploit such possibilities through coercion by denial, including the use of microtargeted IOs against US military personnel in emerging crises, and—as discussed below—the impersonation of US and allied leaders to cripple coalition options before they even begin.

Russian Military IOs in Future Crises: Doctrinal Underpinnings and Recent Developments

The Russian military's GRU (the Main Intelligence Directorate of the Russian Armed Forces) is a leading contributor to the ongoing, long-term campaign that Russia is conducting to influence US elections and corrode the US public's confidence in democratic institutions.[645] However, Russian military publications also offer compressive guidance on employing IOs in conflicts. IOs fall within the broader categories of "information warfare" (*informatsionnaya voyna*) and "information confrontation" (*informatsionnoye protivoborstvo*), which also include cyber operations against enemy systems, electronic warfare, and other activities.[646] The 2011 *Russian Federation Armed Forces' Information Space Activities Concept* emphasized the need to integrate all these components in future confrontations. According to that document, information warfare entails:

The confrontation between two or more states in the information space with the purpose of inflicting damage to the information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefits of the opposing force.[647] These combined operations to shape public and leadership perceptions will occur across the full spectrum of conflict. Assistant Secretary of Defense Christopher Maier notes that Russia seeks "information dominance during peacetime and armed conflict with equal intensity using combined electronic and kinetic means and methods through information-technical, information-psychological, and active measures."[648] Daniel Flynn of the Office

[642] Troianovski, "China Censors the Internet."

[643] Putin, *Military Doctrine*.

[644] DIA, *Russia Military Power*, 37.

[645] SSCI, *Russian Active Measures, Vol. 2*, 7–8 and 63–64.

[646] DIA, *Russia Military Power*, 37–38; Giles, *Handbook of Russian Information Warfare*, 6; Tashev, Purcell, and McLaughlin, "Russia's Information Warfare," 139; and Smith, "How Russia Harnesses Cyberwarfare," 7–8. For a review of additional sources, see Connell and Vogler, *Russia's Approach to Cyber Warfare*, 3–4.

[647] Ministry of Defence of the Russian Federation, *Information Space Activities Concept*, trans. Mazarr et al., *Hostile Social Manipulation*, 54.

[648] *Hearing on Disinformation in the Gray Zone*, Maier statement.

of the Director of National Intelligence (ODNI) notes the threat that this drive for dominance poses for US crisis decision-making: "Russia is adopting coercive strategies involving the orchestrated employment of nonmilitary and military means to deter and compel the United States prior to and after the outbreak of hostilities."[649]

As with China, Russia will tailor its combined attacks for maximum coercive effect during the transition from the dark-gray zone to destructive cyberattacks and kinetic attacks. Drawing on detailed studies of Russian military publications, Timothy Thomas and other analysts argue that we should expect Russia to use IOs in the initial period of war to help seek quick and relatively low-cost victory.[650] Russian military writers S. G. Chekinov and S. A. Bogdanov note that the initial period of war will include psychological attacks, electronic operations, and fire strikes to disorganize government systems, demoralize populations, and prevent leaders from rallying forces to repel aggression. They also contend that mass media will be employed in the initial period of war to stir up chaos and confusion in an adversary's government and military management and control systems.[651] P. A. Doulnev and V. I. Orlyansky emphasize the goal of putting an adversary on the verge of defeat at the beginning of hostilities, accomplished by wreaking havoc on its political and economic situation by (1) using information technology–generated psychological and other types of warfare; and (2) by disabling the adversaries control of the country and armed forces through attacks on strategic installations and infrastructure.[652]

Russia will also structure its use of IOs and cyber/kinetic/electronic warfare operations to manage escalation. Flynn, the ODNI analyst, assesses that the Kremlin may adopt a phased approach to coercive campaigns that pressures the adversary to de-escalate. The United States and its regional allies should be prepared for the following phases of an intensifying crisis:

> Prior to hostilities, Moscow seeks to shape the strategic environment to dissuade US or NATO intervention against Russian security interests. At the onset of hostilities, Russia's goal is to prevent further aggression and compel a de-escalation and end the conflict on terms favorable to Moscow as soon as possible. Russia's approach seeks to negate any benefits an adversary hopes to attain at each level of conflict by signaling capabilities and willingness to impose costs at even higher levels of escalation to dissuade further military operations and compel a de-escalation of hostilities.[653]

The United States should also prepare for abrupt Russian jumps up the escalatory ladder. Rather than gradually intensifying the destruction of US infrastructure and reinforcing US leadership and public fears of further devastation to come, the Kremlin may also seek to shock the United States into backing down by launching comprehensive strikes early in a confrontation.

US defense officials have called for the United States to prepare against such tactics. In June 2015, then US deputy secretary of defense Robert Work and then vice chairman of the Joint Chiefs of Staff Admiral James Winnefeld observed that "Russian military doctrine includes what some have called an 'escalate to de-escalate' strategy—a strategy that purportedly seeks to de-escalate a conventional conflict through coercive threats, including limited

[649] Flynn, "Russia's Evolving Approach to Deterrence," 37.

[650] Thomas, *Russian Military Thought*; Thomas, "Russian Forecasts of Future War"; and Jacobson, "Sino-Russian Convergence."

[651] Thomas, *Russian Military Thought*, 25.

[652] Doulnev and Orlyansky, "Basic Changes in the Character of Armed Struggle."

[653] Flynn, "Russia's Evolving Approach to Deterrence," 40.

nuclear use."[654] Russian statements of military doctrine do not use the term *escalate to de-escalate*.[655] Nevertheless, that doctrine does envision the possible use of both nuclear and nonnuclear weapons to coerce adversary behavior though abrupt and unexpected increases in the adversary's costs of continuing to resist.

The use of these escalatory tactics could magnify the already profound risks that a US–Russian conflict would spiral out of control. As Work and Winnefeld note, escalating to de-escalate would be the equivalent of "playing with fire."[656] But that does not mean that the United States should count on Russian fears of escalation to deter them from conducting combined information-cyberattacks. On the contrary: the Kremlin will seek to use the dangers of spiraling devastation to shape US behavior. Russian military publications note that by intensifying an opponent's fears of escalation, including through the preemptive use of force, it may be possible to compel the opponent to back down in the conflict rather than suffer increasing and ultimately unacceptable damage.[657] Escalation is a tool of coercive operations rather than an impediment to them.

Implications for US Defensive Requirements

China and Russia are deepening the asymmetric advantages they already enjoy in the disinformation realm and will leverage those advantages in future combined attacks. With the Great Firewall and RuNet, these nations will seek to deny access to Western messaging in future crises, while simultaneously using advanced tactics, techniques, and procedures, or TTPs (including the use of US- and allied-based infrastructure) to deliver coercive messaging. US defensive strategies should seek to minimize these asymmetries—not by aping Chinese and Russian repression of their own citizens, but by developing measures to IOs that accompany and seek to magnify the psychological effects of limited, exemplary attacks. The United States and its allies should also pay special attention to the risks and defensive opportunities that the initial period of war will entail. As in Russia's invasions of Georgia and Ukraine, adversaries may seek to employ hybrid warfare tactics to delay and confuse a victim's initial decision-making and then consolidate their gains before the West can respond. Policymakers need to assess how Chinese doctrines for system destruction warfare and Russian equivalents for early disruptive attacks might be paired with such deceptive measures at the outset of warfare. And, in partnership with infrastructure operators, US and allied governments should develop defensive playbooks to employ as crises approach and then cross over the edge of war.

Policymakers should also avoid the temptation to develop playbooks only for attacks that would create cascading effects across multiple sectors (as in natural gas systems) or that could spread across multiple US regions (as in high-voltage transmission systems). Adversaries may initially seek to prevail with exemplary strikes rather than mass-casualty events. Accordingly, a broad range of industries and sector-specific agencies will need to prepare for combined attacks, including those like the Environmental Protection Agency (responsible for water system security) that have little expertise in countering Chinese or Russian malware and messaging. Building an efficient way to fill these

[654] *Hearing on Nuclear Deterrence in the 21st Century*, Work and Winnefeld statement, 4; see also US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault*, 103–104.

[655] Dave Johnson argues that while Russian military doctrine does not employ the term *escalate to de-escalate*, Russia applies doctrine under other terminology that embraces both coercion and escalation management using both nonnuclear and nuclear weapons. See Johnson, *Russia's Conventional Precision Strike Capabilities*, 8 and 67. For a broader analysis and critique of US assessments concerning the use of "escalate to de-escalate" as a coercive tool, see Schneider, "Escalate to De-escalate"; and Ross, "Time to Terminate Escalate to De-escalate."

[656] *Hearing on Nuclear Deterrence in the 21st Century*, Work and Winnefeld statement, 4.

[657] Flynn, "Russia's Evolving Approach to Deterrence," 37.

defensive gaps must be a key focus of US strategies against coercion.

Defeating Customized Attacks

While the military doctrines of China and Russia provide an overview of the coercive threats they pose, countering those threats will require a deeper level of analysis. Both nations will tailor their coercive operations to exploit specific features of American society, the US crisis decision-making process, and security partnerships with regional allies. US policymakers need to assess how adversaries will fine-tune their attacks and adapt US defensive measures accordingly.

Beijing and Moscow will also have to overcome specific US impediments to manipulation—impediments that reflect deeper problems in the causal linkages that drive coercion. In an emerging crisis, threats of punishment are supposed to generate public pressure on enemy leaders to yield. But crises have often had the opposite impact on the behavior of the American public and spurred powerful "rally round the flag" effects. Moreover, while theories of coercion often assume that inflicting public suffering will create mass panic and thereby drive the stricken nation to capitulate, little historical evidence supports that view. The analysis that follows examines how China and Russia can seek to overcome these obstacles. Personalized information operations (IOs) against US leaders are the new normal. However, to drive the perceptions and behavior of policy elites, Beijing and Moscow may also attempt to acquire and exploit a detailed understanding of the US crisis decision-making process. Bureaucratic infighting between US agencies and the organizational routines they tend to follow may offer highly specialized opportunities for attack. US military personnel and other players in the broader game of shaping and implementing US policy offer additional opportunities for customized coercion.

In addition, China and Russia can develop sector-specific attacks to achieve distinctive coercive effects. The financial services sector offers one potential target of such customized operations. The communications sector offers another, especially for selectively cutting off US media to reinforce the impact of adversary messaging. The analysis that follows analyzes threats to both sectors to illustrate the need for infrastructure-specific defensive strategies.

Customization will also be the norm for counter-alliance campaigns. Every US security partner's leadership and population will be targeted with IOs to widen existing fissures with the United States and undermine support for coalition operations. Adversaries may target US theories of victory as well. As previously noted, Russia and China can attack US regional forces and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) to convince the president that it will be too costly, and ultimately futile, to continue fighting. This section analyzes how adversaries may supplement such attacks by disrupting the US domestic infrastructure necessary to "surge" US reinforcements to the crisis zone and achieve coercion by denial.

Mobilizing Public Pressure on the President to Yield: Problems for Attackers and Opportunities for Defense

For decades, political scientists have found that crises tend to bolster support for presidents and their decisions. One survey of public response to wars and intense foreign confrontations found that it is "a basic rule of American politics" that "Americans rally round the president in times of national crisis."[658] Many other studies have reached similar conclusions, with 9/11 providing a prominent example of spiking public support (see Figure 3).[659] Given these repeated instances of rallying behavior, a crisis would seem to be the worst possible time for adversaries to use IOs to sow distrust and foment opposition to a president's decisions.

Yet, rally-round-the-flag effects among the US population may be weaker in future confrontations. Recent conflicts have corroded public confidence that official justifications for US leadership decisions are valid. The threat assessments used by President George W. Bush's administration to justify the invasion of Iraq, including those associated with Iraqi development and possession of weapons of mass destruction, turned out to be greatly (and perhaps intentionally) exaggerated.[660] Senior Obama administration officials offered totally inaccurate assessments of al Qaeda's attacks on the US compound in Benghazi.[661] More recently, revelations regarding internal US government reports on Afghanistan suggest that US leaders across multiple administrations repeatedly misrepresented progress in achieving the war's goals.[662] These repeated official falsehoods could not only corrode future rally-round-the-flag effects but also create an opening for divisive adversary messaging in future confrontations. Polling data indicates that public confidence in US leaders is undergoing precisely such a long-term decline.[663]

The fracturing of US society along partisan lines can further dampen the public's tendency to rally round the flag. Future regional crises are sure to spark disagreements over the wisdom of defending US allies and the potential costs of doing so. By widening the fissures within the public and fostering hostility between Republicans and Democrats—and seeking to intensify those divisions in mass media—Russia is weakening the foundations on which rally-round-the-flag effects once rested.

Past assessments of rally-round-the-flag effects also occurred when US citizens relied on television, newspapers, and other legacy communications systems. The rise of social media has transformed this information environment in ways that offer unprecedented opportunities to generate opposition to the president's crisis polices. As discussed earlier in this study, adversaries can use social media to directly access US citizens. The public is also more prone to sharing inflammatory messaging (even if false) over social media and tend to believe widely distributed stories from humans or bots regardless of their accuracy. Especially important: using AI and other advanced IO technologies, adversaries can microtarget IOs at scale to counter incipient rally-round-the-flag behavior.

Significant portions of the US population will still rally in support of the president in the face of such efforts. The challenge for US counter-messaging and other defensive operations will be to expand

[658] Lindsay, "Rally 'Round the Flag."

[659] Moore, "Bush Job Approval"; Hetherington and Nelson, "Anatomy of a Rally Effect," 37; Lambert, Schott, and Scherer, "Threat, Politics, and Attitudes," 343; and Gershkoff and Kushner, "Shaping Public Opinion," 525. The foundational work for the extensive literature on "rally round the flag" effects is Mueller, *War, Presidents, and Public Opinion*. Pape concludes that the citizens of other nations have frequently displayed behavior equivalent to that of rallying round the flag in the United States. Pape, *Bombing to Win*, 24–25.

[660] Kaufmann, "Threat Inflation," 5–6.

[661] Douthat, "Mystery of Benghazi."

[662] See the *Washington Post*'s Afghanistan Papers series, including Whitlock, "At War with the Truth"; and Johnson, "I Helped Craft the Official Lies."

[663] Pew Research Center, *Public Trust in Government*.

that rally behavior beyond those who voted for the president and to counter adversary efforts to sharpen partisan divisions over the defense of US allies. Policymakers will also need to build preparedness against two additional ways that adversaries can generate public pressure on the president to yield: combined attacks that target infrastructure of special psychological and political significance and the selective cutoff of communications to disrupt US counter-messaging and reinforce the impact of Chinese and Russian IOs.

Sector-Specific Attacks and Levers of Influence: Threats to Banking, Equity Markets, and the Broader Financial System

Past coercive campaigns have inflicted suffering on adversary populations by directly bombing them (as in the London Blitz) or disrupting electric systems and other critical infrastructure essential for public health and safety (as in Operation Allied Force, or OAF). Although Beijing and Moscow could conduct cyberattacks against US infrastructure to inflict suffering, perhaps initially on an exemplary basis, they could also strike other types of targets to generate public pressure on US leaders to yield. One option for doing so would be to heighten the perceived costs of allied defense in a literal way—by disrupting the US financial system to convince Americans that their life savings and economic survival are in jeopardy.

Most cyberattacks on the financial services sector are motivated by greed. Cyber criminals in Russia and other nations are increasingly adept at stealing money from banks and other sources of illicit revenue.[664] The scale of these thefts continues to grow. The Carbanak group targeted financial institutions to steal more than $1 billion between 2013 and 2018. States and state-sponsored attackers have also become prime cyber thieves, with North Korea alone having stolen some $2 billion from at least thirty-eight countries in the past five years.[665] Criminals are also using increasingly sophisticated means of raiding the financial services sector. In February 2016, hackers targeted the central bank of Bangladesh and exploited vulnerabilities in SWIFT, the global financial system's main electronic payment messaging system, in an attempt to steal $1 billion. While most transactions were blocked, $101 million still disappeared. [666]

The Department of the Treasury's Office of Financial Research warns that "wide-reaching theft" (including via cyber means) could cause a broader loss of confidence in the financial system.[667] However, by targeting SWIFT and other critical financial systems and institutions, attackers may destabilize the system not because they have stolen money but because it is their primary goal. The International Monetary Fund (IMF) warns, "Today, the assessment that a major cyberattack poses a threat to financial stability is axiomatic—not a question of if, but when."[668]

Attacks to disrupt the financial system have thus far come from nations that least depend on it. Iran's distributed denial-of-service attacks against nearly fifty major financial institutions between 2011 and 2012 were aimed at achieving systemic effects.[669] The operation disabled computer servers run by these institutions to prevent online banking and other functions and to cause other broad, disruptive impacts.[670] The Justice Department has indicted seven Iranians—working on behalf of the Iranian government, including the Iranian

[664] Fazzini, "'Evil Corp'"; and Perez and Shortell, "North Korean-Backed Bank Hacking."

[665] Maurer and Nelson, "Global Cyber Threat," 2.

[666] Maurer and Nelson, "Global Cyber Threat," 1.

[667] OFR, *2016 Financial Stability Report*.

[668] Maurer and Nelson, "Global Cyber Threat," 2.

[669] DOJ, "Seven Iranians."

[670] *United States v. Ahmad Fathi et al.*

Revolutionary Guard Corps—accused of conducting these attacks.[671]

Other nations have begun to exploit the vulnerability of the financial services sector to IOs. The 2013 Syrian operation to disrupt US equity markets illustrates a mode of attack of special concern with regard to future coercive campaigns. Syrian operatives gained access to the Associated Press's Twitter account and tweeted a fake claim that two explosions had hit the White House and that then-president Barack Obama was injured. The tweet generated panic selling on Wall Street. Within three minutes of the tweet, traders' responses to it erased $136 billion in equity market value.[672]

US markets quickly recovered. However, they did so because television and other reporting (supported by government pronouncements) easily established that the one-time tweet was false. Future adversaries may conduct more sustained operations across a larger number of platforms to disrupt market functions and support those operations with microtargeting, deepfake images, and other sophisticated technologies that will be far more difficult to counter. Most concerning, adversaries may combine such IOs with cyberattacks that exploit the growing vulnerability of the financial system to cyber-induced breakdowns.

Nations with little dependence on the US economy may be especially likely to seek leverage in future confrontations by using combined attacks to incite bank runs, panic selling, and other disruptive effects.[673] China (and, to a lesser extent, Russia) are much more dependent on US markets and the global financial system than Syria, North Korea, and Iran. But we should not ignore the risk that Beijing and Moscow might attack the financial services sector in conjunction with (or as an alternative to) attacks on US infrastructure essential for public safety. On their own, attacks against the latter targets would produce catastrophic effects on US–China economic relations. And in the case of Russia, efforts are already underway to prepare the battlefield. US officials found malware on Nasdaq servers in 2010 that was reportedly developed by Russia's Federal Security Service.[674] It would be prudent to assume that in the years since, Russia has continued to pre-position more sophisticated attack tools that exploit technological trends in the financial services sector and its place in the emerging information environment.

Emerging Threats: Cyberattacks, IOs, and Combined Operations

The IMF's March 2021 analysis of global cyber threats found that two ongoing trends are intensifying the risks of disruption that confront the financial system. First, the system is undergoing "an unprecedented digital transformation" that is being accelerated by the COVID-19 pandemic. Second, "malicious actors" are taking advantage of this transformation and pose a growing threat to the global financial system, financial stability, and confidence in the integrity of the system. Most worrisome are "incidents that corrupt the integrity of financial data, such as records, algorithms, and transactions; few technical solutions are currently available for such attacks, which have the potential to undermine trust and confidence more broadly."[675]

[671] *United States v. Ahmad Fathi et al.*

[672] Fisher, "Syrian Hackers Claim AP Hack."

[673] Fisher, "Syrian Hackers Claim AP Hack."

[674] Brake, *Strategic Risks of Ambiguity*, 3. The National Security Agency reportedly concluded it was possible that the malware—similar but not identical to a strain created by Russian security services—was used by a different government actor such as China. See Robertson, "Russian Malware Infiltrated the Nasdaq Servers."

[675] Maurer and Nelson, "Global Cyber Threat," 2. For additional assessments of vulnerability trends and increasing cyber threats to the sector, see FSB, *Summary Report*, 1; and OFR, *2016 Financial Stability Report*, 38–48. The Federal Reserve Bank of New York (FRBNY) also recently released a report that examines the potential cascading effects of attacks on large US banks. See Eisenbach, Kovner, and Lee, *Cyber Risk and the*

These cyber threats put the US economy at increasing risk. Federal Reserve Board chairman Jerome Powell stated in April 2021 that he is on alert for cyberattacks against US financial systems and companies. In fact, Powell emphasized that he is far more concerned about a cyber incident than he is about encountering a collapse akin to the global financial crisis of 2008. He cites as a special concern that cyberattacks will cripple the ability of financial institutions to track payments, leading to the overall breakdown of the payment network .[676]

A systemic disruption of the financial services sector would also have much broader effects. Erica Borghard notes that the sector serves as a backbone for other parts of the economy. Accordingly, cyberattacks that disrupt critical services, reduce confidence in specific firms or the market itself, or undermine data integrity could have systemic consequences for the entire US economic system and national security.[677]

Disinformation campaigns can disrupt the sector as well. A 2019 attack on the Metro Bank in northwest London illustrates how IOs can achieve such effects in a highly localized way. Dozens of people rushed the bank to demand their cash and jewelry after reading false rumors on WhatsApp that the institution was going under, creating a scene that briefly resembled a Great Depression–style bank run.[678] Jason Healey and coauthors warn that more sophisticated IOs could cause bank runs on a much larger and more disruptive scale.[679] However, that risk is only part of the much broader threat that adversary messaging could pose to the financial services sector.

A 2020 analysis by the Carnegie Endowment for International Peace noted that financial markets are shaped by their information environments and that the internet has transformed how information flows through those markets. That transformation creates new ways for actors to manipulate information in financial markets for malign purposes—for example, through influence operations. The report also finds that while significant attention has focused on the threat of influence operations to elections, "little attention has been paid to how influence operations affect financial markets."[680]

Some studies that do exist contend that recent improvements in IO technologies will not increase threats of systemic failures in the United States. Jon Bateman finds that deepfakes, voice cloning, face-swap video, and other "synthetic media" technologies do not pose a serious threat to the stability of the global financial system or national markets in mature, healthy economies. He also argues major markets seem generally resilient to disinformation campaigns, regardless of the technique used. To threaten market stability, "synthetic media would need to be orders of magnitude more powerful than traditional disinformation tools. There is no reason yet to expect that."[681]

However, the overall threat that IOs pose to the stability of financial systems in the United States and its major security partners is more dire, especially if China and Russia use such operations for coercion. Those nations are sure to integrate synthetic media with other advances in IO technologies and tactics. Microtargeting of social media messaging is the most significant of these advances and is easily paired with deepfakes and voice cloning. With technology that is primitive by today's standards, Russia delivered curated messaging to Americans in the lead-up to the 2016 election. Now, using AI, vast repositories of financial data on the US public, and other tools, Russia and other nations can

U.S. Financial System. For more on the Treasury's call for additional cyber data, see Treasury, "Agency Information Collection Activities."

[676] Vavra, "Fed Chair Deems Cyber Threat Top Risk."

[677] Borghard, *Protecting Financial Institutions against Cyber Threats*, 6.

[678] Edwards, "False Rumor on WhatsApp."

[679] Healey et al., *Future of Financial Stability*, 8.

[680] Maurer and Nelson, *International Strategy*, 68–69.

[681] Bateman, *Deepfakes and Synthetic Media*, 1 and 26.

flood the United States with personalized disinformation to create financial panic and generate coercive pressure.

Adversaries might use such integrated technologies to exploit familiar threat vectors. For example, Iran, China, or Moscow might warn individual customers of every bank in a US region (or even nationwide) that their banks are failing and that they should immediately withdraw their savings and empty their safe-deposit boxes. Another option: building on the 2013 Syrian model, they might use tailored, large-scale messaging to induce panic selling in equity markets.

Adversaries can also seek to create systemic instabilities through new forms of IO-enabled attacks. Equity market managers and their partners quickly reversed the effects of the 2013 Syrian attack. However, they did so in an "uncontested" environment in which the attackers did not target (or were unable to disrupt) response efforts. Future campaigns to induce mass sell-offs and bank runs may include follow-up disinformation to sustain that behavior and impede restoration operations. Adversaries may also use entirely different tactics to create instabilities. The Treasury Department and analysts such as Jason Healey have identified specific "channels" through which cyber events could create a financial crisis. Cyberattacks that corrupt or deny access to financial data could create loss of confidence in the system and other far-reaching effects.[682]

The use of such information attacks for coercion will create special challenges for defense. During an intense crisis with China or Russia, where risks of war (and, possibly, threats of punishment) are already putting the US public on edge, campaigns to create financial panics will occur on favorable cognitive terrain. Financial markets are particularly susceptible to disinformation because market activity is sensitive to fears and speculations driven by emerging crises.[683] Furthermore, social media provides an ideal vehicle for achieving coercion by inciting disruptive behavior. The US public increasingly relies on social media platforms to stay up to date on shifts in stock markets and broader financial trends.[684] The public also depends more heavily on social media when disasters or other fear-inducing events occur. US defensive initiatives will need to account for the combined effects of both dependencies.

Adversaries may also conduct cyberattacks to disable, disrupt, or destroy critical financial sector infrastructure and functions. The Federal Reserve Bank of New York has identified the wholesale payment network as constituting a "natural candidate for a malicious attacker intent on inflicting the largest possible damage to the financial system and the broader economy." In addition to disrupting critical functions, the Bank emphasizes that such attacks could also trigger panic-based runs on banks and spillovers into the financial sector as a whole.[685] We must assume that as the digital transformation of the US and global financial systems continues and new attack surfaces appear, adversaries will identify additional opportunities to pair IOs with cyber-induced disruptions to inflict pain on the economy and pressure US leaders to back down in a confrontation.

Implications for Defense

Financial institutions, the Treasury Department, and academic researchers are taking measures to

[682] OFR, *Cybersecurity and Financial Stability*; and Healey et al., *Future of Financial Stability*, 3–6. The study also provides a useful bibliography of research on cyber risks to the sector on page 6.

[683] The market's plunge beginning on February 24, 2020, may have been driven not only by factual reporting on the virus's global spread and its impact on supply chains, but also by the flood of disinformation surrounding the epidemic. See Rash, "Coronavirus Disinformation"; and Blackbird.AI, *COVID-19 (Coronavirus) Disinformation Report*.

[684] Zubiaga et al., "Detection and Resolution of Rumors."

[685] Eisenbach, Kovner, and Lee, *Cyber Risk and the U.S. Financial System*, 1 and 2.

defend the financial services sector against emerging threats.[686] They are also conducting exercises to help identify and mitigate threats. The Hamilton exercise series simulates a variety of possible attack vectors to identify possible sector vulnerabilities, exercise and refine the use of emergency response playbooks, and strengthen coordination between various sector components and the government. The Financial Services Information Sharing and Analysis Center partners with the Financial Services Sector Coordinating Council and the Treasury Department (the Sector Specific Agency for financial services) to develop and help execute these exercises.[687] In developing scenarios for future exercises, exercise designers should consider options that couple sophisticated IOs with gradually intensifying attacks on financial infrastructure to coerce US crisis decision-making.

The Analysis and Resilience Center for Systemic Risk is addressing the systemic dangers posed by current and emerging cyber threats to the US financial system as well as to energy sector infrastructure. The center conducts analysis of critical systems, assets, and functions; monitors and warns against threats to them; and develops measures to make them more resilient against cyberattacks and other threats.[688] Especially helpful, this approach enables asset owners and their partners to address the interdependences between the financial and energy sectors, as well as help meet their sector-specific challenges.

Countering coercive threats will require specialized measures. The private sector and the Department of the Treasury will need to strengthen preparedness for IOs that occur in the context of regional crises and that use microtargeted messaging at scale to create financial panics. Doing so will require not only getting ahead of emerging IO technologies but also anticipating how China may use financial sector–oriented campaigns within the broader context of informatized warfare. An equivalent effort will be necessary to understand how Russia could align financial crisis–inducing attacks within its own doctrinal precepts for using IOs across the conflict continuum.

Such efforts could begin by borrowing from the campaign analysis that applies to familiar punishment strategies—in other words, strategies that jeopardize public survival through population center bombing or the disruption of infrastructure essential for public health and safety. In the dark-gray realm, China or Russia may conduct IO-only campaigns to begin inciting panic selling, bank runs, or other disruptive behavior and warn that more intensive operations will follow unless the president backs down. As the crisis transitions to the initial period of war, adversaries may conduct combined information-cyberattacks against financial sector infrastructure and functions (including the corruption or denial of critical data) to intensify coercive pressure on US decision-makers. Beijing and Moscow might initially conduct combined attacks on an exemplary basis against a particular institution or function, such as the SWIFT system or the wholesale payment network. But especially in the case of Russia, the US should also be prepared for all-out attacks on the financial system very early in a crisis to shock US leaders into de-escalation.

Asset owners/operators and their government partners will need to develop playbooks for response operations in each of these phases. Tim Maurer and Arthur Nelson have called for an extensive set of preparedness efforts, including for collaboration with social media companies. Financial institutions will need mechanisms for quick coordination with social media platforms to organize content takedowns and should be familiar with the rules on platforms relating to key areas, including impersonation accounts and hacked materials. These institutions and their partners will also need to be ready

[686] Healey et al., *Future of Financial Stability*, 1 and 8.

[687] FS-ISAC, “Exercises.”

[688] ARC, “What We Do.”

to conduct rapid and adaptive counter-messaging, including corrective statements that debunk fake information and calm the markets.[689] And as with defensive partnerships for the defense against other infrastructure attacks, agencies and the private sector will need to exercise their playbooks to identify requirements for further progress and refine their response planning.[690]

Defensive initiatives with US security partners will also be vital given the global nature of many financial system functions. The Financial Stability Board established by the G-20 has published a toolkit to guide cyber incident response and recovery activities.[691] Those preparedness efforts should be expanded to account for IOs and combined attacks. Deeper integration and coordination will also be needed between those responsible for the security of the financial sector and for mitigating the coercive effects of future attacks. A recent IMF report notes that:

> different communities operate in silos and tackle the issue through their respective mandates. The financial supervisory community focuses on resilience, diplomats on norms of state behavior, national security agencies on trying to deter malicious activity, and industry executives on firm-specific rather than sector-specific risks. As lines between financial services firms and tech companies become ever more fuzzy, the lines of responsibility for security are likewise increasingly blurred. The disconnect between the finance, the national security, and the diplomatic communities is particularly pronounced. Financial authorities face unique risks from cyber threats, yet their relationships with national security agencies, whose involvement is necessary to effectively tackle those threats, remain tenuous. This responsibility gap and continued uncertainty about roles and mandates to protect the global financial system fuel risks.[692]

The need to clarify these roles and responsibilities and build deeper international collaboration is all the more important in the context of coercive threats. In regional crises, Beijing and Moscow will seek to raise the costs of opposing their demands for the United States and its security partners. Developing a collaborative approach to defeating financial panics and systemic breakdowns will be essential for allied defense.

Selective Cutoff of US Mass Communications: Threats and Defensive Options

OAF illuminated the advantages that coercive operations can gain by selectively disrupting the opponent's communications systems. During that operation, the US attacked Yugoslavia's television infrastructure while simultaneously broadcasting messages against Milosevic from outside the country. Russia employed similar measures to facilitate its seizure of Crimea. To stifle rally-round-the-flag effects and magnify public pressure on the president to give in to Chinese and Russian demands in future crises, these nations may employ technologically advanced versions of the same strategy.

Selective cutoff operations offer twofold benefits. By ensuring that the victim's population can access only communications networks that the attacker controls, the attacker can exploit that access to flood the population with coercive messaging. At the same time, by disrupting all other networks beyond those that they "own," attackers can impede efforts at counter-messaging by the victim's leadership.

[689] Maurer and Nelson, *International Strategy*, 14 and 68–72.

[690] Borghard, *Protecting Financial Institutions against Cyber Threats*, 10.

[691] FSB, "FSB Encourages Use of Cyber Incident Response and Recovery Toolkit."

[692] Maurer and Nelson, "Global Cyber Threat," 3.

The US has significant vulnerabilities to such selective disruption strategies but also the beginnings of a defensive framework to counter them.

Potential Attack TTPs

Communications cutoff strategies can vary in the degree to which they disrupt systems on which the public relies. Nationwide power outages would create the most extensive disruptions as cell towers, broadcast facilities, and other infrastructure ran out of fuel for backup power generation and as citizens' own devices (e.g., cell phones and personal computers) lost power as well. Leadership and infrastructure communications networks designed to outlast long-duration power outages would presumably remain functional. So too would citizen-operated ham radios. However, opportunities for leaders to communicate with the public would be sharply constrained. Citizens would be left literally and figuratively "in the dark" as community lifelines began to fail.

While the total cutoff of public communications could help achieve coercive effects in a crisis, adversaries might also see benefits in imposing more limited, selective disruptions. The advantage: if attackers can disrupt all communications systems except the ones they control, they can then use those systems to flood the enemy's public with uncontested disinformation. Russia has already used such selective cutoff strategies in attacking Georgia (2008) and Ukraine (2014).

Russia's 2008 intervention in Georgia paired aggressive attacks against communications systems with disinformation over Russian-controlled TV stations and other media in an effort to shape local and regional perspectives. Russia chose specific targets in order to isolate the Georgian government from its most effective means of strategic communication, limiting officials' ability to communicate with Georgian citizens and the outside world. Russian hackers also degraded internet infrastructure and disabled web resources, including government and media sites that could help manage responses to the invasion.[693] As a result of these efforts, the Georgian government initially struggled to counter the Russian propaganda and IO campaign to influence media narratives around the conflict.[694]

The 2014 attack on Ukraine leveraged lessons learned from Georgia and expanded upon them. Russia employed a similar "two sides of the coin" approach to controlling the narrative, both disrupting Ukrainian communications infrastructure and filling the information void with disinformation and propaganda. Early in the operation to seize Crimea, Russian forces occupied the Simferopol internet exchange point and cut cables that connected the Crimean peninsula to the Ukrainian mainland. Russian troops also conducted cyberattacks against telecommunications infrastructure. The result: Crimea's internet, cellular, and landline communications servers were "nearly eliminated."[695] These attacks had "devastating psychological effects" and resulted in total information dominance in Crimea for Russia, greatly complicating the Ukrainian government's efforts to establish situational awareness and serving as a critical enabler for later stages of the conflict.[696]

[693] While plenty of political and circumstantial evidence ties these denial attacks to the Russian government, hard evidence or definitive attribution is lacking. See White, *Lessons from the Russia-Georgia War*, 4.

[694] In particular, Russia carefully managed TV coverage of the events to portray Georgia as the aggressor and Russia as the savior. See USASOC, *Little Green Men*, 14. Over the course of the conflict, however, Georgia was able to gain the upper hand in the information space, and Russia failed to solidify international consensus around its version of events. The Russian military ultimately viewed its IOs in this conflict as a failure that sparked significant reform in improving IO strategy and capabilities. See Iasiello, "Russia's Improved Information Operations," 52–54.

[695] USASOC, *Little Green Men*, 46; and Iasiello, "Russia's Improved Information Operations," 54.

[696] Joyal, "Cyber Threats and Russian Information Warfare"; and Giles, *Handbook of Russian Information Warfare*, 49.

In conjunction with these cutoff operations, Russia used surviving means of communication to dominate the flow of information in Crimea and conducted an IO campaign to shape global narratives surrounding the conflict. Russian disinformation and propaganda, supported by significant cyberespionage operations, proved an effective tool to influence local, regional, and international audiences. Its IO campaign involved a coordinated use of TV broadcasts, digital news, and social media to craft false narratives and obscure the nature and extent of its operations.[697] Russia was able to create sufficient confusion and opacity to delay international responses to its invasion until it was too late.

Not all of these same TTPs will work in coercive campaigns against the United States. As in Russia's attack on Ukraine, we should anticipate that adversaries will seek to cut US undersea cable connections. But Russia will not be able to transmit TV broadcasts to US citizens from its own territory (with the possible exception of small portions of Alaska). However, social media may open up new opportunities for selective disruptions. US citizens will rely heavily on social media in any future crisis. If attackers can manipulate the algorithms that curate social media content to sustain the flow of disinformation while also conducting cyberattacks to disrupt radio and television infrastructure, new forms of selective cutoff may become possible.

Russia and other US adversaries have already proven themselves adept at manipulating social media platforms and are also developing and improving capabilities to block information flows within the United States in a crisis. Combined cyber-information attacks on the US that include communications cutoffs must account for these emerging avenues of compromising US communications. These include the following:

- **Hijacking internet traffic.** Adversaries can monitor, modify, corrupt, and potentially kill US web traffic by distorting the "road map" of the internet.[698] Both Russia and China have been involved in hijacking operations that intercepted traffic from major US companies such as Google, Facebook, and Microsoft and could use such capabilities to selectively disrupt internet access in a crisis.[699]

- **Denial-of-service attacks.** Technological advances are enabling dramatic and persistent increases in the size and complexity of distributed denial-of-service attacks—2018 saw a 273 percent increase in maximum attack size.[700] The president's National Security Telecommunications Advisory Committee (NSTAC) warns that distributed denial-of-service attacks could overwhelm US critical communications infrastructure.[701]

- **Threats to physical communications lines.** Adversaries could cut or otherwise disrupt the vast network of underwater cables that makes up the modern internet. Attacks that cut undersea cables that serve the United States could cause massive losses in bandwidth—especially for services that host most of their data overseas, including Google and Facebook—and affect the commercial internet infrastructure the US government relies on.[702]

- **Supply-chain compromise.** China is currently leading the race toward 5G capabilities. If Huawei and other Chinese companies develop the "backbone" infrastructure for global networks and associated software, the United States would face significant risks of espionage

[697] Iasiello, "Russia's Improved Information Operations," 54–56.

[698] Kruse, "What Is BGP Hijacking, Anyway?"; and Goodin, "Strange Snafu."

[699] Goodin, "Strange Snafu"; and Goodin, "Google Goes Down."

[700] NETSCOUT, *Cloud in the Crosshairs*, 68.

[701] NSTAC, *Report to the President*, 1.

[702] Hinck, "Evaluating the Russian Threat."

and disruption of critical telecommunications infrastructure.[703] Similar concerns exist for other products and components, including microelectronics and the undersea cables mentioned above.[704]

- **Counterspace operations.** Russia, China, Iran, and North Korea are all developing and improving capabilities to disrupt the space systems upon which the US military and civilian data and communications networks rely.[705] Without satellite infrastructure, the Earth-based networks and systems would likely be overwhelmed and the entirety of internet, mobile, and TV networks could be jeopardized.[706]

US systems used for messaging the public and managing the response to cyber-induced infrastructure failures will likely constitute a special target for attack. Indeed, systems used to instruct the public during crises are prone to exploitation and represent a significant target for attacks to undermine service availability and the integrity and content of messages.[707] The Integrated Public Alert and Warning System (IPAWS), which will play a critical role in communicating with the public during combined attacks on the US, is a prime example. IPAWS receives, validates, authenticates, and routes various types of emergency alerts, including messages from the president.[708]

We should expect that combined attacks on the US will include efforts to deny government officials the ability to communicate with the public. However, the risk of adversaries gaining access to such systems and using them to send spoofed messages is equally concerning. A fake presidential alert distributed to cell phones across the nation amid a crisis could generate immense chaos and concern—especially if the adversary also disrupted internet or other communications networks to deny citizens secondary sources of information.

Even before conflict occurs, adversaries could target television, social media, and other privately owned and operated communications infrastructure that US leaders would use to communicate with the public in an escalating confrontation—unless adversaries are already using them to warp public perceptions of the developing crisis and corrode confidence in US leadership.

US Defense Options

Building defenses against selective attacks on mass communications systems must be a key component of broader efforts to strengthen domestic resilience. Federal agencies and communications service providers can help strengthen these defenses. NSTAC, composed of senior executives from major telecommunications companies, service providers, information technology firms, and other relevant sectors, provides a strong foundation for progress. The committee's overall goal is to "develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture."[709] The US telecommunications sector has an extensive history of close collaboration with the federal government to ensure the availability of critical communications services in disasters or potential nation-state attacks.[710] Those efforts should now take on an additional challenge: ensuring the

[703] Lewis, *How Will 5G Shape Innovation and Security*, 1–2 and 9.

[704] See *Economist*, "China's Grip on Electronics Manufacturing"; and Malara and Panchadar, "National-Security Concerns Threaten."

[705] Dalton et al., *By Other Means*, 20.

[706] Dvorsky, "What Would Happen?"

[707] NASEM, *Emergency Alert and Warning Systems*, 69.

[708] IPAWS components include the Wireless Emergency Alerts system, the Emergency Alert System, the National Public Warning System, and more. See WEA Project Team, *Wireless Emergency Alerts*; and FEMA, "IPAWS National Test."

[709] CISA, "About NSTAC."

[710] CSCC, "Communications Sector Partnership."

United States is prepared to defeat communications disruption strategies in future crises.

In addition to threatening or inflicting punishment on the US population and thereby creating pressure on US leaders to back down in a confrontation, China and Russia can also conduct personalized IOs against the president and leadership targets. The *National Counterintelligence Strategy* warns that adversaries are already conducting campaigns to "influence and deceive key decision makers" in the United States.[711] In a crisis, adversaries can tailor such operations to help convince US executive brand officials, legislators, and media pundits that the benefits of defending US allies and interests are not worth the costs of doing so. Russia and China are also strengthening their capabilities to conduct such IOs against another critical target: senior US military officers who help shape regional crisis policies and—together with lower-ranking personnel—carry them out.

Societal Breakdowns and Mass Panic: Unlikely but Deserving of Further Research

Combining IOs and disruptive cyberattacks may enable adversaries to coerce US behavior through an additional means of indirect coercion: the creation of widespread public disorder. Rather than seek to mobilize the public to support crisis response options favored by the attacker, adversaries may attempt to incite public disorder on a massive scale and thereby pressure US leaders to yield in the confrontation.

Terrorist organizations have often sought to create mass fear with the help of their unwitting partners: television stations that distribute and replay horrible images and help inculcate fears of further attacks. Nation-states may seek to replicate and modernize such tactics to incite panic on a greater scale. Cyberattacks can enable enemy nations to more effectively and comprehensively strike water utilities and other community lifelines that have long been potential targets of terrorism.[712] And while television rebroadcasts of cyber-induced disasters can still help magnify public fears, social media and modern disinformation technologies provide extraordinary new opportunities to design IOs for mass panic.

Yet, societies have proven so resilient against past terror campaigns that there are strong reasons to doubt whether even these modern technologies will prove effective. Public behavior in the aftermath of severe earthquakes and other catastrophic natural disasters provides additional evidence of deeply rooted social resilience. Both natural and human-caused events, including those that have followed 9/11, have produced a body of research that is helpful for assessing the threats of panic-induced coercion and possible countermeasures.

In the buildup to World War II, military planners and health care professionals believed that the British public lacked the coping skills to resist a bombing campaign and that the psychological effects of such bombing (including societal breakdown) would be "out of all proportion greater" than the physical effects.[713] These expectations coincided with the theories of strategic air power advanced by Giulio Douhet and his disciples earlier in the twentieth century. Douhet argued that "the effect of such aerial offensives upon morale may well have more influence upon the conduct of the war than their material effects" and that the suffering of the civilian population would quickly drive their nation's leaders to capitulate.[714]

The Blitz produced no such societal breakdown or surrender. Most (though not all) scholars find that

[711] NCSC, *National Counterintelligence Strategy*, 9.

[712] Copeland, *Terrorism and Security Issues*, 1.

[713] Jones, "Air Raids and the Crowd"; and University of Exeter, "Bombing of Britain."

[714] Douhet, *Command of the Air*, 57–58.

Nazi bombings failed to incite public panic. Moreover, while the bombings killed or seriously injured 146,777 civilians across the United Kingdom and caused massive physical destruction, that suffering failed to coerce British leaders into surrendering.[715] Systematic efforts to assess the psychological effects of bombing in other campaigns, including the US Strategic Bombing Survey after World War II, have found that many of these campaigns have failed as well.[716]

The disruption of critical services has rarely created public disorder in peacetime either. Studies of public responses to natural disasters find that citizens typically bond together to assist each other. Widely shared beliefs that disruptive events create mass panic build on pervasive myths.[717] Hurricane Maria, Superstorm Sandy, the 1906 San Francisco earthquake, and many other extraordinarily destructive events have produced moving accounts of victims bonding and assisting each other.[718] That was true even in Hurricane Katrina. Although well-documented reports emerged of rioting and looting in the aftermath of the hurricane and the blackout it created, there were many more reports of altruism, cooperativeness, and camaraderie among the victims of the storm.[719] Broader surveys of the literature on naturally caused catastrophes also find that mutual assistance by survivors (rather than disorder or violence) typifies public behavior in such events.[720] Disaster-induced panic is largely a myth—at least for events caused by Mother Nature.

Terrorism presents a more complicated basis for assessing the risks of mass panic–inducing attacks on the US public. In some respects, attacks by al Qaeda, ISIS, and other terrorist organizations provide a better analogy for possible coercive operations by Russia or other nation-state adversaries. Terror and coercive campaigns differ from natural hazards in terms of their malevolent intent. Acts of terrorism, unlike hurricanes or earthquakes, are strategically designed to incite mass fear and dysfunctional behavior by the public. Larry Beutler and other psychologists find that this human intentionality and other characteristics of a terrorist attack "fundamentally alter human perceptions of the event, increasing their salience and heightening their arousal components" far beyond the behavior responses induced by natural disasters.[721] Coercive operations that combine IOs with disruptive cyberattacks would benefit from the same psychological dynamics.

Terrorism is also similar to coercive campaigns in that both exploit media to achieve their desired effects. Past terrorist attacks exploited a sometimes symbiotic relationship that exists between terrorists and media; terrorists use television and other broadcasts as a conduit for their messaging, and media owners attract viewership by playing (and replaying) the acts of terrorism that are designed to incite public fear.[722] Phil Zimbardo and James Breckenridge note that media coverage also helps terrorists evoke fear that is disproportionately greater than the violence they inflict and plays a critical role in

[715] Jones, "Air Raids and the Crowd."

[716] Pape, *Bombing to Win*, 314; and Pape, "True Worth of Air Power," 117 and 128–130. See also Mueller, *Air Power*, 10.

[717] Traditional conceptions of the "mass panic" theory suggest the public will behave irrationally in such situations and identify crowd behavior as a "source of psychological weakness and maladaptive response." Drury, Novelli, and Stott, "Representing Crowd Behaviour," 19. See also Tierney, Bevc, and Kuligowski, "Metaphors Matter," 57–58.

[718] See, e.g., Seppala, "Disaster Brings People Together"; Auf der Heide, "Common Misconceptions about Disasters," 345; Twigg and Mosel, "Emergent Groups and Spontaneous Volunteers," 444; McSeveny and Waddington, "Human Factors," 11–12; and Acevedo, "Amid Government Mess."

[719] Jacob et al., "Disaster Mythology and Fact," 556; and NRC, *Facing Hazards and Disasters*, 134.

[720] In addition to the sources cited in the previous footnote, see Mawson, "Mass Panic."

[721] Buetler et al., "Mental Health Professionals," 38; Fullerton et al., "Trauma, Terrorism, and Disaster"; and Ditzler, "Malevolent Minds."

[722] Shurkinm, "Terrorism and the Media," 82.

facilitating the psychological processes that intensify the public's fears and apprehensions.[723]

While not the first or only extremist group to use social media to its advantage, ISIS is among the most sophisticated, using a combination of well-produced traditional media content (i.e., images and video) and structured social media networks to effectively disseminate fine-tuned propaganda and incite fear. Most notably, in its initial assault on Mosul in 2014, the group used social media to broadcast brutal images of recent victories and tried to give Iraqi soldiers defending the city the impression that they faced imminent defeat, causing the Iraqi army—which held a significant advantage in numbers and arms—to flee without putting up a significant resistance.[724] Exploitation of traditional and social media in coercive campaigns will benefit from these dynamics as well.

Yet, despite the advantages that terrorists enjoy in driving public behavior, terrorist acts have often failed to induce anything beyond temporary, localized panic—much less societal breakdown. Israeli citizens, for example, have shown remarkable resilience against repeated terror attacks.[725] Indeed, the Israeli government and its citizens place a premium on returning to normal in the immediate aftermath of an attack. Government regulations stipulate that locations of a terror attack must be returned to regular use within three hours and that regular life outside the immediate vicinity of an incident must not be disrupted.[726]

In the United States, the attacks on 9/11 created long-term psychological consequences for survivors and those who repeatedly witnessed the attack on television rebroadcasts.[727] Yet, in that attack and in subsequent acts of terrorism, citizens also displayed the same collaborative behavior and support to victims that characterize responses to natural disasters.[728] Analysis by the Department of Homeland Security (DHS) and the Department of Health and Human Services suggests that US society may also display significant resilience against attacks with chemical and biological weapons.[729] But neither that study nor any other has examined how the use of Chinese or Russian IOs might magnify the psychological impact of such attacks and undermine US government efforts at counter-messaging to avert public panic.

Further research will also be required to determine whether cyberattacks and sophisticated social media messaging can drive mass behavior more effectively than previous TTPs. It is conceivable, for example, that the public's relatively weak understanding of cyberattacks (versus familiar kinetic weapons) will intensify the psychological effects of their threatened or actual use. Martin Libicki speculates that "Public reaction in a major cybercrisis may give new meaning to the concept of 'wild card.' "[730]

It is also possible that the context of an escalating international crisis will heighten these psychological effects. In 2018, as tensions escalated between the United States and North Korea, Hawaiian emergency managers issued a false alert about an incoming ballistic missile attack that sparked

[723] Breckenridge and Zimbardo, "Strategy of Terrorism," 116.

[724] Traditional media in the region also picked up and rebroadcasted ISIS messaging—including both real and false stories—contributing to ISIS's perceived momentum on the battlefield. Some analysts likened it to the fall of France to the 1940 German Blitzkrieg. See Brooking and Singer, "War Goes Viral."

[725] Elran, "Societal Resilience in Israel."

[726] HLMG, *Fighting Terror Effectively*, 16.

[727] Cohen Silver, " '9/11: Ten Years Later,' " 427.

[728] The 9/11 "citizen navy" is an especially dramatic example of such collaborative behavior. In the immediate aftermath of the 9/11 attacks, over one hundred and fifty ferries, tugboats, Coast Guard vessels, and recreational (privately owned) boats shuttled hundreds of thousands of people to Staten Island, Ellis Island, and New Jersey. See Moon, "9/11 Boatlift." The Boston Strong response to the Boston marathon bombing provides another prominent instance of such adaptive behavior. See Beinecke, "Honoring the Community."

[729] DHS and HHS, *Patient Decontamination*, 82–86.

[730] Libicki, *Crisis and Escalation in Cyberspace*, 10.

a brief but intense public panic.[731] It is unknown whether genuine—or manipulated—warnings of cyberattacks in an intense crisis could create equivalent disruptive effects.

Further research will also be needed to develop countermeasures against panic-oriented attacks. The success of community-based resilience initiatives underway in Israel may hold promise for equivalent efforts in the United States. [732] However, Israeli and US societies are markedly different, and resilience programs may need to be altered accordingly. Many of the same measures necessary to defeat the political mobilization of US citizens in a crisis may also be useful against panic-oriented campaigns. Yet, given the risk that adversaries will tailor their messaging to spur societal breakdown versus "garden variety" opposition to US policies, research on specialized measures to address those risks may also be necessary.

Potential Defensive Requirements

As analysis goes forward on how China and Russia may seek to create mass panic, US emergency managers should pursue opportunities to capitalize on underlying resilience of the public against such tactics and adapt existing incident response plans and capabilities to counter coercive campaigns.

Previous sections of this study noted that the Federal Emergency Management Agency (FEMA) has already become an expert in managing rumor-control pages for hurricanes and other disasters and in using messaging over social media to counter false information that might otherwise cause mass panic or social unrest. FEMA is not alone in making such progress. Officials at all levels of government use social media platforms to connect with and provide information to citizens during crises. DHS notes that "social media and collaborative technologies have become critical components of emergency preparedness, response and recovery."[733] That department established a Social Media Working Group for Emergency Services and Disaster Management to "provide recommendations to the emergency preparedness and response community on the use of social media technologies before, during, and after a natural disaster or an act of terrorism or other man-made disaster."[734] Other disaster response partners have begun to incorporate social media into their operational plans as well.[735]

Yet, initiatives by emergency managers to counter social media disinformation will face vastly greater challenges in dealing with coercive campaigns by China and Russia. These nations have much more sophisticated IO tools at their disposal than those used by rumormongers among the US public. Furthermore, as emergency managers increasingly rely on social media to gather information on a disaster, communicate with stricken communities, and help coordinate incident response operations, adversaries may seek to exploit that dependence. In 2020, QAnon supporters in Oregon overwhelmed 911 dispatchers and sheriffs' offices with false reports of arson-induced wildfires.[736] US adversaries may flood FEMA and other emergency management agencies with false reports of infrastructure failures and public disorder to complicate their response to coercive campaigns and magnify the difficulties of counter-messaging. Measures to build on FEMA's ongoing social media initiatives should account for these risks of adversary exploitation.

Emergency managers and infrastructure operators will also need specialized measures to manage government messaging in response to cyber-induced disruptions of water utilities and other systems essential for public health. The accidental spill of

[731] Nagourney, Sanger, and Barr, "Hawaii Panics after Alert."

[732] Elran, "Societal Resilience in Israel."

[733] SMWGESDM, *Countering False Information*, 2.

[734] DHS, "Social Media Working Group (SMWG)."

[735] See, e.g., FEMA, "Social Media and Emergency Preparedness"; and Ogrysko, "Recent Hurricanes."

[736] CNN, "QAnon Fans Spread Fake Claims."

industrial pollutants into the Elk River in West Virginia provides a starting point for assessing these public communications challenges. West Virginia American Water company, which draws on the river to provide drinking water for surrounding communities, only issued a "do not use" order after residents had been drinking the water all day. More severe communications problems emerged when the state and water utility subsequently sought to convince the public that the water had become safe to drink. As officials analyzed ambiguous, difficult-to-find data on the spilled chemicals and their potential public health effects, they lifted the do-not-use order; however, days later, they announced that pregnant women should not drink water from the system.[737] A cyberattack-induced chemical release or attacks on water treatment systems themselves could create equivalent problems for public messaging.

The *National Response Framework* provides the foundation necessary to help emergency managers prepare for such operations. The fourth edition of that framework, released in October 2019, emphasizes for the first time the risk that nation-states may strike US critical infrastructure and "strategically target attacks to exploit interdependencies between infrastructure sectors and magnify cascading failures between them." The framework also warns that adversaries will seek to conduct IOs and spread disinformation in crises to incite panic and disrupt response operations.[738] Building on the framework as a foundation, US policymakers should assess the risks of large-scale combined attacks and develop initiatives to build resilience against them.

Public and private sector partnerships can also limit the cascading failures that adversaries may seek to create. The creation of *Emergency Support Function #14—Cross-Sector Business and Infrastructure* marks an enormous step forward in this regard. *Emergency Support Function #14* provides a critical multisector framework for conducting industry-led, government-supported response operations in major disasters. The accompanying annex lays out the detailed principles and organizational responsibilities necessary to strengthen industry and government preparedness for cascading infrastructure failures, including the identification of critical interdependencies between lifeline infrastructure systems.[739]

Infrastructure owners and operators and their government partners should also prepare to counter IOs at the same time that they harden their systems against cyberattacks. The electricity subsector has already begun to do so. The Electricity Subsector Coordinating Council, for example, has developed playbooks for communicating with the public regarding outages and restoration times in ways that are explicitly designed to ease public concerns about such events. The playbook system also provides electric utilities with an opportunity to coordinate their messaging with governors and other elected officials attempting to inform their constituents.[740] The council is now beginning to account for the risk that adversaries will use disinformation to confuse utility customers about blackouts and recovery operations. Building on that foundation, the United States should expand on these efforts to ensure that utilities and their government partners can deliver public-facing communications to ease citizen concerns in a crisis and provide validated information as a countermeasure against disinformation and rumor. Other sectors should follow suit, especially those that are vulnerable panic behavior, such as the financial services sector and the food and agriculture sector.[741]

The broader imperative lies in integrating cyber and IO defenses. Mutual-assistance systems exemplify

[737] Manuel, "Crisis and Emergency Risk Communication."

[738] FEMA, *National Response Framework*, iii and 6.

[739] FEMA, *Emergency Support Function #14*.

[740] ESCC, *ESCC*, 3.

[741] Attacks on the food-distribution system, for example, may be especially useful for inciting panic behavior. See Shrikant, "Psychology behind the Pre-Hurricane Run."

the nature of this challenge and value of integrative efforts. For decades, electric utilities, water and wastewater systems, natural gas companies, and other components of US infrastructure have been hardening their assets against cyberattacks. They are also developing mutual-assistance systems to help asset operators restore service if their systems are disrupted. The electricity subsector's Cyber Mutual Assistance (CMA) program is making rapid progress in that regard. Building on long-established expertise and coordination mechanisms to provide for mutual assistance in the aftermath of hurricanes and other natural hazards, the CMA program enables electric utilities and natural gas companies to send cyber incident response personnel and other forms of aid to partners stricken by an attack.[742]

But cyberattacks are not like hurricanes or other natural hazards in a critical respect. When a hurricane creates a blackout, utilities thousands of miles away can send bucket trucks, linemen, and other restoration assets to the affected area without fear that the storm will affect their own region. In contrast, China and Russia can conduct cyberattacks against any power company in the United States.[743] In an exemplary strike, they may use social media to warn that a power outage in one city will soon be followed by many others unless the United States yields in a crisis. By conducting microtargeted messaging against utility CEOs and the governors and legislators in the states they serve, adversaries can seek to undermine the willingness of utilities to assist each other. And to be sure, any breakdown in mutual aid (and the resulting threats to public safety in cities that remain blacked out) will become fodder for follow-on messaging.

The larger point: cybersecurity and IO defenses must not become "cylinders of excellence." China and Russia will tailor social media campaigns to magnify the psychological effects of small-scale attacks and convey threats of more punishment to come in ways that exploit the exceptional vulnerabilities of the US public to such messaging. US policymakers and their private sector partners (including social media companies and critical infrastructure owners/operators) need a similar integrated approach to defeat combined information-cyberattacks.

Integrated defense operations must also account for the risk that adversaries will conduct sustained, adaptive campaigns that specially target response and infrastructure restoration operations. Grid owners and operators have extensive expertise in communicating with customers to set realistic expectations and assuage concerns during outages caused by hurricanes, wildfires, and other natural hazards. Unifying messaging with governors and other elected officials on estimated restoration times already presents significant challenges during such events. However, those difficulties will be dwarfed by the problems that IOs may create. While extended infrastructure outages would be cause for concern on their own, adversary IOs could incite additional panic by presenting false (and likely inflated) information regarding the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety. Attackers could also magnify the inherent difficulties of estimating restoration times by employing advanced persistent threats (APTs) that enable repeated reattacks and disruptions in grid service until eradicated from utility networks.[744]

IOs in a crisis could also exploit another opportunity to magnify the psychological effects of a limited attack: the disruption of efforts by emergency managers and infrastructure operators to limit the effects of localized attacks. False reporting during Hurricane Katrina in August 2005 exemplifies the

[742] ESCC, "ESCC's Cyber Mutual Assistance Program."

[743] For more on the challenges of CMA versus mutual assistance against natural hazards, see Stockton, *Superstorm Sandy*.

[744] HSAC, *Final Report*, 7; and Stockton, *Resilience for Grid Security Emergencies*, 36.

disruptive effects that disinformation can have on response operations. As the Coast Guard and private contractors flew helicopters during the event to rescue citizens from flooded homes, media reports emerged that shots were being fired at those helicopters. Such reports were based on scanty (and in many cases, dubious) evidence. Nevertheless, Coast Guard and private sector rescue flights were halted in response.[745] Similarly, reports of looting, violence, and sexual assault contributed to general chaos in the affected population. These largely unsubstantiated rumors were repeated by frightened survivors and ultimately picked up by mainstream media reports, fueling even greater concern.[746]

Targeted disinformation campaigns could produce equivalent effects in future crises. For example, to restore power after a cyberattack, utilities may need to deploy workers to multiple remote electricity substations to perform on-site restoration tasks. False messaging to those employees and local media that active shooters were near the substations, or that those facilities were enveloped in a toxic cloud from a nearby chemical plant, could discourage employees from deploying until their safety and security were assured. IOs against personnel deploying to natural gas compressor stations, water pumping facilities, and other infrastructure nodes could have similar effects. Even false messages targeting such employees could delay the restoration of critical services.

Of course, IOs would be all the more effective if enemy attacks actually were jeopardizing worker safety. Russia has conducted all its test operations against the United States without actually creating toxic chemical facility fires or crippling the integrity of food-distribution systems. As a result, instead of fanning the flames of panic, all truly "on the ground" accounts discredited Russian IOs. But in future crises, even small-scale infrastructure disruptions could prove useful for coercion if supplemented by St. Mary-style IOs and warnings that the US public will suffer increasingly intense punishment until the president accedes to the attacker's demands. The United States should immediately begin to clarify the requirements necessary to counter the coercive effects such exemplary attacks.

IOs against US Leaders

Leadership targeting offers a very "applied" solution to a conceptual problem in deterrence literature. Thomas Schelling and many other theorists of coercion assume for the most part that states involved in coercion are unitary, rational actors.[747] In reality, as Wallace Thies notes, "governments are coalitions of numerous individual decision-makers, virtually all of whom occupy positions within large, semi-autonomous, bureaucratic organizations" and who will speak with many voices at once. . . ."[748] Patrick Bratton argues that because the targeted government is not a rational, unitary actor, coercers "need to know a great deal about the nature of the target to determine whether it is likely to be coercible, and if so, what kinds of threats will be most effective." The difficulty of aligning coercive threats to fit the decision-making process of the victim helps explain why coercive campaigns so often fail and why "targets can rarely be relied upon to listen to the correct messages or draw the right conclusions."[749]

The complexity and malleable nature of the nature of the US crisis decision-making process creates additional problems for leadership-oriented IOs. The structure and processes of the National Security Council (NSC) often change dramatically from one administration to the next. That process also includes a shifting roster of senior officials, all of

[745] Hill and Spangler, "No Evidence Backs Up Reports."

[746] Carr, "More Horrible than Truth."

[747] Bratton, "When Is Coercion Successful?," 104.

[748] Thies, *When Governments Collide*, 13.

[749] Bratton, "When Is Coercion Successful?," 114.

whom bring their own personal and institutional perspectives to bear in advising the president.

However, technologies for gathering and exploiting data on these officials, mapping points of leverage in the West Wing and the national security bureaucracy, and tailoring coercive messaging accordingly are rapidly improving. The Department of Defense (DoD) is already applying advanced analytic techniques to bolster coercive operations abroad. The US Joint Staff calls for relying on subject-matter experts and advanced automated-analysis systems to identify relevant targets for IOs, "including, but not limited to key influencers, centers of influence, and power brokers; and their patterns of behavior, enduring motivations, and collective strengths and weaknesses."[750] General Nakasone framed this pursuit of customization more bluntly: to strengthen the impact of US operations, US personnel are "going to expand our insights of our adversaries . . . We're going to know our adversaries better than they know themselves."[751]

China and Russia are no doubt "getting to know" the inner circles of the Biden administration and the ways in which Biden is restructuring the NSC and its decision-making mechanisms. These nations are almost sure to be collecting personal data on the president's family as well as on key political supporters, campaign donors, and others who advise the president and may be targeted accordingly for personalized influence operations in a regional crisis.

The president's backers and opponents in Congress could become targets of such operations as well. Speaker of the House Nancy Pelosi (D-CA) and other legislators warned in July 2020 that "Congress appears to be the target of a concerted foreign interference campaign, which seeks to launder and amplify disinformation in order to influence congressional activity, public debate, and the presidential election in November."[752] China and Russia may conduct similar IOs to intensify fears and legislative pressure over the potential costs and escalatory risks of a regional confrontation.

Less obvious targets may also prove useful for coercion. Television commentators who routinely shape presidential perceptions could also be targeted with IOs, just as Russia routinely sought to influence journalists in the Cold War with more primitive TTPs. Borrowing a page from OAF, China and Russia could also threaten disruptive cyberattacks against businesses owned by the president's close friends and political supporters. Governors could be targeted with IOs as well, especially in conjunction with threatened or actual cyberattacks against water systems, the electric grid, or other infrastructure essential for the health and safety of their citizens.

Social media gives adversaries direct access to these leadership targets. Inauthentic Twitter accounts tied to Chinese, Iranian, and Russian intelligence services directed thousands of tweets at then-president Donald Trump. President Trump retweeted posts from phony Russian accounts and from over one hundred other unverified users. The fifty accounts he followed while president (that therefore showed up on his feed) include those of his family, Fox News hosts, and others who are themselves targeted for influence.[753] For example, Donald Trump Jr. has frequently retweeted posts from Twitter accounts operated by Russia's GRU-supported IRA.[754] IRA personnel also monitored Trump administration officials' reactions to their tweets, enabling them to refine their TTPs for follow-on operations.[755]

[750] JCS, *JCOIE*, 32.

[751] Temple-Raston, "Why Russia May Have Stepped Up."

[752] Williams, "Foreign Disinformation Campaign."

[753] McIntire, Yourish, and Buchanan, "Trump's Twitter Feed"; and Logan, "Twitter Found More than 50,000 Russia-Linked Accounts."

[754] Stancy Correll, "Members of Trump's Family."

[755] Birnbaum, "Mueller Identified 'Dozens' of US Rallies"; and Mueller, *Investigation into Russian Interference*, 34.

China has conducted similar operations. According to former president Trump's national security advisor, Robert C. O'Brien, Chinese hackers attempted to break into the private email accounts of members of the president's family. O'Brien also "reported that the Chinese were trying to phish the Gmail accounts of Republican campaign officials, Trump family members, Trump administration officials."[756]

The private sector can help detect and defeat such attacks. For example, O'Brien's reporting on the Chinese operation was based on information provided by Microsoft. But social media platforms can inadvertently help adversaries customize their attacks. These platforms collect vast amounts of data on users and their interactions that adversaries can leverage to support their IOs. Rep. Stephen Lynch (D-MA), chairman of the House Oversight Committee's subcommittee on national security, recently warned Facebook that "by collecting personal information on U.S. government personnel who have access to classified information," foreign adversaries may exploit that access and data to "exert undue foreign influence in U.S. policy making," including during "future military conflicts or diplomatic disputes."[757] Gathering personal information about US personnel and their social networks can help adversaries refine their messaging and better understand how targeted individuals can serve in broader influence operations.

However, these known means of social media access represent only part of the threat. Russia and China are likely holding in reserve more sophisticated means of messaging top-level officials in crises, as opposed to routine, ongoing influence and intelligence-gathering campaigns against the president and policy elites. They can also reinforce these IOs by threatening or conducting attacks on US infrastructure of special concern to the president or other senior decision-makers. The *National Counterintelligence Strategy* warns that improvements in adversary capabilities to conduct such attacks "likely are aimed at influencing or coercing U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption."[758] We should prepare for the possibility that adversaries will focus on the infrastructure of highest value to US leaders and their political supporters, just as NATO allies did in OAF.

Developing US Defensive Options

To strengthen defenses against coercive threats to senior US officials, government agencies and researchers will first need to determine which of these threats pose the greatest risks of coercing decision-making and then prioritize those threats for further analysis. The National Counterintelligence and Security Center recently announced the launch of an array of federal initiatives to protect the United States from foreign influence. Yet, while the center warns that adversaries will seek to "influence and deceive key decision makers," none of these new efforts specifically address the need to develop countermeasures against such targeted coercive operations.[759] Nor have any other US agencies proposed initiatives to clarify defensive requirements against this clear and present threat.

Gaining detailed intelligence on adversary TTPs to manipulate senior US officials should become a key focus of new US efforts to detect, deter, and counter foreign influence activities.[760] Opportunities also exist to support those intelligence efforts with self-assessment of potential vulnerabilities of the US decision-making process to leadership IOs. Existing studies of that process, such as Graham Allison and Philip Zelikow's classic *Essence of*

[756] Gertz, "Chinese Hackers."

[757] Eversden, "TikTok a National Security Risk?"

[758] NCSC, *National Counterintelligence Strategy*, 6.

[759] NCSC, *National Counterintelligence Strategy*, 9.

[760] NCSC, *National Counterintelligence Strategy*, 9.

Decision, provide a foundation for such research and supporting exercises.[761]

Each of the three models of crisis decision-making examined by Allison and Zelikow can be repurposed to identify possible means of coercion. The rational actor model, in which a nation chooses calculated, reasonable actions in response to the strategic problem it confronts, offers the most application to the design of leadership-level IOs. . .[762] Borrowing from that model, and disaggregating it to the level of individual decision-makers rather than treating the United States as a unitary actor, an adversary would conduct customized IOs against senior officials to heighten their perceived costs (and reduce their expected benefits) of continuing to defend US allies in a regional crisis.[763]

Allison and Zelikow's organizational behavior model provides an additional basis for self-assessment. This model accounts for the distinctive logic, capacities, culture, and procedures of large government that can help drive their behavior in ways that the rational actor model would not predict.[764] China and Russia may seek to anticipate and take advantage of these organizational predispositions in IOs and combined attacks.

The third model of crisis decision-making offered by these authors is that of government politics and bargaining between players in the national government. This model is especially useful in the age of microtargeted messaging. Adversaries can design IOs to exploit the conflict policy of US officials and their political agendas.[765] During crises, US opponents would microtarget their messaging accordingly and use direct access to senior officials via social media and other means to shape their behavior.

Press reports indicate that the US is already conducting equivalent operations abroad. According to accounts of US Cyber Command actions prior to the 2018 midterm elections, the command targeted IRA individual workers with emails, pop-up messages, and text messages aimed at spreading confusion and discord. Some operatives were reportedly so perturbed that they launched an internal investigation to root out presumed insiders leaking personnel data.[766]

We should expect Beijing and Moscow to conduct equivalent operations against US agency staffers and senior officials. Russia has a long-established doctrinal basis for conducting personalized operations against an opponent's leadership team. As noted earlier in this study, Russia's use of *reflexive control* entails the practice of predetermining an adversary's decision-making in Russia's favor by altering key factors in the adversary's perceptions of the conflict.[767] Reflexive control operations seek to influence the opponent's initial assessment of the crisis. Those operations also seek to shape the opponent's objectives and convince them to voluntarily make a series of decisions that advance Russia's

[761] Allison and Zelikow, *Essence of Decision*. For more recent studies of senior-level decision-making and National Security Council policy operations, see Keller, Yang, and James, "Decision-Making in U.S. Foreign Policy Crises"; Hale, Hale, and Dulek, "Decision Processes during Crisis Response"; Gans, *White House Warriors*; and Rothkopf, *Running the World*.

[762] The rational actor paradigm provides the description of the rational actor model most useful for assessing vulnerabilities to adversary disinformation. Allison and Zelikow, *Essence of Decision*, 23–30 passim.

[763] For an analysis of how leadership perceptions and beliefs drive state decision-making and provide an essential supplement to rational actor models of state behavior and broader theories of structural realism, see Jervis, *Perceptions and Misperceptions*, 62–113.

[764] Allison and Zelikow, *Essence of Decision*, 5.

[765] Allison and Zelikow, *Essence of Decision*, 6 and 255–258.

[766] Nakashima, "U.S. Cybercom Contemplates Information Warfare."

[767] For NATO and other studies on reflexive control, its origins in Soviet doctrine, and its recent use in conflicts with Ukraine, see Kasapoglu, *Russia's Renewed Military Thinking*; Giles, *Handbook of Russian Information Warfare*; Snegovaya, *Putin's Information Warfare in Ukraine*; and Kowalewski, "Disinformation and Reflexive Control."

goals.[768] Recent studies have examined how Russia employed reflexive control to confuse and delay the response of Ukrainian leaders and Western policymakers to the 2014 invasion of Crimea.[769] Efforts to identify US defensive requirements against coercion should account for the danger that such tactics (and their Chinese equivalents) will be used against US leaders and those who advise them.

Adversaries may also seek to influence decision-makers by exploiting political divisions between them. The most obvious way to do so is to leverage partisan conflicts and—drawing on lessons learned from Russia's campaign against US voters—taint options unfavorable to the attacker by tying them to the president's domestic political opponents. Customized IOs can also exploit political dynamics within the executive branch. As noted in Allison and Zelikow's governmental politics model, senior officials sometimes advocate policies that maximize their agency's standing or their own personal power vis-à-vis other "players" in the decision-making process.[770] Attackers can design IOs to take advantage of this competition for power and advance them to disrupt or shape adversary behavior. USCYBERCOM's development of IOs to counter interference in the 2020 election reportedly included disinformation tailored to exploit rivalries within the Russian government and powerful elites.[771] US defensive requirements should include measures to anticipate and counter the use of such politically informed operations against senior US officials.

The US should also intensify efforts to prevent adversaries from infiltrating federal networks and using that data to help target IOs against senior officials. China and other adversaries have repeatedly penetrated US agencies responsible for securing sensitive personal data on government employees (including those who would play key roles in crisis decision-making). In the February 2020 attack on the Defense Information Security Agency, more than personal identifiable information was at risk. The Agency also provides direct telecommunications and IT support to the president, the chairman of the Joint Chiefs of Staff, and others who represent prime targets for manipulation.[772] Adversary access to such protected communications would enable a whole new realm of deceptive and disruptive IO tactics. Maintaining the security of these networks, stanching the exfiltration of sensitive data on senior officials, and anticipating the use of that data to blackmail US leaders or customize IOs against them constitute crucial defensive requirements against coercion.

An additional analytic effort beyond the scope of this study will be essential to refine US defensive requirements: an assessment of the decision-making characteristics of and sources of influence on individuals who are currently in government and those who will replace them in subsequent years. US security and counterintelligence organizations are best prepared to conduct such close-hold analysis. However, to support their work, red-teaming the US crisis decision-making process may prove valuable. DoD employs cyber red teams "to emulate a potential adversary's exploitation or attack capabilities against a targeted mission or capability."[773] These teams seek to realistically emulate the TTPs that specific adversaries will use to strike defense networks and other assets and thereby help the department strengthen its defenses against them.

An equivalent approach should help guide measures to defeat IOs against senior leaders. In particular, federal departments and agencies should use red-teaming to examine how potential adversaries

[768] Kasapoglu, *Russia's Renewed Military Thinking*, 5–6; and Giles, *Handbook of Russian Information Warfare*, 19–20.

[769] Snegovaya, *Putin's Information Warfare in Ukraine*, 7; and Kasapoglu, *Russia's Renewed Military Thinking*, 5.

[770] Allison and Zelikow, *Essence of Decision*, 256–258 and 298.

[771] Nakashima, "U.S. Cybercom Contemplates Information Warfare."

[772] DISA, "DISA's Mission Partner Support."

[773] CJCS, *Department of Defense Cyber Red Team*, A-1.

are likely to assess and exploit the processes of and sources of influence over US crisis decision-making. The resulting analysis can help clarify requirements for US defense against coercion by Russia, China, or other potential opponents.

Conducting red team analyses will be challenging. Those teams will need specialized IO and cyber expertise to perform their work. They will also need an understanding of the psychological dynamics that undergird coercion and the process by which crisis policies are made in the White House Situation Room and beyond. The same skills and knowledge will be required to conduct net assessments that can identify emerging gaps in US preparedness. Moreover, any such red-teaming of the US decision-making process would need to account for significant political sensitivities and would need to be closely held to prevent adversaries from acquiring a road map for how to attack.

An additional option is to conduct war games and exercises to better anticipate IO threat vectors and opportunities to counter them. Public agencies and private companies are employing new war game designs and supporting technologies to increase their value for analysis and problem-solving, including the use of role-playing and social media tools.[774] Exercise planners can also design threat scenarios to closely replicate anticipated attack vectors.[775] Such red-teaming and war-gaming efforts should be structured to inform each other on a continuing basis, thereby providing an increasingly realistic means of assessing possible avenues of attack and a basis for testing potential countermeasures and building defensive expertise.

Coercing US Military Personnel: A Special Opportunity for Customized Direct Influence Campaigns

While Cabinet officials and the NSC staff offer especially attractive targets for direct influence campaigns, China and Russia may also conduct personalized campaigns against other targets who could help shape crisis decision-making and operations. US military personnel constitute one potential focus for coercion. Combatants in previous conflicts have often used IOs to achieve military benefits through psychological means. A frequent goal of such operations is to induce an opponent's forces to surrender or desert the battlefield. The US has gained significant benefits from such operations in Operation Desert Storm and Operation Iraqi Freedom. IOs against Iraqi forces were most valuable for inducing troops to surrender or desert rather than suffer US bombings or ground assault. During Desert Storm, the United States distributed millions of leaflets urging desertions via leaflet bombs dropped by F-16s and B-52 bombers, 155-mm leaflet artillery rounds, and other delivery means. US forces also conducted sustained radio broadcasts and loudspeaker operations.[776] The US later refined and intensified these IOs in Operation Iraqi Freedom.

These IOs helped take multiple Iraqi units off the battlefield without risking US lives. A DoD assessment found that over 44 percent of Iraqi units in the Kuwait theater of operations deserted before and during Desert Storm, with tens of thousands of enemy personnel surrendering in the two operations; almost all of those who had seen or possessed

[774] NATO's Crisis Management Exercise 2019, for example, modeled real-word decision-making mechanisms and partner crisis management procedures. See NATO, "Crisis Management Exercise 2019."

[775] DHS's Cyber Storm exercise series provides especially detailed exercises of the federal government's cyber-response mechanisms and decision-making systems. That series could be leveraged to create an equivalent for domestic decision-making against information operations during a crisis. See DHS, "Cyber Storm VI."

[776] Jones and Summe, "Psychological Operations," 2–5; and JCS, *Military Information Support Operations*, iv–4.

US leaflets had taken the actions the leaflets encouraged.[777]

US IOs have achieved equivalent successes in other campaigns. In Operation Just Cause (1989), for example, Spanish-speaking US personnel phoned Panamanian military commanders urging them to have their units put away their weapons and assemble on nearby parade grounds or face annihilation by US forces. This campaign (dubbed the "Ma Bell Mission" for its exploitation of telephone access to senior Panamanian officers) helped induce almost two thousand troops to surrender.[778]

Counter-military IOs conducted in conjunction with the threatened or actual use of force serve as "force multipliers." A comprehensive DoD review of such operations found that they often weaken the effectiveness of opposing forces and help achieve US objectives at reduced cost.[779]

Russia is already conducting intensive influence operations against the US military to achieve different, precrisis goals and is doing so by using vastly more sophisticated means. Rather than using leaflet-carrying bombs or artillery shells, Russia is using Twitter and other social media platforms to message US troops or gain personal data on them for future targeted disinformation efforts.[780] And instead of seeking large-scale desertions, adversaries are looking to gain long-term strategic benefits that could also help lay the groundwork for tactical IOs to confuse or disrupt military operations in future confrontations.

At the strategic level, the US public tends to place special trust in military personnel and veterans. Their ability to influence the public makes both groups especially valuable targets for Russian IOs seeking to sow public discord and achieve other strategic goals.[781] A recent Oxford University study found that Twitter enables significant and persistent interactions between current and former US military personnel and a broad network of Russia-focused accounts, including those advancing conspiracy theories and other divisive content.[782] In the first half of 2015, a temporary breach in GRU security enabled researchers to uncover the intensity of such counter-military IOs by the GRU's "Fancy Bear" organization (aka APT28).[783] Of all the individuals Fancy Bear targeted for phishing during that period beyond the borders of the former Soviet Union, 41 percent were current or former military personnel.[784]

Adversaries may target US troops not only to exploit their influence over the broader public but also to create dissention within their own units to weaken morale and operational readiness. DoD personnel have identified disinformation on social media as a high-risk problem that could erode "trust and confidence" in the ranks.[785] Adversaries could also attempt to use microtargeted IOs to confuse or delay decision-making by officers and their troops in a crisis.[786] In addition, opponents could use social media accounts and personal devices to gather exploitable intelligence for more traditional military goals, such as tracking troop and ship movements as forces deploy to a regional crisis.[787]

Such IOs constitute a specialized version of the counterintelligence threats that have long confronted

[777] These potential actions included desertion, defection, abandoning equipment, or surrender. See Jones and Summe, "Psychological Operations," 5–7.

[778] Friedman, "U.S. PSYOP in Panama."

[779] Lamb, *Psychological Operations*, 19–20.

[780] Gallacher et al., "Junk News"; and Schreckinger, "How Russia Targets the U.S. Military."

[781] Gallacher et al., "Junk News."

[782] Gallacher et al., "Junk News."

[783] For more on the designation of Fancy Bear as an arm of the GRU, see SSCI, *Russian Active Measures, Vol. 2*, 63.

[784] Schreckinger, "How Russia Targets the U.S. Military."

[785] Seldin, "Russia Influence Operations."

[786] Krull, "Foreign Disinformation Is a Threat."

[787] For an example of how smartphone applications can undermine operational security, see Hsu, "Strava Heat Map"; and Perrett, "US Troops Are Still Posting."

DoD. Instead of using labor-intensive means to recruit spies and other insider threats in barrooms and brothels, adversaries can now use personalized social media operations to influence the behavior of military personnel for strategic and tactical advantages.[788] Ed Wilson, then-deputy assistant secretary of defense for cyber policy, noted in 2018 that he was concerned about Russian IOs against US military personnel. "We know it goes on," he said. "That's why we've amped up and increased the attention that we're paying" to such operations and developing countermeasures accordingly.[789]

Veterans associations are calling for additional countermeasures as well. A study by the Vietnam Veterans of America found that Russia was stealing and exploiting data on former military personnel to conduct influence operations against them and manipulate them to widen US societal and partisan divisions. For example, Russian operatives established and maintained the "Being Patriotic" Facebook page for veterans that has gained hundreds of thousands of followers and regularly posts divisive political messages under the guise of supporting US troops. Other Russian and Iranian IOs are targeting the families of US troops stationed abroad to seek leverage over deployed units of the 82nd Airborne Division and other military components.[790]

China is moving beyond its Office of Personnel Management hack to gather additional data on civilian US defense officials and military officers. Chinese intelligence services are using fake social media accounts to connect with high-ranking and influential members of the intelligence and defense communities centered in and around Washington, DC. Chinese operatives are also harvesting social media and online data regarding US Navy personnel. To provide intelligence to the Chinese military and other clients, one Chinese company is tagging Navy vessels such as the USS *Dwight Eisenhower* and Nimitz carriers with ID numbers and then cataloging relevant social media posts and websites for those priority targets. The database has assigned hashes and collated information on officers, including former chief of naval operations John M. Richardson. Entries on former acting secretary of the navy Thomas Modly named his wife and four children, described his educational and private sector background, and included a placeholder for building a psychological profile.[791]

DoD's January 2020 warning to all armed forces personnel to delete TikTok from their government-provided smartphones represents one such countermeasure.[792] But DoD must stay ahead of intensifying adversary attempts to influence and strengthen their future connectivity with US troops. For example, while DoD has banned military personnel from using TikTok on their government phones, China can still gather data and tee up influence operations by accessing the personal devices widely used by these personnel.[793] DoD should also account for the risk that Beijing and Moscow will seek to exploit extremist movements within the armed forces.[794] Indeed, policymakers should assume that these nations will capitalize on all such opportunities to use US military personnel to corrode democracy, and—potentially—disrupt the execution of contingency plans for regional confrontations.

[788] Heller, "Make Counterintelligence a Main Effort"; and Paul and Waltzman, "How the Pentagon Should Deter." For more on the use of social media to recruit insiders, see Stockton, *Security from Within*.

[789] Seldin, "Russia Influence Operations."

[790] Kredo, "U.S. Military Members"; and Rempfer, Snow, and Altman, "Families of Deployed Paratroopers."

[791] Shih, "Chinese Firm Harvests Social Media."

[792] In response to the Pentagon's guidance, the US Army and Navy have banned TikTok from government phones. See Vigdor, "U.S. Military Branches Block Access."

[793] Army officials state that the armed services lack the authority and resources to enforce bans on personal devices that almost all troops use. See Perrett, "US Troops Are Still Posting."

[794] DoD IG, *Evaluation of Department of Defense Efforts*.

Coercion of US Allies

Targeting IOs against US security partners offers adversaries an additional means of prevailing in regional crises, especially if those operations are integrated with coercive messaging against the president and American public. China and Russia are already conducting disinformation campaigns to weaken the cohesion of NATO and other alliances. Those nations are also using IOs to cast doubt on the willingness and ability of the United States to live up to its defense commitments. In future crises, Beijing and Moscow are likely to sharpen the focus of such messaging to undermine allied support for coalition operations. They may also warn US security partners that they will suffer horrific consequences if they fail to yield and employ the same advanced technologies and customization tactics that they will use against the US public and senior officials.

Strategies to defeat such coercive operations will require initiatives over and above those necessary within the United States. Collaboration with US allies must also account for the risk of combined attacks to discourage, delay, and disrupt alliance decision-making, including through updated versions of the "hybrid" TTPs that Russia has used against Ukraine. Less likely—but still worth accounting for—is the risk that adversaries will seek to achieve coercion by denial and disrupt the flow of forces crucial for US victory in regional confrontations.

Targeting Specific Regional Partners

Alliances and bilateral security treaties are central to the US *National Defense Strategy* and constitute a key advantage in competing for regional influence. The strategy emphasizes that "mutually beneficial alliances and partnerships are crucial to our strategy, providing a durable, asymmetric strategic advantage that no competitor or rival can match."[795]

Security partners are also crucial to US plans and capabilities for regional crises. The strategy notes that the partners "provide complementary capabilities and forces along with unique perspectives, regional relationships, and information that improve our understanding of the environment and expand our options. Allies and partners also provide access to critical regions, supporting a widespread basing and logistics system that underpins the Department's global reach." Accordingly, a key US goal is to develop new partnerships "to reinforce regional coalitions and security cooperation" and strengthen the ability of US and allied forces to "act together coherently and effectively to achieve military objectives" in regional contingencies.[796]

Given the importance of alliances and bilateral defense treaties to US global power, it is hardly a surprise that China and Russia are conducting IO campaigns to weaken them. In response, NATO is developing new programs and coordination mechanisms to counter those operations. A growing number of US allies in Asia are also launching initiatives against Chinese efforts to drive wedges between those nations and the United States. In addition, the United States and its security partners should anticipate specific opportunities for adversaries to play "divide and rule" in future crises and manipulate allied perceptions of the costs and benefits of coalition operations. It is especially important that we account for the risk that adversaries will fuel and reinforce doubts the United States and its allies have about their willingness to defend each other, thereby increasing the chances they actually will capitulate rather than facing the punishment that IOs warn is coming.

Alliance Coercion and Crisis Decision-Making

Russia's IOs seek not only to weaken the overall cohesion of NATO but also to specifically undermine the confidence of European members that the

[795] DoD, *National Defense Strategy*, 8.

[796] DoD, *National Defense Strategy*, 9.

United States will come to their aid when they most need assistance. A study team appointed by NATO's secretary general reported in November 2020 that "the last ten years have been characterised by questions about the commitment of the United States to the defence of the European continent" and other threats to alliance cohesion.[797] Russia is also tailoring its IOs to undermine ongoing efforts to strengthen allied preparedness.[798] Most recently, for example, Moscow conducted deceptive messaging to disrupt planning and force realignments for the Enhanced Forward Presence initiative along NATO's eastern flank, an initiative launched in part in response to Russia's invasion of Ukraine and its continuing threats against other central European countries.[799]

China can also use IOs to exploit uncertainties about the extent and reliability of US defense commitments. Taiwan is especially notable in this regard. Robert O'Brien, while serving as US national security advisor, stated that there's "a lot of ambiguity about what the United States would do in response to an attack by China on Taiwan."[800] This long-standing policy of "strategic ambiguity" gives the US flexibility in dealing with crises involving Taiwan. China considers Taiwan its province and has vowed to bring Taiwan under its control, by force if necessary. But the policy also opens the door to IOs against Taiwan's leaders that seek to convince them that the United States will ultimately abandon them in a crisis rather than risk an escalating war with a nuclear-armed adversary and that resistance against forcible reunification would be futile and costly.

US military bases provide adversaries with additional opportunities to corrode US security partnerships and conduct coercive IOs. As noted in the US *National Defense Strategy*, US defense installations abroad are crucial for US plans and capabilities to conduct regional operations. Yet, as in Okinawa, the presence of these bases can also generate fierce political opposition and help adversaries advance broader disinformation efforts.[801] There is also the risk of host nations disrupting these the operations of these bases. In July 2016, for example, the Turkish government cut off power to the US Incirlik Air Base as it conducted intensive strikes against ISIS.[802] The base used emergency generators to sustain operations during the multiday outage. However, in future crises, adversaries may pressure host nations to widen and sustain such disruptive measures rather than suffer attacks on their own populations and infrastructure.

All such IOs will benefit from the same advances in TTPs that China and Russia are employing against the United States. Just as these nations are seeking to widen and exploit divisions in American society and microtarget their messaging accordingly, they are doing so in operations against US security partners. China's systematic disinformation campaign aimed at Taiwan exemplifies this focus on social and political polarization to amplify the spread and impact of its messaging.[803] Russian operations against US allies in Europe display increasingly sophisticated means of targeting and delivering anti-US and anti-NATO information campaigns. The Ghostwriter campaign is targeting audiences in Lithuania, Latvia, and Poland with narratives critical of the NATO presence in eastern Europe. The campaign uses website compromises and spoofed email accounts to disseminate fabricated content, including falsified news articles, quotes, correspondence, and other documents designed to appear as

[797] Reflection Group, *NATO 2030*, 21.

[798] Giles, *Handbook of Russian Information Warfare*, 22.

[799] Bugajski, *Why Does Moscow?*

[800] Brunnstrom, "U.S Warns China."

[801] Denyer and Kashiwagi, "On Japan's Okinawa." For more on the broader Chinese disinformation campaign against Japan that includes Okinawa as a focus, see Morgan, "Is Japan Putting Up A Good Enough Fight?"

[802] Bruton, Williams, and Kube, "Incirlik Air Base."

[803] Corcoran, Crowley, and Davis, *Disinformation Threat Watch*.

if coming from military officials and political figures in the target countries. This falsified content has been referenced as source material in articles and op-eds authored by at least fourteen inauthentic personas posing as locals, journalists, and analysts within those countries.[804]

The Secondary Infektion campaign uses additional TTPs to undermine NATO cohesion and portray the United States as an unreliable ally. While active on Reddit, Medium, Twitter, Quora, Facebook, and YouTube, Secondary Infektion operatives posted false and politically explosive stories—often based on images of "leaked" documents—on internet forums and then amplified them in various languages across a range of platforms. The "leaks" typically exposed some dramatic geopolitical scandal, such as a prominent Kremlin critic's corrupt dealings or secret American plans to overthrow pro-Kremlin governments around the world.[805]

The operation also impersonates Western leaders in its messaging. It has included fake letters, tweets, and blog posts from leaders and officials including former US secretary of state Mike Pompeo, former White House chief of staff General John Kelly, various members of the US Senate Foreign Affairs and Intelligence committees, and senior representatives of the German, British, and Ukrainian governments.[806]

These TTPs are ideally suited to foster doubts about the willingness of allies to stay the course in a regional confrontation. Allied leaders can use secure communications systems to clarify their positions on whether and how to contest adversary steps to prevail in an intensifying crisis. However, for IOs against legislators, social media influencers, and the public, the use of impersonated messaging and forged documents could provide "evidence" that allies are unreliable and will back down in the face of threats of punishment. Adversaries can also integrate such disinformation measures against US and allied audiences to magnify their effects. The American public will no doubt be told that NATO members consider the president unreliable and that given the danger that the United States will abandon them, they no longer think that NATO can prevail against Russia at an acceptable level of suffering. European publics will be treated to the flip side of the same messaging. New plans for allied coordination will be needed to defeat such spiraling, mutually reinforcing narratives.

Moreover, while the president and allied leaders can use security communications to reduce their vulnerability to impersonated messaging and other advanced TTPs, they will hardly be immune to leadership-oriented operations. Just as China and Russia are gathering sensitive personal data on US senior officials, they are conducting similar operations against US allies. For example, the US Defense Intelligence Agency reports that the People's Liberation Army's (PLA) intelligence department is collecting and analyzing intelligence information regarding senior-level officers from Taiwan, Japan, and other defense establishments of interest. We should expect China and Russia to use such data to microtarget IOs against officials who will coordinate alliance crisis operations and manage the fears and policy conflicts that these adversaries will seek to foster.

Implications for Coalition Defense

Defeating coercive IOs that target US alliances will require a more detailed analysis of specific coordination mechanisms and other points of vulnerability that adversaries will seek to exploit. NATO decision-making under Article 5 of the treaty that founded the organization should be an immediate focus of such efforts. Under Article 5, an attack on one member "shall be considered an attack

[804] Mandiant, *'Ghostwriter' Influence Campaign*.

[805] Nimmo et al., *Secondary Infektion*.

[806] Nimmo et al., *Secondary Infektion*.

against them all."[807] That commitment to collective defense provides a crucial means of deterring Russian attacks on NATO's members and, if deterrence fails, defeating such attacks. But another fundamental aspect of NATO decision-making creates vulnerabilities to Russian interference. The organization's *NATO 2030* report (November 2020) notes that "the principle of consensus is a cornerstone of the Alliance that guarantees the ability of all members, irrespective of size, to decisively influence outcomes." Recent years, however, "have also seen a rise in the incidence of single-country blockages"—that is, the decision by one member to prevent action by the organization.[808] In future crises, Russia could use coercive IOs to incentivize a member to delay or block NATO's response to an intensifying crisis.

The 2030 report calls on NATO to review and bolster as needed its ability to implement agreed-upon decisions and procedures that have been reached by consensus and ensure that it can act in a timely fashion, "especially during a crisis."[809] The organization should also take the next step and develop plans to counter Russian coercion of a blocking state to forestall collective defense.

Measures to defeat coalition-oriented IOs should also account for the crucial role that social media will play in shaping public (and, potentially, leadership) perceptions of a crisis. The fact that Facebook and other social media platforms are multinational enterprises creates challenges for developing playbooks and industry–government coordination mechanisms to block coercive messaging against US audiences. Expanding such initiatives to encompass European and Asian allies would entail still greater difficulties. Nevertheless, given the risks that China and Russia will exploit the global reach of social media platforms and use them to fuel spiraling disbelief in allied defense commitments, US efforts to collaborate with platform owners should include security partners as well.

Coercion by Denial

Robert Pape argues that while threats of punishment often fail to achieve their coercive goals, coercion by denial can offer a more effective strategy. This form of coercion succeeds "when force is used to exploit the opponent's military vulnerabilities, thereby making it infeasible for the opponent to achieve its political goals by continued military efforts." Coercion by denial seeks to alter an opponent's calculus of costs and benefits in a different way than by inflicting suffering. To paraphrase Pape: if an attacker convinces opposing leaders that they can no longer achieve their objectives, the costs they previously considered bearable now become intolerable. Faced with military failure, the opponent will concede "in order to avoid suffering further losses to no purpose."[810]

Pape also notes that "For coercion though denial to succeed, the coercer must exploit the particular vulnerabilities of the opponent's specific strategy."[811] One potential vulnerability is of special concern to current and former Pentagon officials: the dependence of the United States on surging forces from American territory to regional confrontations and the risk that adversaries will establish a fait accompli before those forces can arrive.

Very large-scale cyber and/or kinetic attacks on US transportation systems and supporting infrastructure would be required to disrupt US surge operations. Such attacks could provoke a US response that would inflict costs unacceptable to Chinese and Russian leaders. The US should take every measure necessary to help convince those leaders that if they were to strike US infrastructure, they would indeed pay an unacceptable

[807] North Atlantic Treaty, April 4, 1949.

[808] Reflection Group, *NATO 2030*.

[809] Reflection Group, *NATO 2030*.

[810] Pape, *Bombing to Win*, 1 and 10.

[811] Pape, *Bombing to Win*, 30.

price. In addition, however, policymakers should also reduce the possible gains that China and Russia could hope to achieve by exploiting vulnerabilities in US regional warfighting strategies.

Defending the Surge Layer

The US maintains far fewer ground and air forces abroad than it did during the Cold War. To defend US allies and interests in major regional conflict, DoD would first need to mobilize reinforcements at home and deploy them to the contested area. Those forces will be enormously capable once they arrive. Rather than allowing the United States to bring the full brunt of its military power to bear in a crisis, opponents may seek disrupt the flow of forces to the region while also establishing and consolidating local military superiority that would be costly for US leaders to overturn.

In 2015, then-deputy secretary of defense Robert Work noted that "almost all our combat power" is now based within the United States. If a regional confrontation emerged and the United States began preparing to deploy forces accordingly, "you now have to assume that you're going to be under intense cyber attack even before you move."[812] That assumption remains valid today. Under the *2012 National Defense Strategy*, the US military will seek to blunt an adversary's initial attacks in a regional conflict while "surging" the forces to the area to achieve victory.[813] Disrupting surge operations constitutes an opportunity for China and Russia to counter the US strategy and—paired with IOs—convince US leaders that they have no chance of prevailing at an acceptable cost.

In addition to striking US forces as they near the conflict zone, adversaries may attack civilian-operated transportation systems within the United States that are essential for surge operations. The US Transportation Command (USTRANSCOM) relies on civilian air, shipping, and other transportation assets to rapidly deploy US forces in times of crisis. Commercial carriers supply 90 percent of the capacity to take troops to war, and cargo industry companies move 40 percent of military material.[814] Civilian ports in Los Angeles, Long Beach, and other cities also provide critical supplements to navy installations for loading and deploying personnel and warfighting material. And of course, all such ports and supporting transportation networks depend on the availability of grid-provided power to function.

USTRANSCOM leaders are concerned that adversaries may conduct cyberattacks to disrupt regional deployments. In 2018, General Darren McDew, then-combatant commander of USTRANSCOM, noted that "adversaries no longer have to stop us with bombs or bullets; all they have to do is slow us down with ones and zeroes." McDew emphasized that "every one of our potential adversaries understands our vulnerabilities in rail."[815] However, China has been implanting APTs across a broad array of the contactor systems on which DoD transportation depends.[816] Russia is doing so as well. The Office of the Director of National Intelligence has determined that "Moscow is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure" during a crisis.[817] The net result, according to the US *National Security Strategy*: cyber weapons enable adversaries to attempt attacks that would "cripple our economy and our ability to deploy our military forces."[818]

The defense of Taiwan from Chinese military conquest exemplifies these risks. Michèle Flournoy, a

[812] Peniston, "Era of Grand Strategy."

[813] DoD, *National Defense Strategy*, 9.

[814] Mazmanian, "Transcom Head Warns."

[815] Mazmanian, "Transcom Head Warns."

[816] SASC, "Chinese Intrusions." Of course, adversaries could also strike in-theater forces and US military ships, submarines, and bombers as they traveled thousands of miles from their US bases to the conflict zone. See Brose, *Kill Chain*.

[817] *Hearing on Worldwide Threat Assessment*, Coats statement, 5.

[818] White House, *National Security Strategy*, 27.

former undersecretary of defense for policy, offers a specific example of adversary planning for such attacks. She states that "Chinese military planning for taking Taiwan by force envisions early cyberattacks against the electric power grids around key military bases in the United States, to prevent the deployment of U.S. forces to the region."[819] Consistent with Chinese military doctrine, the PLA is also likely to strike US command and control networks in the early stages of conflict to put in-place and arriving US forces at a further disadvantage.[820]

Anti-surge cyberattacks would go forward in tandem with operations to achieve initial military dominance in the crisis region and the rapid deployment of additional forces to deny US access to the area. Elbridge Colby, former deputy assistant secretary of defense for strategy and force development, testified to Congress in January 2019 that China and Russia will seek to establish a fait accompli in regional confrontations. Their first step to do so will be to overpower US allies in the region. Then, by extending anti-access/area denial networks and other forces to extend a "defensive umbrella" over their new gains, China and Russia would "render the prospect of ejecting their occupying forces too difficult, dangerous, and politically demanding for Washington and its allies to undertake, or undertake successfully."[821] Christian Brose, a former staff director of the Senate Armed Services Committee, argues that using this strategy would leave US leaders with two available options: "surrender and lose or fight and lose. The bigger question at that point would be whether that future president would even be willing to go to war at all."[822]

The potential effects of such strategies on US decision-making suggest a new broader understanding of what constitutes coercion. A number of analysts argue that coercive campaigns are distinct from fait accompli strategies. The Russian invasion of Ukraine highlights this distinction. Dan Altman writes that instead of threatening to attack Ukraine if Kiev failed to relinquish Crimea (which would have constituted coercion), Russia instead occupied Crimea and achieved its goals by imposing a fait accompli.[823] Michael Fischerkeller draws a similar dichotomy. He argues that "the *fait accompli* is distinct in principle from coercion, which describes demands, signaling, and interaction."[824]

However, in view of Chinese and Russian military doctrines, these nations are almost certain to supplement their efforts to establish local military dominance (and to disrupt US surge operations) with IOs to convince US policymakers that continued defense of US allies will be bloody and futile. Efforts to manipulate US perceptions of the costs and benefits of US military operations constitute the essence of coercion. Measures to defeat such manipulation should become a new component of regional contingency planning and be incorporated in the updated *National Defense Strategy* that the Biden administration will issue in 2022.

US defense partners should also be included in such initiatives. If China or Russia were to take the enormous escalatory risks of striking US ports and supporting rail and road systems, they would also be likely to attack the ports in allied territory that will be receiving American forces. The Pentagon has established an elaborate system for joint reception, staging, onward movement, and integration (JRSOI) of troops and supporting assets deploying to a crisis zone.[825] Targeting transportation systems essential for JRSOI in a conflict zone can help

[819] Flournoy, "How to Prevent a War in Asia."

[820] DIA, *China Military Power*, 46. The Combined Information-Cyberattacks section of this study examines how attacks on command and control and other networks contribute to China's broader strategy of "system destruction warfare" and the implications of defending the United States against combined cyber-information attacks.

[821] *Hearing on China and Russia*, Colby statement, 3–4.

[822] Brose, *Kill Chain*.

[823] Altman, "By Fait Accompli, Not Coercion."

[824] Fischerkeller, "Fait Accompli."

[825] JCS, *Deployment and Redeployment Operations*, viii.

adversaries seek the "end-to-end" disruption of US surge operations.

The same is true of targeting the power grids and other systems that enable allied ports to function. The Philippines highlights the benefits that attacks could have for coercion by denial. While the US defense relationship with the Philippines has frayed since the election of President Rodrigo Duterte in 2016, the US alliance with that nation is crucial for countering Chinese ambitions in Southeast Asia and protecting regional security.[826] Those ambitions extend to holding the Philippine power grid hostage to cyberattacks. A 2019 report by the Philippine government found that the nation's electric system was currently "under the full control" of the Chinese government, which has the "full capability to disrupt" that system. In particular, "our national security is completely compromised due to the control and proprietary access" that Chinese engineers have to the grid's SCADA (supervisory control and data acquisition) systems.[827]

The implantation of malware on the power grids of US security partners around the globe constitutes a less overt but increasingly severe threat to JRSOI operations. Helping US security partners reduce their vulnerabilities to infrastructure disruptions should become part of the overall US strategy to defeat counter-surge operations and—more broadly—limit any possible adversary hopes of achieving coercion by denial.

Conclusions and Next Steps

The United States is at risk of suffering yet another failure of imagination. Even as we develop increasingly sophisticated plans and capabilities to coerce adversaries in future crises, we ignore the danger that adversaries will do the same to us.

The assessment of coercive threats in this study provides a foundation for developing a US strategy to defeat them. However, the Constitution will be just as important for guiding our defensive initiatives. China and Russia are taking advantage of the First Amendment to flood Americans with disinformation and corrode public faith in democratic governance. They will exploit this same advantage to shape US public perceptions and drive leadership decision-making in future crises, even as they wall off their own populations from messaging they fear.

Yet, the First Amendment does not give Americans the right to shout "fire" in a crowded theater. We must not allow adversaries to engage in the information-age equivalent of such panic-inducing behavior, by threatening American families with horrific punishment or—in combined attacks—intensifying the terror that exemplary strikes will create. Federal agencies and their social media partners should immediately begin to develop specialized criteria to block coercive messaging during future crises, and create the tools and coordination mechanisms to do so in the face of cyberattacks on US communications networks and the use of selective cutoff strategies.

Policymakers and researchers should also prioritize two additional initiatives beyond those examined in this study. The first is to *take advantage* of the fact that the Department of Defense (DoD) is light-years ahead of other federal departments in coercive technologies and expertise, and expand defense support to these departments and their private sector partners. Second, the United States should develop plans, capabilities, and policy pronouncements to deter coercive information operations (IOs) and combined attacks—perhaps by threatening to share information with Chinese and Russian citizens information that their rulers dread.

[826] Green, *U.S. Alliance with the Philippines*.

[827] Griffiths, "China Can Shut Off."

Defense Support

DoD assistance to other departments has already proven valuable against election influence campaigns. During the 2018 midterm elections, DoD not only suppressed Russian attacks at their source in St. Petersburg but also helped the Department of Homeland Security (DHS) protect US election infrastructure at home. USCYBERCOM and the National Security Agency (NSA) shared indicators of potential compromises with DHS to help the department defend election infrastructure. DoD also shared threat indicators with the Federal Bureau of Investigation (FBI) to support that organization's efforts to counter foreign trolls on social media.[828] DoD should build on these information-sharing models to help its interagency partners conduct equivalent domestic operations against coercive campaigns.

Providing data on threats and vulnerabilities to the private sector will be essential as well. Supported with data from DoD and other agencies in the US intelligence community, DHS's Cybersecurity and Infrastructure Security Agency (CISA) provided extensive threat and vulnerability data to 2020 election infrastructure vendors and operators (including state election officials) to bolster their defenses against foreign manipulation or interference.[829] DoD and broader federal intelligence support for private sector infrastructure security also goes far beyond election systems. In February 2020, for example, DoD, DHS, and the Department of Energy (DOE) launched a new Energy Sector Pathfinder initiative to increase information sharing and exercises with each other and with electric utilities to counter cyber threats.[830] Building on Pathfinder and dozens of other initiatives within and beyond the energy sector will be vital for defeating cyberattacks that seek to coerce US behavior by jeopardizing public health and safety or (for coercion by denial) by disrupting the flow of US forces to regional crises.

Options for closer public–private operational coordination during crises are also emerging. For example, in October 2020, USCYBERCOM reportedly disrupted the Trickbot botnet, a network of at least one million hijacked computers run by Russian-speaking criminals that might otherwise have been used to disrupt the 2020 elections.[831] Simultaneously, Microsoft obtained a federal court order to disable the IP addresses associated with Trickbot servers and worked with telecom providers around the world to disrupt the network.[832] But new mechanisms for public–private coordination will be necessary to take down enemy infrastructure in crises, when adversaries will seek to disrupt or exploit US telecom systems and social media platforms to deliver coercive messaging. Defense-informed suppression operations will also need to keep pace with rapid shifts in the threat. A case in point: shortly after the Microsoft/USCYBERCOM operation, Trickbot's creators reconfigured the malware to evade detection and infect their victims' firmware.[833]

Military exercises offer another opportunity for near-term defense support. In May 2021, the Air Force conducted its first-ever information warfare "flag" exercise and held an initial information warfare "weapons and tactics" conference in November 2020. Those efforts are designed to help prepare Air Force personnel to "think about perceptions and behaviors and sentiments of different audiences around the world" and integrate that thinking into operational plans and tactics.[834] At the National Training center, the US Army has established a mock internet—one with "Tweeter" instead of

[828] Nakasone and Sulmeyer, "How to Compete in Cyberspace," 7.

[829] CISA, "Election Infrastructure Security."

[830] DOE, "Pathfinder Initiative."

[831] Nakashima, "Cyber Command."

[832] Fung, "Microsoft Disrupted a Massive Hacking Operation."

[833] Greenberg, "Internet's Most Notorious Botnet."

[834] Pomerleau, "Information Warfare Test Exercises"; and Pomerleau, "Air Force Prepares."

Twitter—to help military personnel exploit social media abroad and understand the vulnerabilities those media create.[835] DHS and other agencies would benefit from participating in equivalent exercises and training programs reoriented toward countering coercive operations against the United States. Exercise components (including scenarios) created by the military could provide a head start on creating domestic-focused variants. Over time, including civilian agencies, social media companies, and military units in joint exercises could also help them develop plans and capabilities for integrated defensive operations at home and abroad.

Sharing and repurposing military technologies for use abroad provides an additional opportunity for defense support. The development of artificial intelligence (AI) and machine learning tools offers a prime option. The Joint Artificial Intelligence Center's Joint Information Warfare is developing a new tool, Entropy, to reduce the cognitive burden on personnel performing military information support operations to shape adversary thinking.[836] AI tools could offer similar benefits for the personnel of DHS and other agencies responsible for countering coercive operations against the United States. Sharing DoD's machine learning and AI technologies with those agencies could help them develop such defensive tools far more rapidly than would otherwise be possible. The same is true of the Defense Advanced Research Projects Agency's tools for automatic detection of deepfake videos and other DoD-funded technology initiatives.[837]

The National Guard offers additional opportunities for defense support to civilian agencies and the private sector. Over the past decade, state National Guard organizations have been partnering with their local electric utilities and other infrastructure owners to help them protect against and recover from cyberattacks. State adjutant generals, the National Guard Bureau, and DoD policymakers should explore how those support capabilities might be applied to help counter combined IO-cyberattacks. In the Guard's Cyber Shield 20 exercise, defense against influence operations was a key focus for participating cyber protection teams, state agencies, and industry partners.[838] Building on the findings of that exercise could help accelerate the development of options for Guard support for civil authorities and the private sector against coercive operations.

Deterrence

The United States can pursue a mix of two basic strategies to deter coercive campaigns: denial and cost imposition. As formulated by Glenn Snyder early in the Cold War, deterrence by denial is achieved by "the capability to deny the other party any gains from the move which is to be deterred."[839] Other analysts contend that denial can also function by increasing the costs (or "work factor") that adversaries will incur by attacking relative to the benefits they hope to achieve.[840] The Cyberspace Solarium Commission report argues that "in cyberspace, deterrence by denial works by increasing the costs to the attacker—beyond just financial costs—of breaching the deterring state's defenses."[841]

Denying or sharply reducing the benefits that adversaries expect to achieve through coercive campaigns should be central to US deterrence efforts. This study has identified a broad array of defensive measures that could weaken the effectiveness of coercive campaigns, and thereby reduce

[835] Pomerleau, "Fake Internet."

[836] Pomerleau, "Pentagon's AI Center."

[837] NBC Nightly News, "Defense Department Agency Developing Tech."

[838] Pomerleau, "National Guard Cyber Exercise"; and IMD, "Cyber Warriors."

[839] Snyder, "Deterrence and Power." See also Snyder, *Deterrence and Defense*, 14–15; Mazarr, *Understanding Deterrence*, 2; and Davis, "Toward Theory for Dissuasion."

[840] Nye, "Deterrence and Dissuasion," 54 and 56.

[841] CSC, *Official Report*, 26.

the gains that Beijing and Moscow could hope to achieve through IOs and combined attacks. Some of these options, including the development of integrated cyber-IO defensive playbooks, can and should begin immediately. Others will take years of analysis and experimentation, most importantly for educating Americans to be more discerning consumers of social media and less prone to be sitting ducks for Chinese and Russian IOs.

Increasing the attacker's costs of conducting coercive campaigns could also contribute to deterrence. For example, if US agencies and social media companies can improve their capabilities to filter deepfakes, adversaries intent on using fake messaging would need to invest in evasion technologies. Broader defensive measures to block coercive IOs and facilitate US counter-messaging could also increase Chinese and Russian costs of conducting effective campaigns. And of course, to help deter combined information-cyberattacks, initiatives to strengthen the cyber resilience of US infrastructure and other potential targets could significantly increase the work factor for potential adversaries.

Yet, because many of these denial-related efforts will take so long to accomplish, the United States should simultaneously pursue a second approach to deterrence: cost imposition. We should seek to convince Chinese and Russian leaders that if they launch a coercive attack, the United States will respond by imposing costs that those leaders would find unacceptable.

Different types of response options may be required to deter (and, if necessary, retaliate against) coercive campaigns at various points across the conflict continuum. At the most destructive end of that spectrum, combined attacks that incurred mass US casualties and fell into the "significant" category of the US Cyber Incident Severity Schema would almost certainly incur an equally devastating US response. The administration should do everything necessary to ensure the credibility of that response posture and convince Russia and Chinese leaders that they would incur unacceptable costs if they launched a catastrophic combined attack. American leaders should also stick with the long-standing policy that the United States would not necessarily respond to cyberattacks (or, presumably, combined information-cyberattacks) in kind, but could also use other types of forces for response operations.

The puzzles for US deterrence lie at the lower end of the conflict continuum. In the precrisis gray-zone competition that is constantly underway, USCYBERCOM is already imposing costs on Russia for its ongoing campaigns to corrode US democratic governance and implant malware on critical infrastructure. But what deterrence posture should we adopt against Chinese and Russian operations in the dark-gray zone, where the risks of war are surging and IOs threaten American families with horrific punishment? Moreover, how can the US deter exemplary attacks during the initial period of warfare, in which China and Russia would inflict carefully limited damage yet (thanks to personalized messaging) create intense public fears and pressure on US leaders to yield?

The law of armed conflict provides a starting point for developing threats of cost imposition that are aligned with these crisis phases. DoD's Law of War Manual specifies that US military operations should follow the principles of military necessity, humanity, proportionality, distinction, and honor.[842] Further legal and ethical analysis will be required to apply many of these principles to the information realm. However, proportionality provides a relatively clear-cut foundation for developing options to impose costs and for creating declaratory policies that reflect them.

The Law of War Manual states that "Proportionality may be defined as the principle that even where one is justified in acting, one must not act in a way that

[842] Law of War Manual, 1013–1025. See also Genaro Phillips, "Unpacking Cyberwar."

is unreasonable or excessive."[843] In applying this principle, "Proportionality generally weighs the justification for acting against the expected harms to determine whether the latter are disproportionate in comparison to the former."[844] US plans for imposing retaliatory costs on an opponent should be designed accordingly. In responding to an IO-only campaign, it would almost certainly be disproportional to inflict massive casualties on the opponent's population, unless the harm inflicted by killing so many civilians was somehow outweighed by the military justification for doing so. Furthermore, given the danger that the opponent would react to such an attack by launching an equally devastating counterstrike, threats that the president would respond to an IO-only strike in this fashion would be neither believable nor prudent.

The United States should develop response options against coercive campaigns that follow principles of proportionality and that are likely to be deemed credible by Chinese and Russian leaders. These options should be scaled to the phases of an escalating crisis and the levels of destruction they would entail, from IO-only campaigns during the dark-gray phase, through exemplary strikes that cause carefully limited damage but powerful coercive effects, through large-scale disruptions of US infrastructure.

US responses to IOs and combined attacks need not exactly mirror the opponent's choice of targets and weaponry. Indeed, being able to respond in kind to cyberattacks on US infrastructure may not be sufficient to deter coercive campaigns. The United States must convince opposing leaders that if they launch a coercive campaign, they will suffer costs that outweigh any possible gains. These leaders may attach a much higher value to military forces, command and control networks, and other assets apart from the critical infrastructure that sustains their citizens' lives. Above all, they may fear the loss of what keeps them in power.

We may be able to exploit those fears and help deter coercive attacks by including IOs in our response options. In addition to the police forces, surveillance infrastructure, and broader domestic security architecture that help Chinese and Russian leaders maintain their grip on their respective populations, control over publicly available information is a powerful tool for their self-preservation. Beijing uses the Great Firewall to reinforce that control. The Kremlin has the plans and capabilities to erect an equivalent barrier in future crises.

The logic of deterrence might suggest that we should hold at risk what our adversaries hold dear: their ability to wall off their citizens from messaging that might undermine their rule or generate opposition to their crisis decision-making. The precepts of proportionality might also seem to permit the use of IOs in response to coercive campaigns. If China or Russia launched such campaigns against the American public, it could seem perfectly reasonable for the United States to deliver counter-messaging to the Chinese and Russian publics, while holding back from destructive cyberattacks as long as our adversaries did the same.

Yet, incorporating IOs into the US deterrent posture would entail major technical problems and escalatory perils. To respond in kind to enemy messaging, the United States would need the ability to punch holes in adversary firewalls and maintain US access to the adversary's population as the crisis evolved. Achieving those capabilities, and convincing foreign leaders that the United States possesses them, could be difficult.

Even if penetrating adversary firewalls were technically feasible, doing so in response to coercive IOs might be inordinately dangerous. Russian leaders (and perhaps those in China as well) have carefully assessed the implications of the color revolutions for their own continued rule. If those leaders believed that American IOs could indeed jeopardize their

[843] Law of War Manual, 60.

[844] Law of War Manual, 61.

regimes, US response options that might seem proportional in our eyes could be perceived as vastly more provocative in Beijing and Moscow.

Weighing the deterrent benefits against the escalatory risks of threatening or employing IOs should become a priority for future analysis. In "Some Fundamental Principles of Deterrence," Craig Fields offers propositions that could help guide such assessments. He emphasizes that rather than seeking to deter countries, we must focus on deterring the specific individuals and decision-makers in those countries who "decide whether or not to unleash an attack on the United States." Fields also notes that "deterrence of an individual is an exercise in psychology, not physics," and that we therefore need the "very best collection and analysis regarding the individuals we want to deter."[845]

That will be especially true in crafting IOs that seek to directly influence leadership perceptions of the costs and benefits of coercive campaigns against the United States. The United States could also exploit leadership beliefs in crafting messages for other targets. As noted above, Chinese and Russian authorities may fear that information campaigns could prompt citizens to question their rule and oppose their crisis policies. Targeting leadership cronies offers another deterrent option. Drawing a page from the Operation Allied Force (OAF) playbook, the United States might deliver customized IOs to the political, military, and economic elites that help keep Chinese and Russian regimes in power. A credible US ability to conduct such operations might help convince foreign leaders that coercive campaigns would be too costly.

There is no guarantee, however, that foreign leaders would fear American IOs even if we made them a prominent feature of our deterrent posture. These leaders may doubt whether public or crony-focused messaging will have any impact on the stability of their regimes, given their extensive internal security forces and other instruments of domestic control. Concerns that American IOs could provoke a catastrophic response could turn out to be entirely unfounded. We may face the opposite problem: that adversaries will deem our IOs ineffectual and irrelevant to their assessments of costs and benefits. That possibility makes it all the more important to maintain the credibility of other US instruments of deterrence. But we should also examine how emerging technologies can help us develop IO response options that opponents will someday dread, while also building defenses to reduce the gains that foreign leaders can hope to achieve through coercion in future crises.

[845] Fields, "Some Fundamental Principles of Deterrence."

Bibliography

Acevedo, Nicole. "Amid Government Mess, Hurricane Maria Survivors Lack Access to Philanthropic Aid." *NBC News*, September 19, 2019. https://www.nbcnews.com/news/latino/amid-government-mess-hurricane-maria-survivors-lack-access-philanthropic-aid-n1056221.

Ackerman, Robert K. "Naval Warfighting Embraces the Full Spectrum of Information." *SIGNAL*, March 1, 2019. https://www.afcea.org/content/naval-warfighting-embraces-full-spectrum-information.

ACPD (Advisory Commission on Public Diplomacy). *Public Diplomacy and the New "Old" War: Countering State-Sponsored Disinformation*. Washington, DC: Department of State, September 2020. https://www.state.gov/wp-content/uploads/2020/09/Public-Diplomacy-and-the-New-Old-War-Countering-State-Sponsored-Disinformation.pdf.

Adamsky, Dmitry (Dima). *Cross-Domain Coercion: The Current Russian Art of Strategy*. Proliferation Papers 54. Paris: Institut Français des Relations Internationales, November 2015. https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

AEP (Public-Private Analytic Exchange Program). *Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue*. Washington, DC: DHS, October 2019. https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

Air Combat Command Public Affairs. "Air Combat Command Announces 24 and 25 AF Merger." April 4, 2019. https://www.acc.af.mil/News/Article-Display/Article/1805297/air-combat-command-announces-24-and-25-af-merger/.

Alba, Davey. "How Russia's Troll Farm Is Changing Tactics before the Fall Election." *New York Times*, March 29, 2020. https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html.

Allen-Ebrahimian, Bethany. "China Takes a Page from Russia's Disinformation Playbook." *Axios*, March 25, 2020. https://www.axios.com/coronavirus-china-russia-disinformation-playbook-c49b6f3b-2a9a-47c1-9065-240121c9ceb2.html.

Allison, Graham, and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd ed. Boston: Addison Wesley Longman, Inc., 1999.

Altman, Dan. "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries." *International Studies Quarterly* 61, no. 4 (December 2017): 881–891. https://academic.oup.com/isq/article/61/4/881/4781720?login=true.

Amini, Sajjad, Fabio Pasqualetti, and Hamed Mohsenian-Rad. "Dynamic Load Altering Attacks against Power System Stability: Attack Models and Protection Schemes." *IEEE Transactions on Smart Grid* 9, no. 4 (July 2018): 2862–2872. https://ieeexplore.ieee.org/document/7723861.

AP (Associated Press). "Facebook's Zuckerberg Is the Focus of Latest Doctored Video." June 13, 2019. https://apnews.com/8f68040962074a3ab2f9634d8fcd0a3b.

———. “I Never Said That! High-Tech Deception of ‘Deepfake’ Videos.” *CBS News*, July 2, 2018. https://www.cbsnews.com/news/i-never-said-that-high-tech-deception-of-deepfake-videos/.

———. “Zuckerberg Says Facebook Must Stand Up for Free Speech.” February 1, 2020. https://apnews.com/c3291531831d19ff0eaf8d91aa1415a0.

ARC (Analysis and Resilience Center for Systemic Risk). “What We Do.” Accessed June 21, 2021. https://systemicrisk.org/what-we-do/.

Arkin, William M. “Ask Not for Whom the Phone Rings.” *dot.mil* (blog). *Washington Post*, October 11, 1999. http://www.washingtonpost.com/wp-srv/national/dotmil/arkin101199.htm.

Art, Robert J. “To What Ends Military Power?” *International Security* 4, no. 4 (Spring 1980): 3–35. https://doi.org/10.2307/2626666.

Art, Robert J., and Kelly M. Greenhill. “Coercion: An Analytical Overview.” In *Coercion: The Power to Hurt in International Politics*, edited by Kelly M. Greenhill and Peter Krause. Oxford: Oxford University Press, 2018.

Auf der Heide, Erik. “Common Misconceptions about Disasters: Panic, the ‘Disaster Syndrome,’ and Looting.” In *The First 72 Hours: A Community Approach to Disaster Preparedness*, edited by Margaret O’Leary, 340–380. Lincoln, NB: iUniverse, Inc., 2004. https://www.atsdr.cdc.gov/emergency_response/common_misconceptions.pdf.

Austin, Lloyd J. “Message to the Force.” Memorandum, March 4, 2021. https://www.airforcemag.com/app/uploads/2021/03/SECRETARY-LLOYD-J-AUSTIN-III-MESSAGE-TO-THE-FORCE.pdf.

Baozhu, Yu. “The ‘Chinese Times’ [Huaxia Shibao] Builds a Bridge of China–US Cultural Exchange.” *Military Correspondent*, January 2012.

Barger, Michael G. “Psychological Operations Supporting Counterinsurgency: 4th PSYOP Group in Vietnam.” Master’s thesis, US Military Academy, 2007. https://apps.dtic.mil/dtic/tr/fulltext/u2/a471075.pdf.

Barnes, Julian E., and Adam Goldman. “Russia Trying to Stoke U.S. Racial Tensions before Election, Officials Say.” *New York Times*, March 10, 2020. https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html.

Barrett, Devlin. “Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack.” *Washington Post*, August 24, 2017. https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html.

Barrett, Paul M. *Tackling Domestic Disinformation: What the Social Media Companies Need to Do*. New York: NYU Stern Center for Business and Human Rights, March 2019. https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_domestic_disinformation_digital?e=31640827/68184927.

Barrett, Paul M., Tara Wadhwa, and Dorothée Baumann-Pauly. *Combating Russian Disinformation: The Case for Stepping Up the Fight Online*. New York: NYU Stern Center for Business and Human Rights, July 2018. https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_stern_cbhr_combating_russian_di?e=31640827/63115656.

Barry, John. “NATO’s Game of Chicken.” *Newsweek*, July 25, 1999. https://www.newsweek.com/natos-game-chicken-168728.

Bateman, Jon. *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios*. Washington, DC: Carnegie Endowment for International Peace, July 2020. https://carnegieendowment.org/files/Bateman_FinCyber_Deepfakes_final.pdf.

BBC News. “Coronavirus: Russia Denies Spreading US Conspiracy on Social Media.” February 23, 2020. https://www.bbc.com/news/world-us-canada-51599009.

———. “US President Joe Biden ‘Pauses’ TikTok and WeChat Bans.” February 12, 2021. https://www.bbc.com/news/technology-56041209.

Beauchamp-Mustafaga, Nathan. “Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations.” *China Brief* 19, no. 16 (September 2019): 24–37. https://jamestown.org/wp-content/uploads/2019/09/Read-the-09-06-2019-CB-Issue-in-PDF.pdf?x97873.

Beinecke, Richard. “Honoring the Community That Helped Heal Boston.” *WBUR*, April 17, 2017. https://www.wbur.org/cognoscenti/2017/04/17/boston-bombing-three-years-mental-health-richard-beinecke.

Bendett, Samuel. “Sneak Preview: First Draft of Russia’s AI Strategy.” *Defense One*, September 10, 2019. https://www.defenseone.com/technology/2019/09/whats-russias-national-ai-strategy/159740/.

Bengani, Priyanjana. “Hundreds of ‘Pink Slime’ Local News Outlets Are Distributing Algorithmic Stories and Conservative Talking Points.” *Columbia Journalism Review*, December 18, 2019. https://www.cjr.org/tow_center_reports/hundreds-of-pink-slime-local-news-outlets-are-distributing-algorithmic-stories-conservative-talking-points.php.

Benjamin, Daniel, and Steven Simon. “How Fake News Could Lead to Real War.” *Politico*, July 5, 2019. https://www.politico.com/magazine/story/2019/07/05/fake-news-real-war-227272.

Berger, Samuel R. “Winning the Peace in Kosovo.” As Prepared for Delivery, Remarks to the Council on Foreign Relations, Washington, DC, July 26, 1999. https://clintonwhitehouse3.archives.gov/WH/New/html/19990726.html.

Berry, Rob. “Russian Trolls Tweeted Disinformation Long before U.S. Election.” *Wall Street Journal*, February 20, 2018. https://www.wsj.com/graphics/russian-trolls-tweeted-disinformation-long-before-u-s-election/.

Biasini, Nick, Kendall McKay, and Matt Valites. *The Building Blocks of Political Disinformation Campaigns*. San Jose, CA: Cisco Systems, August 2020. https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/094/386/original/Talos_Disinformation_2020.pdf.

Bickert, Monika. *Charting a Way Forward: Online Content Regulation*. Menlo Park, CA: Facebook, February 2020. https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf.

Biddle, Sam, Paulo Victor Ribeiro, and Tatiana Dias. “Invisible Censorship.” *Intercept*, March 16, 2020. https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/.

Bing, Christopher. "U.S. Agency That Handles Trump's Secure Communication Suffered Data Breach." Reuters, February 20, 2020. https://www.reuters.com/article/us-usa-defense-breach/u-s-agency-that-handles-trumps-secure-communication-suffered-data-breach-idUSKBN20E27A.

Biran, Omer. "How Bots Can Generate Value for Enterprises." *Digitalist Magazine*, December 12, 2018. https://www.digitalistmag.com/cio-knowledge/2018/12/12/how-bots-can-generate-value-for-enterprises-06194857.

Birnbaum, Emily. "Mueller Identified 'Dozens' of US Rallies Organized by Russian Troll Farm." *The Hill*, April 18, 2019. https://thehill.com/policy/technology/439532-mueller-identified-dozens-of-us-rallies-organized-by-russian-troll-farm.

Blackbird.AI. *COVID-19 (Coronavirus) Disinformation Report*. New York: Blackbird.AI, February 2020. https://www.blackbird.ai/wp-content/uploads/2020/02/Blackbird.AI-Disinformation-Report-COVID-19.pdf.

Blinken, Antony J., and Lloyd J. Austin III. "America's Partnerships Are 'Force Multipliers' in the World." *Washington Post*, March 14, 2021. https://www.washingtonpost.com/opinions/2021/03/14/americas-partnerships-are-force-multipliers-world/.

Blitz, Marc Jonathon. "Lies, Line Drawing, and (Deep) Fakes." *Oklahoma Law Review* 71, no. 1 (2018): 59–116. https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=1343&context=olr.

Bochman, Andrew, and Sarah Freeman. *Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)*. Boca Raton, FL: CRC Press, 2021.

Bonazzo, John. "Fake News about Hurricane Florence Is Flooding Social Media—Here's How to Avoid It." *Observer*, September 12, 2018. https://observer.com/2018/09/hurricane-florence-fake-news-all-over-social-media/.

Bond, Shannon. "Over 400 Advertisers Hit Pause on Facebook, Threatening $70 Billion Juggernaut." *NPR*, July 1, 2020. https://www.npr.org/2020/07/01/885853634/big-brands-abandon-facebook-threatening-to-derail-a-70b-advertising-juggernaut.

Bond, Shannon, and Bobby Allyn. "As Authorities Probe Twitter Hack, Ex-FBI Officials Warns: 'Get Ready for Copycats.'" *NPR*, July 16, 2020. https://www.npr.org/2020/07/16/892033751/twitter-hack-under-investigation-by-fbi-and-new-york-state.

Bondy, Matthew. *Bad Bots: The Weaponization of Social Media*. Brief No. 9.2. Williamsburg, VA: College of William and Mary Project on International Peace and Security, 2017. https://www.wm.edu/offices/global-research/projects/pips/_documents/pips/2016-2017/Bondy.Matthew.pdf

Bongar, Bruce, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo, eds. *Psychology of Terrorism*. New York: Oxford University Press, August 2007.

Borghard, Erica D. *Protecting Financial Institutions against Cyber Threats: A National Security Issue*. Washington, DC: Carnegie Endowment for International Peace, September 2018. https://carnegieendowment.org/files/WP_Borghard_Financial_Cyber_formatted_complete.pdf.

Borghard, Erica D., and Shawn W. Lonergan. “The Logic of Coercion in Cyberspace.” *Security Studies* 26, no. 3 (2017): 452–481. https://doi.org/10.1080/09636412.2017.1306396.

Boston Globe. “No More Snuff Videos on Facebook.” April 19, 2017. https://www.bostonglobe.com/opinion/editorials/2017/04/18/more-snuff-videos-facebook/JTuexLVKlxloZ7kPYbBfyL/story.html.

Botye, Kenneth J. “An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War over Ukraine.” *Journal of Information Warfare* 16, no. 1 (Winter 2017): 88–111. https://www.jstor.org/stable/26502878.

Boyd, Danah. “You Think You Want Media Literacy . . . Do You?” *Points* (blog). Data & Society, March 9, 2018. https://points.datasociety.net/you-think-you-want-media-literacy-do-you-7cad6af18ec2.

Bradshaw, Samantha. “Disinformation Optimised: Gaming Search Engine Algorithms to Amplify Junk News.” *Internet Policy Review* 8, no. 4 (2019): 1–24. https://policyreview.info/node/1442/pdf.

Bradshaw, Samantha, and Philip N. Howard. *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. Oxford: Oxford University Internet Institute, July 2018. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

———. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford: Oxford University Internet Institute, August 2019. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

Brake, Benjamin. *Strategic Risks of Ambiguity in Cyberspace*. Contingency Planning Memorandum No. 24. Washington, DC: Council on Foreign Relations, May 14, 2015. https://cdn.cfr.org/sites/default/files/pdf/2015/05/CPA_ContingencyPlanningMemo_24.pdf.

Brangetto, Pascal, and Matthijs A. Veenendaal. “Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations.” Paper presented at the 2016 8th International Conference on Cyber Conflict, May–June 2016, Tallinn, Estonia. https://ccdcoe.eu/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf.

Braswell, Bryan. “Evolving the Information Warfare Commander.” *CHIPS*, July–September 2017. https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=9422.

Bratton, Patrick C. “When Is Coercion Successful?” *Naval War College Review* 58, no. 3 (Summer 2005): 99–120. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2050&context=nwc-review.

Breckenridge, James N., and Philip G. Zimbardo. “The Strategy of Terrorism and the Psychology of Mass-Mediated Fear.” In *Psychology of Terrorism*, edited by Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo, 116–133. New York: Oxford University Press, 2006. https://doi.org/10.1093/med:psych/9780195172492.001.0001.

Breland, Ali. “The Bizarre and Terrifying Case of the ‘Deepfake’ Video That Helped Bring an African Nation to the Brink.” *Mother Jones*, March 15, 2019. https://www.motherjones.com/politics/2019/03/deepfake-gabon-ali-bongo/.

Brooking, Emerson T., and P. W. Singer. “War Goes Viral: How Social Media Is Being Weaponized across the World.” *Atlantic*, November 2016. https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

Brose, Christian. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York: Hachette Books, 2020. https://www.hachettebookgroup.com/titles/christian-brose/the-kill-chain/9780316533362/#module-whats-inside.

Brown, Justine. “Can You Make Disaster Information Go Viral?” *Government Technology*, January 21, 2015. https://www.govtech.com/gov-experience/GT-Can-You-Make-Disaster-Information-Go-Viral.html.

Brunnstrom, David. “U.S. Warns China against Taiwan Attack, Stresses U.S. ‘Ambiguity. Reuters, October 7, 2020. https://cn.reuters.com/article/us-usa-china-taiwan-idUSKBN26T01W.

Bruton, F. Brinley, Abigail Williams, and Courtney Kube. “Incirlik Air Base: Post-Coup Power Cut Remains at U.S. Site.” *NBC News*, July 20, 2016. https://www.nbcnews.com/storyline/turkey-military-coup/incirlik-air-base-post-coup-power-cut-remains-u-s-n613086.

Buetler, Larry E., Gil Reyes, Zeno Franco, and Jennifer Housley. “The Need for Proficient Mental Health Professionals in the Study of Terrorism.” In *Psychology of Terrorism*, edited by Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo, 32–55. New York: Oxford University Press, 2006.

Bugajski, Janusz. *Why Does Moscow View NATO as a Threat?* Washington, DC: Center for European Policy Analysis, July 23, 2019. https://cepa.org/moscows-anti-nato-deception/.

Bulger, Monica, and Patrick Davidson. *The Promises, Challenges, and Futures of Media Literacy*. New York: Data & Society, February 2018. https://datasociety.net/pubs/oh/DataAndSociety_Media_Literacy_2018.pdf.

Bumgarner, John, and Scott Borg. *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*. Washington, DC: US Cyber Consequences Unit, August 2009.

Burgess, Richard R. “ADM Trussler: Information Warfare ‘All About Speed for Advantage.’ ” *Seapower*, November 2020. https://seapowermagazine.org/adm-trussler-information-warfare-all-about-speed-for-advantage/.

Bush, Daniel, and Alex Zaheer. “Bing’s Top Search Results Contain an Alarming Amount of Disinformation.” Stanford University Freeman Spogli Institute for International Studies, December 17, 2019. https://fsi.stanford.edu/news/bing-search-disinformation.

Butcher, Paul. “COVID-19 as a Turning Point in the Fight against Disinformation.” *Nature* 4 (2021): 7–9. https://www.nature.com/articles/s41928-020-00532-2.

Butrimas, Vytautas, Jaroslav Hajek, Sukhodolia Oleksandr, Bobro Dmytro, and Sergii Karasov. *Hybrid Warfare against Critical Energy Infrastructure: The Case of Ukraine*. Energy Security: Operational Highlights. Vilnius, Lithuania: NATO Energy Centre of Excellence, 2020. https://enseccoe.org/data/public/uploads/2020/11/d1_hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.pdf.

BuzzFeedVideo. "You Won't Believe What Obama Says in This Video!" YouTube, April 17, 2018. https://www.youtube.com/watch?v=cQ54GDm1eL0.

Byman, Daniel L., and Matthew C. Waxman. "Kosovo and the Great Air Power Debate." *International Security* 24, no. 4 (Spring 2000): 5–38. https://doi.org/10.1162/016228800560291.

Byman, Daniel L., Matthew C. Waxman, and Eric Larson. *Air Power as a Coercive Instrument*. Santa Monica, CA: RAND Corp., 1999. https://www.rand.org/pubs/monograph_reports/MR1061.html.

Carr, David. "More Horrible than Truth: News Reports." *New York Times*, September 19, 2005. https://www.nytimes.com/2005/09/19/business/media/more-horrible-than-truth-news-reports.html.

Cavaiola, Lawrence J., David C. Gompert, Martin Libicki. "Cyber House Rules: On War, Retaliation and Escalation." *Survival* 57, no. 1 (2015): 81–104. https://doi.org/10.1080/00396338.2015.1008300.

CBS News. "Doctored Nancy Pelosi Video Highlights Threat of 'Deepfake' Tech." May 25, 2019, last updated May 26, 2019. https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/.

Cerulus, Laurens. "How Ukraine Became a Test Bed for Cyberweaponry." *Politico*, February 14, 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

Chekinov, Sergei, and Sergei Bogdanov. "The Art of War in the Early 21st Century: Issues and Opinions." *Military Thought* 24 (2015).

———. "The Nature and Content of a New-Generation War." *Military Thought* 22, no. 4 (2013): 12–23. https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf.

Chemerinsky, Erwin. "False Speech and the First Amendment." *Oklahoma Law Review* 71, no. 1 (2018): 1–15. https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=1340&context=olr.

Chen, Adrian. "The Agency." *New York Times Magazine*, June 2, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

Chesney, Robert, and Danielle Citron. *Disinformation on Steroids: The Threat of Deep Fakes*. Washington, DC: Council on Foreign Relations, October 16, 2018. https://www.cfr.org/report/deep-fake-disinformation-steroids.

Chessen, Matt. *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy . . . and What Can Be Done about It*. Washington, DC: Atlantic Council, September 2017. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-madcom-future/.

Chin, Kimberly. "Facebook to Review Content Policies Related to Civil Unrest, Violence." *Wall Street Journal*, June 5, 2020. https://www.wsj.com/articles/facebook-to-review-content-policies-related-to-civil-unrest-violence-11591407729.

Chiu, Allyson. “Facebook Wouldn’t Delete an Altered Video of Nancy Pelosi. What about One of Mark Zuckerberg?” *Washington Post*, June 12, 2019. https://www.washingtonpost.com/nation/2019/06/12/mark-zuckerberg-deepfake-facebook-instagram-nancy-pelosi/.

Chu, Hyon S. “Clickbait, the Attention Economy, and the End of Journalism.” *Medium*, November 19, 2016. https://medium.com/%40hyonschu/clickbait-the-attention-economy-and-the-end-of-journalism-c4f16d2c447d.

CISA (Cybersecurity and Infrastructure Security Agency). “About NSTAC.” Last updated October 27, 2020. https://www.cisa.gov/about-nstac.

———. “Alert (AA20-352A), Advanced Persistent Threat of Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations.” December 17, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

———. “CIPAC Cross Sector Enduring Security Framework Working Group Agendas.” Accessed January 15, 2021. https://www.cisa.gov/publication/cipac-cs-esf-agendas.

———. “Countering Foreign Influence Task Force.” Accessed January 15, 2021. https://www.cisa.gov/cfi-task-force.

———. “Election Infrastructure Security.” Accessed January 15, 2021. https://www.cisa.gov/election-security#:~:text=The%20Cybersecurity%20and%20Infrastructure%20Security,that%20supports%20the%20Nation’s%20elections.&text=Storage%20facilities%20for%20election%20and,to%20include%20early%20voting%20locations.

———. “Foreign Interference.” Accessed January 15, 2021. https://www.cisa.gov/publication/foreign-interference.

———. “#Protect2020 Rumor vs. Reality.” Accessed January 15, 2021. https://www.cisa.gov/rumorcontrol.

———. *#Protect2020 Strategic Plan*. Washington, DC: DHS, February 2020. https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan_FINAL%202.7.20%20508.pdf.

———. “Sector Specific Agencies.” Accessed January 15, 2021. https://www.cisa.gov/sector-specific-agencies.

CJCS (Chairman of the US Joint Chiefs of Staff). *Department of Defense Cyber Red Team Certification and Accreditation*. Manual CJCSM 6510.03. Washington, DC: Joint Chiefs of Staff, February 28, 2013. https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651003.pdf?ver=2016-02-05-175711-083.

Clausewitz, Carl von. *On War*. Translated by J. J. Graham, New York: E. P. Dutton and Co., 1918. https://oll.libertyfund.org/titles/clausewitz-on-war-vol-1.

CNN. “QAnon Fans Spread Fake Claims about Real Fires in Oregon.” September 11, 2020. https://www.cnn.com/2020/09/11/tech/qanon-oregon-fire-conspiracy-theory/index.html.

Coalson, Robert. “The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations in 2014.” *Military Review* (January–February 2016): 23–29. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.

Coaston, Jane. "Trump's Social Media Executive Order, Explained." *Vox*, May 29, 2020. https://www.vox.com/2020/5/29/21273198/trump-section-230-social-media-executive-order-explained.

Cohen Silver, Roxane. "An Introduction to '9/11: Ten Years Later.' " *American Psychologist* 66, no. 6 (September 2011): 427–428. https://doi.org/10.1037/a0024804.

Cohen, Rachel S. "16th Air Force Launches Information Ops for the Digital Age." *Air Force Magazine*, December 1, 2019. https://www.airforcemag.com/article/16th-air-force-launches-information-ops-for-the-digital-age/.

Cole, Samantha. "New Deepfake Method Can Put Words in Anyone's Mouth." *VICE*, January 24, 2020. https://www.vice.com/en_us/article/g5xvk7/researchers-created-a-way-to-make-realistic-deepfakes-from-audio-clips.

Collier, Kevin, and Ken Dilanian. "Russian Internet Trolls Hired U.S. Journalists to Push Their News Website, Facebook Says." *NBC News*, September 1, 2020. https://www.nbcnews.com/tech/tech-news/russian-internet-trolls-hired-u-s-journalists-push-their-news-n1239000.

Conger, Kate. "Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says." *New York Times*, October 30, 2019. https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html.

Conger, Kate, Mike Isaac, Katie Benner, and Nicole Perlroth. "Former Twitter Employees Charged with Spying for Saudi Arabia." *New York Times*, published November 6, 2019; updated November 8, 2019. https://www.nytimes.com/2019/11/06/technology/twitter-saudi-arabia-spies.html.

Connell, Michael, and Sarah Vogler. *Russia's Approach to Cyber Warfare*. Arlington, VA: CNA, March 2017. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Cook, Chaveso, and Liam Collins. "PSYOP, Cyber, and InfoWar: Combating the New Age IED." Modern Warfare Institute, April 6, 2021. https://mwi.usma.edu/psyop-cyber-and-infowar-combating-the-new-age-ied/.

Copeland, Claudia. *Terrorism and Security Issues Facing the Water Infrastructure Sector*. CRES Report RL32189. Washington, DC: CRS, December 15, 2010. https://fas.org/sgp/crs/terror/RL32189.pdf.

Corcoran, Casey, Bo Julie Crowley, and Raina Davis. *Disinformation Threat Watch: The Disinformation Landscape in East Asia and Implications for US Policy*. Cambridge, MA: Belfer Center for Science and International Affairs, May 2019. https://www.belfercenter.org/sites/default/files/2019-06/PAE/DisinfoWatch%20-%202.pdf.

Cordesman, Anthony H. *The Lessons and Non-Lessons of the Air and Missile Campaign in Kosovo*. Washington, DC: CSIS, September 2003. https://www.csis.org/analysis/lessons-and-non-lessons-air-and-missile-campaign-kosovo.

Costello, John, and Joe McReynolds. *China's Strategic Support Force: A Force for a New Era*. China Strategic Perspectives, no. 13. Washington, DC: National Defense University Press, October 2018. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

Countering Russian Influence through Interagency Coordination and Leadership Act, H.R. 4209, 116th Cong., 1st Sess. (introduced August 27, 2019). https://www.congress.gov/116/bills/hr4209/BILLS-116hr4209ih.pdf.

Cowan, David, and Chaveso Cook. “What’s in a Name? Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change.” *Military Review*, March 6, 2018. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/PSYOP/.

Cox, Matthew. “Less Door-Kicking, More Influencing: The Changing Role of Special Operators.” Military.com, May 12, 2020. https://www.military.com/daily-news/2020/05/12/less-door-kicking-more-influencing-changing-role-special-operators.html.

Critical Electric Infrastructure Security, 16 U.S.C. §824o–1, https://www.law.cornell.edu/uscode/text/16/824o-1.

CSC (US Cyberspace Solarium Commission). *Official Report*. CSC: Washington, DC: March 2020. https://www.solarium.gov/report.

CSCC (US Communications Sector Coordinating Council). “Communications Sector Partnership with Government.” Accessed January 15, 2021. https://www.comms-scc.org/government-partnership.

CTIA. *2019 Annual Survey Highlights*. Washington, DC: CTIA, June 2019. https://api.ctia.org/wp-content/uploads/2019/06/2019-Annual-Survey-Highlights-FINAL.pdf.

Cunningham, Fiona. “Was China behind Last October’s Power Outage in India? Here’s What We Know.” *Washington Post*, April 29, 2021. https://www.washingtonpost.com/politics/2021/04/29/was-china-behind-last-octobers-power-outage-india-heres-what-we-know/.

Daalder, Ivo H., and Michael E. O’Hanlon. *Winning Ugly: NATO’s War to Save Kosovo*. Washington, DC: Brookings Institution, October 1, 2001. https://www.brookings.edu/book/winning-ugly/.

Dalton, Melissa, Kathleen H. Hicks, Megan Donahoe, Lindsey Sheppard, Alice Hunt Friend, Michael Matlaga, Joseph Federici, Matthew Conklin, and Joseph Kiernan. *By Other Means. Part II: U.S. Priorities in the Gray Zone*. Washington, DC: CSIS, August 2019. https://www.csis.org/analysis/other-means-part-ii-adapting-compete-gray-zone.

Damiani, Jesse. “Chinese Deepfake App Zao Goes Viral, Faces Immediate Criticism over User Data and Security Policy.” *Forbes*, September 3, 2019. https://www.forbes.com/sites/jessedamiani/2019/09/03/chinese-deepfake-app-zao-goes-viral-faces-immediate-criticism-over-user-data-and-security-policy.

Davis, Paul K. “Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy.” Working paper, RAND Corp., Santa Monica, CA, January 2014. https://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf.

Dean, Brian. “Google’s 200 Ranking Factors: The Complete List (2021).” *Backlinko*. Updated January 22, 2020. https://backlinko.com/google-ranking-factors.

Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (April 9, 2019). https://www.congress.gov/bill/116th-congress/senate-bill/1084.

Defence Committee. "Oral Evidence: Russia: Implications for UK Defence and Security, HC 763." March 1, 2016. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/oral/29915.html.

Defense Media Activity. "U.S., Allies Aim to Maintain Free, Open Indo-Pacific Region." DoD News, August 9, 2018. https://www.pacom.mil/Media/News/News-Article-View/Article/1598294/us-allies-aim-to-maintain-free-open-indo-pacific-region/.

Defense One. "C4ISR: The Military's Nervous System." Accessed January 21, 2021. https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/.

Denyer, Simon, and Akiko Kashiwagi. "On Japan's Okinawa, U.S. Military Is Accused of Contaminating Environment with Hazardous Chemical." *Washington Post*, May 24, 2019. https://www.washingtonpost.com/world/asia_pacific/on-japans-okinawa-us-military-blamed-for-contaminating-environment-with-hazardous-chemical/2019/05/24/ca3ba342-7c84-11e9-b1f3-b233fe5811ef_story.html.

Dholakia, Utpal. "How to Use Social Affinity Groups to Engage Customers." *Psychology Today* (blog), November 17, 2015. https://www.psychologytoday.com/us/blog/the-science-behind-behavior/201511/how-use-social-affinity-groups-engage-customers.

DHS (US Department of Homeland Security). "Cyber Storm VI: National Cyber Exercise." Accessed January 15, 2021. https://www.dhs.gov/cisa/cyber-storm-vi.

———. *Homeland Threat Assessment*. Washington, DC: DHS, October 2020. https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

———. *National Cyber Incident Response Plan*. Washington, DC: DHS, December 2016. https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

———. "Social Media Working Group (SMWG) for Emergency Services and Disaster Management Program." Accessed January 15, 2021. https://www.dhs.gov/science-and-technology/smwg.

DHS (Department of Homeland Security) and HHS (Department of Health and Human Services). *Patient Decontamination in a Mass Chemical Exposure Incident: National Planning Guidance for Communities*. Washington, DC: DHS and HHS, December 2014. https://www.dhs.gov/sites/default/files/publications/Patient%20Decon%20National%20Planning%20Guidance_Final_December%202014.pdf.

———. *Homeland Threat Assessment*. Washington, DC: DHS, October 2020. https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

DHS I&A (Department of Homeland Security Office of Intelligence and Analysis). *Malicious Cyber Actors Likely to Continue Exploiting Vulnerabilities in Water and Wastewater System Networks*. Washington, DC: DHS, May 20, 2021.

DIA (Defense Intelligence Agency). *Challenges to Security in Space*. Washington, DC: DIA, January 2019. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

———. *China Military Power: Modernizing a Force to Fight and Win*. Washington, DC: DIA, 2019. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf.

———. *Russia Military Power: Building a Military to Support Great Power Aspirations*. Washington, DC: DIA, 2017. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937.

DiResta, Renee. "Computational Propaganda: If You Make It Trend, You Make It True." *Yale Review* 106, no. 4 (October 2018): 12–29. https://doi.org/10.1111/yrev.13402.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. *The Tactics & Tropes of the Internet Research Agency*. Washington, DC: US Senate, October 2019. https://digitalcommons.unl.edu/senatedocs/2/.

DISA (Defense Information Systems Agency). "DISA's Mission Partner Support." Accessed January 15, 2021. https://www.disa.mil/About/Our-Work/Mission-Partners.

Distil Networks. *2019 Bad Bot Report: The Bot Arms Race Continues*. Arlington, VA: Distil Networks, 2019.

Ditzler, T. F. "Malevolent Minds: The Technology of Terrorism." In *Understanding Terrorism: Psychosocial Roots, Consequences, and Interventions*, edited by Fathali M. Moghaddam and Anthony J. Marsella. Washington, DC: American Psychological Association, 2004.

Dizikes, Peter. "Study: On Twitter, False News Travels Faster than True Stories." *MIT News*, March 8, 2018. http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

DoD (US Department of Defense). *Conduct of the Persian Gulf War: Final Report to Congress*. Pursuant to Title V of the Persian Gulf Conflict Supplemental Authorization and Personnel Benefits Act of 1991 (Pub. L. No. 102-25). Washington, DC: GPO, 1992. https://www.globalsecurity.org/military/library/report/1992/cpgw.pdf.

———. *DoD Directive 3020.40: Mission Assurance (MA)*. Washington, DC: DoD, effective November 29, 2016, Change 1 effective September 11, 2018. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983.

———. *Defense Science Board Task Force Report on Cyber Deterrence*. Washington, DC: DoD, February 2017. https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

———. *DoD Instruction 3020.45: Mission Assurance (MA) Construct*. Washington, DC: DoD, effective August 14, 2018. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf?ver=2018-08-14-081232-450.

———. "DOD, USAF Warfare Center to Build a 5G Network, Test Prototype Software at Nellis." May 28, 2020. https://www.defense.gov/Newsroom/Releases/Release/Article/2200307/dod-usaf-warfare-center-to-build-a-5g-network-test-prototype-software-at-nellis/.

———. *Law of War Manual.* Washington, DC: DoD, December 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

———. *Mission Assurance Strategy*. Washington, DC: DoD, April 2012. https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.

———. *Strategy for Operations in the Information Environment*. Washington, DC: DoD, June 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

———. *Summary of the 2018 National Defense Strategy*. Washington, DC: DoD, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

DoD IG (Department of Defense Inspector General). *Evaluation of Department of Defense Efforts to Develop and Implement Policy and Procedures Addressing Ideological Extremism within the U.S. Armed Forces*. January 14, 2021. https://media.defense.gov/2021/Jan/14/2002565175/-1/-1/1/D2021-DEV0PB-0079.000_REDACTED.PDF.

DOE (US Department of Energy). *Advanced Metering Infrastructure and Customer Systems*. Washington, DC: DOE, September 2016. https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf.

———. *Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure*. Washington, DC: DOE, April 20, 2021. https://www.energy.gov/sites/default/files/2021-04/RFI%20Ensuring%20the%20Continued%20Security%20of%20US%20Critical%20Electric%20Infrastructure%2004202021.pdf.

———. *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*. Washington, DC: DOE, January 2017. https://www.energy.gov/sites/prod/files/2017/02/f34/Chapter%20IV--Ensuring%20Electricity%20System%20Reliability%2C%20Security%2C%20and%20Resilience.pdf.

———. "U.S. Department of Energy, U.S. Department of Homeland Security, and U.S. Department of Defense Announce Pathfinder Initiative to Protect U.S. Energy Critical Infrastructure." February 3, 2020. https://www.energy.gov/articles/us-department-energy-us-department-homeland-security-and-us-department-defense-announce.

DOJ (US Department of Justice). "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting over 78 Million People." Press release 19-502. May 9, 2019. https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including.

———. *Report of the Attorney General's Cyber Digital Task Force*. Washington, DC: DOJ, July 2018. https://www.justice.gov/ag/page/file/1076696/download.

———. "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector." Press release 16-348. March 24, 2016. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

———. "Three Individuals Charged for Alleged Roles in Twitter Hack," Northern District of California US Attorney's Office." US Attorney's Office, Northern District of California, press release. July 31, 2020. https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack.

DOS (US Department of State). *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*. Washington, DC: DOS, August 2020. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

———. "Global Engagement Center." Accessed January 15, 2021. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center.

Douhet, Giulio. *The Command of the Air*. Translated by Dino Ferrari. Washington, DC: USAF History and Museums Program, 1998. http://www.airforcemag.com/MagazineArchive/Documents/2013/April%202013/0413keeperfull.pdf.

Doulnev, P. I., and Orlyansky, V. I. "Basic Changes in the Character of Armed Struggle in the First Third of the 21st Century." *Journal of the Academy of Military Science* no. 1 (2015): 46.

Douthat, Ross. "The Mystery of Benghazi." *New York Times*, October 13, 2012. https://www.nytimes.com/2012/10/14/opinion/sunday/douthat-the-mystery-of-benghazi.html?_r=1.

Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos, June 13, 2017. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.

Drury, John, David Novelli, and Clifford Stott. "Representing Crowd Behaviour in Emergency Planning Guidance: 'Mass Panic' or Collective Resilience?" *Resilience* 1, no. 1 (2013): 18–37. https://doi.org/10.1080/21693293.2013.765740.

DSB (Defense Science Board). *Task Force on Cyber Deterrence*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2017. https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf.

Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110–417, [div. A], title X, §1056, Oct. 14, 2008, 122 Stat. 4610. https://uscode.house.gov/statviewer.htm?volume=122&page=4610.

Dupuy, Arnold C., Dan Nussbaum, Vytautas Butrimas, and Alkman Granitsas. "Energy Security in the Era of Hybrid Warfare." *NATO Review*, January 13, 2021. https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html.

Durkalec, Jacek. *Nuclear-Backed "Little Green Men:" Nuclear Messaging in the Ukraine Crisis*. Warsaw: Polish Institute of International Affairs, July 2015. https://www.files.ethz.ch/isn/193514/Nuclear%20Backed%20%E2%80%9CLittle%20Green%20Men%E2%80%9D%20Nuclear%20Messaging%20in%20the%20Ukraine%20Crisis.pdf.

Duster, Chandelis. "Energy Secretary Says Adversaries Have Capability of Shutting Down US Power Grid," *CNN*, June 6, 2021. https://www.cnn.com/2021/06/06/politics/us-power-grid-jennifer-granholm-cnntv/index.html.

Dvorsky, George. "Hackers Have Already Started to Weaponize Artificial Intelligence." *Gizmodo*, September 11, 2017. https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425.

———. "What Would Happen If All Our Satellites Were Suddenly Destroyed?" *Gizmodo*, June 4, 2015. https://io9.gizmodo.com/what-would-happen-if-all-our-satellites-were-suddenly-d-1709006681.

DW. "Germany's Government Approves Hate Speech Bill." February 19, 2020. https://www.dw.com/en/germanys-government-approves-hate-speech-bill/a-52433689.

Eberhardt, Robin. "Jesse Watters Falls for Fake Shark Photo in Houston Flooding." *The Hill*, August 29, 2017. https://thehill.com/homenews/media/348362-jesse-watters-believes-fake-shark-photo-amid-harvey-floods.

Echosec Systems. "What Is VKontakte and Why Should You Care?" Echosec Systems (blog), August 25, 2017. https://www.echosec.net/blog/what-is-vk-and-why-should-you-care.

Economist. "China's Grip on Electronics Manufacturing Will Be Hard to Break." October 11, 2018. https://www.economist.com/business/2018/10/11/chinas-grip-on-electronics-manufacturing-will-be-hard-to-break.

Edwards, Jim. "A False Rumor on WhatsApp Started a Run on a London Bank." *Business Insider*, May 13, 2019. https://www.businessinsider.com/whatsapp-rumour-started-run-on-metro-bank-2019-5.

E-ISAC (Electricity Information Sharing and Analysis Center). *E-ISAC End of the Year Report: January 1–December 31, 2016*. Atlanta, GA: NERC, 2017. https://www.eisac.com/cartella/Asset/00006271/E-ISAC_2016_End_of_Year_Report.pdf?parent=64137.

EIS Council (Electric Infrastructure Security Council). *Electric Infrastructure Protection (EPRO®) Handbook II: Volume 1—Fuel*. Washington, DC: EIS Council, 2016. https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf.

———. *Electric Infrastructure Protection (EPRO®) Handbook II: Volume 2—Water*. Washington, DC: EIS Council, July 2016. https://www.eiscouncil.org/App_Data/Upload/7f41c325-654e-4c67-be3d-6941645f4485.pdf.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee. *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*. Staff Report 909. New York: Federal Reserve Bank of New York, January 2020; revised June 2020. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf.

Elran, Meir. "Societal Resilience in Israel: How Communities Succeed Despite Terrorism." *Foreign Affairs*, March 23, 2017. https://www.foreignaffairs.com/articles/israel/2017-03-23/societal-resilience-israel.

Emmott, Robin. "Russia Deploying Coronavirus Disinformation to Sow Panic in West, EU Document Says." Reuters, March 18, 2020. https://www.reuters.com/article/us-health-coronavirus-disinformation/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says-idUSKBN21518F.

Engler, Alex. *Fighting Deepfakes When Detection Fails*. AI Governance Series. Washington, DC: Brookings Institution, November 14, 2019. https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/.

Engstrom, Jeffrey. *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*. Santa Monica, CA: RAND Corp., 2018. https://doi.org/10.7249/RR1708.

Erlanger, Steven. "Crisis in the Balkans: In Belgrade; NATO Missiles Strike a Center of State-Linked TV and Radio." *New York Times*, April 22, 1999. https://www.nytimes.com/1999/04/21/world/crisis-balkans-belgrade-nato-missiles-strike-center-state-linked-tv-radio.html.

ESCC (Electricity Subsector Coordinating Council). *ESCC: Electricity Subsector Coordinating Council*, Washington, DC: ESCC, July 2019. https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure_July2019.ashx?la=en&hash=6895DE9CB737C2EB81D9E-8CA063F0223F6F0B471.

———. "The ESCC's Cyber Mutual Assistance Program." January 2021. https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/CMA/Cyber-Mutual-Assistance-Program-One-Pager_013119.ashx?la=en&hash=F4D3445C75E3B9884458E403390DBBD120F9D8D4.

Esper, Mark T. "Message to the Force on Accomplishments in Implementation of the National Defense Strategy." Transcript. DoD, July 7, 2020. https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2266872/secretary-of-defense-mark-t-esper-message-to-the-force-on-accomplishments-in-im/.

———. Speech delivered at RAND Corp., September 16, 2020. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2350362/secretary-of-defense-speech-at-rand-as-delivered/.

Estes Cohen, Sara. "Sandy Marked a Shift for Social Media Use in Disasters." *Government Technology*, March 7, 2013. https://www.govtech.com/em/disaster/Sandy-Social-Media-Use-in-Disasters.html.

Eversden, Andrew. "Is Using TikTok a National Security Risk?" *Fifth Domain*, December 16, 2019. https://www.fifthdomain.com/congress/capitol-hill/2019/12/16/is-using-tiktok-a-national-security-risk/.

Facebook. *Detailed Report: May 2020 Coordinated Inauthentic Behavior Report*. Facebook: Menlo Park, CA: June 2020. https://about.fb.com/wp-content/uploads/2020/06/May-2020-Detailed-CIB-Report.pdf.

———. "It's Time for Updated Internet Regulations." Accessed February 15, 2021. https://about.fb.com/regulations/?utm_source=ads&utm_medium=GS&utm_content=489243000419&utm_campaign=2021Q1.

———. "New Steps to Protect the US Elections." September 3, 2020. https://about.fb.com/news/2020/09/additional-steps-to-protect-the-us-elections/.

Fazzini, Kate. "'Evil Corp': Feds Charge Russians in Massive $100 Million Bank Hacking Scheme." *CNBC*, December 5, 2019. https://www.cnbc.com/2019/12/05/russian-malware-hackers-charged-in-massive-100-million-bank-scheme.html.

FBI (US Federal Bureau of Investigation). “Combating Foreign Influence.” Accessed January 15, 2021. https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

FCW. “Can the IC Police Foreign Disinformation on Social Media?” *FCW*, May 28, 2019. https://fcw.com/articles/2019/05/28/warner-intel-misinformation-center.aspx?s=fcwdaily_300519.

Feaver, Peter. “Blowback: Information Warfare and the Dynamics of Coercion.” *Security Studies* 7, no. 4 (1998): 88–120. https://doi.org/10.1080/09636419808429359.

Feldman, Brian. “It’s Time to End ‘Trending.’ ” *New York Magazine*, February 21, 2018. https://nymag.com/intelligencer/2018/02/trending-on-social-media-is-worthless.html.

FEMA (US Federal Emergency Management Agency). “Community Lifelines.” Accessed March 16, 2021. https://www.fema.gov/emergency-managers/practitioners/lifelines

———. “Coronavirus Rumor Control.” Accessed April 6, 2020. https://www.fema.gov/coronavirus-rumor-control.

———. *Emergency Support Function #2—Communications Annex*. Washington, DC: FEMA, June 2015. https://www.fema.gov/sites/default/files/2020-07/fema_ESF_2_Communications.pdf.

———. *Emergency Support Function #14—Cross-Sector Business and Infrastructure*. Washington, DC: FEMA, October 2019. https://www.fema.gov/sites/default/files/2020-07/fema_ESF_14_Business-Infrastructure.pdf.

———. *Emergency Support Function #15—External Affairs Annex*. Washington, DC: FEMA, June 2015. https://www.fema.gov/sites/default/files/2020-07/fema_ESF_15_External-Affairs.pdf.

———. “Hurricane Florence Rumor Control.” Last updated October 19, 2018. https://www.fema.gov/florence-rumors.

———. “The IPAWS National Test.” Last updated July 24, 2019. https://www.fema.gov/emergency-alert-test.

———. *National Response Framework*. 4th ed. Washington, DC: DHS, October 28, 2019. https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf.

———. “Social Media and Emergency Preparedness.” Last updated April 16, 2018. https://www.fema.gov/news-release/2018/04/16/social-media-and-emergency-preparedness.

Fields, Craig. “Some Fundamental Principles of Deterrence.” Unpublished manuscript, last modified 2020. Microsoft Word file.

1st Special Forces Command, Airborne. *A Vision for 2021 and Beyond*. Fort Bragg, NC: US Army Special Operations Command, 2020. https://www.soc.mil/USASFC/Documents/1sfc-vision-2021-beyond.pdf.

Fischerkeller, Michael. “The Fait Accompli and Persistent Engagement in Cyberspace.” *War on the Rocks*, June 24, 2020. https://warontherocks.com/2020/06/the-fait-accompli-and-persistent-engagement-in-cyberspace/.

Fischerkeller, Michael, and Richard Harknett. *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*. Alexandria, VA: Institute for Defense Analyses, May 2018. https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.

———. "Persistent Engagement and Cost Imposition: Distinguishing between Cause and Effect." *Lawfare* (blog), February 6, 2020. https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

Fisher, Max. "Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?" *Washington Post*, April 23, 2013. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.5f18c84aa015.

Flournoy, Michèle A. "How to Prevent a War in Asia." *Foreign Affairs*, June 18, 2020. https://www.foreignaffairs.com/articles/united-states/2020-06-18/how-prevent-war-asia.

Flynn, Daniel. "Russia's Evolving Approach to Deterrence." In *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper*, edited by Nicole Peterson. Boston: NSI, Inc., May 2019. https://www.politico.com/f/?id=0000016b-a5a1-d241-adff-fdf908e00001.

Fogarty, Stephen, and Bryan Sparling. "Enabling the Army in an Era of Information Warfare." *Cyber Defense Review* 5 no. 2 (Summer 2020): 17–26. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fogarty_Sparling_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053231-950.

Foster, Tom. "How Russian Trolls Are Using American Businesses as Their Weapons." *Inc. Magazine*, May 2019. https://www.inc.com/magazine/201905/tom-foster/russian-trolls-facebook-social-media-attacks-brands-hoax-fake-disinformation.html.

Freberg, Karen, Kristin Graham, Karen McGaughey, and Laura A. Freberg. "Who Are the Social Media Influencers? A Study of Public Perceptions of Personality." *Public Relations Review* 37, no. 1 (2011): 90–92. https://doi.org/10.1016/j.pubrev.2010.11.001.

Freedberg, Sidney Jr. "Fog of Information War: Army Asks Civilians, Allies for Aid." *Breaking Defense*, September 25, 2019. https://breakingdefense.com/2019/09/fog-of-information-war-army-asks-civilians-allies-for-aid/.

Frenkel, Sheera, Nathaniel Popper, Kate Conger, and David E. Sanger. "A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam." *New York Times*, published July 15, 2020; last updated July 17, 2020. https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html.

Fried, Daniel, and Alina Polyakova. *Democratic Defense against Disinformation*. Washington, DC: Atlantic Council Eurasia Center, March 2018. https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf.

———. *Democratic Defense against Disinformation 2.0*. Washington, DC: Atlantic Council Eurasia Center, June 2019. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf.

Friedman, Herbert A. "U.S. PSYOP in Panama (Operation Just Cause)." Psywarrior, July 1, 2002. http://www.psywarrior.com/PanamaHerb.html.

Friedman, Uri. "Here's What Foreign Interference Will Look Like in 2020." *Nextgov*, August 12, 2019. https://www.nextgov.com/cybersecurity/2019/08/heres-what-foreign-interference-will-look-2020/159107/.

Friedman Lissner, Rebecca. "Preventing a Credibility Crisis in American's Most Important Alliance." *War on the Rocks*, March 10, 2107. https://warontherocks.com/2017/03/preventing-a-credibility-crisis-in-americas-most-important-alliance/.

Fruhlinger, Josh. "The OPM Hack Explained: Bad Security Practices Meet China's Captain America." *CSO Online*, February 12, 2020. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

FSB (Financial Stability Board). "FSB Encourages Use of Cyber Incident Response and Recovery Toolkit." Press release, October 19, 2020. https://www.fsb.org/2020/10/fsb-encourages-use-of-cyber-incident-response-and-recovery-toolkit/.

———. *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*. Basel, Switzerland: FSB, October 13, 2017. https://www.fsb.org/wp-content/uploads/P131017-1.pdf.

FS-ISAC (Financial Services Information Sharing and Analysis Center). "Exercises." Accessed January 15, 2021. https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf.

Fuhrmann, Matthew, and Todd Seschser. *Nuclear Weapons and Coercive Diplomacy*. Cambridge: Cambridge University Press, 2017.

Fullerton, Carol S., Robert J. Ursano, Ann E. Norwood, and Harry H. Holloway. "Trauma, Terrorism, and Disaster." In *Terrorism and Disaster: Individual and Community Mental Health Interventions*, edited by Robert J. Ursano, Carol S. Fullerton, and Ann E. Norwood, 1–17. New York: Cambridge University Press, 2003.

Fung, Brian. "Microsoft Disrupted a Massive Hacking Operation That Could Have Affected the US Election." *CNN Business*, October 12, 2020. https://www.cnn.com/2020/10/12/tech/microsoft-election-ransomware/index.html.

Galeotti, Mark. "The 'Gerasimov Doctrine' and Russian Non-Linear War." *In Moscow's Shadows* (blog), June 7, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

———. "I'm Sorry for Creating the 'Gerasimov Doctrine.' " *Foreign Policy*, March 5, 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

———. *Putin's Hydra: Inside Russia's Intelligence Services*. Policy Brief. Berlin: European Council on Foreign Relations,May11,2016.https://ecfr.eu/publication/putins_hydra_inside_russias_intelligence_services/.

Gallacher, John D., Vlad Barash, Philip N. Howard, and John Kelly. "Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns against US Military Personnel and Veterans." *OII Blogs*. Oxford University Internet Institute, October 9, 2017. http://blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2017/10/Junk-News-on-Military-Affairs-and-National-Security-1.pdf.

Gallo, Jason A., and Clare Y. Cho. *Social Media: Misinformation and Content Moderation Issues for Congress*. Washington, DC: Congressional Research Service, January 27, 2021. https://crsreports.congress.gov/product/pdf/R/R46662.

Gans, John. *White House Warriors: How the National Security Council Transformed the American Way of War*. New York: Liveright, 2019.

GAO (US Government Accountability Office). *Deepfakes*. GAO-20-379SP. Washington, DC: GAO, February 20, 2020. https://www.gao.gov/products/GAO-20-379SP.

———. *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*. Report GAO-21-81. Washington, DC: GAO, March 2021. https://www.gao.gov/products/gao-21-81.

Garamone, Jim. "U.S., Allies Aim to Maintain Free, Open Indo-Pacific Region." DoD News, August 8, 2018. https://www.defense.gov/Explore/News/Article/Article/1596903/us-allies-aim-to-maintain-free-open-indo-pacific-region/.

Gareyev, Makhmut. "If There Were War Tomorrow." Originally published in Russian in *Armeyskiy Sbornik*, April 1, 2003. Translated in Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva. *The Growing Need to Focus on Modern Political Warfare*. Santa Monica, CA: RAND Corp., 2019. https://doi.org/10.7249/RB10071.

Gellman, Barton. "Allied War Struck Broadly in Iraq." *Washington Post*, June 23, 1991. https://www.washingtonpost.com/archive/politics/1991/06/23/allied-air-war-struck-broadly-in-iraq/e469877b-b1c1-44a9-bfe7-084da4e38e41/.

Genaro Phillips, Kyle. "Unpacking Cyberwar," *Joint Force Quarterly* 70 (3rd Quarter 2013): 70–75. https://ndupress.ndu.edu/portals/68/documents/jfq/jfq-70/jfq-70_70-75_phillips.pdf.

George, Alexander L. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War.* Washington, DC: United States Institute of Peace, 1992.

George, Alexander, and William Simons. *The Limits of Coercive Diplomacy*. Boulder, CO: Westview Press, 1994.

Gerasimov, Valery. "The Value of Science Is in the Foresight." Originally published in Russian in *Military-Industrial Kurier*, February 27, 2013. Translated in Robert Coalson. "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations in 2014." *Military Review* (January–February 2016): 23–29. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.

Gershkoff, Amy, and Shana Kushner. "Shaping Public Opinion: The 9/11-Iraq Connection in the Bush Administration's Rhetoric." *Perspectives on Politics* 3, no. 3 (September 2005): 525–537. https://doi.org/10.1017/S1537592705050334.

Gertz, Bill. "Stratcom Worried by Slow Pace of U.S. Nuclear Modernization." *Washington Free Beacon*, July 31, 2017. http://freebeacon.com/national-security/stratcom-worried-slow-pace-u-s-nuclear-modernization/.

———. "O'Brien: Chinese Hackers Targeted Emails of Trump Family, Campaign." *Washington Times*, September 30, 2020. https://www.washingtontimes.com/news/2020/sep/30/robert-c-obrien-chinese-hackers-targeted-emails-of/.

Ghosh, Dipayan, and Ben Scott. *Digital Deceit: The Technologies behind Precision Propaganda on the Internet*. Policy Paper. Washington, DC: New America, January 23, 2018. https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/.

———. "Disinformation Is Becoming Unstoppable." *Time*, January 24, 2018. https://time.com/5112847/facebook-fake-news-unstoppable/.

Giles, Keir. *Handbook of Russian Information Warfare*. Fellowship Monograph 9. Rome: NATO Defense College, November 2016. http://www.ndc.nato.int/news/news.php?icode=995.

———. *The Next Phase of Russian Information Warfare*. Riga, Latvia: NATO StratCom Center of Excellence, 2016. https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Glazer, Emily. "Facebook Removes Trump Campaign Ads for Violating Policy on Use of Hate Symbol." *Wall Street Journal*, June 19, 2020. https://www.wsj.com/articles/facebook-removes-trump-campaign-posts-ads-for-violating-policy-11592504003.

Gleicher, Nathaniel. "Removing Coordinated Inauthentic Behavior from China." Facebook, August 19, 2019. https://newsroom.fb.com/news/2019/08/removing-cib-china/.

———. "Removing Coordinated Inauthentic Behavior from Russia." Facebook, March 12, 2020. https://about.fb.com/news/2020/03/removing-coordinated-inauthentic-behavior-from-russia/.

Goldman, Adam, Julian E. Barnes, Maggie Haberman, and Nicholas Fandos. "Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump." *New York Times*, February 20, 2020. https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html.

Golebiewski, Michael, and Danah Boyd. *Data Voids: Where Missing Data Can Easily Be Exploited*. New York: Data & Society, May 2018. https://datasociety.net/wp-content/uploads/2018/05/Data_Society_Data_Voids_Final_3-1.pdf.

Goodin, Dan. "Google Goes Down after Major BGP Mishap Routes Traffic through China." *Ars Technica*, November 13, 2018. https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/.

———. "Strange Snafu Misroutes Domestic US Internet Traffic through China Telecom." *Ars Technica*, November 6, 2018. https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom/.

Google. *How Google Fights Disinformation*. Mountain View, CA: Google, February 2019. https://www.blog.google/documents/37/How_Google_Fights_Disinformation.pdf.

Graff, Garrett M. "The Man Who Speaks Softly—and Commands a Big Cyber Army." *Wired*, October 13, 2020. https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*. Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2013. https://www.files.ethz.ch/isn/163664/pub1147.pdf.

Green, Michael. *The U.S. Alliance with the Philippines*. Washington, DC: CSIS, December 3, 2020. https://www.csis.org/analysis/us-alliance-philippines.

Greenberg, Andy. "The Internet's Most Notorious Botnet Has an Alarming New Trick." *Wired*, December 3, 2020. https://www.wired.com/story/trickbot-botnet-uefi-firmware/#:~:text=The%20hackers%20behind%20TrickBot%20have,them%20persist%20on%20devices%20undetected.

Greene, Jay, and Ellen Nakashima. "Microsoft Seeks to Disrupt Russian Criminal Botnet It Fears Could Seek to Sow Confusion in the Presidential Election." *Washington Post*, October 12, 2020. https://www.washingtonpost.com/technology/2020/10/12/microsoft-trickbot-ransomware/.

Griffiths, James. "China Can Shut Off the Philippines' Power Grid at Any Time, Leaked Report Warns." CNN, November 26, 2019. https://www.cnn.com/2019/11/25/asia/philippines-china-power-grid-intl-hnk/index.html.

Grynkewich, Alexus. "Introducing Information as a Joint Function." *Joint Force Quarterly* 89 (2nd Quarter 2018): 6–7. https://apps.dtic.mil/dtic/tr/fulltext/u2/1056964.pdf.

Gurzu, Anca. "Hackers Threaten Smart Power Grids." *Politico*, January 4, 2017. http://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/.

Guynn, Jessica, and Kevin McCoy. "Zuckerberg Vows to Weed Out Facebook 'Fake News.' " *USA Today*, November 13, 2016; updated November 14, 2016. https://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/.

Ha, Matthew, and Alice Cho. "China's Coronavirus Disinformation Campaigns Are Integral to Its Global Information Warfare Strategy." Foundation for the Defense of Democracies, April 30, 2020. https://www.fdd.org/analysis/2020/04/30/chinas-coronavirus-disinformation-campaigns-are-integral-to-its-global-information-warfare-strategy/.

Hale, Joanne E., David P. Hale, and Ronald E. Dulek. "Decision Processes during Crisis Response: An Exploratory Investigation." *Journal of Managerial Issues* 18, no. 3 (Fall 2006): 301–320. https://www.jstor.org/stable/40604542.

Hansen, Aaron, Jason Staggs, and Sujeet Shenoi. "Security Analysis of an Advanced Metering Infrastructure." *International Journal of Critical Infrastructure Protection* 18 (September 2017): 3–19.

Harris, Brent. "Preparing the Way Forward for Facebook's Oversight Board." Facebook, January 28, 2020. https://about.fb.com/news/2020/01/facebooks-oversight-board/.

Harsono, Hugh. "China's Surveillance Technology Is Keeping Tabs on Populations around the World." *Diplomat*, June 18, 2020. https://thediplomat.com/2020/06/chinas-surveillance-technology-is-keeping-tabs-on-populations-around-the-world/.

Harwell, Drew. "Facebook Acknowledges Pelosi Video Is Faked but Declines to Delete It." *Washington Post*, May 24, 2019. https://www.washingtonpost.com/technology/2019/05/24/facebook-acknowledges-pelosi-video-is-faked-declines-delete-it/.

———. "Top AI Researchers Race to Detect 'Deepfake' Videos: 'We Are Outgunned.'" *Washington Post*, June 12, 2019. https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/.

Harwell, Drew, and Eva Dou. "Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says." *Washington Post*, December 8, 2020. https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighurminorities-alert-police-report-says/.

Harwell, Drew, and Tony Romm. "TikTok's Beijing Roots Fuel Censorship Suspicion as It Builds a Huge U.S. Audience." *Washington Post*, September 15, 2019. https://beta.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience.

Haugh, Timothy D., Nicholas J. Hall, and Eugene H. Fan. "16th Air Force and Convergence for the Information War." *Cyber Defense Review* 5, no. 2 (Summer 2020): 29–43. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20V5N2%20Summer%202020-r7.pdf.

Healey, Jason. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): 1–15. https://doi.org/10.1093/cybsec/tyz008.

Healey, Jason, Patricia Mosser, Katheryn Rosen and Adriana Tache. *The Future of Financial Stability and Cyber Risk*. Washington, DC: Brookings Institution, October 2018. https://www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf.

Healey, Jason, and Robert Jervis. "The Escalation Inversion and Other Oddities of Situational Cyber Stability." *Texas National Security Review* 3, no. 4 (2020): 30–53. https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/.

Hearings on Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century, Before the Committee on Homeland Security and Governmental Affairs, United States Senate, 111th Cong. (2010). Statement of Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, US Department of Homeland Security. https://www.govinfo.gov/content/pkg/CHRG-111shrg58034/html/CHRG-111shrg58034.htm.

Hearing on China and Russia, Before the Senate Committee on Armed Services, 116th Cong. (2019). Statement of Elbridge A. Colby, Director of the Defense Program, Center for a New American Security. https://www.armed-services.senate.gov/imo/media/doc/Colby_01-29-19.pdf.

Hearing on Disinformation in the Gray Zone: Opportunities, Limitations, Challenges, Before the House Armed Services Committee Subcommittee on Intelligence and Special Operations, 117th Cong. (2021). Statement of Christopher Maier, Acting Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, Neill Tipton, Director of Defense Intelligence (Collections and Special Programs), and James Sullivan, Defense Intelligence Officer for Cyber, Defense Intelligence Agency. https://sof.news/pubs/Witness-Statement-HSISO-disinformation-hearing-20210316.pdf.

Hearing on the Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cyberspace, Before the House Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, 116th Cong. (2020). Statement of General Paul Nakasone, Commander, Unites States Cyberspace Command. https://armedservices.house.gov/_cache/files/e/d/ed0549b9-c479-4ae0-943d-66cf8fd933c1/AEDF855100875FF9DBB6F5E7472F6E36.nakasone-cybercom-hasc-posture-statement-final-3-13-19.pdf.

Hearing on the National Security Challenge of Artificial Intelligence, Manipulated Media, and "Deepfakes," Before the Permanent Select Committee on Intelligence, 116th Cong. (2019). Statement of David Doermann, professor at SUNY Empire Innovation and director of the Artificial Intelligence Institute at the University at Buffalo. https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-DoermannD-20190613.pdf.

———. Statement of Clint Watts, distinguished research fellow at the Foreign Policy Research Institute; nonresident fellow at the Alliance for Securing Democracy, German Marshall Fund of the United States; and author. https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-WattsC-20190613.pdf.

———. Statement of Danielle Keats Citron, Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law. https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-CitronD-20190613.pdf.

———. Statement of Jack Clark, policy director, OpenAI. https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-ClarkJ-20190613.pdf.

Hearing on Innovation Opportunities and Vision for the Science and Technology Enterprise, House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems, 117th Cong. (February 23, 2021). Statement of Christine Fox, Assistant Director, Johns Hopkins University Applied Physics Laboratory. https://docs.house.gov/meetings/AS/AS35/20210223/111234/HHRG-117-AS35-Wstate-FoxC-20210223.pdf.

Hearing on Nuclear Deterrence in the 21st Century, Before the US House Committee on Armed Services, 114th Cong. (June 25, 2015). Statement of Robert Work, Deputy Secretary Of Defense; and James Winnefeld, Vice Chairman of the Joint Chiefs of Staff. https://docs.house.gov/meetings/AS/AS00/20150625/103669/HHRG-114-AS00-Wstate-WinnefeldJrUSNJ-20150625.pdf.

Hearing on the United States Northern Command and United States Strategic Command in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program, Before the Senate Armed Services Committee, 116th Cong. (February 26, 2019). Statement of General Terrence O'Shaughnessy, United States Air Force; Commander, United States Northern Command and North American Aerospace Defense Command. https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-26-19.pdf.

Hearing on the United States Northern Command and United States Strategic Command in Review of the Defense Authorization Request for Fiscal Year 2021 and the Future Years Defense Program, Before the Senate Armed Services Committee, 116th Cong. (February 13, 2020). Statement of General Terrence O'Shaughnessy, United States Air Force; Commander, United States Northern Command and North American Aerospace Defense Command). https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-13-20.pdf.

Hearing on the Worldwide Threat Assessment of the U.S. Intelligence Community, Before the Select Committee on Intelligence of the United States Senate, 116th Cong. (2019). Statement of Daniel R. Coats, Director of National Intelligence. https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf.

Hearing on Worldwide Threats, Before the Select Committee on Intelligence of the United States Senate, 117th Cong. (2021). Statement of Avril Haines, Director of National Intelligence. https://www.dni.gov/files/documents/Newsroom/Testimonies/2021-04-14-ATA-Opening-Statement-FINAL.pdf.

Heath, Timothy. "Beijing's Influence Operations Target Chinese Diaspora." *War on the Rocks*, March 1, 2018. https://warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora.

Heller, Christian H. "Make Counterintelligence a Main Effort." *Proceedings* 144, no. 10 (October 2018). https://www.usni.org/magazines/proceedings/2018/october/make-counterintelligence-main-effort.

Hern, Alex. "Revealed: How TikTok Censors Videos That Do Not Please Beijing." *Guardian*, September 25, 2019. https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

Herrmann, Jon. *Resilience against the Weaponized Narrative and Disinformation: Defending America's National Security against Adversary Information Operations*. White paper submitted to the Committee on a Decadal Survey of Social and Behavioral Sciences for Applications to National Security, National Academy of Sciences, Engineering, and Medicine, 2017. https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_179824.pdf.

Hetherington, Marc J., and Michael Nelson. "Anatomy of a Rally Effect: George W. Bush and the War on Terrorism." *PS: Political Science and Politics* 36, no. 1 (January 2003): 37–42. https://doi.org/10.1017/S1049096503001665.

Hill, Kashmir. "Hurricane Sandy, @ComfortablySmug, and the Flood of Social Media Misinformation." *Forbes*, October 30, 2012. https://www.forbes.com/sites/kashmirhill/2012/10/30/hurricane-sandy-and-the-flood-of-social-media-misinformation/.

Hill, Miriam, and Nicholas Spangler. "No Evidence Backs Up Reports of Rescue Helicopters Being Fired Upon." *McClatchy*, October 2, 2005; updated May 24, 2007. http://www.mcclatchydc.com/latest-news/article24450577.html.

Hinck, Garrett. "Evaluating the Russian Threat to Undersea Cables." *Lawfare* (blog), March 5, 2018. https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

History.com Editors. "Gulf War Ground Offensive Begins." *History*. Accessed January 15, 2021. https://www.history.com/this-day-in-history/gulf-war-ground-offensive-begins.

Hitchens, Theresa. "JROC Struggles to Build 'Information Advantage' Requirement." *Breaking Defense*, September 17, 2020. https://breakingdefense.com/2020/09/jroc-struggles-to-build-information-advantage-requirement/.

Hitchens, Theresa. "New Strategy Aims to Up DoD, IC Game to Counter Disinformation." *Breaking Defense*, March 16, 2021. https://breakingdefense.com/2021/03/new-strategy-aims-to-up-dod-ic-game-to-counter-disinformation/.

HLMG (High Level Home Front Group). *Fighting Terror Effectively: An Assessment of Israel's Experience on the Home Front*. Madrid: Friends of Israel Initiative, 2016. http://www.high-level-military-group.org/pdf/hlmg-fighting-terror-effectively.pdf.

Hoffmann, Stacie, Emily Taylor, and Samantha Bradshaw. *The Market of Disinformation*. Oxford: Oxford University Internet Institute, October 2019. https://oxtec.oii.ox.ac.uk/wp-content/uploads/sites/115/2019/10/OxTEC-The-Market-of-Disinformation.pdf.

Hollister, Sean. "Three People Have Been Charged for Twitter's Huge Hack, and a Florida Teen Is in Jail." *Verge*, July 31, 2020. https://www.theverge.com/2020/7/31/21349920/twitter-hack-arrest-florida-teen-fbi-irs-secret-service.

Honest Ads Act, H.R. 2592, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/2592.

Honest Ads Act, S. 1356, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1356.

Horwitz, Jeff, and Deepa Seetharaman. "Facebook Executives Shut Down Efforts to Make the Site Less Divisive." May 26, 2020, *Wall Street Journal*. https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

Hosmer, Stephen T. "The Information Revolution and Psychological Effects." In *Strategic Appraisal: The Changing Role of Information in Warfare*, edited by Zalmay Khalilzad, John P. White, Andy W. Marshall, 217–251. Santa Monica, CA: RAND Corp., 1999. https://doi.org/10.7249/MR1016

———. *The Conflict over Kosovo: Why Milosevic Decided to Settle When He Did*. Santa Monica, CA: RAND Corp., 2001. https://www.rand.org/pubs/monograph_reports/MR1351.html.

HSAC (Homeland Security Advisory Council). *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*. Washington, DC: DHS, June 2016. https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf.

———. *Interim Report of the Countering Foreign Influence Subcommittee*. Washington, DC: DHS, May 21, 2019. https://www.dhs.gov/sites/default/files/publications/ope/hsac/19_0521_final-interim-report-of-countering-foreign-influence-subcommittee.pdf.

Hsu, Jeremy. "The Strava Heat Map and the End of Secrets." *Wired*, January 29, 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Huang, Y. Linlin, Kate Starbird, Mania Orand, Stephanie A. Stanek, and Heather T. Pedersen. "Connected through Crisis: Emotional Proximity and the Spread of Misinformation Online." In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, March 2015. http://faculty.washington.edu/kstarbi/CSCW_Proximity_Huang_Starbird_FINAL.pdf.

Huguet, Alice, Jennifer Kavanagh, Garrett Baker, and Marjory S. Blumenthal. *Exploring Media Literacy Education as a Tool for Mitigating Truth Decay*. Santa Monica, CA: RAND Corp., 2019. https://doi.org/10.7249/RR3050.

Human Rights Watch. "US: Trump Attacks Social Media Platforms." May 29, 2020. https://www.hrw.org/news/2020/05/29/us-trump-attacks-social-media-platforms.

Huxley, Tim, and William Choong. *Asia Pacific Regional Security Assessment 2019*. London: IISS, May 2019. https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5.

Iasiello, Emilio J. "Russia's Improved Information Operations: From Georgia to Crimea." *Parameters* 47, no. 2 (Summer 2017): 51–63. https://www.hsdl.org/?abstract&did=803998.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). "Alert (TA17-163A): CrashOverride Malware." June 12, 2017, last revised July 27, 2017. https://www.us-cert.gov/ncas/alerts/TA17-163A.

———. "ICS Alert (ICS-ALERT-17-206-01): CRASHOVERRIDE Malware." July 25, 2017. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01.

IMD (Idaho Military Division). "Cyber Warriors Train alongside Key State Partners." Idaho Military Division, September 25, 2020. https://www.imd.idaho.gov/cyber-warriors-train-alongside-key-state-partners/.

Insikt Group. *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion*. Cyber Threat Analysis CTA-2019-0306. Somerville, MA: Recorded Future, March 2019. https://go.recordedfuture.com/hubfs/reports/cta-2019-0306.pdf.

Isaac, Mike. "Facebook Moves to Limit Election Chaos in November." *New York Times*, September 3, 2020. https://www.nytimes.com/2020/09/03/technology/facebook-election-chaos-november.html.

———. "Why Everyone Is Angry at Facebook over Its Political Ads Policy." *New York Times*, November 22, 2019. https://www.nytimes.com/2019/11/22/technology/campaigns-pressure-facebook-political-ads.html.

Isaac, Mike, and Cecilia Kang. "Facebook Says It Won't Back Down from Allowing Lies in Political Ads." *New York Times*, January 9, 2020. https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html.

Isaac, Mike, and Davey Alba. "Big Tech Companies Meeting With U.S. Officials on 2020 Election Security." *New York Times*, September 4, 2019. https://www.nytimes.com/2019/09/04/technology/2020-election-facebook-google.html.

Isaac, Mike, and Kate Conger. "Google, Facebook and Others Broaden Group to Secure U.S. Election." *New York Times*, August 12, 2020. https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html.

ISO-NE (ISO New England). *Operational Fuel-Security Analysis*. Holyoke, MA: ISO-NE, January 17, 2018. https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf.

Jablanski, Danielle, Herbert S. Lin, and Harold A. Trinkunas. "Retweets to Midnight: Assessing the Effects of the Information Ecosystem on Crisis Decision Making between Nuclear Weapons States." In *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict*, edited by Harold A. Trinkunas, Herbert Lin, and Benjamin Loehrke. Stanford, CA: Harvard Institution Press, 2020.

Jackson, Dean. "Issue Brief: How Disinformation Impacts Politics and Public." National Endowment for Democracy, May 29, 2018. https://www.ned.org/issue-brief-how-disinformation-impacts-politics-and-publics/.

Jacob, Binu, Anthony R. Mawson, Payton Marinelle, and John C. Guignard. "Disaster Mythology and Fact: Hurricane Katrina and Social Attachment." *Public Health Reports* 123, no. 5 (2008): 555–566. https://doi.org/10.1177/003335490812300505.

Jacobson, Eric. "Sino-Russian Convergence in the Military Domain," *New Perspectives in Foreign Policy* no. 15 (Spring 2018): 3–10. https://csis-website-prod.s3.amazonaws.com/s3fs-public/180322_jacobson_sino_russian_convergence.pdf?OHY2N5MpraTzV9ZTKJ9p1den0tjFNWZy.

JCS (US Joint Chiefs of Staff). *Deployment and Redeployment Operations*. Joint Publication 3-35, Washington, DC: JCS, January 10, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_35.pdf.

———. *Doctrine for the Armed Forces of the United States*. Joint Publication 1, Washington, DC: JCS, March 25, 2013; incorporating Change 1, July 12, 2017. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

———. *Information Operations*. Joint Publication 3-13. Washington, DC: JCS, November 27, 2012; incorporating Change 1, November 20, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

———. *Joint Concept for Operating in the Information Environment (JCOIE)*. Washington, DC: JCS, July 25, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

———. *Joint Operational Access Concept (JOAC)*. Version 1. Washington, DC: DoD, January 17, 2012. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joac_2012.pdf?ver=2017-12-28-162010-227.

———. *Joint Operations*. Joint Publication 3-0. Washington, DC: JCS, January 17, 2017; incorporating Change 1, October 22, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

———. *Military Information Support Operations*. Joint Publication 3-13.2. Washington, DC: JCS, January 7, 2010; incorporating Change 1, December 20, 2011. https://info.publicintelligence.net/JCS-MISO.pdf.

Jensen, Benjamin. "The Cyber Character of Political Warfare." *Brown Journal of World Affairs* 24, no. 1 (Fall/Winter 2017), 159–171.

Jervis, Robert. *Perceptions and Misperceptions in International Relations*. Princeton, NJ: Princeton University Press, 1976.

Johnson, Brian David. *Information Disorder Machines: Weaponizing Narrative and the Future of the United States of America*. Tempe, AZ: Arizona State University Threatcasting Lab, 2019. https://threatcasting.asu.edu/sites/default/files/2019-11/01threatcasting-2019-IDM.pdf.

Johnson, Dave. *Russia's Approach to Conflict — Implications for NATO's Deterrence and Defence*. Research Paper No. 111. Rome: NATO Defense College, April 2015. https://www.files.ethz.ch/isn/190782/rp_111.pdf.

———. *Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds*. Livermore Papers on Global Security No. 3. Livermore, CA: Lawrence Livermore National Laboratory, February 2018. https://cgsr.llnl.gov/content/assets/docs/Precision-Strike-Capabilities-report-v3-7.pdf.

Johnson, Derek B. "ODNI Creates New Position Dedicated to Election Security." ODNI, July 22, 2019. https://www.dni.gov/index.php/newsroom/news-articles/item/2024-odni-creates-new-position-dedicated-to-election-security.

Johnson, Derek B., and Susan Miller. "The Dangers of 'Deep Fakes.' " *GCN*, July 18, 2018. https://gcn.com/articles/2018/07/18/deep-fakes.aspx.

Johnson, Lauren Kay. "I Helped Craft the Official Lies to Sell the War in Afghanistan." *Washington Post*, December 15, 2019, B1, B5.

Jones, Edgar. "Air Raids and the Crowd—Citizens at War." *The Psychologist* 29, no. 6 (June 2016): 486–487. https://thepsychologist.bps.org.uk/volume-29/june/air-raids-and-crowd-citizens-war.

Jones, Jeffrey B., and Jack N. Summe. "Psychological Operations in Desert Shield, Desert Storm and Urban Freedom." Landpower Essay Series No 97-3. Arlington, VA: Association of the United States Army, August 1997. https://www.ausa.org/sites/default/files/LPE-97-3-Psychological-Operations-in-Desert-Shield-Desert-Storm-and-Urban-Freedom.pdf.

Jones, Jeffrey M. "U.S. Media Trust Continues to Recover from 2016 Low." Gallup, October 12, 2018. https://news.gallup.com/poll/243665/media-trust-continues-recover-2016-low.aspx.

Jones, Seth G. *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare*. CSIS Brief. Washington, DC: CSIS, October 2018. https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

Joyal, Paul M. "Cyber Threats and Russian Information Warfare." *inFOCUS* (Winter 2016). https://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/.

Kahn, Herman. *On Escalation: Metaphors and Scenarios*. New York: Routledge, 2017.

Kania, Elsa B., and John Costello. "The Strategic Support Force and the Future of Chinese Information Operations." *Cyber Defense Review* 3, no. 1 (Spring 2018): 105–118. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR_V3N1_SPRG2018_Complete.pdf.

Kasapoglu, Can. *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*. Research Paper 121. Rome: NATO Defense College Research Division, October 2017. http://www.ndc.nato.int/news/news.php?icode=877.

Katz, Justin. "Nakasone Deflects Senators' Invitations to Seek Domestic Spying Powers." *FCW*, April 14, 2021. https://fcw.com/articles/2021/04/14/katz-nakasone.aspx.

Katzenbach, Edward. "The Horse Cavalry in the Twentieth Century: A Study on Policy Response." In *Public Policy*, edited by Carl Friedrich and Seymour Harris, 120–150. Cambridge, MA: Harvard Graduate School of Public Administration, 1958.

Kaufmann, Chaim. "Threat Inflation and the Failure of the Marketplace of Ideas: The Selling of the Iraq War." *International Security* 29, no. 1 (Summer 2004): 5–48. https://doi.org/10.1162/0162288041762940.

Kavanagh, Jennifer, and Michael D. Rich. *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. Santa Monica, CA: RAND Corp., 2018. https://doi.org/10.7249/RR2314.

Keck, Zachary. "Russia Threatens Nuclear Strikes over Crimea." *Diplomat*, July 11, 2014. https://thediplomat.com/2014/07/russia-threatens-nuclear-strikes-over-crimea/.

Keller, Jonathan, Edward Yang, and Patrick James. "Decision-Making in U.S. Foreign Policy Crises: Presidential Leadership and Outcomes." Paper presented at Penn State Peace Science Society (International), South Bend, IN, October 22, 2016. https://sites.psu.edu/pssi/files/2016/10/Keller-Yang-and-James_Peace-Science-Society_8-October-2016-2a0zcq4.pdf.

Kelly, Terrence, David C. Gompert and Duncan Long. *Smarter Power, Stronger Partners, Volume I: Exploiting U.S. Advantages to Prevent Aggression*. Santa Monica, CA: RAND Corp. 2016. https://doi.org/10.7249/RR1359.

Kent, Thomas. *Striking Back: Overt and Covert Options to Combat Russian Disinformation*. Washington, DC: Jamestown Foundation, 2020.

Ker, Nic. "Is the Political Aide Viral Sex Video Confession Real or a Deepfake?" *Malay Mail*, June 12, 2019. https://www.malaymail.com/news/malaysia/2019/06/12/is-the-political-aide-viral-sex-video-confession-real-or-a-deepfake/1761422.

Khusyaynova v. United States (Criminal Complaint). United States District Court for the Eastern District of Virginia, September 28, 2018. https://www.justice.gov/opa/press-release/file/1102316/download.

Kinetz, Erika. "Army of Fake Fans Boosts China's Messaging on Twitter." Associated Press, May 12, 2021. https://apnews.com/article/asia-pacific-china-europe-middle-east-government-and-politics-62b13895aa6665ae4d887dcc8d196dfc.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111, no. 3 (2017): 484–501. https://doi.org/10.1017/S0003055417000144.

King, Rachel. "Automation May Hamper Grid Recovery in Outage Caused by Cyberattack." *Wall Street Journal*, May 19, 2016. https://www.wsj.com/articles/BL-CIOB-9792.

Klepper, David. "Cyborgs, Trolls and Bots: A Guide to Online Misinformation." Associated Press, February 7, 2020. https://apnews.com/4086949d878336f8ea6daa4dee725d94.

Kliman, Daniel, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche. *Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations*. Washington, DC: CNAS, May 2020. https://www.cnas.org/publications/reports/dangerous-synergies.

Klonick, Kate. "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression." *Yale Law Journal* 129, no. 8 (2020): 2232–2605. https://www.yalelawjournal.org/pdf/KlonickFeature_dsekuux4.pdf.

Knight Commission on Trust. *Media and Democracy, Crisis in Democracy: Renewing Trust in America*. Washington, DC: Aspen Institute, 2019. https://csreports.aspeninstitute.org/documents/Knight2019.pdf.

Konkel, Frank. "DISA Confirms Breach Affecting 200,000 People." *Nextgov*, February 21, 2020. https://www.nextgov.com/cybersecurity/2020/02/disa-confirms-data-breach-affecting-200000-people/163258/.

Kornbluh, Karen, and Ellen P. Goodman. *Safeguarding Digital Democracy: Digital Innovation and Democracy Initiative Roadmap*. DIDI Roadmap, no. 4. With contributions by Eli Weiner. Washington, DC: German Marshall Fund of the United States, March 2020. http://www.gmfus.org/sites/default/files/Safeguarding%20Democracy%20against%20Disinformation_v7.pdf.

Kowalewski, Annie. "Disinformation and Reflexive Control: The New Cold War." *Georgetown Security Studies Review*, February 1, 2017. https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/.

Kranz, Michal. "Russian Bots Reportedly Pushed a Thanksgiving Food Poisoning Hoax on Twitter as Practice for Influencing the 2016 Election." *Business Insider*, February 21, 2018. https://www.businessinsider.com/russian-bots-thanksgiving-turkey-walmart-food-poisoning-hoax-2018-2.

Krasodomski-Jones, Alex, Josh Smith, Elliot Jones, Ellen Judson, and Carl Miller. *Warring Songs: Information Operations in the Digital Age*. London: Demos, May 2019. https://demos.co.uk/wp-content/uploads/2019/05/Warring-Songs-final-1.pdf.

Kredo, Adam. "U.S. Military Members, Families Hit with Hacks from Russia, Terror Orgs." *Washington Free Beacon*, February 6, 2020. https://freebeacon.com/national-security/u-s-military-members-families-hit-with-hacks-from-russia-terror-orgs/.

Krull, Matthew. "Foreign Disinformation Is a Threat to Military Readiness, Too." *Defense One*, February16,2018.https://www.defenseone.com/ideas/2018/02/foreign-disinformation-threat-military-readiness-too/146076/.

Kruse, Megan. "What Is BGP Hijacking, Anyway?" *Internet Society* (blog), May 7, 2018. https://www.internetsociety.org/blog/2018/05/what-is-bgp-hijacking-anyway/.

Kuleshov, Yu E., B. B. Zhutdiev, and D. A. Fedorov. "Информационно-психологическое противоборство в современных условиях: теория и практика" [Information-psychological warfare in modern conditions: theory and practice]. *Vestnik Akademii Voyennykh Nauk* [Journal of the Academy of Military Science] 46, no. 1 (2014).

Lamb, Christopher J. *Review of Psychological Operations: Lessons Learned from Recent Operational Experience*. Washington, DC: National Defense University Press, September 2005. https://fas.org/irp/eprint/lamb.pdf.

Lambert, Alan J., J. P. Schott, and Laura Scherer. "Threat, Politics, and Attitudes: Toward a Greater Understanding of Rally-'Round-the-Flag Effects." *Current Directions in Psychological Science* 20, no. 6 (December 2011): 343–348. https://doi.org/10.1177/0963721411422060.

Lamberth, Megan. "The Dangers of Manipulated Media in the Midst of a Crisis." *Net Politics* (blog). Council on Foreign Relations, February 12, 2020. https://www.cfr.org/blog/dangers-manipulated-media-midst-crisis.

Lambeth, Benjamin S. *NATO's Air War for Kosovo: A Strategic and Operational Assessment*. Santa Monica, CA: RAND Corp., 2001. https://doi.org/10.7249/MR1365.

Lange-Ionatamišvili, Elina. *Analysis of Russia's Information Campaign against Ukraine*. Riga, Latvia: NATO StratCom Center of Excellence, 2015. https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine.

Lectures on the Command of Joint Campaigns [联合战役指挥教程]. Military Science Press, 2013.

Lee, Kristine, and Karina Barbesino. *Challenging China's Bid for App Dominance*. Washington, DC: CNAS, January 22, 2020. https://www.cnas.org/publications/commentary/challenging-chinas-bid-for-app-dominance.

Lee, Yimou, David Lague, and Ben Blanchard. "China Launches 'Gray-Zone' Warfare toSubdue Taiwan." Reuters, December 10, 2020. https://www.reuters.com/investigates/special-report/hongkong-taiwan-military/.

Leetaru, Kalev. "History Tells Us Social Media Regulation Is Inevitable." *Forbes*, April 22, 2019. https://www.forbes.com/sites/kalevleetaru/2019/04/22/history-tells-us-social-media-regulation-is-inevitable/#7dfdf52121be.

Lerman, Rachel. "Trump Issues Executive Orders against TikTok and WeChat, Citing National Security Concerns." *Washington Post*, August 7, 2020. https://www.washingtonpost.com/technology/2020/08/06/trump-tiktok-executive-order/.

———. "Twitter Hack Triggers Investigations and Lawmaker Concerns." *Washington Post*, July 16, 2020. https://www.washingtonpost.com/technology/2020/07/16/twitter-security-breach-response/.

Lewis, James Andrew. *How Will 5G Shape Innovation and Security: A Primer*. Washington, DC: CSIS, December 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5G-Primer_WEB.pdf.

———. *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: CSIS, January 1, 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_Reconsidering-Cybersecurity_Web.pdf.

———. *Toward a More Coercive Cyber Strategy*. Washington, DC: CSIS, March 10, 2021. https://www.csis.org/analysis/toward-more-coercive-cyber-strategy.

Li, Niu, Li Jiangzhou, and Xu Dehui. "Planning and Application of Strategies of Information Operations in High-Tech Local War." *Zhongguo Junshi Kexue* [China military science], no.4 (2000).

Libicki, Martin C. "The Convergence of Information Warfare." *Strategic Studies Quarterly* 11, no. 1 (Spring 2017): 49–65. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf.

———. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND Corp., 2012. https://www.rand.org/pubs/monographs/MG1215.html.

Lim, Gabrielle, Etienne Maynier, John Scott-Railton, Alberto Fittarelli, Ned Moran, and Ron Deibert. *Burned after Reading: Endless Mayfly's Ephemeral Disinformation Campaign*. Toronto: Citizen Lab, University of Toronto: May 14, 2019. https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/.

Lin, Herbert. "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations." *Lawfare* (blog) September 6, 2018. https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations.

———. "Doctrinal Confusion and Cultural Dysfunction in DOD." *Cyber Defense Review* 5, no. 2 (Summer 2020): 89–106. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Lin_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053232-230.

———. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 3, no. 6 (Fall 2012): 46–70. https://www.jstor.org/stable/26267261.

———. "The Existential Threat from Cyber-Enabled Information Warfare." *Bulletin of the Atomic Scientists* 74, no. 4 (2019): 187–196. https://doi.org/10.1080/00963402.2019.1629574.

Lin, Herb, and Max Smeets. "What Is Absent from the U.S. Cyber Command 'Vision.'" *Lawfare* (blog), May 3, 2018. https://www.lawfareblog.com/what-absent-us-cyber-command-vision.

Lin, Herbert, and Jaclyn Kerr. "On Cyber-Enabled Information/Influence Warfare and Manipulation." Working paper for *Oxford Handbook of Cybersecurity, 2019* (forthcoming). August 13, 2017. https://ssrn.com/abstract=3015680.

Lindsay, James M. "Rally 'Round the Flag." Brookings, March 25, 2003. https://www.brookings.edu/opinions/rally-round-the-flag/.

Lindsay, Jon, and Eric Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." In *The Power to Hurt: Coercion in Theory and Practice*, edited by Kelly Greenhill and Peter Krause. New York: Oxford University Press, 2018.

Loeb, Vernon. "Yugoslav Military Is Formidable Foe." *Washington Post*, April 3, 1999. https://www.washingtonpost.com/wp-srv/inatl/daily/april99/forces040399.htm.

Logan, Bryan. "Twitter Found More than 50,000 Russia-Linked Accounts That Actively Shared Election-Related Material—and Trump Interacted with Them Hundreds of Times." *Business Insider*, January 19, 2018. https://www.businessinsider.com/twitter-found-more-russian-bots-trump-interacted-with-many-2018-1.

Loong, Lee Hsien. “The Endangered Asian Century: America, China, and the Perils of Confrontation.” *Foreign Affairs*, July/August 2020. https://www.foreignaffairs.com/articles/asia/2020-06-04/lee-hsien-loong-endangered-asian-century.

Lopez, C. Todd. “Challenging Russian Information Operations Requires Whole-of-Government Approach.” DoD, March 14, 2019. https://www.defense.gov/Explore/News/Article/Article/1785455/challenging-russian-information-operations-requires-whole-of-government-approach/.

Madrigal, Alexis C. “#BostonBombing: The Anatomy of a Misinformation Disaster.” *Atlantic*, April 19, 2013. https://www.theatlantic.com/technology/archive/2013/04/-bostonbombing-the-anatomy-of-a-misinformation-disaster/275155/.

Malara, Neha, and Arjun Panchadar. “National-Security Concerns Threaten Undersea Cable to China: WSJ.” Reuters, August 28, 2019. https://www.reuters.com/article/us-usa-trade-china/national-security-concerns-threaten-undersea-cable-to-china-wsj-idUSKCN1VI1I9.

Malicious Deep Fake Prohibition Act of 2018, S. 3805 , 115th Cong., 2nd Sess. (December 12, 2018). https://www.congress.gov/115/bills/s3805/BILLS-115s3805is.pdf.

Mandiant. *‘Ghostwriter’ Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests*. Milpitas, CA: FireEye, 2020. https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf.

Manuel, John. “Crisis and Emergency Risk Communication: Lessons from the Elk River Spill.” *Environment Health Perspectives* 122, no. 8 (August 2014): A214–A219. https://ehp.niehs.nih.gov/doi/10.1289/ehp.122-a214.

Marks, Joseph. “The Cybersecurity 202: SCIF Fight Shows Lawmakers Can Be Their Own Biggest Cybersecurity Vulnerability.” *Washington Post*, October 24, 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/10/24/the-cybersecurity-202-scif-fight-shows-lawmakers-can-be-their-own-biggest-cybersecurity-vulnerability/5db077dc88e0fa5ad928d9fb/.

Martineau, Kim. “New Study Highlights Power of Crowd to Transmit News on Twitter.” Columbia University Data Science Institute, June 15, 2016. https://datascience.columbia.edu/news/2016/new-study-highlights-power-of-crowd-to-transmit-news-on-twitter/.

Marwick, Alice, and Rebecca Lewis. *Media Manipulation and Disinformation Online*. New York: Data & Society, May 2017. https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

Matishak, Martin. “Intelligence Community Creating Hub to Gird against Foreign Influence.” *Politico*, April 26, 2021. https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604.

Maurer, Tim, and Arthur Nelson. “The Global Cyber Threat.” *Finance and Development*, March 2021. https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf.

———. *International Strategy to Better Protect the Financial System against Cyber Threats*. Washington, DC: Carnegie Endowment for International Peace, November 2020. https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf.

Mawson, Anthony R. "Understanding Mass Panic and Other Collective Responses to Threat and Disaster." *Psychiatry* 68, no. 2 (2005): 95–113. https://doi.org/10.1521/psyc.2005.68.2.95.

Mazarr, Michael J. *Understanding Deterrence*. Santa Monica, CA: RAND Corp., 2018. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

Mazarr, Michael J., Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden. *Hostile Social Manipulation: Present Realities and Emerging Trends*. Santa Monica, CA: RAND Corp., 2019. https://doi.org/10.7249/RR2713.

Mazarr, Michael J., Ryan Bauer, Abigail Casey, Sarah Heintz, and Luke J. Matthews. *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*. Santa Monica, CA: RAND Corp., 2019. https://doi.org/10.7249/RR2714.

Mazmanian, Adam. "Transcom Head Warns of Cyber Risks to Civilian Infrastructure." *FCW*, April 10, 2018. https://fcw.com/articles/2018/04/10/transcom-cyber-mcdew.aspx.

McAuley, James. "France Moves toward a Law Requiring Facebook to Delete Hate Speech within 24 Hours." *Washington Post*, July 9, 2019. https://www.washingtonpost.com/world/europe/france-moves-toward-a-law-requring-facebook-to-delete-hate-speech-within-24-hours/2019/07/09/d43b24c2-a25d-11e9-a767-d7ab84aef3e9_story.html.

McCabe, David, Ana Swanson, and Erin Griffith. "TikTok's Proposed Deal Seeks to Mollify U.S. and China." *New York Times*, September 14, 2020. https://www.nytimes.com/2020/09/14/technology/deal-tiktok-us-china-trump.html.

McFaul, Michael, ed. *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*. Stanford, CA: Stanford University, 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/stanford_cyber_policy_center-securing_american_elections.pdf.

McIntire, Mike, Karen Yourish, and Larry Buchanan. "In Trump's Twitter Feed: Conspiracy-Mongers, Racists and Spies." *New York Times*, November 2, 2019. https://www.nytimes.com/interactive/2019/11/02/us/politics/trump-twitter-disinformation.html.

McSeveny, Kerry, and David Waddington. "Human Factors in Crisis, Disaster and Emergency: Some Policy Implications and Lessons of Effective Communication." In *Application of Social Media in Crisis Management: Advanced Sciences and Technologies for Security Applications, Transactions on Computational Science and Computational Intelligence*, edited by Babak Akhgar, Andrew Staniforth, and David Waddington, 11–20. Cham: Springer, 2017. https://doi.org/10.1007/978-3-319-52419-1_2.

Medvedev, Dmitry. *The Military Doctrine of the Russian Federation*. Moscow: Kremlin, 2010. Translated by the Carnegie Endowment. https://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

Meredith, Sam. "Here's Everything You Need to Know about the Cambridge Analytica Scandal." *CNBC*, March 21, 2018. https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html.

Meserole, Chris, and Alina Polyakova. "The West Is Ill-Prepared for the Wave of 'Deep Fakes' That Artificial Intelligence Could Unleash." *Order from Chaos* (blog). Brookings Institution, May 25, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash/.

Metaxas, Panagiotis Takis. "Web Spam, Social Propaganda and the Evolution of Search Engine Rankings." In *Web Information Systems and Technologies: WEBIST 2009*, Lecture Notes in Business Information Processing, vol. 45, edited by José Cordeiro and Joaquim Filipe. Berlin, Heidelberg: Springer, 2010. https://doi.org/10.1007/978-3-642-12436-5_13.

Metz, Cade. "How Facebook Is Transforming Disaster Response." *Wired*, November 10, 2016. https://www.wired.com/2016/11/facebook-disaster-response/.

Metz, Cade, and Scott Blumenthal. "How A.I. Could Be Weaponized to Spread Disinformation." *New York Times*, June 7, 2019. https://www.nytimes.com/interactive/2019/06/07/technology/ai-text-disinformation.html.

Meyer, Robinson. "The Grim Conclusions of the Largest-Ever Study of Fake News." *Atlantic*, March 8, 2018. https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/.

Miller, James N., Jr., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict*. Washington, DC: Center for a New American Security, September 2017. https://www.cnas.org/publications/reports/a-new-era-in-u-s-russian-strategic-stability.

Miller, Leslie. "How YouTube Supports Elections." *YouTube Official Blog*, February 3, 2020. https://youtube.googleblog.com/2020/02/how-youtube-supports-elections.html.

Ministry of Defence of the Russian Federation. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space*. Moscow: Russian Ministry of Defense, 2011.

———. *Russian Federation Armed Forces' Information Space Activities Concept, 2011*. Moscow: Kremlin, January 2012. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Minority Staff of the House Science, Space, and Technology Committee Subcommittee on Oversight. *Old Tactics, New Tools: A Review of Russia's Soft Cyber Influence Operations*. Washington, DC: US Congress, November 2017. https://science.house.gov//imo/media/doc/Russian%20Soft%20Cyber%20Influence%20Operations%20-%20Minority%20Staff%20Report%20-%20November%202017.pdf?1.

Mohan, Athira M., Nader Meskin, and Hasan Mehrjerdi. "A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems." *Energies* 13, no. 15 (2020): 3860. https://doi.org/10.3390/en13153860.

Mohsin, Maryam. "10 TikTok Statistics That You Need to Know in 2020." *Oberlo*, September 3, 2020. https://www.oberlo.com/blog/tiktok-statistics.

Moon, Jay. "9/11 Boatlift: The Largest Marine Evacuation in History." *INSH*, August 1, 2019. https://insh.world/history/the-great-boat-lift-of-911/.

Moore, David W. "Bush Job Approval Reflects Record 'Rally' Effect." Gallup, September 18, 2001. https://news.gallup.com/poll/4912/bush-job-approval-reflects-record-rally-effect.aspx.

Morgan, Forrest E., Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff. *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, CA: RAND Corp., 2008. https://www.rand.org/pubs/monographs/MG614.html.

Morgan, Jason. "Is Japan Putting Up a Good Enough Fight against China's Propaganda Warfare?" *Japan Forward*, August 2, 2020. https://japan-forward.com/bookmark-is-japan-putting-up-a-good-enough-fight-against-chinas-propaganda-warfare/.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War*. Santa Monica, CA: RAND Corp., 2019. https://www.rand.org/pubs/research_reports/RR2942.html.

Moz. "What Is SEO?" Accessed January 15, 2021. https://moz.com/learn/seo/what-is-seo.

Mueller, John E. *War, Presidents, and Public Opinion*. New York: John Wiley & Sons, 1973.

Mueller, Karl P. *Air Power*. Santa Monica, CA: RAND Corp., 2010. https://www.rand.org/content/dam/rand/pubs/reprints/2010/RAND_RP1412.pdf.

Mueller, Robert S., III. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Volume I. Washington, DC: DOJ, March 2019. https://www.justice.gov/storage/report.pdf.

Murray, Mark. "Poll: Americans Give Social Media a Clear Thumbs-Down." *NBC News*, April 5, 2019. https://www.nbcnews.com/politics/meet-the-press/poll-americans-give-social-media-clear-thumbs-down-n991086.

Nagourney, Adam, David E. Sanger, and Johanna Barr. "Hawaii Panics after Alert about Incoming Missile Is Sent in Error." *New York Times*, January 13, 2018. https://www.nytimes.com/2018/01/13/us/hawaii-missile.html.

Nakashima, Ellen. "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election." *Washington Post*, October 9, 2020. https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.

———. "Fewer Opportunities and a Changed Political Environment in the US May Have Curbed Moscow's Election Interference This Year, Analysts Say." *Washington Post*, November 17, 2020. https://www.washingtonpost.com/national-security/russia-failed-to-mount-major-election-interference-operations-in-2020-analysts-say/2020/11/16/72c62b0c-1880-11eb-82db-60b15c874105_story.html.

———. “Trump Confirms Cyberattack on Russian Trolls to Deter Them during 2018 Midterms.” *Washington Post*, July 11, 2020. https://www.washingtonpost.com/national-security/trump-confirms-cyberattack-on-russian-trolls-to-deter-them-during-2018-midterms/2020/07/11/66a845e8-c2c3-11ea-b178-bb7b-05b94af1_story.html.

———. “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms.” *Washington Post*, February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

———. “U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election.” *Washington Post*, December 25, 2019. https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

———. “U.S. Undertook Cyber Operation Against Iran as Part of Effort to Secure the 2020 Election.” *Washington Post*, November 3, 2020. https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html.

———. “Why the Sony Hack Drew an Unprecedented U.S. Response against North Korea.” *Washington Post*, January 15, 2015. https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html?utm_term=.3511141ab432.

Nakasone, Paul, and Michael Sulmeyer. “How to Compete in Cyberspace.” *Foreign Affairs*, August 25, 2020. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

NASEM (National Academies of Sciences, Engineering, and Medicine). *Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions*. Washington, DC: National Academies Press, 2018. https://www.nap.edu/catalog/24935/emergency-alert-and-warning-systems-current-knowledge-and-future-research.

National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, 130 Stat. 2646 (2016). https://www.gpo.gov/fdsys/pkg/PLAW-114publ328/pdf/PLAW-114publ328.pdf.

NATO. “Crisis Management Exercise 2019.” Press release, May 3, 2019. https://www.nato.int/cps/en/natohq/news_165844.htm.

NBC Nightly News. “Defense Department Agency Developing Tech to Detect Doctored Images.” April 18, 2018. Video. https://www.nbcnews.com/nightly-news/video/defense-department-agency-developing-tech-to-detect-doctored-images-1214083651797.

NCSC (National Counterintelligence and Security Center). *National Counterintelligence Strategy of the United States of America 2020–2022*. Washington, DC: NCSC, January 7, 2020. https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

Necsutu, Madalin. "Russia Accuses US of Plotting 'Coloured Revolution' in Moldova." *BalkanInsight*, October 21, 2020. https://balkaninsight.com/2020/10/21/russia-accuses-us-of-plotting-coloured-revolution-in-moldova/.

Nemr, Christina, and William Gangware. *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*. Washington, DC: Park Advisors, March 2019. https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

NERC (North American Electric Reliability Corporation). *CIP-014-2—Physical Security*. Atlanta, GA: NERC, effective October 2, 2015. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf.

———. *GridEx V Grid Security Exercise: Lessons Learned Report*. Atlanta, GA: NERC, March 2020. https://www.eisac.com/cartella/Asset/00008427/TLP_WHITE_GridEx_V_Public_After_Action_Report.pdf?parent=123814.

———. *2018 Long-Term Reliability Assessment*. Atlanta, GA: NERC, December 2018. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2018_12202018.pdf.

———. *Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System*. Atlanta, GA: NERC, November 2017. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SPOD_11142017_Final.pdf.

NETSCOUT. *Cloud in the Crosshairs: NETSCOUT's 14th Annual Worldwide Infrastructure Security Report*. Westford, MA: NETSCOUT, March 2019. https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf.

Newton, Casey. "Google Has Been Unusually Proactive in Fighting COVID-19 Misinformation." *Verge*, March 11, 2020. https://www.theverge.com/interface/2020/3/11/21173135/google-coronavirus-misinformation-youtube-covid-19-twitter-manipulated-media-biden.

Nguyen, Nicole. "Doomscrolling: Why We Just Can't Look Away." *Wall Street Journal*, June 7, 2020. https://www.wsj.com/articles/doomscrolling-why-we-just-cant-look-away-11591522200.

Ni, Adam, and Bates Gill. "The People's Liberation Army Strategic Support Force: Update 2019." *China Brief* 19, no. 10 (May 2019): 6–27. https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

NIC (National Intelligence Council). *Foreign Threats to the 2020 US Federal Elections*. Washington, DC: Office of the Director of National Intelligence, March 10, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

Nimmo, Ben, Camille Francois, C. Shawn Eib, Lea Ronzaud, Rodrigo Ferreira, Chris Hernon, and Tim Kostelancik. *Exposing Secondary Infektion: Forgeries, Interference, and Attacks on Kremlin Critics across Six Years and 300 Sites and Platforms*. New York: Graphika, 2020. https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf.

Niquet, Valérie. “China’s Coronavirus Information Warfare.” *Diplomat*, March 24, 2020. https://thediplomat.com/2020/03/chinas-coronavirus-information-warfare/.

North Atlantic Treaty. Apr. 4, 1949, 34 UNTS 243; 43 AJILs 159. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

NRC (National Research Council). *Facing Hazards and Disasters: Understanding Human Dimensions*. Washington, DC: National Academies Press, 2006. https://www.nap.edu/catalog/11671/facing-hazards-and-disasters-understanding-human-dimensions.

NSCAI (National Security Commission on Artificial Intelligence). *Final Report*. Arlington, VA: NSCAI, April 12, 2012. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

NSTAC (National Security Telecommunications Advisory Committee). *NSTAC Report to the President on Internet and Communications Resilience*. Washington, DC: DHS, November 16, 2017. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (2017): 44–71. https://direct.mit.edu/isec/article/41/3/44/12147/Deterrence-and-Dissuasion-in-Cyberspace.

———. “Protecting Democracy in an Era of Cyber Information War.” *Governance in an Emerging World* 318 (November 2018): https://www.hoover.org/research/protecting-democracy-era-cyber-information-war.

ODNI (US Office of the Director of National Intelligence). *Annual Threat Assessment of the US Intelligence Community*. Washington, DC: ODNI, April 9, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

———. *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution*. Washington, DC: ODNI, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

———. *A Guide to Cyber Attribution*. Washington, DC: ODNI, September 14, 2018. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

OFR (US Department of the Treasury Office of Financial Research). *Cybersecurity and Financial Stability: Risks and Resilience*. Viewpoint 17-01. Washington, DC: Treasury, February 15, 2017. https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf.

———. *2016 Financial Stability Report*. Washington, DC: Treasury, December 2016. https://www.financialresearch.gov/financial-stability-reports/2016-financial-stability-report/.

Ogrysko, Nicole. “Recent Hurricanes Have the Coast Guard Rethinking Social Media’s Role in Rescue and Response.” *Federal News Network*, September 21, 2017. https://federalnewsnetwork.com/management/2017/09/recent-hurricanes-have-the-coast-guard-rethinking-social-medias-role-in-rescue-and-response/.

O’Meara, Sarah. “Will China Overtake the U.S. in Artificial Intelligence Research?” *Scientific American*, August 21, 2019. https://www.scientificamerican.com/article/will-china-overtake-the-u-s-in-artificial-intelligence-research/.

Onishi, Norimitsu, and Matthew L. Wald. “Months Later, Sniper Attack at Power Hub Still a Mystery.” *New York Times*, February 5, 2014. https://www.nytimes.com/2014/02/06/us/months-later-sniper-attack-at-power-hub-still-a-mystery.html.

Oremus, Will. “How a 199-Word Local Crime Brief Became Facebook’s Most-Shared Story of 2019.” *Slate*, March 29, 2019. https://slate.com/technology/2019/03/facebook-most-viral-story-texas-child-predator.html.

Ortutay, Barbara. “Facebook Civil Rights Audit: ‘Serious Setbacks’ Mar Progress.” Associated Press, July 8, 2020. https://apnews.com/94189e0798d2ca7701d5c248c2843dbe.

Osborne, Charlie. “Bad Bots Now Make Up 20 Percent of Web Traffic.” *ZDNet*, April 17, 2019. https://www.zdnet.com/article/bad-bots-focus-on-financial-targets-make-up-20-percent-of-web-traffic/.

OSD (US Office of the Secretary of Defense). *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2018*. Washington, DC: OSD, May 16, 2018. https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF.

———. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2019*. Washington, DC: OSD, May 2, 2019. https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

———. *Military and Security Developments Involving the People’s Republic of China 2020: Annual Report to Congress*. Washington, DC: DoD, September 2020. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

Pape, Robert. *Bombing to Win*. Ithaca, NY: Cornell University Press, 1996.

———. “The True Worth of Air Power.” *Foreign Affairs* 83, no. 2 (March–April 2004). https://www.foreignaffairs.com/articles/2004-03-01/true-worth-air-power.

Paris, Britt, and Joan Donavan. *Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence*. New York: Data & Society, September 2019. https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf.

Paul, Christopher. “Is It Time to Abandon the Term Information Operations?” *RealClear Defense*, March 11, 2019. https://www.realcleardefense.com/articles/2019/03/11/is_it_time_to_abandon_the_term_information_operations_114252.html.

Paul, Christopher, and Marek N. Posard. “Artificial Intelligence and the Manufacturing of Reality.” *The RAND Blog*, January 20, 2020. https://www.rand.org/blog/2020/01/artificial-intelligence-and-the-manufacturing-of-reality.html.

Paul, Christopher, and Miriam Matthews. *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica, CA: RAND Corp., 2016. https://doi.org/10.7249/PE198.

Paul, Christopher, and Rand Waltzman. "How the Pentagon Should Deter Cyber Attacks." *Strategy Bridge*, January 10, 2018. https://thestrategybridge.org/the-bridge/2018/1/10/how-the-pentagon-should-deter-cyber-attacks.

Peilin, Sheng, and Li Xue. "On 'Media Decapitation.'" *Journal of the PLA Nanjing Institute of Politics* (May 2006): 114–117.

Peniston, Bradley. "Work: 'The Age of Everything Is the Era of Grand Strategy.'" *Defense One*, November 2, 2015. http://www.defenseone.com/management/2015/11/work-age-everything-era-grand-strategy/123335/.

Pennycook, Gordon, Tyrone Cannon, and David G. Rand. "Prior Exposure Increases Perceived Accuracy of Fake News." *Journal of Experimental Psychology: General* 147, no. 12 (2018): 1–61. https://ssrn.com/abstract=2958246.

Peralta, Eyder. "Obama Says Sony Should Not Have Pulled Film over Threats." *NPR*, December 19, 2014. https://www.npr.org/sections/thetwo-way/2014/12/19/371894427/fbi-formally-accuses-north-korea-in-sony-hacking.

Perez, Evan, and David Shortell. "North Korean-Backed Bank Hacking on the Rise, US Officials Say." *CNN*, March 1, 2019. https://www.cnn.com/2019/03/01/politics/north-korea-cyberattacks-cash-bank-heists/index.html.

Perrett, Connor. "US Troops Are Still Posting to TikTok Despite Partial Ban over Chinese Spy Concerns, and There's Not Much the Defense Department Can Do about It." *Business Insider*, January 10, 2020. https://www.businessinsider.com/us-military-still-posting-tiktok-despite-partial-ban-troops-2020-1.

Perrin, Andrew, and Monica Anderson. "Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged since 2018." *Fact Tank*. Pew Research Center, April 10, 2019. https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.

Pew Research Center. *Americans' Views of Government: Low Trust, but Some Positive Performance Ratings*. Washington, DC: Pew Research Center, September 14, 2020. https://www.pewresearch.org/politics/2020/09/14/americans-views-of-government-low-trust-but-some-positive-performance-ratings/.

———. *Public Trust in Government: 1958–2019*. Washington, DC: Pew Research Center, April 11, 2019. https://www.people-press.org/2019/04/11/public-trust-in-government-1958-2019/.

Pirumov, V. S. *Informatsionnoe Protivoborstvo* [Information confrontation]. Moscow, 2010.

Pocheptsov, Georgii. "The First Cognitive War in the World (Ukraine, Crimea, Russia)." Accessed March 30, 2021. https://www.academia.edu/10057232/FIRST_COGNITIVE_WAR.

Pomerantsev, Peter, and Michael Weiss. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. New York: Institute of Modern Russia, November 2014. https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

Pomerleau, Mark. “Air Force Held First Information Warfare Test Exercises.” *C4ISRNET*, May 19, 2021. https://www.c4isrnet.com/information-warfare/2021/05/19/air-force-held-first-information-warfare-test-exercises/.

———. “Air Force Prepares for Its First Information Warfare Exercise.” *C4ISRNET*, November 17, 2020. https://www.c4isrnet.com/information-warfare/2020/11/17/us-air-force-prepares-for-its-first-information-warfare-exercise/.

———. “DoD Identifies Top Information Operations Adviser.” *C4ISRNet*, October 15, 2020. https://www.c4isrnet.com/information-warfare/2020/10/15/dod-identifies-top-information-operations-adviser/.

———. “The Fake Internet the Army Uses to Train Cyberwarriors.” *Fifth Domain*, July 5, 2018. https://www.fifthdomain.com/it-networks/2018/07/05/the-fake-internet-the-army-uses-to-train-cyberwarriors/.

———. “How the Marines Are Mobilizing Forces for Information Warfare.” *C4ISRNET*, December 20, 2017. https://www.c4isrnet.com/c2-comms/2017/12/20/how-the-marines-are-mobilizing-forces-for-information-warfare/.

———. “National Guard Cyber Exercise to Increase Focus on Information Operations.” *C4ISRNET*, September 2, 2020. https://www.c4isrnet.com/cyber/2020/09/02/national-guard-cyber-exercise-to-increase-focus-on-information-operations/.

———. “A New Name—and Focus—for Army Cyber Command?” *C4ISRNET*, August 21, 2019. https://www.c4isrnet.com/show-reporter/technet-augusta/2019/08/21/a-new-name-and-focus-for-army-cyber-command/.

———. “Pentagon’s AI Center to Field New Psychological Operations Tool.” *C4ISRNET*, September 11, 2020. https://www.c4isrnet.com/artificial-intelligence/2020/09/11/pentagons-ai-center-to-field-new-psychological-operations-tool/.

———. “SecDef Nominee Pledges to Evaluate Information Operations.” *C4ISRNet*, January 20, 2021. https://www.c4isrnet.com/information-warfare/2021/01/20/secdef-nominee-pledges-to-evaluate-information-operations/.

———. “What Cyber Command’s ISIS Operations Means for the Future of Information Warfare.” *C4ISRNET*, June 18, 2020. https://www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/.

———. “What Is Industry’s Role in Information Warfare?” *C4ISRNET*, July 19, 2019. https://www.c4isrnet.com/information-warfare/2020/07/19/whats-industry-role-in-dod-information-warfare-efforts/.

———. “Why a Marine information Warfare Unit Knows It Can Win.” *C4ISRNET*, June 10, 2020. https://www.c4isrnet.com/information-warfare/2020/06/10/why-a-marine-information-warfare-unit-knows-it-can-win/.

Popescu, Nicu. “Russian Cyber Sins and Storms.” European Council on Foreign Relations, October 10, 2018. https://www.ecfr.eu/article/commentary_russian_cyber_sins_and_storms/.

Popp, George, and Sarah Canna. *The Characterization and Conditions of the Gray Zone*. Boston: NSI Inc., Winter 2016. http://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf.

Posard, Marek N., Hilary Reininger, and Todd C. Helmus. *Countering Foreign Interference in U.S. Elections*. Santa Monica, CA: RAND Corp., 2021. https://www.rand.org/pubs/research_reports/RRA704-4.html.

Pritchard, Stephen. "The Readers' Editor on . . . Reporting in Haste." *Guardian*, February 27, 2016. https://www.theguardian.com/media/2016/feb/28/the-readers-editor-on-reporting-in-haste.

Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. §230, https://www.law.cornell.edu/uscode/text/47/230.

Pruitt, Sarah. "How a Five-Day War with Georgia Allowed Russia to Reassert Its Military Might." *History*, August 8, 2018; updated September 4, 2018. https://www.history.com/news/russia-georgia-war-military-nato.

Putin, Vladimir. *Doctrine of Information Security of the Russian Federation*. Moscow: Kremlin, December 5, 2016. https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

———. *Military Doctrine of the Russian Federation*. Moscow: Kremlin, 2014. Translated by the Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland. June 29, 2015. https://rusemb.org.uk/press/2029.

Radin, Andrew, Alyssa Demus, and Krystyna Marcinek. *Understanding Russian Subversion: Patterns, Threats, and Responses*. Santa Monica, CA: RAND Corp., February 2020. https://doi.org/10.7249/PE331.

Rash, Wayne. "Coronavirus Disinformation May Have Contributed to Market Drop." *Forbes*, February 24, 2020. https://www.forbes.com/sites/waynerash/2020/02/24/coronavirus-disinformation-may-have-contributed-to-market-drop/#3d98bf4c25a7.

Raymond, Brian. "Forget Counterterrorism, the United States Needs a Counter-Disinformation Strategy." *Foreign Policy*, October 15, 2020. https://foreignpolicy.com/2020/10/15/forget-counterterrorism-the-united-states-needs-a-counter-disinformation-strategy/.

Reality Check Team. "Social Media: How Do Other Governments Regulate It?" *BBC News*, February 12, 2020. https://www.bbc.com/news/technology-47135058.

Reiber, Jonathan. *A Public, Private War: How the U.S. Government and U.S. Technology Sector Can Build Trust and Better Prepare for Conflict in the Digital Age*. CLTC White Paper Series. Berkeley, CA: UC Berkeley Center for Long-Term Cybersecurity and Technology for Global Security, November 2019. https://cltc.berkeley.edu/2019/12/17/a-public-private-war/.

Rempfer, Kyle, Shawn Snow, and Howard Altman, "Families of Deployed Paratroopers Received 'Menacing' Messages, Warned to Double-Check Social Media Settings." *Military Times*, January 15, 2020. https://www.militarytimes.com/flashpoints/2020/01/15/family-members-of-deployed-paratroopers-receiving-menacing-messages-warned-to-double-check-social-media-settings/.

Reflection Group Appointed by the NATO Secretary General. *NATO 2030: United for a New Era*. November 25, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

Reuters. "Russia Accuses US of Promoting Revolution in Belarus." *New York Post*, September 16, 2020. https://nypost.com/2020/09/16/russia-accuses-us-of-promoting-revolution-in-belarus-toughens-stance/.

Resnikov, Oleksii. "Russia Remains Unwilling to End Seven-Year Ukraine War." *UkraineAlert* (blog). Atlantic Council, January 9, 2021. https://www.atlanticcouncil.org/blogs/ukrainealert/russia-remains-unwilling-to-end-seven-year-ukraine-war/.

Riikonen, Ainikki. "Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China." *Strategic Studies Quarterly* 13, no. 4 (winter 2019): 122–145. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-4/Riikonen.pdf.

Riley, Tonya. "The Cybersecurity 202: Investigations into Russian, North Korean Hackers Are Shaping Biden's Foreign Policy." *Washington Post*, February 18, 2021. https://www.washingtonpost.com/politics/2021/02/18/cybersecurity-202-investigations-into-russian-north-korean-hackers-are-shaping-biden-foreign-policy-anne-neuberger-cybersecurity-biden-administration-cybersecurity/.

Robertson, Adi. "Russian Malware Infiltrated the Nasdaq Servers, Says Businessweek." *Verge*, July 17, 2014. https://www.theverge.com/2014/7/17/5912159/russian-malware-infiltrated-the-nasdaq-stock-exchange-says-businessweek.

Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva. *The Growing Need to Focus on Modern Political Warfare*. Santa Monica, CA: RAND Corp., 2019. https://doi.org/10.7249/RB10071.

Rocca, Joseph. "Understanding Generative Adversarial Networks (GANs)." *Towards Data Science*, January 7, 2019. https://towardsdatascience.com/understanding-generative-adversarial-networks-gans-cd6e4651a29.

Rodriguez, Salvador. "The FBI Visits Facebook to Talk about 2020 Election Security, with Google, Microsoft and Twitter Joining," *CNBC*, September 4, 2019. https://www.cnbc.com/2019/09/04/facebook-twitter-google-are-meeting-with-us-officials-to-discuss-2020-election-security.html.

Romm, Tony, and Elizabeth Dwoskin. "Trump Signs Order That Could Punish Social Media Companies for How They Police Content, Drawing Criticism and Doubts of Legality." *Washington Post*, May 28, 2020. https://www.washingtonpost.com/technology/2020/05/28/trump-social-media-executive-order/.

Romm, Tony, and Isaac Stanley-Becker. "Facebook, Twitter Disable Sprawling Inauthentic Operation That Used AI to Make Fake Faces." *Washington Post*, December 20, 2019. https://www.washingtonpost.com/technology/2019/12/20/facebook-twitter-disable-sprawling-inauthentic-operation-that-used-ai-make-fake-faces/.

Roose, Kevin. "After Las Vegas Shooting, Fake News Regains Its Megaphone." *New York Times*, October 2, 2017. https://www.nytimes.com/2017/10/02/business/las-vegas-shooting-fake-news.html.

Roose, Kevin, Sheera Frenkel, and Nicole Perlroth. "Tech Giants Prepared for 2016-Style Meddling. But the Threat Has Changed." *New York Times*, March 20, 2020. https://www.nytimes.com/2020/03/29/technology/facebook-google-twitter-november-election.html.

Rosenbach, Eric, Maria Barsallo Lynch, Siobhan Gorman, Preston Golson, Robby Mook, Nick Anway, Gabe Cederberg, et al. *The Election Influence Operations Playbook for State and Local Election Officials. Part 1: Understanding Election Mis and Disinformation*. Cambridge, MA: Harvard Kennedy School Belfer Center for Science and International Affairs, September 2020. https://www.belfercenter.org/sites/default/files/2020-09/IO%20Playbook%202%20Part%201.pdf.

Rosenberg, Matthew, and Julian E. Barnes. "A Bible Burning, a Russian News Agency and a Story Too Good to Check Out." *New York Times*, August 11, 2020. https://www.nytimes.com/2020/08/11/us/politics/russia-disinformation-election-meddling.html.

Rosenberger, Laura, and David Salvo. *The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies*. Washington, DC: German Marshall Fund, June 26, 2018. http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies.

Rosenberger, Laura, and Zack Cooper. "Why It's Time for the U.S. to Start Pushing Back against Chinese Information Operations." *Washington Post*, September 9, 2019. https://www.washingtonpost.com/opinions/2019/09/09/why-its-time-us-start-pushing-back-against-chinese-information-operations/.

Rosenworcel, Jessica. Remarks delivered to the State of the Net Conference, Washington, DC, January 28, 2020. https://docs.fcc.gov/public/attachments/DOC-362122A1.pdf.

Ross, Jay. "Time to Terminate Escalate to De-escalate—It's Escalation Control." *War on the Rocks*, April 24, 2018. https://warontherocks.com/2018/04/time-to-terminate-escalate-to-de-escalateits-escalation-control/.

Roth, Yoel, and Ashita Achuthan. "Building Rules in Public: Our Approach to Synthetic & Manipulated Media," Twitter (blog), February 4, 2020. https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html.

Rothkopf, David. *Running the World: The Inside Story of the National Security Council and the Architects of American Power*. New York: PublicAffairs, 2006.

Rumer, Eugene. *The Primakov (Not Gerasimov) Doctrine in Action*. Washington, DC: Carnegie Endowment for Peace, June 2019. https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.

Ryan, Kevin. "Is 'Escalate to Deescalate' Part of Russia's Nuclear Toolbox?" *Russia Matters*, January 8, 2020. https://www.russiamatters.org/analysis/escalate-deescalate-part-russias-nuclear-toolbox.

Sanger, David E., and Steven Lee Myers. "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology." *New York Times*, November 29, 2018. https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.

Sanger, David E., Nicole Perlroth, and Julian E. Barnes. "As Understanding of Russian Hacking Grows, So Does Alarm." *New York Times*, January 2, 2021. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

SANS ICS and E-ISAC (Industrial Control Systems and Electricity Information Sharing and Analysis Center). *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, DC: E-ISAC, March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

SASC (US Senate Armed Services Committee). "SASC Investigation Finds Chinese Intrusions into Key Defense Contractors." Press release. September 17, 2014. https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors.

Savage, Charlie. "Trump's Order Targeting Social Media Sites, Explained." *New York Times*, May 28, 2020. https://www.nytimes.com/2020/05/28/us/politics/trump-twitter-explained.html.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

Schmitt, Eric, and Steven Lee Myers. "Crisis in the Balkans: The Bombing; NATO Said to Focus Raids on Serb Elite's Property." *New York Times*, April 19, 1999. https://www.nytimes.com/1999/04/19/world/crisis-balkans-bombing-nato-said-focus-raids-serb-elite-s-property.html.

Schneider, Mark B. "Escalate to De-escalate." *Proceedings* 143, no. 2 (February 2017). https://www.usni.org/magazines/proceedings/2017/february/escalate-de-escalate.

Schreckinger, Ben. "How Russia Targets the U.S. Military." *Politico*, June 12, 2017. https://www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247.

Schulte, Gregory. "Deterring Attack: The Role of Information Operations." *Joint Force Quarterly* 85 (Winter 2002–03), 84–89.

———. "Revisiting NATO's Kosovo Air War: Strategic Lessons for an Era of Austerity." *Joint Force Quarterly* 17 (4th Quarter 2013): 14–19.

Schwille, Michael, Anthony Atler, Jonathan Welch, Christopher Paul, and Richard C. Baffa. *Intelligence Support for Operations in the Information Environment: Dividing Roles and Responsibilities between Intelligence and Information Professionals*. Santa Monica, CA: RAND Corp., 2020. https://www.rand.org/pubs/research_reports/RR3161.html.

Scola, Nancy. "Inside the Ad Boycott That Has Facebook on the Defensive." *Politico*, July 3, 2020. https://www.politico.com/news/magazine/2020/07/03/activists-advertising-boycott-facebook-348528.

Seldin, Jeff. "Russia Influence Operations Taking Aim at US Military." *VOA News*, November 2, 2018. https://www.voanews.com/usa/russia-influence-operations-taking-aim-us-military.

Seppala, Emma. "How the Stress of Disaster Brings People Together." *Scientific American*, November 6, 2012. https://www.scientificamerican.com/article/how-the-stress-of-disaster-brings-people-together/.

Shearer, Elisa. "Social Media Outpaces Print Newspapers in the U.S. as a News Source." *Fact Tank*. Pew Research Center, December 18, 2018. https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

Shearer, Elisa, and Katerina Eva Matsa. "News Use across Social Media Platforms 2018." Pew Research Center, September 10, 2018. https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/.

Shih, Gerry. "Chinese Firm Harvests Social Media Posts, Data of Prominent Americans and Military." *Washington Post*, September 14, 2020. https://www.washingtonpost.com/world/asia_pacific/chinese-firm-harvests-social-media-posts-data-of-prominent-americans-and-military/2020/09/14/b1f697ce-f311-11ea-8025-5d3489768ac8_story.html.

Shimer, David. *Rigged: America, Russia, and One Hundred Years of Covert Electoral Interference*. New York: Random House, 2020.

Shrikant, Aditi. "The Psychology behind the Pre-Hurricane Run to the Grocery Store." *Vox*, October 10, 2018. https://www.vox.com/the-goods/2018/9/12/17851440/hurricane-michael-shopping-preparedness.

Shu, Catherine, and Jonathan Shieber. "Facebook, Reddit, Google, LinkedIn, Microsoft, Twitter and YouTube Issue Joint Statement on Misinformation." *Tech Crunch*, March 16, 2020. https://techcrunch.com/2020/03/16/facebook-reddit-google-linkedin-microsoft-twitter-and-youtube-issue-joint-statement-on-misinformation/.

Shurkinm, Joel N. "Terrorism and the Media." In *Psychology of Terrorism*, edited by Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, and Philip G. Zimbardo, 81–86. New York: Oxford University Press, 2006.

Shutka, Megan. "NAVIFOR, Information Warfare Enterprise at WEST 2019." Defense Visual Information Distribution Service (DVIDS), February 14, 2019. https://www.dvidshub.net/news/310833/navifor-information-warfare-enterprise-west-2019.

Silverman, Craig. "These Fake Local News Sites Have Confused People for Years. We Found Out Who Created Them." *BuzzFeed News*, posted February 6, 2020; last updated April 2, 2020. https://www.buzzfeednews.com/article/craigsilverman/these-fake-local-news-sites-have-confused-people-for-years.

———. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook." *BuzzFeed News*, November 16, 2016. https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

Silverman, Craig, and Dean Sterling Jones. "Hackers Are Breaking into Websites and Adding Links to Game Google." *BuzzFeed News*, posted December 18, 2019; last updated December 22, 2019. https://www.buzzfeednews.com/article/craigsilverman/hackers-website-links-backlinks-seo-spam.

Silverman, Craig, and Jeremy Singer-Vine. "Most Americans Who See Fake News Believe It, New Survey Says." *BuzzFeed News*, December 6, 2016. https://www.buzzfeednews.com/article/craigsilverman/fake-news-survey.

Simon, Luis. "Demystifying the A2/AD Buzz." *War on the Rocks*, January 4, 2017. https://warontherocks.com/2017/01/demystifying-the-a2ad-buzz/.

Singer, P. W., and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt, 2018.

Smith, Aaron. *U.S. Smartphone Use in 2015*. Washington, DC: Pew Research Center, April 1, 2015. https://www.pewresearch.org/internet/2015/04/01/us-smartphone-use-in-2015/.

Smith, Adam. "Facebook Knew Its Algorithm Made People Turn against Each Other but Stopped Research." *Independent*, May 28, 2020. https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-algorithm-bias-right-wing-feed-a9536396.html.

Smith, David J. "How Russia Harnesses Cyberwarfare." *Defense Dossier* 4 (2012): 7–11. http://www.insidethecoldwar.com/files/august2012.pdf.

Smith, Ian. "Bolton Confirms China Was behind OPM Data Breaches." *FedSmith*, September 21, 2018. https://www.fedsmith.com/2018/09/21/bolton-confirms-china-behind-opm-data-breaches/.

SMWGESDM (Social Media Working Group for Emergency Services and Disaster Management). *Countering False Information on Social Media in Disasters and Emergencies*. Washington, DC: DHS, March 2018. https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf.

Snegovaya, Maria. *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*. Washington, DC: Institute for the Study of War, September 2015. http://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Snyder, Glenn. *Deterrence and Defense: Toward a Theory of National Security*. Princeton, NJ: Princeton University Press, 1961.

Snyder, Glenn H. "Deterrence and Power." *The Journal of Conflict Resolution* 4, no. 2 (1960): 163–178. http://www.jstor.org/stable/172650.

SSCI (US Senate Select Committee on Intelligence). *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media*. 116th Cong., 1st Sess., October 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

———. *Volume 3: U.S. Government Response to Russian Activities*. 116th Cong., 2nd Sess., February 6, 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf.

———. *Volume 4: Review of the Intelligence Community Assessment*. 116th Cong., 1st Sess., publicly released April 21, 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume4.pdf.

Stamos, Alex, Sergey Sanovich, Andrew Grotto, and Allison Berke. "Combatting Organized Disinformation Campaigns from State-Aligned Actors." In *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Election and Beyond*, edited by Michael McFaul, 43–52. Stanford, CA: Stanford University, 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/stanford_cyber_policy_center-securing_american_elections.pdf.

Stancy Correll, Diana. "Members of Trump's Family and Campaign Staff Retweeted a Russian 'Troll Farm.' " *Business Insider*, October 18, 2017. https://www.businessinsider.com/trump-family-retweeted-russian-troll-farm-2017-10.

Stanley Foundation. *Three Tweets to Midnight: Nuclear Crisis Stability and the Information Ecosystem*. Policy memo. Muscatine, IA: Stanley Center for Peace and Security, November 2017. https://stanleycenter.org/publications/policy_memo/SPCNP2017PMb.docx.pdf.

Starbird, Kate. "How a Crisis Researcher Makes Sense of Covid-19 Misinformation." *OneZero*, March 9, 2020. https://onezero.medium.com/reflecting-on-the-covid-19-infodemic-as-a-crisis-informatics-researcher-ce0656fa4d0a.

Steinmetz, Katy. "How Your Brain Tricks You into Believing Fake News." *Time*, August 9, 2018. http://time.com/5362183/the-real-fake-news-crisis/.

Stockton, Paul. *Resilience for Grid Security Emergencies: Opportunities for Industry–Government Collaboration*. National Security Perspective NSAD-R-18-037. Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018. https://www.jhuapl.edu/Content/documents/ResilienceforGridSecurityEmergencies.pdf.

———. *Securing the Grid from Supply-Chain Based Attacks*. Idaho Falls, ID: Idaho National Laboratory, September 2020. https://inl.gov/wp-content/uploads/2020/09/StocktonEOReport.pdf.

———. *Security from Within: Independent Review of the Washington Navy Yard Shooting*. Washington, DC: DoD, November 2013. https://www.hsdl.org/?abstract&did=751015.

———. *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System*. National Security Perspective NSAD-R-15-075. Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2016. https://www.jhuapl.edu/Content/documents/PostCyberAttack.pdf.

Stockton, Paul N., with John P. Paczkowski. "Strengthening Mission Assurance against Emerging Threats Critical Gaps and Opportunities for Progress." *Joint Force Quarterly* 95 (4th Quarter 2019): 22–31. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-95/jfq-95.pdf.

Strout, Nathan. "How the Pentagon Is Tackling Deepfakes as a National Security Problem." *C4ISRNET*, August 29, 2019. https://www.c4isrnet.com/information-warfare/2019/08/29/how-the-pentagon-is-tackling-deepfakes-as-a-national-security-problem/.

Sullivan, Mark. " 'It's a Prodigious Problem': How Google's Jigsaw Is Sniffing Out Faked Images." Fast Company, February 5, 2020. https://www.fastcompany.com/90460173/googles-thinktank-jigsaw-is-wading-into-the-fight-against-disinformation.

Tashev, Blagovest, Michael Purcell, and Brian McLaughlin. "Russia's Information Warfare: Exploring the Cognitive Dimension." *MCU Journal* 10, no. 2 (Fall 2019): 129–147. https://doi.org/10.21140/mcuj.2019100208.

Tavernise, Sabrina. "Will the Coronavirus Kill What's Left of Americans' Faith in Washington?" *New York Times*, May 23, 2020. https://www.nytimes.com/2020/05/23/us/coronavirus-government-trust.html.

Taylor, Adam. "Russia Could Disconnect Itself from Global Internet during a Crisis, Putin Adviser Says." *Washington Post*, December 29, 2016. https://www.washingtonpost.com/news/worldviews/wp/2016/12/29/russia-could-disconnect-itself-from-global-internet-during-a-crisis-putin-adviser-says/.

Temple-Raston, Dina. "Why Russia May Have Stepped Up Its Hacking Game." *NPR*, January 29, 2021. https://www.npr.org/2021/01/29/960810672/why-russia-may-have-stepped-up-its-hacking-game.

Thai, Joseph. "The Right to Receive Foreign Speech." *Oklahoma Law Review* 71, no. 1 (2018): 269–320. https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=1348&context=olr.

Theohary, Catherine. *Defense Primer: Information Operations*. CRS In Focus IF10771. Washington, DC: Congressional Research Service, December 15, 2020. https://crsreports.congress.gov/product/pdf/IF/IF10771.

———. *Information Warfare: Issues for Congress*. CRS Report R45142. Washington, DC: Congressional Research Service, March 5, 2018. https://fas.org/sgp/crs/natsec/R45142.pdf.

Thies, Wallace. *When Governments Collide: Coercion and Diplomacy in the Vietnam Conflict, 1964–1968*. Berkeley, CA: University of California Press, 1980.

Thomas, Timothy L. "Nation-State Cyber Strategies: Examples from China and Russia." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: NDU Press, April 2009. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850.

———. "Russian Forecasts of Future War." *Military Review* (May/June 2019): 84–93. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-19/Thomas-Russian-Forecast.pdf.

———. *Russian Military Thought: Concepts and Elements*. McLean, VA: MITRE, August 2019. https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf.

———. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations." *Defence Strategic Communications* 1, no. 1 (Winter 2015): 11–26. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/195076/download.

Thompson, Scott, and Christopher Paul. "Paradigm Change: Operational Art and the Information Joint Function." *Joint Force Quarterly* 89 (2nd Quarter 2018): 8–14. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1490645/paradigm-change-operational-art-and-the-information-joint-function/.

Thompson, Wayne. *To Hanoi and Back: The United States Air Force and North Vietnam, 1966–1973*. Washington, DC: United States Air Force, 2000. https://media.defense.gov/2010/Oct/01/2001309673/-1/-1/0/ToHanoiAndBack.pdf.

Thomsen, Jacqueline, Nate Robson, and Mike Scarcella. "'Unlawful and Unenforceable': Legal Experts Deride Trump's Attempt to Target Social Media Companies." *National Law Journal*, May 28, 2020. https://www.law.com/nationallawjournal/2020/05/28/unlawful-and-unenforceable-legal-experts-deride-trumps-attempt-to-target-social-media-companies.

Thomson, Scott K., and Christopher E. Paul. "Paradigm Change: Operational Art and the Information Joint Function." *Joint Force Quarterly* 89 (2nd Quarter 2018): 8–14. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89.pdf?ver=2018-04-19-153711-177.

Tierney, Kathleen, Christine Bevc, and Erica Kuligowski. "Metaphors Matter: Disaster Myths, Media Frames, and Their Consequences in Hurricane Katrina." *Annals of the American Academy of Political and Social Science* 604, no. 1 (2006): 57–81. https://doi.org/10.1177/0002716205285589.

Timberg, Craig. "Critics Say Facebook's Powerful Ad Tools May Imperil Democracy. But Politicians Love Them." *Washington Post*, December 9, 2019. https://www.washingtonpost.com/technology/2019/12/09/critics-say-facebooks-powerful-ad-tools-may-imperil-democracy-politicians-love-them/.

———. "Russians Struggled to Spread DNC Files until Wikileaks Helped, Report Says." *Seattle Times*, November 12, 2019, https://www.seattletimes.com/nation-world/russians-struggled-to-spread-dnc-%EF%AC%81les-until-wikileaks-helped-report-says/.

Timberg, Craig, and Eva Dou. "Pro-China Propaganda Campaign Exploits U.S. Divisions in Videos Emphasizing Capitol Attack." *Washington Post*, February 4, 2021. https://www.washingtonpost.com/technology/2021/02/04/china-propaganda-capitol-videos/.

Timberg, Craig, and Tony Romm. "It's Not Just the Russians Anymore as Iranians and Others Turn Up Disinformation Efforts ahead of 2020 Vote." *Washington Post*, July 25, 2019. https://www.washingtonpost.com/technology/2019/07/25/its-not-just-russians-anymore-iranians-others-turn-up-disinformation-efforts-ahead-vote/?utm_term=.7153b37d96c6.

Timberg, Craig, Ellen Nakashima, and Tony Romm. "In Fast-Moving Pandemic, Sources of Falsehoods Spread by Text, Email, WhatsApp and TikTok Elude Authorities." *Washington Post*, March 16, 2020. https://www.washingtonpost.com/technology/2020/03/16/disnfo-texts-trump-quarantine/.

Tirpak, John. "U.S. Poorly Integrates CCMDs, Hasn't Figured Out Hybrid, Hyten Says." *Air Force Magazine*, March 10, 2021. https://www.airforcemag.com/u-s-poorly-integrates-cocoms-hasnt-figured-out-hybrid-hyten-says/.

Tolbert, Julian H. "Crony Attack: Strategic Attack's Silver Bullet?" Master's thesis, Air University, November 2006. https://apps.dtic.mil/dtic/tr/fulltext/u2/a462291.pdf.

Tracy, Marc. "Google Made $4.7 Billion from the News Industry in 2018, Study Says." *New York Times*, June 9, 2019. https://www.nytimes.com/2019/06/09/business/media/google-news-industry-antitrust.html.

Treasury (US Department of the Treasury). "Agency Information Collection Activities; Proposed Collection; Comment Request; Financial Sector Critical Infrastructure Cybersecurity Survey." *Federal Register* 85, no. 14 (2020): 3761–3762. https://www.govinfo.gov/content/pkg/FR-2020-01-22/pdf/2020-00898.pdf.

Troianovski, Anton. "China Censors the Internet. So Why Doesn't Russia?" *New York Times*, February 21, 2021. https://www.nytimes.com/2021/02/21/world/europe/russia-internet-censorship.html.

TruePic. "Our Technology: A Holistic Approach to a Complex Problem." Accessed January 15, 2021. https://truepic.com/technology/.

Trump, Donald. *Executive Order on Addressing the Threat Posed by TikTok*. Washington, DC: White House, August 6, 2020. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

———. *Executive Order on Preventing Online Censorship*. Washington, DC: White House, May 28, 2020. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-preventing-online-censorship/.

———. *Executive Order on Securing the United States Bulk-Power System*. Washington, DC: White House, May 1, 2020. https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system.

Tucker, Eric. "FBI Official: Russia Wants to US 'Tear Ourselves Apart.'" Associated Press, February 24, 2020. https://apnews.com/a55930e0a02d2e21d8ed2be7bc496a6f.

———. "General Says Attacks by Foreign Hackers Are 'Clarion Call.'" Associated Press, March 25, 2021. https://apnews.com/article/elections-hacking-united-states-russia-presidential-elections-bd87969fd1e13e0f0b2dca51e297469f.

Tucker, Patrick. "Key Official: Defense Information Operations 'Not Evolving Fast Enough.'" *Defense One*, March 17, 2021. https://www.defenseone.com/technology/2021/03/key-official-defense-information-operations-not-evolving-fast-enough/172742/.

Tully, Phillip, and Lee Foster. "Repurposing Neural Networks to Generate Synthetic Media for Information Operations." *Threat Research* (blog). FireEye, August 5, 2020. https://www.fireeye.com/blog/threat-research/2020/08/repurposing-neural-networks-to-generate-synthetic-media-for-information-operations.html.

Turek, Matt. "Media Forensics (MediFor)." Defense Advanced Research Projects Agency. Accessed January 15, 2021. https://www.darpa.mil/program/media-forensics.

Twigg, John, and Irina Mosel. "Emergent Groups and Spontaneous Volunteers in Urban Disaster Response." *Environment and Urbanization* 29, no. 2 (October 2017): 444–458. https://doi.org/10.1177/0956247817721413.

Twitter. "Political Content." Twitter for Business. Accessed January 15, 2021. https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html.

———. "An Update on Our Security Incident." Twitter (blog), last updated July 30, 2020. https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.

Twitter Safety. "Information Operations Directed at Hong Kong." Twitter (blog), August 19, 2019. https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html.

Tzu, Sun. *Art of War*. Translated by Lionel Giles. Classic Etexts Series. Leicester, UK: Allandale Online Publishing, 2000. https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf.

Uberti, David. "Microsoft Warns of Chinese Hackers Targeting Email Product." *Wall Street Journal*, March 2, 2021. https://www.wsj.com/articles/microsoft-warns-of-chinese-hackers-targeting-email-product-11614725915?mod=article_inline.

United States v. Ahmad Fathi et al. United States District Court, Southern District of New York, March 24, 2016. https://www.justice.gov/opa/file/834996/download.

United States v. Hua and Shilong. United States District Court, Southern District of New York, December 17, 2018. http://fm.cnbc.com/applications/cnbc.com/resources/editorialfiles/2018/12/20/China%20case.pdf.

United States v. Internet Research Agency (18 U.S.C. §§ 2, 371, 1349, 1028A). United States District Court for the District of Columbia. https://www.justice.gov/file/1035477/download.

United States v. Netyksho et al. United States District Court for the District of Columbia, July 13, 2018. https://www.justice.gov/file/1080281/download.

University of Exeter. "The Bombing of Britain Exhibition 1940–1945 Exhibition." In *Bombing, States and Peoples in Western Europe 1940–1945: The Project Exhibition*. University of Exeter Centre for the Study of War, State and Society. https://humanities.exeter.ac.uk/history/research/centres/warstateandsociety/projects/bombing/exhibitions/.

USAF (US Air Force). *Practical Design: The Coercion Continuum. Annex 3-0 to United States Air Force Doctrine*. Montgomery, AL: Lemay Center for Doctrine, 2016. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-D15-OPS-Coercion-Continuum.pdf.

———. "Sixteenth Air Force (Air Forces Cyber)." Accessed January 15, 2021. https://www.16af.af.mil/About-Us.

US House of Representatives. *John S. McCain National Defense Authorization Act for Fiscal Year 2019 Conference Report*. Report 115-874. 115th Cong., 2nd Sess., July 25, 2018. https://www.govinfo.gov/content/pkg/CRPT-115hrpt874/pdf/CRPT-115hrpt874.pdf.

USASOC (US Army Special Operations Command). *Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014*. Fort Bragg, NC: USASOC, June 2015. https://www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf.

USCESRC (U.S.-China Economic and Security Review Commission). *2019 Report to Congress*. 116th Cong., 1st Sess. Washington, DC: GPO, November 2019. https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf.

USCYBERCOM (US Cyber Command). *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: DoD, June 14, 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

USN (US Navy). *Navy Cryptologic & Cyber Warfare Community Vision*. Washington, DC: USN, February 8, 2019. https://media.defense.gov/2020/May/18/2002301996/-1/-1/1/CW_COMMUNITY_VISION.PDF.

USNA (US Naval Academy). "Information Warfare Community (IWC)." Accessed January 15, 2021. https://www.usna.edu/CyberCenter/Outreach/index.php.

US Senate Committee on Foreign Relations (Minority Staff). *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*. 115 Cong., 2nd Sess. Washington, DC: GPO, January 2018. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

US Senate Committee on Homeland Security and Government Affairs. *Protecting Cyberspace as a National Asset Act of 2010*. Report 111-368. 111th Cong., 2nd Sess. https://www.congress.gov/111/crpt/srpt368/CRPT-111srpt368.pdf.

Valeriano, Brandon. “How Rival States Employ Cyber Strategy: Disruption, Espionage, and Degradation.” In *Cyber Strategy: The Evolving Character of Power and Coercion*, Brandon Valeriano, Benjamin Jensen, and Ryan Maness. New York: Oxford University Press, 2018.

———. “Introduction: Are Cyber Strategies Coercive?” In *Cyber Strategy: The Evolving Character of Power and Coercion*, Brandon Valeriano, Benjamin Jensen, and Ryan Maness. New York: Oxford University Press, 2018.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press, 2018.

Vasquez, Christian. “DOE Official: More Money, Power Needed to Protect Grid.” *E&E News*, August 6, 2020. https://www.eenews.net/energywire/stories/1063689119.

Vavra, Shannon. “Fed Chair Deems Cyber Threat Top Risk to the Financial Sector.” *Cyberscoop*, April 12, 2021. https://www.cyberscoop.com/federal-reserve-chairman-jerome-powell-cyberattack/.

Vigdor, Neil. “U.S. Military Branches Block Access to TikTok App amid Pentagon Warning.” *New York Times*, January 4, 2020. https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html.

Vilmer, Jean-Baptiste Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera. *Information Manipulation: A Challenge for Our Democracies*. Paris: CAPS (Ministry for Europe and Foreign Affairs) and IRSEM (Ministry for the Armed Forces), August 2018. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

Vilmer, Jean-Baptiste Jeangène, and Paul Charon. “Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare.” *War on the Rocks*, January 21, 2020. https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.

Vogels, Emily A. “Millennials Stand Out for Their Technology Use, but Older Generations Also Embrace Digital Life.” *Fact Tank*. Pew Research Center, September 9, 2019. https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/.

Volz, Dustin, and Robert McMillan. “Massive Hacks Linked to Russia, China Exploited U.S. Internet Security Gap.” *Wall Street Journal*, March 10, 2021. https://www.wsj.com/articles/massive-hacks-linked-to-russia-china-exploited-u-s-internet-security-gap-11615380912.

Vosoughi, Soroush, Deb Roy, and Sinan Aral. “The Spread of True and False News Online.” *Science* 359, no. 6380 (2018): 1146–1151. https://doi.org/10.1126/science.aap9559.

Vranica, Suzanne, and Deepa Seetharaman. “Facebook Tightens Controls on Speech as Ad Boycott Grows.” *Wall Street Journal*, June 26, 2020. https://www.wsj.com/articles/unilever-to-halt-u-s-ads-on-facebook-and-twitter-for-rest-of-2020-11593187230.

VSMWG (Virtual Social Media Working Group) and First Responders Group. *Using Social Media for Enhanced Situational Awareness and Decision Support*. Washington, DC: DHS, June 2014. https://www.dhs.gov/sites/default/files/publications/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf.

Waddell, Kaveh. "Kremlin-Sponsored News Does Really Well on Google." *Atlantic*, January 25, 2017. https://www.theatlantic.com/technology/archive/2017/01/kremlin-sponsored-news-does-really-well-on-google/514304/.

Wadley, Jared. "New Study Analyzes Why People Are Resistant to Correcting Misinformation, Offers Solutions." University of Michigan News, September 20, 2012. https://news.umich.edu/new-study-analyzes-why-people-are-resistant-to-correcting-misinformation-offers-solutions/.

Wagner, Kurt. "Facebook Meets with FBI to Discuss 2020 Election Security." *Bloomberg*, September 4, 2019. https://www.bloomberg.com/news/articles/2019-09-04/facebook-meets-with-fbi-to-discuss-2020-election-security.

Wakefield, Jane. "Russia 'Successfully Tests' Its Unplugged Internet." *BBC News*, December 24, 2019. https://www.bbc.com/news/technology-50902496.

War Powers of President, 47 U.S.C. §606, https://www.law.cornell.edu/uscode/text/47/606.

Warzel, Charlie. "Epstein Suicide Conspiracies Show How Our Information System Is Poisoned." *New York Times*, August 11, 2019. https://www.nytimes.com/2019/08/11/opinion/jeffrey-epstein-suicide-conspiracies.html.

Washington Post. Afghanistan Papers. *Washington Post*, 2019. https://www.washingtonpost.com/graphics/2019/investigations/afghanistan-papers/documents-database/.

Watson, Paul. "Yugoslav Opposition Works to Gain Support of Milosevic's Police Forces." *Los Angeles Times*, October 6, 2000. https://www.latimes.com/archives/la-xpm-2000-oct-06-mn-32498-story.html.

Watts, Clint. *Advanced Persistent Manipulators and Social Media Nationalism: National Security in a World of Audiences*. Aegis Series Paper No. 181. Stanford, CA: Hoover Institution, September 2018. https://www.hoover.org/sites/default/files/research/docs/watts_webreadypdf.pdf.

WEA Project Team. *Wireless Emergency Alerts Cybersecurity Risk Management Strategy for Alert Originators*. Special Report CMU/SEI-2013-SR-018. Pittsburgh: Carnegie Mellon University Software Engineering Institute, March 2014. https://resources.sei.cmu.edu/asset_files/SpecialReport/2014_003_001_87729.pdf.

Weaver, Courtney. "Putin Was Ready to Put Nuclear Weapons on Alert in Crimea Crisis." *Financial Times*, March 15, 2015. www.ft.com/intl/cms/s/0/41873ed2-cb60-11e4-8ad9-00144feab7de.html.

Weedon, Jen, William Nuland, and Alex Stamos. *Information Operations and Facebook*. Version 1.0. Menlo Park, CA: Facebook, April 27, 2017. https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf.

Weiss, Brennan. "From 'Crazy' to 'Regret'—Here's How Facebook's Positions on Russian Interference Evolved over Time." *Business Insider*, November 1, 2017. https://www.businessinsider.com/facebook-changing-statements-russian-meddling-2016-election-2017-11.

Wemer, David A. "Here's How to Fight Disinformation." *New Atlanticist* (blog). Atlantic Council, October 2, 2018. https://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-how-to-fight-disinformation.

Werchan, Jason. "Required US Capabilities for Combatting Russian Activities Abroad." In *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper*, edited by Nicole Peterson, 135–137. Boston: NSI, Inc., May 2019. https://nsiteam.com/social/wp-content/uploads/2019/05/SMA-Russian-Strategic-Intentions-White-Paper-PDF-compressed.pdf.

Wheeler, Tom. "Could Donald Trump Claim a National Security Threat to Shut Down the Internet?" *TechTank* (blog). Brookings Institution, June 25, 2020. https://www.brookings.edu/blog/techtank/2020/06/25/could-donald-trump-claim-a-national-security-threat-to-shut-down-the-internet/.

White House. *National Security Strategy of the United States of America*. Washington, DC: White House, December 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

———. *Presidential Policy Directive — United States Cyber Incident Coordination*. Washington, DC: White House, July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

White, Sarah P. *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*. West Point, NY: Modern War Institute at West Point, March 20, 2018. https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.

Whitlock, Craig. "At War with the Truth." *Washington Post*, December 9, 2019. https://www.washingtonpost.com/graphics/2019/investigations/afghanistan-papers/afghanistan-war-confidential-documents/.

Wicker, Roger F. Letter to Jack Dorsey, July 16, 2020. https://www.commerce.senate.gov/services/files/52B17AD0-58C4-4F01-AEBB-A0F260E533B3.

Williams, Heather, and Alexi Drew. *Escalation by Tweet: Managing the New Nuclear Diplomacy*. London: King's College London, July 2020. https://www.kcl.ac.uk/csss/assets/10957%E2%80%A2twitterconflictreport-15july.pdf.

Williams, Katie Bo. "Foreign Disinformation Campaign Is Targeting Congress, Top Dems Say." *Defense One*, July 20, 2020. https://www.defenseone.com/threats/2020/07/foreign-disinformation-campaign-targeting-congress-top-dems-say/167035/.

Williams, Pete. "FBI Chief Wray: Russia Works '365 Days a Year' to Undermine American Democracy." *NBC News*, April 26, 2019. https://www.nbcnews.com/politics/national-security/fbi-chief-wray-russia-works-365-days-year-undermine-american-n999086.

Wilson, Tom, and Kate Starbird. "Cross-Platform Disinformation Campaigns: Lessons Learned and Next Steps." *Harvard Kennedy School Misinformation Review* 1, no. 1 (January 2020): 1–11. https://doi.org/10.37016/mr-2020-002.

Wong, Edward, Matthew Rosenberg, and Julian E. Barnes. "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say." *New York Times*, April 22, 2020. https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html.

Woodruff Swan, Betsy. "State Report: Russian, Chinese and Iranian Disinformation Narratives Echo One Another." *Politico*, April 21, 2020. https://www.politico.com/news/2020/04/21/russia-china-iran-disinformation-coronavirus-state-department-193107.

Woodruff Swan, Betsy, and Bryan Bender. "Spy Chiefs Look to Declassify Intel after Rare Plea from 4-Star Commanders." *Politico*, April 26, 2021. https://www.politico.com/news/2021/04/26/spy-chiefs-information-war-russia-china-484723.

Woolley, Samuel. "We're Fighting Fake News AI Bots by Using More AI. That's a Mistake." *MIT Technology Review*, January 8, 2020. https://www.technologyreview.com/2020/01/08/130983/were-fighting-fake-news-ai-bots-by-using-more-ai-thats-a-mistake/.

Work, Robert O., and Greg Grant. *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics*. Washington, DC: CNAS, June 2019. https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Work-Offset-final-B.pdf.

Yates, Chelsea. "Dissecting Disinformation." University of Washington College of Engineering, October 8, 2018. https://www.engr.washington.edu/news/article/2018-10-08/dissecting-disinformation.

Zetter, Kim. "SolarWinds Hack Infected Critical Infrastructure, Including Power Industry." *Intercept*, December 24, 2020. https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/.

Zhengzhong, Chen. "Preliminary Thoughts about Strengthening Cyber News Media in Wartime." *Military Correspondent*, July 2014.

Zubiaga, Arkaitz, Ahmet Aker, Kalina Bontcheva, Maria Liakata, and Rob Procter. "Detection and Resolution of Rumors in Social Media: A Survey." *ACM Computing Surveys* 51, no. 2 (June 2018): 32-1–32-36. https://doi.org/10.1145/3161603.

Zuckerberg, Mark. "Mark Zuckerberg: The Internet Needs New Rules. Let's Start in These Four Areas." *Washington Post*, March 30, 2019. https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

Acknowledgments

I am enormously grateful to the APL editorial, graphics, and production team and my APL project supervisor, Matt Schaffer, who offered invaluable recommendations and insights to guide my analysis. My special thanks as well to Rob Denaburg, who performed superb research during the early stages of this study. The study also benefited from criticism and improvements suggested by David Batz; Andy Bochman; Bob Butler; Donald Duncan and the other participants in my formative presentation to APL; Craig Fields; Sarah Freeman; Christine Fox; Robert Giesler; Richard Girven and his RAND colleagues; Emily Goldman; Heather McMahon; Jim Miller; Maegen Nix; Rob Schrier; Michelle Van Cleave; Walter Weiss and the DARPA team; Lt. Col. Andrew Wonpat; Virginia Wright; and many other colleagues and reviewers whose input proved most helpful. The findings and recommendations in the study are my own, however, and do not represent the policies of DoD or any other government agency.

About the Author

Paul Stockton is a senior fellow of APL and leads Paul N. Stockton LLC, a strategic advisory firm in Santa Fe, New Mexico. He previously served as the managing director of Sonecon LLC and was the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In his current capacity, Dr. Stockton helps electric utilities, trade associations, and the Electricity Subsector Coordinating Council strengthen preparedness against emerging cyber threats. He chairs the Grid Resilience for National Security subcommittee of DOE's Electricity Advisory Committee. He also assists with cybersecurity initiatives for the water and wastewater sector and helps government and industry build preparedness against cascading, cross-sector failures.

Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation, associate provost of the Naval Postgraduate School, and director of the school's Center for Homeland Defense and Security. Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DoD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Resilience for Grid Security Emergencies: Opportunities for Industry–Government Collaboration* (Laurel, MD: APL, 2018) and numerous other publications. He served as the facilitator of the GridEx IV and V exercises (2017 and 2019, respectively) and is a member of the Strategic Advisory Committee of the Idaho National Laboratory, the board of directors of Analytic Services, Inc., and other public and private sector boards.

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY