NOVEMBER 2021

INFLUENCE AND ESCALATION

Implications of Russian and Chinese Influence Operations for Crisis Management

AUTHORS
Rebecca Hersman
Eric Brewer
Lindsey Sheppard
Maxwell Simon

A Report of the **CSIS Project on Nuclear Issues**

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

NOVEMBER 2021

INFLUENCE AND ESCALATION

Implications of Russian and Chinese Influence Operations for Crisis Management

AUTHORS
Rebecca Hersman
Eric Brewer
Lindsey Sheppard
Maxwell Simon

A Report of the **CSIS Project on Nuclear Issues**

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD
Lanham • Boulder • New York • London

ABOUT CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

ISBN: 978-1-5381-4045-1 (pb); 978-1-5381-4046-8 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.org

ACKNOWLEDGMENTS

The authors would like to thank Kelly Greenhill, Elsa Kania, Michael Mazarr, and Olga Belogolova for their valuable feedback and participation in the workshops that preceded this report. The authors would also like to thank Peter Wood, Joe McReynolds, David Santoro, and Jaclyn Kerr for their careful review of and constructive comments on the scenarios developed for this report. The authors would also like to thank Nicholas Adamopoulos for his help in editing the report and pushing it over the finish line.

This research was made possible through the support of the United States Defense Threat Reduction Agency (DTRA). The opinions, findings, views, conclusions, or recommendations contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DTRA or the U.S. government.

CONTENTS

EXECUTIVE SUMMARY

Technology-enabled influence operations, including disinformation, will likely figure prominently in adversary efforts to impede U.S. crisis response and alliance management in high-risk, high-impact scenarios under a nuclear shadow. Both Russia and China recognize their conventional military disadvantage vis-à-vis conflict with the United States. As a result, both nations use sub-conventional tactics and operations to support their preferred strategies for achieving favorable outcomes while attempting to limit escalation risks. Such strategies include an array of activities loosely identified as influence operations, focused on using and manipulating information in covert, deniable, or obscure ways to shape the strategic environment.

Defining Influence Operations

Influence operations are activities designed to distract, disrupt, dissuade, or distort the targeted country's perception of a situation. In doing so, influence operations affect a country's ability to act effectively in its own interests by manipulating the information environment at either the micro or macro level in ways that are often covert, unattributable, or deniable. At the macro level, these activities could seek to fracture public support and undermine public confidence in leaders and institutions, exploit weaknesses and divisions between allies and partners to undermine collective action, or simply create delays and diversions in ways that confer strategic advantage to the adversary. At the micro level, influence operations may target individuals (including decisionmakers), groups, or communities to encourage actions that may disrupt, delay, or discourage effective actions.

Influence Tactics

Today's influence operations reflect a convergence of old-school influence techniques from the Cold War with tactics only possible in an increasingly digitized age. Influence operations and tactics can use singular, one-off approaches or can combine various means to enhance the impact of the operation and increase chances of success. These include tactics such as hack and leak operations, forgeries, elite or media co-optation, inciting flash mobs, bribery, coercion and intimidation, flooding the information zone, false flag operations, causing chaos to provide cover for riskier influence operations, and microtargeting. State-based organizations and other actors with advanced intelligence collection capabilities and the resources to leverage emerging digital-influence technologies will continue to find influence operations valuable in supporting various pre-conflict strategies, especially as digital technology allows such operations to flourish at low cost, with limited attribution, and with accelerated speed and penetration.

Influence Technologies

Influence operations are tightly interwoven with the digital information environment, leveraging a constant stream of content reaching information consumers through a wide range of platforms and devices. Modern algorithmic techniques provide the ability to automate the processing and creation of data while also supporting precision targeting of specific segments of populations or certain individuals. These operations can be highly cost and labor efficient, utilizing existing trends in media dissemination that may be automated without a human operating each account. Technologically advanced influence operations carried out by adversary states can exploit digital pathways to both precisely target individuals or specific groups and broadly message the general public in target nations. Digital content-generation capabilities and online marketing techniques, alongside the mapping of digital human networks, are rapidly advancing in sophistication and effect.

Artificial intelligence (AI) and machine learning (ML) may be used to both manipulate existing media and to create new media in support of influence operations. As researchers develop more sophisticated techniques, it is becoming increasingly difficult for human observers and even computers to detect manipulated and fabricated content. ML algorithms also enable online marketing and recommendations to target content more precisely at individuals online based on user interests and attributes; however, influence operations may also exploit these techniques to ensure content is viewed and spread. Furthermore, social media sites document flows of information between individuals and groups as well as how actors, groups, and entities relate to one another, allowing actors with access to network analysis tools, sentiment analysis processes, and bot networks to automate previously labor-intensive aspects of influence operations. As individuals increasingly rely on social media as a news source, this trend will continue to provide readymade pathways for adversaries to exploit both human biases and the technology itself for modern influence operations.

Escalation Pathways

While influence operations pose significant challenges in times of relative peace by imposing costs on target states and advancing the perpetrator's strategic objectives, the escalation risks associated with such activities during crisis or conflict may be underappreciated. Research to date has struggled to identify clear causal linkages between sub-conventional activities, information weaponization, and military escalation, leading some scholars to conclude that the risk of unintended escalation to military conflict via sub-conventional tactics is overstated. Two aspects of this relationship may be poorly recognized: the potential for influence operations to succeed beyond the initial goals of the aggressor, and the potential for influence operations to converge with other actions to culminate in a scenario far closer to an out-and-out crisis than was initially intended. In periods of crisis or conflict, the escalatory potential of such activities may be higher while patterns and pathways of escalation involving influence operations may evade the step-based and comparatively linear expectations for escalation and crisis management so prevalent among national security decisionmakers.

- Influence operations may complicate crises between nuclear-armed states by degrading states' capacity to appropriately manage crisis escalation.

- The speed, scale, and precision of influence operations have increased as adversaries become more adept at generating real-world, physical actions from primarily virtual tools leading to faster and less attributable impacts.
- The speed and distribution advantages offered by influence operations may prove particularly effective in complicating states' abilities to manage third-party relationships through allies and partners.
- Four primary factors seem to drive escalatory potential: the geopolitical context surrounding the operation, the level of control the state has over the influence operation, the potential consequences for the targeted nation, and political complexity of the target state's alliance network.

Key Findings

- Influence operations will continue to rely primarily on tried-and-true tactics and remain largely the prerogative of state-based actors.
- However, the new digitized information environment that permeates every facet of society and the emerging digital tools to take advantage of that environment are increasing the speed, precision, and scale with which influence campaigns can reach and manipulate their desired targets.
- That same speed, precision, and scale—and the novelty of some of these technologies—suggest that future influence operations and their effects may be harder for their executors and their targets to predict and control.
- The web of U.S. alliances creates a larger attack surface for malign actors to exploit in efforts to degrade alliance cohesion.
- Democratic governments may have few authorities to directly counter and put an end to adversary influence operations during a crisis because private sector platforms serve as the primary conduit for information and content.
- While technology can help the United States detect and respond to disinformation operations and their associated challenges, the U.S. government cannot rely solely on technical solutions to combat influence operations.
- Greater coordination between Russia and China on influence operations would pose significant challenges for the United States and its allies and partners.

Recommendations

- Gaming and exercising by the U.S. government and nongovernmental organizations are essential tools to anticipate potential influence operations and recognize attendant escalation and crisis management risks.
- The United States and its allies should create a "crisis playbook" standardizing coordination procedures to synchronize responses to short-term tactical information operations.
- The National Science Foundation (NSF) and Defense Advanced Research Projects Agency (DARPA) should direct research investment into digital

defense technologies that can enable timely and accurate detection of dangerous AI-created content such as deepfakes and forged or false information.

- The U.S. intelligence community, in cooperation with the Department of Homeland Security and Department of Defense, should invest in capabilities to monitor the information environment in real time and build the capacity to disseminate information and coordinate across agencies and departments quickly.
- The United States should synchronize its understanding of adversary information operations with allies and clarify the risks and benefits of different approaches to deterring, combating, or countering such efforts.
- The Office of the Director of National Intelligence (ODNI) and Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) should implement public-private partnerships to create emergency coordination mechanisms and disinformation containment actions when public health, security, or safety is at stake.
- The executive branch and U.S. Congress should prioritize initiatives to enhance societal and institutional resiliency.

INTRODUCTION

Russia and China both emphasize the importance of a full-spectrum approach to achieving their long-term strategic aims and managing crisis and conflict. Both countries also emphasize sub-conventional tactics and operations in support of their efforts to achieve favorable outcomes while limiting escalation risks. This approach assumes, implicitly, and in some cases explicitly, that by staying below the threshold for conventional war, strategic objectives can be pursued at relatively low cost.

Any emerging crisis or conflict with Russia or China would likely be accompanied by efforts to influence the United States and its allies and partners in ways that help Moscow and Beijing achieve their strategic objectives at the lowest possible level of military violence. These efforts can include actions such as a show of force, deterrence posturing, diplomatic engagement, and even strategic messaging—powerful and recognizable tools within the pre-conflict tool kit. While potent forces of influence, these actions are largely direct and attributable.

Such a strategy, however, would also likely include an array of activities loosely identified as influence operations. Influence operations focus on using—and indeed manipulating—information in covert, deniable, or obscure ways to shape the strategic environment in a manner favorable to a country's interests. These operations can include preliminary or pre-crisis efforts to prepare the information environment and pre-position influence-related assets, capabilities, and resources in anticipation of future events. They may also include a variety of activities associated with an unfolding crisis or conflict.

And yet, as these activities and operations increasingly engage strategic-level interests, capabilities, and risks—within U.S. territory, infrastructure, institutions, and governing elites, or those of close allies and partners—existing adversary assumptions about the potential for escalation may not prove sound. Neither is it clear that U.S. leaders are well prepared to detect and counter such activities, enhance the resilience of key institutions, individuals, and communities to the risks posed by these tactics, or respond to these activities in the context of crisis or conflict in ways that manage escalation and prevent conflict while avoiding any form of pre-conflict capitulation. In other words, how can the United States prevent an adversary from gaining strategic benefit through the use of these tactics while also preventing crisis and escalation to war?

PROJECT OBJECTIVE AND SCOPE

A misinformation newsstand is seen in midtown Manhattan on October 30, 2018, aiming to educate news consumers about the dangers of disinformation, or fake news, in the lead-up to the U.S. midterm elections.

This project uses a scenario-based methodology to illustrate ways in which Russian or Chinese influence operations, enabled by emerging technology, could affect crisis management and alliance cohesion in Europe and Asia.

The report's key research question is: *How might Russia and China use technology-enabled influence operations, including disinformation, to impede U.S. crisis response and alliance management in high-risk, high-impact scenarios under a nuclear shadow?*

The study has four main goals:

1. Identify a range of tactics and technologies likely to challenge U.S. detection and response to influence operations, especially when employed during crisis or conflict;
2. Develop a spanning set of scenarios—four focused on Russia and four focused on China—that invite potential escalation risks and demonstrate how these tools and tactics could be employed to challenge detection, response, and crisis management;
3. Explore a range of potential escalatory pathways and destabilizing consequences if adversary influence operations engage strategic interests and targets in high-risk scenarios; and
4. Identify key takeaways and recommendations for policymakers to better identify and defend against adversary influence operations.

PHOTO SOURCE: ANGELA WEISS/AFP/GETTY IMAGES

DEFINING INFLUENCE OPERATIONS

Influence operations are activities designed to distract, disrupt, dissuade, or distort a targeted country's perception of a situation. In doing so, influence operations affect a country's ability to act effectively in its own interests by manipulating the information environment at either the micro or macro level in ways that are often covert, unattributable, or deniable. Indeed, all influence operations contain an element of deception—sources may be masked, content may be doctored, information acquisition methods or other actions may be covert, or online accounts may not be authentic.[1]

Influence operations are closely related to information operations, which are generally defined according to U.S. military doctrine 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."[2] While information operations and influence operations share many similar characteristics, tactics, and tools, there are important differences. Information operations tend to be tactical in nature and military in form and execution. By contrast, influence operations may be of longer duration, need not be immediately associated with any direct military confrontation, are more strategic and broad in intent and objective, and engage a far more diverse set of targets, which may be civilian or societal in nature.[3] Such operations could include, but are not limited to, the weaponization of social media using "deepfakes" and other techniques capable of sowing confusion about the words and intentions of U.S. leaders and decisionmakers, the use of microtargeting against companies and individuals to disrupt vital infrastructure and supply chains, and the manipulation of open-source analysis and investigations to shift blame on the global stage. While the United States gains greater strategic advantage by forcing others to "fight in the light," Russia and China have many incentives to stay in the shadows, behind a cloak of deniability.[4] Influence operations are highly useful for such indirect methods of conflict and may be perceived as less risky or escalatory if Russia or China believes these actions can be taken without opening the door to direct military conflict.

In particular, influence operations seek to manipulate the information environment in ways that undermine the target nation's ability to act in its own interest through both macro- and micro-level targets and objectives. At the macro level, these activities could seek to: fracture public support and undermine public confidence in leaders and institutions; exploit or exacerbate existing societal, economic, or political cleavages; sow fear and doubt about necessary courses of action; exploit weaknesses and divisions between allies and partners to undermine collective action; or simply create delays and diversions in ways that confer strategic advantage to the adversary. At the micro level, influence operations may target individuals (including decisionmakers), groups, or communities to encourage actions that may disrupt, delay, or discourage effective actions. In these cases, influence operations may appeal to existing sympathies, biases, or predispositions of individuals or groups or may use targeted threats, deception, extortion, or other coercive tactics. In many cases, influence operations may simply "throw gasoline" on existing divisions or controversies, such as election fraud, with ready-made amplifiers and influencers. In other cases, such operations can provide a "spark" that naturally feeds the preexisting sympathies and pathologies in communities of influence. A number of Covid-19 misinformation and disinformation narratives as well a variety of active measures related to the Organisation for the Prohibition of Chemical Weapons (OPCW) and the whistleblower scandal fall into this category.

"Influence operations may be of longer duration, need not be immediately associated with any direct military confrontation, are more strategic and broad in intent and objective, and engage a far more diverse set of targets, which may be civilian or societal in nature."

Influence operations can, and often do, involve intrusive cyber techniques—including potential networked attacks conducted through malicious code, hacking, spoofing, tampering, and data manipulation.[5] However, not all cyber operations—such as cyber espionage designed to extract information of value, major critical infrastructure attacks designed to inflict significant economic hardship, or cyberattacks intended as direct punitive or retaliatory measures—are influence operations, especially when such operations are fairly public and attributable.

INFLUENCE TACTICS, TECHNIQUES, AND TRENDS

We have a responsibility to protect your information. If we can't, we don't deserve it.

You may have heard about a quiz app built by a university researcher that leaked Facebook data of millions of people in 2014. This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to make sure this doesn't happen again.

We've already stopped apps like this from getting so much information. Now we're limiting the data apps get when you sign in using Facebook.

We're also investigating every single app that had access to large amounts of data before we fixed this. We expect there are others. And when we find them, we will ban them and tell everyone affected.

Finally, we'll remind you which apps you've given access to your information – so you can shut off the ones you don't want anymore.

Thank you for believing in this community. I promise to do better for you.

Mark Zuckerberg

A man reads a full-page advertisement taken out by Mark Zuckerberg, the chairman and chief executive officer of Facebook, to apologize for the large-scale leak of personal data from the social network, on the back page of a newspaper.

PAST AND CURRENT INFLUENCE OPERATIONS

States have been using deceptive information to achieve political objectives (at least in ways that resemble contemporary disinformation operations) since at least the 1920s.[6] While advances in digital-influence technologies and a more networked society pose new challenges for policymakers, the fundamental objectives of influence operations remain the same: influence operations exist to create or exacerbate division—amplifying existing hostility between communities in a single country, creating distrust between governments and their citizens, or driving wedges between allies. Influence operations may be designed to target those interests and objectives directly, or to target unrelated issues in ways that distract, disrupt, or delay the targeted country's ability to detect and respond effectively. In many ways, these operations function as cost-imposition techniques. Even if the targeted country ultimately identifies the influence operation, attributes it correctly, and counters it effectively, these techniques can greatly increase the financial, political, diplomatic, and other resources required to achieve an acceptable outcome.

Since their inception, influence operations have been intricately linked to intelligence operations. Indeed, the forgeries and leaks that characterized NATO-Eastern Bloc competition were largely a battle of "spy agency versus spy agency."[7] A near-constant informational contest played out across Europe during the Cold War between the CIA (Central Intelligence Agency) and BND (West German intelligence) on one side, and the KGB (Soviet Russia's Committee for State Security) and HVA (East German intelligence) on the other. Successful measures included, for example, the U.S.-based publication of a 1974 "tell-all" book detailing global KGB operations.[8]

The turn of the century and the rise of the internet marked an important turning point in influence operations. Anonymous internet activism and a drive for hyper-transparency contributed to the emergence of "leaking culture" and platforms such as Cyrptome (and its descendent, WikiLeaks) for mass influence campaigns carried out by individual activists or state actors. Information designed to manipulate was less attributable, more easily hidden behind the veneer of transparency activism, and accessible by anyone.

Wider use of the internet in the 2000s led to a convergence of old-school influence techniques from the Cold War—technical intelligence collection and the leaking of compromising information (sometimes true, sometimes a mix of true and false)—with tactics only possible in an increasingly digitized era such as hacking and internet-enabled sabotage. While many information operations during the Cold War were funneled through journalists and mainstream media organizations, governments retained considerable control over these activities and the actors involved in their execution. Today, various internet platforms and social media sites can be used to surface information to a broader audience, at a higher tempo, and with greater deniability, but also with considerably less control and recallability.

> *Even if the targeted country ultimately identifies the influence operation, attributes it correctly, and counters it effectively, these techniques can greatly increase the financial, political, diplomatic, and other resources required to achieve an acceptable outcome.*

This convergence of tried-and-true influence tactics with new influence-enabling technologies means that state-based organizations and other actors with advanced intelligence collection capabilities and the resources to leverage emerging digital-influence technologies will continue to find influence operations valuable in supporting various pre-conflict strategies. State-based organizations will also continue to have the technological edge in adapting and incorporating advanced enabling technologies and leveraging digital platforms to meet their objectives even as they may have less control over the effects of these operations once unleashed in the digital environment.

For Russia, contemporary influence campaigns have revealed a tendency to flood the information zone with conspiracy theories and other false narratives to confuse, distract, and distort the truth while obfuscating its own behavior. Moscow's aggressive disinformation efforts following the 2018 Novichok nerve agent attack on former Russian double agent Sergei Skripal in the United Kingdom is one example of this tactic. News reports suggest that this disinformation campaign was executed by a specialized intelligence cell as part of an ongoing campaign to destabilize Europe, suggesting these sub-conventional attacks can have multiple goals and targets and will pose an enduring challenge to the United States and its allies.[9]

PHOTO SOURCE: OLI SCARFF/AFP/GETTY IMAGES

Meanwhile, Chinese influence operations have historically focused on burnishing China's image—promoting positive narratives and suppressing criticism at home and abroad with a range of tools. These tools include economic warfare and China's increasingly large, elite intermediary network abroad.[10] Some scholarship, however, suggests a convergence between Russian and Chinese influence strategies. Indeed, China seems to be learning from Russian strategies—the People's Liberation Army (PLA) has sent teams to visit Russia to discuss information operations and social media-based influence tactics, and Chinese military articles have extensively referenced Russian influence operations in Syria and Ukraine as models to imitate.[11] During the Covid-19 crisis, China appears to be adopting a more confrontational disinformation approach and global influence strategy through the use of false flag conspiracy theories, global assistance campaigns, and bargaining strategies involving pandemic-related data and research with the World Health Organization. In a departure from past information efforts, Chinese information manipulation has become more extreme, focusing on creating conflicting narratives to sow discord and undermine governmental institutions in the targeted countries, suggesting Beijing views past tactics as inadequate for the Covid-19 crisis.[12]

Russia and China appear to be increasingly ambitious in their targeting, expanding influence campaigns from their near abroad to a global scale. Both countries are growing their presence on Western social media platforms, building on propaganda efforts from other U.S. adversaries, and adopting new digital tools for information spread.[13] According to a required filing under the Foreign Agents Registration Act, China's annual spending on foreign influence efforts in the United States increased sixfold between 2016 and 2020.[14] Russia's infamous Internet Research Agency (IRA), a social media troll factory based in St. Petersburg and Moscow, also has a dedicated "America department" and a multi-million-dollar annual budget.[15] Despite reports of its minimal impact, the IRA highlights Russia's continued attention on the United States and its willingness to adapt its influence operations to new platforms.[16]

A more competitive security landscape means that Russia, China, and other countries will increasingly find value in exploiting the new information environment and digital technologies to achieve their influence aims. The relative low cost of these operations for the perpetrators, as compared to the much higher costs imposed on the targeted country, suggests that such lines of effort will continue and expand in the years to come. Understanding the options available to U.S. adversaries requires understanding several technological trends and developments that characterize the emerging digital environment in which the United States, its allies, and potential adversaries will operate.

INFLUENCE TACTICS

Influence operations and tactics can use singular, one-off approaches or combine various means to enhance the impact of the operation and increase chances of success. While modern influence tactics often harness new technologies and social media, at their core they often exploit tried-and-true tactics to pursue their objectives. These include tactics such as:

Hack and Leak: Hack and leak operations work by publicizing genuine, sensitive internal communications or other confidential material accessed through technical intelligence collection methods. By highlighting improper behavior of decisionmakers to their constituents, revealing internal government policy documents or communications to partner countries, or releasing private personal information about individuals ("doxing"), this tactic seeks to influence public discourse, decisionmaking, or other behavior. For example, a 2013 Russian digital-influence operation targeted EU and U.S. officials amid antigovernment protests in Ukraine. Seeking to drive a wedge between the United States and Europe, Russian operators simultaneously released two intercepted phone calls—one between U.S. officials criticizing the European Union's unwillingness to threaten sanctions on the Ukrainian government, and the other by EU officials reacting to reports of U.S. frustration.[17] More recently, a vast Russian intrusion into the Democratic National Committee's (DNC) servers in the run-up to the 2016 U.S. presidential election resulted in a WikiLeaks document dump that revealed organizational bias in favor of then-candidate Hillary Clinton, ultimately leading to the resignation of the chairwoman of the DNC.[18]

Forgery: An important complement to hack and leak operations, forgery involves the "leaking" of modified or completely falsified information. Forgery occurs behind the veneer of a hack and leak operation—or, more effectively, in combination with one—to circulate a mix of genuine and doctored content to make the "bombshell" forgery appear more credible. For example, in an attempt to disrupt global U.S. intelligence operations, the KGB in 1966 released a book titled *Who's Who in the CIA*, listing thousands of alleged U.S. intelligence operatives abroad.[19] In reality, only a subset of officials listed were actual CIA officers—scores of others were just regular diplomats.[20] Contemporary forgeries, ranging from deepfakes and fabricated audio to doctored satellite imagery, leverage modern technologies to further distort truth.

Elite and Media Co-optation: State actors may court witting and unwitting press organizations, individual journalists, or other prominent public figures into spreading and amplifying false information or deliberately casting doubt on authoritative information. These groups and individuals may be reputable news outlets but may also portray themselves as legitimate sources, transparency activists, or as being in other roles acting on behalf of the public interest. These individuals or organizations can serve as vehicles for spreading foreign-driven disinformation, exacerbating societal divisions and tensions, and eroding trust in government. In one instance, then-UK Labour Party leader Jeremy Corbyn referenced leaked documents indicating his opponents wanted to weaken the National Health Service. The documents turned out to be connected to a Russian influence campaign.[21] China also relies on its more public-facing United Front—an extensive network of elite intermediaries responsible for influencing Chinese civil society and foreign entities—to advance its objectives, though it also uses private diplomacy. Combined, these entities take advantage of their ambiguous connections to the state to court elites and other decisionmakers abroad while maintaining deniability.[22]

Flash Mob: Influence operations can directly produce real-world effects by instigating protests, unrest, and other mass gatherings. "Flash mobs" may be targeted at the societal level but also at a specific region, community, or ideological group. Evidence indicates Russia in particular has used Facebook groups to infiltrate existing activist networks and organize real-world rallies and protests, in some cases designed to exacerbate racial tensions in the United States. For example, posing as an organization focused on fighting racism, Russian influence operators created viral videos and paid advertisements to drive engagement with a now removed online group, Black Elevation, organizing rallies in 2017 across multiple cities that were then unwittingly promoted by local chapters of the Black Lives Matter movement.[23] Indeed, according to Facebook disclosures, groups it had removed from the platform in 2018 created approximately 30 real-world gatherings in roughly one year.[24] Although the January 6, 2021, attack on the U.S. Capitol was not the result of foreign instigation, the information environment in the lead-up to the attack highlights how foreign actors could exploit similar events in the future: a chorus of influential far-right and anti-government figures operating on niche social media platforms and private groups encouraged congregation and violent action in Washington, D.C., as a joint session of Congress was set to formalize the results of the 2020 presidential election.[25]

Bribery: State-based actors may seek to directly influence decisionmakers or other high-impact actors through the use of coercive threats, bribery, and financial incentives to convince them to adopt positions or take actions that are advantageous to the targeting state. For example, during the Cold War, the East German Main Directorate for Reconnaissance was able to successfully bribe two members of the West German parliament to cast anonymous votes in favor of then-chancellor Willy Brandt (and his Ostpolitik policy of détente toward the Soviet bloc) in a 1972 vote of no confidence.[26] Brandt survived the vote of no confidence by two votes, a direct result of the bribery campaign. More recently, three elite interlocutors with connections to China funneled millions of dollars to John Ashe, a prominent diplomat from Antigua and Barbuda and then-president of the UN General Assembly, in 2013 and 2014 in exchange for various favors, including support for UN infrastructure projects and government contracts for Chinese companies.[27] By relying on intermediaries with more opaque connections to the state, China was able to exert influence with individuals who may rebuff offers from those with more explicit connections to the party-state.[28]

Coercion/Intimidation: Influence operators may leverage compromising (or forged) information on government officials or other elites to convince them to take a certain course of action under threat of disclosure. Aggressive harassment campaigns could be waged by armies of online trolls as well as government officials. Attacks, including personal onslaughts, doxing, lawfare, and threats against family members are particularly potent means to intimidate individuals into avoiding certain actions, such as speaking out against human rights violations or continuing investigative work. One recent instance of an online harassment campaign is the China-driven targeting of Vicky Xu, an Australia-based journalist and researcher reporting on human rights violations in Xinjiang.[29] The rise of ransomware attacks reinforces the potential of financial coercion to compel cooperation with influence objectives.

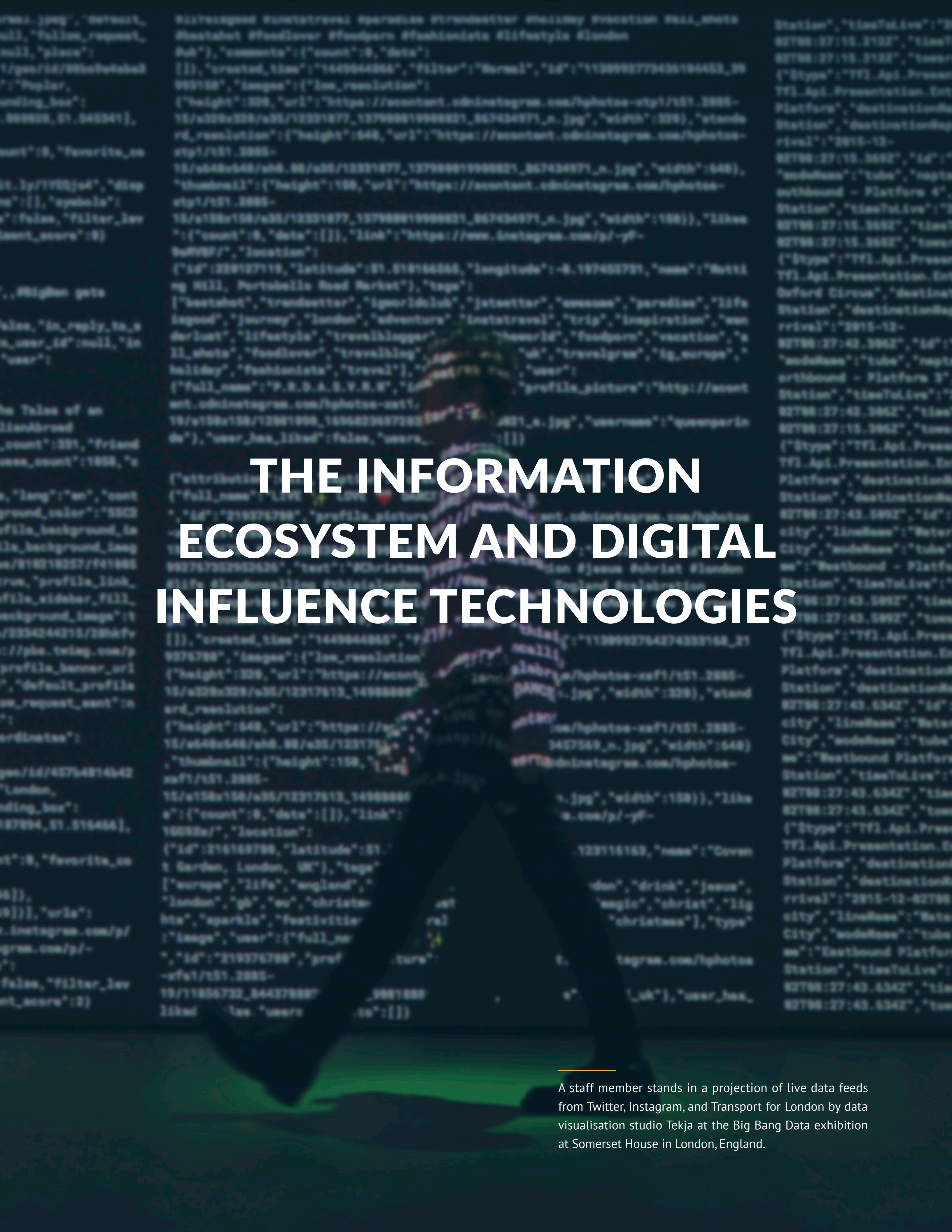
Flood the Zone: Given the decreasing cost of producing and diffusing information, and the vastly larger volume of content generated in the internet age, a state-actor may seek to undermine authoritative information as a crisis unfolds by inundating the information environment with conspiracy theories and other false narratives. Beginning in the immediate aftermath of Russia's failed assassination of Sergei Skripal in Salisbury, England, for example, Russian state media, state-connected Twitter accounts, and government officials released 46 divergent explanations for the attack in an effort to undermine the investigation. By promoting a range of false narratives, such campaigns aim to make it harder for ordinary citizens to differentiate fact from false information, to confuse and distract the public from aggressive or objectionable behavior, and to ultimately dodge attribution.[30]

False Flag: False flag operations seek to shift blame for atrocities or other hostile acts by framing another country or actor. Influence actors may take advantage of situations with internationally inaccessible evidence to stage or doctor evidence, advance conspiracy theories, or both. For instance, the Russian and Syrian governments have accused the Syrian Civil Defence Forces (known as the "White Helmets")—a volunteer rescue organization operating in warzones across Syria—of staging chemical weapons attacks and other bombings in an attempt to frame the Assad government. This narrative has been amplified by an army of conspiracy theorists and Russia-connected social media trolls to frame the organization as a militant group rather than a humanitarian one.[31]

Chaos Cover: In the context of crisis or conflict, U.S. adversaries will likely use multiple influence operations simultaneously. State actors may use one set of influence operations to create confusion, distraction, and chaos that serve as a "cover" or feint for more targeted and potentially riskier influence operations elsewhere. Similarly, influence operations that target broad societal elements can be effective "cost-imposition" tactics, absorbing time, resources, attention span, and media attention in ways that create adversary freedom to conduct more targeted attacks elsewhere. For example, the 2007 Bronze Soldier crisis allowed Russian actors to execute a series of increasingly sophisticated cyberattacks against Estonia under the cover of largely manufactured outrage against the movement of a Soviet war memorial from central Tallinn to the outskirts of the city.[32] After Russian-language media outlets spread false claims that the Estonian government had destroyed the memorial, riots broke out across Tallinn, providing cover for waves of increasingly intense denial of service (DoS) and distributed denial of service (DDoS) cyberattacks from Russian computers against Estonian digital news media, banking, and government platforms.[33] The Russian government was able to maintain a veil of plausible deniability throughout the crisis by claiming that the cyberattacks were being carried out by those involved in the civil unrest and riots.

Microtargeting: A vast body of legally accessible, commercially available, and highly concentrated user data is available for purchase by anyone at scale, enabling the creation of comprehensive digital profiles of large numbers of people, but also specific individuals or decisionmakers. By gaining a detailed picture of an individual's preferences, habits, and worldview, operations can be more closely tailored to specific individuals and more capable of reshaping preferences or impacting behavior in ways that favor desired influence-related outcomes. Microtargeting has become more prominent in recent U.S. presidential election cycles and has become an increasingly attractive and affordable method for actors to influence political discourse.[34] During the 2016 presidential election cycle, Russia-connected accounts spent $100,000 on political Facebook advertisements, utilizing microtargeting strategies to identify and influence pivotal voter demographics.[35]

A more competitive security landscape means that Russia, China, and other countries will increasingly find value in exploiting the new information environment and digital technologies to achieve their influence aims. The relative low cost of these operations for the perpetrators, as compared to the much higher costs imposed on the targeted country, suggests that such lines of effort will continue and expand in the years to come. More information is publicly available about Russian use of these tactics in historical and more recent examples, but China is a close observer of these operations and, as some of their actions throughout the Covid-19 pandemic suggest, will adapt some of these approaches to suit their own objectives.[36] Understanding the options available to U.S. adversaries requires understanding several technological trends and developments that characterize the emerging digital environment in which the United States and its allies, and their potential adversaries, will operate.



THE INFORMATION ECOSYSTEM AND DIGITAL INFLUENCE TECHNOLOGIES

A staff member stands in a projection of live data feeds from Twitter, Instagram, and Transport for London by data visualisation studio Tekja at the Big Bang Data exhibition at Somerset House in London, England.

Advances in digital technologies are transforming the speed, precision, and scale with which influence campaigns can reach and manipulate their desired targets.

Technological advances are enhancing the ability of countries and other actors to refine and tailor these operations to specific individuals and communities, complicating the ability of targeted countries to detect and counter false information, and obscuring effective attribution. Influence operations of the future are likely to be more intrusive, prevalent, and disruptive because of an evolving information ecosystem and the digital influence technologies that will enable actors to manipulate their audience.

Three primary drivers characterize the evolving information ecosystem.

First, the amount, availability, and utility of data are dramatically increasing while also becoming more concentrated. Arguably the most significant trend in technology in the twenty-first century is the exponential growth of data and the ability to use that data. Data is also becoming more concentrated. Five massive companies—Apple, Alphabet (the parent company of Google), Amazon, Facebook, and Microsoft—are responsible for the vast majority of data collection, management, and information processing, maintaining dominant market positions in the United States and abroad.[37] Similar patterns are at play among China's technology giants—Baidu, Alibaba, and Tencent. The information environment is immensely networked and interdependent, and the information accumulation occurring across the many services and products offered by these companies enables the creation of enormous databases. Individuals are almost constantly interacting with the internet, and every action one takes—from using a search engine, watching a movie, and making a social media post, to ordering food, shopping, calling an Uber, and booking a flight—is being used by companies to collect valuable information and create detailed digital profiles of individuals. It was these portraits that fueled revelations about perceived overreach from Cambridge Analytica's consulting work during the 2016 Trump presidential campaign.[38]

These profiles can be used to tailor experiences and target advertisements, but they can also be harnessed and exploited to enable highly targeted influence campaigns at both the micro and macro level. The same digitization and concentration that make this data useful to businesses also make it vulnerable to theft and manipulation by state actors. Today, adversaries can access and use a variety of personal information leveraging computerized algorithms to drive digital influence.

Second, the infosphere is fragmenting into echo chambers and information bubbles. Before the rise of the internet, Americans predominantly received their news from three major network television stations—ABC, NBC, and CBS—which together accounted for nearly 90 percent of the television audience.[39] The same three trusted sources served as gatekeepers to information and provided fairly homogeneous, general news content designed for wide appeal.[40] Today, however, consumers get their information from a wide variety of sources—including specialized news websites, blogs, and social media feeds. Whereas journalists were long the arbiters of information and its validity, today information flows directly from content creators to content consumers and increasingly targets specific segments of the population rather than the public as a whole.[41] Further, algorithmic recommendation engines designed to boost individual engagement tailor information presented on digital platforms by drawing on large bodies of personal data, including existing information consumption patterns, geographic location, and demographics.[42]

This results in a media landscape in which individuals are locked into echo chambers and information loops that align with their preferences and are resistant to contrary views—a dynamic that aids radicalization, manipulation, and the

PHOTO SOURCE: PETER MACDIARMID/GETTY IMAGES FOR SOMERSET HOUSE spread of disinformation.[43] Further, encrypted messaging is becoming the norm for person-to-person or small-group conversations. As communications move beyond publicly available social media, efforts to prevent, observe, and disrupt influence operations become harder.[44] As one study notes, "fragmentation undermines the shared social institutions of information awareness that once provided the leading bulwark against disinformation and social manipulation."[45]

Finally, the Internet of Things (IoT) is dramatically increasing potential points of attack or intrusion into everyday lives. IoT refers to the expanding networks of "smart" objects—things with a unique identifier (an IP address) and connection to the internet—that are capable of sending and receiving information. It includes everything from mobile phones, watches, thermometers, and refrigerators, to streetlights, factory equipment, medical devices, and cars. IoT is often referred to as the next "mega-trend" in cyberspace, building upon decades of milestones in digital connectivity.[46] Advances in social media, data collection, and cloud computing are enabling the creation of networks with enormous numbers of interconnected objects that communicate among themselves.[47] As a result, IoT is predicted to have implications for economic growth and development across a range of sectors, including manufacturing, agriculture, transportation, and healthcare.[48]

Growing interactions with internet-connected devices mean there is also a dramatic increase in potential points of attack or intrusion in individuals' everyday lives. Objects in the IoT are by definition deeply interconnected; as a result, intrusions into IoT devices could provide points of entry into other parts of a network, as well as the data those devices collect, process, and relay elsewhere.[49] As the network of IoT objects becomes more expansive, with closer integration into industry, governance, and individual lives, opportunities grow for hostile interference into these systems. This interference ranges from obstruction of physical systems, such as industrial equipment or public utilities, to data theft and manipulation. Moreover, securing such systems is immensely complex as new devices and sensors are constantly being added to interconnected networks, opening new points of vulnerability to influence tactics.[50]

DIGITAL INFLUENCE TECHNOLOGIES

Against the backdrop of the evolving information ecosystem, new technologies for content creation and digital marketing may be adapted and deployed in service of influence operations, in the form of "precision propaganda."[51] Technologically advanced influence operations carried out by Russia, China, and others can exploit digital pathways to both precisely target individuals or specific groups and broadly message the general public in target nations. Taken together, these trends improve the speed, quality, penetration, deniability, and precision of influence operations by combining tried-and-true tactics with accessible new technologies.

Modern influence operations rely heavily on the connectivity of the internet and social media, where individuals and communities gather in virtual fora and where a constant stream of content reaches information consumers at lower cost and across a wide range of platforms and devices. Algorithmic techniques provide the ability to automate the processing and creation of data while also supporting precision targeting of specific segments of populations or certain individuals.[52] These operations can utilize existing trends in media dissemination that may be automated without a human driving each account. For example, the accessibility of the internet allows for misleading content to be introduced through a blog and then elevated to the mainstream. Meanwhile, rapid advancement in the manipulation of digital media makes it much more difficult to detect fabricated or adulterated content in text, image, or video.

Three broad categories of activity are being used by Russia and China to conduct influence operations against target populations: (1) content creation with artificial intelligence (AI) and machine learning (ML);[53] (2) the mapping of digital human networks and social structure;[54] and (3) adoption of online marketing and advertising techniques.[55] The spanning set of scenarios that look forward nearly 10 years into the future (see Appendix A for Russia-based scenarios and Appendix B for the China-based scenarios) incorporate these technologies in various ways, though Russia and China are actively exploiting each of these technologies in some way today.

Content Creation with Artificial Intelligence and Machine Learning

AI and ML may be used to both manipulate existing media and to create new media in support of influence operations. The sections below detail three areas used in influence operations in the digital era: deepfakes, cheapfakes, and language recognition and generation models. As researchers develop more sophisticated techniques, it is becoming increasingly difficult for human observers and even computers to detect manipulated and fabricated content. The battle between creation and detection technology in influence operations will intensify in the areas of photo, video, and text deepfakes and cheapfakes through the creation of false data or manipulation of information to distort the truth.[56] For these techniques, AI's ability to create synthetic media, such as deepfakes, will soon outpace its ability to identify that media, a gap that is expected to widen.[57] Thus, a reliance solely on AI-driven solutions to counter AI-created disinformation may be inadequate.

Figure 1 summarizes the technologies that may be used to create content for influence operations.

Deepfakes

Deepfake is an "umbrella term for visual and audio content that is manipulated or generated through the use of machine learning."[58] On the spectrum of audiovisual manipulation presented by Britt Paris and Joan Donovan, deepfakes are "both the most computationally reliant and also the least publicly accessible means of manipulating media."[59] The technique uses a type of ML called generative adversarial networks (GANs) to create content by pitting two neural networks against one another to generate or manipulate content. Given a set of training data (for example, photos of human faces), one neural network (the generator) creates content while another neural network (the discriminator) determines the authenticity of the new content based on the training data.[60] Described as a game, the generator "wins" when it creates a realistic instance of synthetic data, while the discriminator "wins" when it detects the synthetic data. The result is realistic content that is difficult to detect with the human eye, and sometimes with computers as well.

Deepfake photos of humans are used for a variety of purposes online—for example, to obfuscate identity for both malicious and benign purposes—and are readily accessible to the average user. For instance, the website This Person Does Not Exist compiles deepfake images of human faces that in fact do not exist.[61] Deepfake images are not limited to human faces. U.S. national security experts are concerned about the use of deepfake satellite photos to mislead a variety of actors, including decisionmakers, deployed military personnel, and the general public.[62] However, the most convincing content is currently relatively difficult to produce. For example, a widely circulated deepfake video of actor Tom Cruise required an experienced creator working with a convincing Tom Cruise impersonator, where "each clip took weeks of work . . . using the open-source DeepFaceLab algorithm as well as established video editing tools."[63] As James Vincent writes for The Verge, "creating the fakes took two months to train the base AI models (using a pair of NVIDIA RTX 8000 GPUs) on footage of Cruise, and days of further processing for each clip. After that, [the video creator] had to go through each video, frame by frame, making small adjustments to sell the overall effect; smoothing a line here and covering up a glitch there."[64] While such time and effort are not out of the realm of possibility for state and non-state actors, it means that convincing deepfakes, particularly videos, would likely need to be planned in

Figure 1: Content Creation with Artificial Intelligence and Machine Learning

Deepfakes

The use of machine learning and artificial intelligence for audiovisual manipulation and content generation to create realistic images, video, and audio that are difficult to detect as false by humans and computers.

Cheapfakes

The use of conventional audiovisual manipulation techniques, such as Photoshop, to generate or manipulate images, video, audio, or text in a manner that distorts or falsifies the original content's meaning and context.

Language Generation and Machine Translation

The use of machine learning and artificial intelligence to recognize, translate, and interpret human language and to generate realistic human-language content.

advance when incorporated into influence operations.

Cheapfakes

"Cheapfakes" or "shallow fakes" refer to conventional audiovisual manipulation techniques, such as Photoshop, to generate or manipulate images, video, audio, or text in a manner that distorts or falsifies the original content, meaning, or context. While cheapfakes are related to deepfakes, they are often of lower quality, faster, require less expertise to produce, and are therefore easier to detect. Cheapfakes may also include the recontextualization of content, such as posting an old photo with a misleading caption. In a recent example during the Covid-19 pandemic, photos that predated the Covid-19 vaccine trials depicting patients with a medical condition circulated on Twitter and Facebook alongside claims of side effects from Covid-19 vaccine trials.[65] Though the claim was quickly disproven through a reverse image search, the misleading content continued to spread through social media channels.

The motivation behind cheapfakes is often not to make a convincing case for false data but instead to provide quick, reactionary measures to distort the truth, cast doubt in the minds of an audience, and "flood the zone" with content before established media and authorities can respond. While deepfakes may be impressive in their quality, the ease with which cheapfakes can be created and the speed at which they spread make this technology a staple of influence operations.[66]

Language-Generation Models and Machine Translation

Natural language processing (NLP) is a discipline of AI dedicated to creating computer systems that can "read, decipher, understand, and make sense of the human languages."[67] It draws on the science of AI and ML as well as linguistics and computer science to recognize, translate, and interpret human language and to generate realistic human-language content. Some common examples of the use of machine translation and language generation are the Siri voice assistant on Apple iPhones and the Amazon Alexa virtual assistant.

However, while virtual assistants may be useful in everyday life, language generation models and machine translation capabilities are advancing in ways that may improve the quality of influence operations. Advances in machine translation have improved the quality of automated language translation capability, allowing users to translate between languages more accurately.[68] The most notable development in language generation was the publication of results from OpenAI's Generative Pre-trained Transformer 3 (GPT-3) language model in July 2020.[69] GPT-3 is a language model capable of producing realistic text content that is often difficult to distinguish as computer generated.[70]

Improving machine translation capability and language generation has the potential to reduce the language barriers in conducting influence operations in a foreign country. These capabilities may reduce the need for human translators. They may also allow for the generation of more realistic content in a target language, complicating detection systems that often rely on the mistakes in language or syntax that would not be made by a native speaker. However, because these developments are relatively new, it is unclear exactly how the advancement and spread of large-scale language models will impact influence operations.[71]

Mapping of Digital Human Networks and Social Structure

While social media platforms are places for people to gather, share personal anecdotes, and consume news, they are also data sources on human networks and social structures that may be exploited for influence operations. Social media sites document flows of information between individuals and groups as well as how actors, groups, and entities relate to one another.

Open-source analytic tools allow for an evolution of labor-intensive processes that influence operation practitioners would have had to manually conduct in decades past. For example, the Russian targeting of expatriate populations in the early 1920s required years of careful cultivation of human assets to influence and target specific groups, much of which was in person and required significant travel.[72] By contrast, through network analysis tools, sentiment analysis, and bot networks, adversaries can automate aspects of influence operations that were previously labor intensive. Adversaries can more deftly navigate through social media networks to reach influencers and groups, measure audience reception to adapt and refine content, and automate the spread of content to further the operation.

Figure 2 summarizes the technologies that may be used to map and visualize digital human networks and social structure.

Figure 2: Understanding Digital Human Networks and Social Structure

Network Mapping

The use of interactions and relationships on social media sites to map and visualize human networks and social structures to document flows of information and how actors, groups, and entities relate to one another.

Sentiment Analysis

The use of data from user interactions and posts about social media content to gauge feelings and sentiment regarding a product beyond metrics such as clicks or likes.

Bot Network

The use of a network of malware-infected computers and internet-connected devices to automatically collect information, post, or interact with content on social media and websites at the direction of a bot network operator or owner.

Network Mapping

For actors looking to better understand target social networks, network mapping provides a means to analyze and visualize the connections between accounts and groups within a network and the strength of those connections. While experienced computer programmers could create their own analytic tools, network analysis tools that can process social media data to map human connections and reveal information on influential individuals and groups are openly available.[73] For example, researchers at the University of Washington Seattle used these techniques and Twitter data to analyze and visualize the spread of disinformation on the platform, establish the network separation between different political groups in the United States, and identify influential users within networks.[74]

Adversaries could use network analysis to identify communities, such as influential accounts and information sources, and connectivity between individuals and groups, including polarization and information bubbles. Network mapping also automates the human labor required in previous decades of influence operations to probe, understand, and map networks to identify targets for desired effects and also improves the accuracy and scope of analysis.

Sentiment Analysis

Sentiment analysis processes the information and data in content, beyond metrics such as clicks or likes, to assess how audiences are thinking, feeling, and reacting at a given time. It includes the use of speech recognition and translation to automatically interpret human-language content. While sentiment analysis is used by advertisers to understand how consumers respond to products and content, sentiment analysis may also be used to further understand a specific audience, such as gauging trends in conversations and reporting.[75] Sentiment analysis tools are available openly or as paid services through companies that specialize in the technique. Sentiment analysis can be used in influence operations to further knowledge of target populations, assess emotions and reactions to certain topics, such as "hot button" issues in a population, and adapt and refine content as audiences respond to it.

Bot Networks

Bot networks are networks of malware-infected computers and internet-connected devices that automatically collect information, post, or interact with content on social media and websites at the direction of a bot network operator or owner. Bot networks are used in influence operations on social media to automate and amplify the spread of content by automatically posting content, following accounts of other users, interacting with content to boost impact, and acting as influencer accounts by gaining their own following.[76] While a bot is relatively easy to detect by social media users if the account was created recently and has a limited social network, bots become more realistic and convincing when combined with AI-content generation and experience gained from human actors.

Adoption of Online Marketing and Advertising Techniques

Online marketing and recommendations rely on ML algorithms to target content and product recommendations more precisely at individuals online based on user interests and attributes.[77] However, these techniques may also be exploited for influence operations to ensure content is viewed and spread. This "precision propaganda" is driven in part by the adaptation of online marketing and advertising techniques.[78] Through advertising and marketing capabilities available online, adversaries could take advantage of content recommendation engines, social media testing, and data-driven targeted advertising to ensure messages and materials in support of influence operations reach a receptive audience.

Figure 3 summarizes the online marketing and advertising technologies that may be used in influence operations.

Social Media Testing

Social media testing is the use of social media platforms to test marketing strategies and products by first assessing which content generates the most "clicks" or interest and then refining strategies and products based on the feedback. Social media testing is relatively accessible, including from a cost standpoint, either directly through social media sites or in coordination with firms that work with businesses or actors to create and execute testing strategies. Social media testing strategies could be used by adversaries who seek to systematically "improve" content in their influence operation campaign. For content that could be adapted to advertisements or business platforms, such as political advertisements, adversaries could use social media testing to increase engagements with content by measuring engagements, testing audience receptivity, and refining content accordingly.

Content Recommendation Engines

Content recommendation engines use ML and data about users' interests, past activity, and preferences to recommend relevant content. Social media platforms and third-party trackers use data of users' previous viewing and consumption habits to provide content to that user most likely to generate engagements (such as clicks, "likes," and reactions). For example, both Twitter and Facebook have implemented an "algorithmic timeline" feature that displays information based on user preference rather than showing posts in strictly chronological order.[79] On Twitter, research has shown that users are overwhelmingly exposed to political opinions that agree with their own preexisting beliefs.[80] Facebook's adaptive, ML-based algorithms display posts and advertisements based on highly specific predictions of what people are most likely to click on and share, predictions that are themselves drawn from extensive information of users' past activity on the site.[81] Moreover, several Facebook studies have apparently confirmed that its existing models increase polarization by elevating inflammatory, extremist content.[82]

Search engines are likewise not immune from exploitation. While Google makes active use of algorithms to influence search results, it does not publicly disclose metrics of its searches and rarely releases specific information on the frequent adjustments it makes to its immensely complicated search algorithms. Though Google asserts that its algorithmic solutions are designed to elevate breaking news and authoritative information sources, personal search history and prior search patterns are important factors in

Figure 3: Adapting Online Marketing and Advertising Techniques

Social Media Testing

The use of social media platforms to test marketing strategies and products by assessing which content generates the most "clicks" or interest and refining strategies and products based on the feedback.

Content Recommendation Engines

The use of algorithms to recommend content to users based on previous viewing and consumption habits to provide content most likely to generate engagements, such as clicks, "likes," reactions, and shares.

Targeted Advertising

The use of information about user attributes, behaviors, or geographic location ("geofencing") to tailor advertisements and content to maximize clicks and engagement.

search result generation.[83] Since content recommendation engines are designed to increase revenue by boosting user engagement, adversaries can exploit the algorithmic distribution system to ensure the spread of content during an influence operation by creating and disseminating content that users are most likely to react to, such as controversy, disinformation, and hate speech.[84]

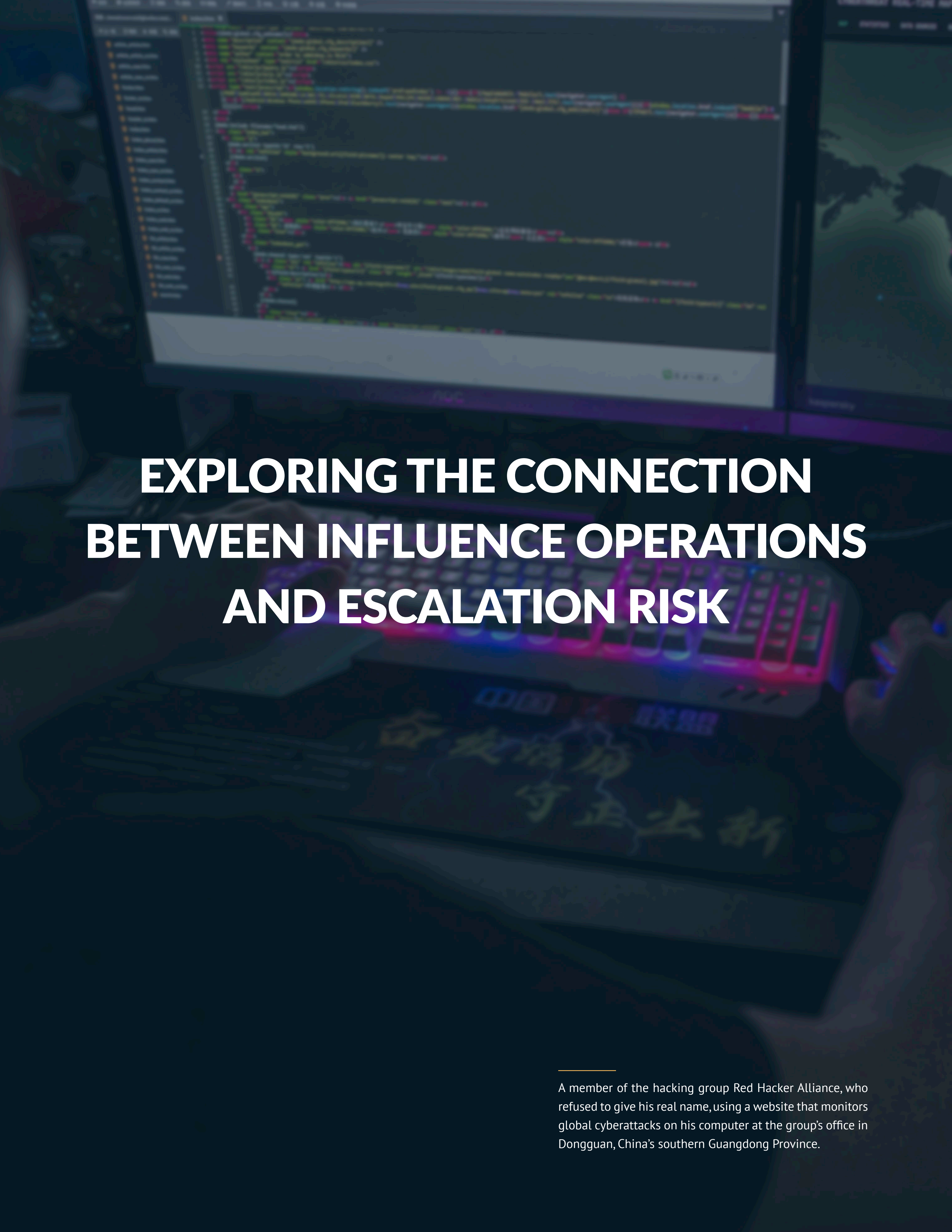
Targeted Advertising

Advertisers and social media sites use targeted advertising to tailor advertisements to maximize clicks and engagement. This approach takes the volumes of available data about user attributes, behaviors, browsing patterns, or geographic location ("geofencing") to determine which users see which content, with the goal of maximizing engagements and revenue.[85] Targeted advertising techniques may also be used in attempts to sway audience opinion instead of selling a product. Social media platforms provide advertisers avenues to use data collected on the platform, by the advertiser or marketer and by third-party trackers elsewhere on the internet, to computationally direct content to users in ways that users have little control over beyond large-scale online behavior modification.[86] Reporting on the Cambridge Analytica scandal demonstrates the possibility that social media data can be used to direct advertisements, political messaging, and other content.[87] Adversaries could use targeted advertising to increase the precision of influence operations by microtargeting specific audiences or populations.

TECHNOLOGY DEVELOPMENT MARCHES FORWARD

The digital content-generation capabilities discussed above are rapidly advancing in terms of the quality of content, reduced production time, and increasing availability and accessibility to a variety of actors. Influence operations are now tightly interwoven with the digital information environment, with a constant stream of content reaching information consumers through a wide range of platforms and devices. In the case of digital marketing and content recommendation, these technologies underpin the modern digital economy; they are "baked in" to the products and platforms used globally on a daily basis. In addition to functioning as a central mechanism for social connection and linking businesses to consumers, individuals increasingly rely on social media as a news source.[88] This reliance provides a ready pathway for adversaries to exploit human cognitive and social biases for modern influence operations, in addition to exploiting the technology itself.[89]

The myriad instances of misinformation spread during the Covid-19 pandemic and various attempts at election interference globally demonstrate that adversaries are increasingly turning to digital campaigns to gain an advantage in geopolitical competition. Indeed, a Facebook report notes that in the time span between the 2016 U.S. election that drew mainstream attention to the topic and the lead up the 2020 U.S. election, influence operations on the platform became more targeted, deniable, and technically obfuscated, as well as diversified across platforms.[90] While inspired by real-world events, the spanning set of scenarios discussed below serves as a mechanism to explore how the use of these technologies for influence operations may evolve. The scenarios also examine how these technologies and influence tactics may interact—sometimes in unpredictable ways—to create potential escalation risks.



EXPLORING THE CONNECTION BETWEEN INFLUENCE OPERATIONS AND ESCALATION RISK

A member of the hacking group Red Hacker Alliance, who refused to give his real name, using a website that monitors global cyberattacks on his computer at the group's office in Dongguan, China's southern Guangdong Province.

Influence operations pose significant challenges in times of relative peace by imposing costs, distracting decisionmakers, and sowing division and discord in ways that favor a perpetrator's strategic objectives.

However, the escalation risks associated with such activities may be underappreciated.[91] The scope, speed, penetration, and impact of digitally enabled influence operations exacerbate the understanding and communication of thresholds, limit recallability, and suggest the creation of security dilemma dynamics in ways that are poorly recognized.

Research to date has struggled to identify clear causal linkages between sub-conventional activities (e.g., cyberattacks), information weaponization, and military escalation. This apparent lack of causality has led some scholars to conclude that the risk of unintended escalation to military conflict via sub-conventional tactics is overstated.[92] However, most research has not fully appreciated what might happen if influence operations "succeed beyond their wildest dreams" and achieve an objective far faster and to an extent unintended by their executor, or converge with other actions and events (intended or not) that culminate in a "tipping point." Moreover, some research suggests that while escalatory risks of such sub-conventional tactics may be limited during periods of relative peace, their escalatory potential may increase significantly in periods of crisis or conflict when risks of misinterpretation or miscalculation may be higher.[93]

These tactics are especially problematic in crises between nuclear-armed states, as influence operations may undermine or stress states' abilities to clearly communicate their intentions and affect their capacity to "dial up" or "dial down" (e.g., military maneuvers, deployments, and diplomatic outreach)—actions that are important to both sides' escalation management. They could also prove particularly complex in managing third-party dynamics through allies and partners, especially given the speed and distribution advantages these tactics offer. Finally, patterns of escalation emanating from these forms of sub-conventional aggression may resist the step-based and comparatively linear progression of conflict so fundamental to the collective understanding of escalation risk and crisis management. Rather, future escalation pathways, fueled by the explosion in digitally enabled technologies and the pursuit of sub-conventional dominance, may follow decidedly discontinuous patterns and traverse through unexpected weaknesses in collective deterrence and defense.[94]

The risks of influence operations impacting escalation pathways are of particular concern as the speed, scale, and precision of influence operations increase and as adversaries become more adept at generating real-world, physical actions from primarily virtual tools. New digital technologies appear to hold the prospect of making influence operations faster, more powerful, more targetable, and more deniable—offering unprecedented levels of automation, scale, precision, speed, and perceived authenticity. Those greater impacts would seem to raise the stakes, and potentially the risks for escalation. Escalation risks may be further complicated when influence operations target third-party allies and partners in ways that may shift the balance of interests and complicate allied assurance efforts in the context of the perception and misperception challenges such scenarios can present.

ESCALATION PATHWAYS

Real-world cases of sub-conventional tactics—including influence operations—among nuclear-armed states leading to strategic escalation risks are, thankfully, limited. As such, clear causal linkages remain unproven. That said, as with so many aspects of strategic stability and deterrence, exploring theoretical pathways and gaming decisionmaking processes provide essential tools for informing an understanding of risk and offering techniques of escalation management. Anticipating such pathways and pre-positioning tools for

PHOTO SOURCE: NICOLAS ASFOURI/AFP/GETTY IMAGES

"The risks of influence operations impacting escalation pathways are of particular concern as the speed, scale, and precision of influence operations increase and as adversaries become more adept at generating real-world, physical actions from primarily virtual tools. New digital technologies appear to hold the prospect of making influence operations faster, more powerful, more targetable, and more deniable—offering unprecedented levels of automation, scale, precision, speed, and perceived authenticity."

transparency, communication, and response are essential for managing and reducing escalation risks, especially when a crisis or even a conflict is already underway and the likelihood of misperception may be significantly higher than in a pre-crisis environment.[95] The following six hypothetical escalation pathways are not exhaustive but offer a variety of conceptual paths by which escalation risks could be triggered by digital technology-enabled influence operations, especially when employed in periods of crisis or conflict. While each of these pathways is described as an idealized type, multiple, intersecting pathways would likely be engaged simultaneously in a real crisis scenario.

Too Big to Win: Russian and Chinese doctrines seek to achieve strategic outcomes without engaging in traditional forms of warfare, but assumptions about the non-escalatory nature of influence operations seem likely to falter when the stakes get too high and the targeted country is faced with a choice between capitulation and conflict. Influence operations that seek or achieve profound outcomes, such as annexation of sovereign territory, governmental coup, alliance collapse, or loss of strategic assets, infrastructure, or supply chains, may well trigger the rapid or asymmetric military escalation they sought to avoid. Strategic victory without consequences or risk of war may be an unrealistic and potentially dangerous objective, especially between powerful strategic competitors.

Catastrophic Success: What happens when a previously successful influence tactic or approach goes too far or backfires, unintentionally crossing an escalatory threshold? The lack of control or recallability of influence operations coupled with the potential virality of technology-enabled digital content could lead to sudden, unanticipated, and disproportionate effects. Escalation management requires that clear thresholds be known, communicated, and observed. And yet, the effects of digital influence operations may be particularly difficult to control or contain as such thresholds are poorly understood. Influence operations could inadvertently achieve unintended, excessive, or destabilizing effects with escalatory risks by inducing societal violence or disabling systems, institutions, or infrastructure. Confidence in the non-escalatory nature of past influence operations may encourage future risk or threshold testing, leading to unexpectedly escalatory outcomes.

Mercenary Effect: States often rely on nongovernmental or quasi-governmental actors to carry out influence operations in ways that expand reach and favor deniability, but which can also reduce control. Driven by competition for favor and resources as well as external interests, these "influencers for hire" may operate outside of governmental or military channels and with little appreciation of the strategic stakes or thresholds involved. Such forces often act according to, or are motivated by, their own proclivities and pathologies, which may not correspond to those of the sponsoring or encouraging state. These dynamics could make escalatory pressures difficult to recognize and hard to manage, especially as the interests of the state sponsor and the influence operator diverge. Moreover, once set in motion, these actors may be difficult to recall, redirect, or recalibrate regardless of their escalatory potential.

Disinformation Racing: It is possible that a country targeted by influence operations may seek to respond in kind and fight fire with fire, unleashing competitive dynamics and a potentially escalatory spiral. Once engaged in a series of increasingly risky "tit-for-tat" digital informational attacks, it may be difficult to define and anticipate the points at which the influencing stops and the shooting starts. Moreover, as parties competitively counter influence with influence and lies with lies, compounding effects could complicate the communications necessary for effective crisis management.

Intrusion Confusion: Given their relative opacity, obscured attribution, and distributed nature, detecting, scoping, and evaluating hostile influence activities may be very difficult, especially during periods of heightened conflict or crisis. Upon detecting influence activities, a country may struggle to determine the scope of an attack and the parameters of the intrusion, potentially ascribing motives and capabilities beyond what actually exist. By fueling perceptions of vulnerability and weakness, such operations may prompt more escalatory responses, especially given the heightened pressure to act that is often present at times of crisis.

Decision Disruption: Influence operations can complicate decisionmaking processes in the targeted state and disrupt crisis management in escalatory ways. For example, a subset of decisionmakers or actors within a wider political context may believe the disinformation disseminated by malign actors for influence purposes, exacerbating internal disagreements and delaying effective response. Such operations could also increase public demands for information and action from decisionmakers by leaking (or fabricating) sensitive information such as confidential policy documents, war plans, or internal communications. Finally, influence operations could complicate decisionmaking when the United States and its allies have a divergent understanding or interpretation of unfolding events.

These archetypal escalation pathways are designed to illuminate the ways in which influence operations, as tools of strategic competition in the sub-conventional domain, may pose new and complex escalation challenges between highly competitive powers. Through witting and unwitting proxies, these operations reach well inside a country's digital homeland and can strike at the heart of a country's institutions, values, and populations. In general, it seems that the escalatory risks associated with adversary influence operations are directly linked to four primary factors:

- **Context:** What other geopolitical factors are shaping the way an influence operation is being perceived and interpreted? Are other hostile actions or behaviors accompanying the influence operations? Are events unfolding in a period of relative peace, crisis, or conflict? Influence operations can be expected to complicate crisis decisionmaking and management by eroding confidence in public information, undermining decisionmaking processes, and complicating crisis communications. The context in which they occur will substantially impact their escalatory potential.
- **Control:** How much direct control does the state have over these activities? Can it reasonably expect to recalibrate operations that prompt escalatory risk? Are these activities recallable or is this a fire-and-forget operation for which there is little control once the operations are initiated?
- **Consequences:** What are the stakes associated with the operation and the magnitude of potential consequences, either deliberate or inadvertent? Are the fundamental interests of the targeted nation under attack? If so, then the risk of escalatory response is heightened. Are the effects sudden, widespread, and disproportionate? The responses may be likewise.
- **Complexity:** Are these largely bilateral operations involving two competing states or are they instead unfolding on a multilateral basis across multiple regions, states, and organizations simultaneously? Given the additional points of vulnerability, broader attack surface, and complex multi-nodal crisis management requirements, alliances may be especially vulnerable to influence operations that seek to sow division, confusion, and disarray while simultaneously constraining response options for individual states.

A SCENARIO-BASED APPROACH

While some studies have attempted to better understand the role of influence operations on security issues, few efforts have focused on how influence operations might be used in times of crisis between nuclear-armed states, especially in terms of the reliability and credibility of extended deterrence relationships.[96] Even in cases where influence operations may not produce direct nuclear risks, actions that could trigger the risk of military confrontation and escalate conflict between nuclear-armed states will always include the specter of nuclear miscalculation, nuclear coercion, or even nuclear use—an inevitable nuclear shadow. As such, any state of crisis or conflict between nuclear-armed adversaries can invoke escalation risks and raise the stakes and complexity associated with influence operations.

Moreover, the range of nuclear crisis scenarios today are larger, more complex, and of longer duration than the classic launch-under-attack scenarios that drove plans and requirements in years past. A sudden or "bolt from the blue" crisis might leave little time for influence operations to achieve desired effects. However, in reality most crises occur over longer periods of time, across a broader range of the conflict spectrum, and with more extended periods of ambiguity. These scenarios could unfold under a broad range of timelines and circumstances, leaving plenty of opportunity for an adversary to employ information-based attacks to greater effect.

> *"Even in cases where influence operations may not produce direct nuclear risks, actions that could trigger the risk of military confrontation and escalate conflict between nuclear-armed states will always include the specter of nuclear miscalculation, nuclear coercion, or even nuclear use—an inevitable nuclear shadow."*

And yet, with limited historical case data, opportunities for rigorous and realistic analysis of the escalation pathways explored above and their implications for crisis decisionmaking are limited. To address this challenge, this study developed a spanning set of eight scenarios—four in a Russia/Europe context and four that focus on a China/Asia context.[97] The scenarios are designed to be thought provoking and illustrate a range of underappreciated circumstances in which influence operations may complicate crisis management between the United States (and its allies and partners) and Russia or China. In addition, they are designed to capture a diverse range of factors to test potential escalatory dynamics and identify areas of concern for further study and analysis. These factors include:

- **Intensity:** Influence operations could have different escalatory potential based on the temporal level of background intensity.[98] Whereas a particular influence campaign may have moderate effects during peacetime, it is possible that the same measures during a time of crisis or conflict could tip the scales and prompt further escalation. For each region, at least one scenario examines a situation in which the influence activities trigger some kind of crisis event in and of themselves. The others consider the use of influence operations when crisis or conflict is already underway.
- **Alliance Dynamics:** Influence operations have long targeted perceived vulnerabilities in U.S. global alliances, seeking to drive a wedge between the United States and its allies and partners. Several scenarios across both the Russia- and China-focused sets explore the challenges future influence operations may pose for U.S. alliance management in high-stakes crises.
- **Operational Concepts:** Scenarios examine the implications of a range of potential tactics as they may be employed in a digital information environment—from hack and leak operations and forgery to complex microtargeting, extortion, and intimidation campaigns.
- **Technical Tools and Digital Influence Technologies:** The scenarios incorporate a set of digital technologies that are either actively being exploited by adversaries for influence or are poised to introduce a new capability to the influence operation tool kit.

These scenarios or vignettes cannot inherently determine or validate escalation risks associated with influence operations, but they can be used to guide discussions and cultivate new strategic concepts among decisionmakers and analysts. As such, the scenarios help to tee up the complex interface between influence operations and crisis management and identify potential escalatory risks and pitfalls. They do not predict or anticipate specific escalatory steps, which might result in over-steering toward high-risk, but not necessarily inevitable outcomes. Rather each scenario suggests a plausible crisis or conflict context in which technology-enabled influence operations could take on added significance; employs a range of influence targets, tools, and concepts that might confront decisionmakers in a crisis; and proposes a series of decision points or questions that will challenge decisionmakers to adjudicate escalation risks in the course of crisis decisionmaking. Throughout, the escalation pathways described above offer considerations and potential risks that should be accounted for in the decisionmaking process in ways that may differ from the more ladder-like approaches offered by traditional deterrence and escalation theory. Still, more work is needed to advance scenario development and related war-gaming to account for different types of triggers and the potential for multifaceted, horizontal escalation challenges in crisis that primarily unfold below the level of conventional armed conflict.

To ensure plausibility and technical feasibility, each scenario underwent a detailed review by outside technical and regional experts.

> *"The scenarios help to tee up the complex interface between influence operations and crisis management and identify potential escalatory risks and pitfalls."*

Figures 4 and 5 summarize the key components included across the Russia- and China-focused scenarios. Each scenario is elaborated on in Appendix A and Appendix B, respectively, to include background contextual information and a detailed "key events timeline" summarizing influence efforts and the key digital influence technologies employed. They are followed by relevant decision points for policymakers.

OVERVIEW OF THE RUSSIA-BASED SCENARIOS

Across the Russia-based scenarios, influence operations are utilized to interfere with the ability of the United States and NATO to respond to Russian actions and advance its broader objectives vis-à-vis Europe and the United States.

In the first scenario, increased Russian interference in Ukrainian elections spurs renewed calls for Ukraine to join NATO. Meanwhile, NATO uncovers a highly aggressive digital blackmail campaign targeting senior officials from an anonymous group calling into question how the alliance should respond to the intrusion and events in Ukraine and sowing divisions across NATO allies. This scenario incorporates influence tactics, such as forgery, coercion and intimidation, and microtargeting, and elements of the "Intrusion Confusion" pathway to show how difficulties identifying the scope, source, and motives of an intrusion could present escalation risks.

In the second scenario, seeking to distract from civil unrest and respond to perceived U.S. interference, Russia mounts a complex, covert influence operation that exploits existing social and political cleavages in the United States and Europe. As online speech migrates to physical violence, pressure mounts on U.S. policymakers to attribute responsibility to Russia and to forcefully respond. This scenario features flash mob and flood the zone tactics while also testing the lower bounds of what constitutes "Catastrophic Success" as likely Russian-instigated misinformation and hate speech begins to inspire physical attacks.

In scenario three, Russia exploits growing anti-nuclear sentiment among U.S. allies—including through leaking falsified information—to suggest flaws in the new U.S. nuclear command, control, and communications (NC3) system could lead to accidental nuclear use. With the assistance of Russian bots and other social media techniques, the information proliferates into the mainstream and is picked up by anti-nuclear organizations and others critical of U.S. nuclear weapons—intensifying calls among some NATO allies to abandon nuclear sharing arrangements. This scenario uses influence tactics such as forgery, elite and media co-optation, and flood the zone. The potential impact of the influence operations on the U.S. nuclear deterrent and NATO, and the fact that some U.S. lawmakers and allied officials believe the disinformation, draws on the "Too Big to Win" and "Decision Disruption" escalation pathways.

In the fourth scenario, aggressive behavior by a Russian aircraft results in a crash and the death of a Norwegian and Russian pilot. Russia releases manipulated footage of the confrontation and pushes its narrative, shifting blame for a fatal accident onto the Norwegian pilot and prompting a crisis within NATO over how to respond. This scenario, using elements of the "Decision Disruption" pathway, demonstrates how even relatively unsophisticated influence operations, once picked up and magnified in the media cycle, can be difficult to correct and may drive U.S. and allied government response times.

OVERVIEW OF THE CHINA-BASED SCENARIOS

In the China-based scenarios, China utilizes a range of influence tactics to distract from domestic issues while also trying to increase the costs of responding to crises for the United States or its allies.

In scenario one, facing growing criticism of its human rights abuses, China responds with a multifaceted influence campaign using tactics such as forgery, coercion and intimidation (including doxing), and elite and media co-optation in an attempt to boycott U.S. companies, force sympathetic politicians in the United States, Europe, and Asia to adopt pro-China narratives, and intimidate journalists. As Congress and allies pressure the U.S. administration to respond, decisionmakers face choices about whether and how to out China's role ("Intrusion Confusion") and whether to respond with their own cyber measures ("Disinformation Racing").

In the second scenario, as tensions increase between Taiwan and China in the Taiwan Strait, Beijing leaks forged documents and audio intended to undermine Taiwan's confidence in the United States and raise U.S. concerns that Taiwan seeks to entrap the United States in a conflict. Meanwhile, Taiwan mounts its own lobbying effort to enlist U.S. support while planning its own cyber operation against China. This forces difficult decisions on U.S. policymakers about how to coordinate a response with Taiwan without triggering further escalation. This scenario draws on the "Decision Disruption" and "Disinformation Racing" escalation pathways.

In the third scenario, China forges evidence of a cover-up of a newly discovered mass grave of Korean "comfort women," reigniting long-standing South Korean-Japanese tensions—which Chinese-linked actors amplify. This puts a halt to growing trilateral cooperation between the United States, Japan, and South Korea and strains their ability to respond to Chinese aggression near the Senkaku/Diaoyu Islands. This scenario draws on the "Mercenary Effect" to show how influence operations initiated through official diplomatic social media and state-directed sleeper cells can spread beyond government direction into protest and social media campaigns coordinated through private citizens' networks.

Finally, in the fourth scenario, China manipulates and fabricates evidence to suggest that India instigated a deadly confrontation along the Line of Actual Control (LAC). A likely Chinese influence campaign to put pressure on the Indian government to capitulate backfires, further raising tensions and sowing discord among members of the Quadrilateral Security Dialogue ("the Quad") as to how they should respond to India's appeals for support. In this scenario, China employs a variety of influence tactics, including forgery and sophisticated coercion and intimidation methods, designed to fracture Indian support for a conflict with China. When this backfires, the "Too Big to Win" and "Catastrophic Success" pathways become triggered, risking an intensification to wider war.

Figure 4: Russia-Focused Scenarios

SCENARIOS

FACTORS

	NATO Extortion Campaign	Promoting Extremism	Nuclear Crisis of Confidence	Deconfliction Breakdown
Spectrum of Conflict and Context	**Competition** NATO-Russian tensions are rising and high-profile instances of Russian interference in Ukraine have led to renewed calls for NATO membership.	**Competition** Following an illegitimate election in Russia, large protests erupt across major Russian cities, with Russian officials alleging Western governments are stoking unrest.	**Competition/Crisis** Russia is fielding high-threat nuclear systems following the expiration of New START. The International Campaign to Abolish Nuclear Weapons (ICAN) is gaining popularity in Europe.	**Crisis/Conflict** NATO and Russian military exercises are occurring near one another in the Arctic. Norwegian and Russian pilots die following aggressive maneuvers from a Russian MiG fighter near a Norwegian F-16.
Russian Objectives	**(1)** Influence debate on Ukrainian calls for NATO membership; **(2)** foment division within NATO; **(3)** create distrust in internal communications and networks.	**(1)** Distract from internal unrest and illegitimate election practices; **(2)** exacerbate unrest and internal division in Western countries.	**(1)** Leverage ICAN movement to drive a wedge in NATO; **(2)** achieve strategic military advantage by encouraging anti-nuclear sentiment in Europe and the United States.	**(1)** Deny responsibility for the crash and portray Norway as the aggressor; **(2)** delay or prevent collective response through NATO.
Influence Tactics/ Key Events	Senior NATO officials reveal aggressive anonymous digital bribery, extortion, and manipulation attempts; investigations reveal a massive intrusion by an SVR intelligence unit, of unknown scope.	Hate-inspired vandalism across the United States prompts protests across several major U.S. and European cities; anti-hate groups call for counter protests across the United States and Europe; an active shooter event occurs.	Forged correspondence between Defense Department officials is leaked detailing risk of unintentional nuclear launch; activist protests occur across Europe.	Doctored video from MiG camera depicts aggressive maneuvers from the Norwegian fighter; deconfliction communications break down; Russia teases a "grand reveal" of evidence that will prove Norway is at fault.
Critical Technologies	Creation of comprehensive digital profiles of several prominent U.S. and NATO officials; comprehensive computational propaganda and bot direct messaging campaign.	Network mapping to identify influential figures in far-left and far-right movements; deepfake videos from key figures; spread of conspiracies and operational protest instructions through encrypted messaging apps.	"Constituent calls" targeting Congress (fabricated AI-generated audio bots); geofenced ad campaign in Washington and European capitals.	Social media sentiment analysis; computational propaganda bots and human-operated accounts inundating Twitter and the comment sections of Facebook posts, YouTube videos, and online news articles.
Alliance Challenges	Navigating multiple national-level investigations into intrusions; coordinating response to extortion attempts with NATO allies.	Working with European partners and determining an appropriate role for NATO to address aggressive domestic interference.	Engaging with allies on declaratory policy amid political fallout of influence operations, including in NATO and other multilateral fora.	Balancing divergent response preferences among NATO allies, whether immediate punitive action or de-escalation until end of investigations.
Critical Decision Point(s)	What immediate steps should be taken by member states and the secretary general vis-à-vis Russia in response to its intrusion, intimidation, and extortion attempts, if any? How should the United States navigate the investigation into Russia's manipulation, given trade-offs between transparency and loss of public confidence?	Should the United States consider the incident an armed attack, given the possibility of Russian involvement or instigation even if not directly responsible for the attack and subsequent loss of life? Should it prioritize collective action through NATO or focus on a unilateral response?	What immediate steps should the United States take to punish Russia for its actions (e.g., sanctions, release of incriminating information)? Should it classify the influence campaign as an attack on the National Coalition of Certification Centers?	Should the United States take immediate action to support Norway or instead pursue a collective response through NATO, given some members' preference for a less assertive or immediate response?

Figure 5: China-Focused Scenarios

SCENARIOS

FACTORS

	Counterinfluence Campaign	Cross-Strait Encroachment	Alliance Cohesion in Asia	Line of Actual Control Border Tensions
Spectrum of Conflict and Context	**Competition** Investigative reports detail human rights abuses and extrajudicial killings in Tibet, creating renewed international momentum to punish China.	**Crisis** PLA assets are increasingly entering Taiwan's airspace and territorial waters. Taiwan's DPP-led government calls on the United States to provide diplomatic and military support.	**Crisis/Conflict** Growing U.S.-ROK-Japan coordination is increasingly viewed in Beijing as anti-China collusion. PLA forces clash with Japanese forces on the Senkaku/Diaoyu Islands.	**Crisis/Conflict** Amid Indian general elections, Sino-Indian border incident leads to casualties on both sides. U.S. intelligence is inconclusive on which country instigated the confrontation.
Chinese Objectives	**(1)** Distract the international community from human rights abuses; **(2)** intimidate and dissuade governments from sanctions or other punishments.	**(1)** Dissuade U.S. involvement in the intensifying crisis; **(2)** portray U.S.-Taiwan aggressive intent.	**(1)** Inhibit a trilateral response to escalating tensions; **(2)** instigate historical animosity between Japan and ROK; **(3)** eclipse maritime confrontations.	**(1)** Portray India as aggressor of border incidents; **(2)** foment division inside India; **(3)** avoid larger conflict.
Influence Tactics/ Key Events	Officials encourage boycotts of Western brands; legislators in Europe are blacklisted; efforts to amplify U.S. hypocrisy on human rights and intimidate journalists increase; "peace advocates" mobilize in Europe.	Forged Taiwan Ministry of National Defense Department policy paper requesting U.S. support is leaked; competing influence efforts by China and Taiwan drive heated debate in the United States; cognitive warfare campaign is prosecuted on Taiwanese population.	Officials disclose forged evidence of Japanese cover-up of WWII atrocities, prompting mass protests in ROK and Japan; Beijing threatens economic penalties on ROK if it does not stay neutral.	Real and fake video depicts Indian aggression at border; disinformation campaign implies Indian instigation for political purposes; India appeals to partners to confirm its narrative.
Critical Technologies	Human network analysis techniques to micro-target influential legislators to sway elite opinion; geofenced targeting of Congress and EU Parliament.	Deepfake audio portraying Taiwanese officials' discussions in favor of entangling the United States in conflict; coordinated interjection of content into Taiwanese debate.	"Sleeper cell" bots; network analysis to identify influential activists; doctored photos of Japanese military buildup on Senkaku/Diaoyu.	AI-generated audio implicating India; use of encrypted messaging platforms to disseminate "evidence" and organize protests; use of stolen cell phones of Indian soldiers to generate misleading data.
Alliance Challenges	Countering China's efforts to drive a wedge between the United States and allies; coordinating an effective allied response.	Working with regional partners (including Taiwan) to address unfolding crisis amid heated U.S. domestic debate.	Protecting trilateral progress in security cooperation and in response to the crisis, despite renewed tensions.	Affirming support for India while also coordinating with regional partners to stabilize the situation.
Critical Decision Point(s)	Should the United States and allies pursue responses that may promote tit-for-tat escalation dynamics (e.g., sanctions on Chinese officials, diplomatic expulsions, counter-influence strategies) or prioritize de-escalation?	Should the United States counter the influence campaign with one of its own, immediately reject the memo's authenticity, or ignore it altogether? Who, if anyone, should it blame for the forgery if its source is initially inconclusive?	Should U.S. decisionmakers prioritize trilateral coordination, both in response to the influence campaign and to PLA-Japanese clashes, if ROK prefers a more conciliatory approach to the crisis?	What strategies could help reduce disinformation racing in the crisis—should the United States publicly support the version of events put forward by India or instead aim to diffuse tensions?

KEY FINDINGS AND RECOMMENDATIONS

In this handout photo provided by the White House, President Joe Biden meets with his national security team for an operational update on the situation in Afghanistan.

KEY FINDINGS

1. **Influence operations will continue to rely primarily on tried-and-true tactics and remain mostly the prerogative of state-based actors.** The core tactics of state-based influence campaigns—for example, forgery, hack and leak, and co-optation of the media—and their overarching goals have not changed. Information-based influence operations still seek to promote division and disruption, drive wedges between allies, and exacerbate internal tensions within adversary societies—all with the objective of advancing state interests short of the use of force. State-based actors, at times relying on or employing non-state groups or organizations, will likely continue to be uniquely capable of effectively leveraging the information environment-related technologies to effectively prosecute influence operations—a result of advanced intelligence collection, extensive resource allocation, and motivation.

2. **However, the new digitized information environment that permeates every facet of society, along with emerging digital tools to take advantage of that environment, is increasing the speed, precision, and scale with which influence campaigns can reach and manipulate their desired targets.** It is unclear how the influence objectives of adversaries may change as manipulation efforts become cheaper, wider spread, and potentially more effective. New technologies may eventually give rise to truly new influence operation tactics.

3. **That same speed, precision, and scale—and the novelty of some of these technologies—suggest that future influence operations and their effects may be harder for their executors and their targets to predict and control.** Compounding this challenge is the tendency of state-based actors to innovate and try multiple tactics to "see what sticks" and to rely on actors only loosely affiliated with the government that can be harder to control. In this environment, it may be difficult for countries to attribute influence operations and to know their own red lines in advance, let alone identify what actions might cross them. This could make escalation and crisis management more challenging for the United States, its allies, and adversaries.

4. **The web of U.S. alliances creates a larger attack surface for malign actors to exploit in an attempt to degrade alliance cohesion.** Just as the U.S. alliance system (along with open debate and the free flow of information) constitutes the country's greatest asymmetric advantage over its strategic competitors, it is also a key vulnerability, compounding the challenges information-based influence operations pose to open, democratic countries. Alliance cohesion requires constant attention and tending and, as a result, provides a relatively high-value, low-cost target for disinformation efforts both during times of relative peace and in crisis or conflict.

5. **Democratic governments may have few authorities to directly counter and put an end to adversary influence operations during a crisis because private sector platforms serve as the primary conduit for information and content.** While the United States and allied governments may seek to be active players in the information environment during a crisis, decisions on what information remains on platforms and who sees it ultimately reside with private sector companies.

6. **While technology can help the United States detect and respond to disinformation operations and their associated challenges, the U.S. government cannot rely solely on technical solutions to combat influence operations.** In the cat and mouse game of generation and detection, both academic and private sector organizations continue to develop AI technologies to detect deepfakes and AI-generated language in particular. In turn, adversaries will continue to adapt to U.S. efforts to detect and counter influence operations. Language-generation models continue to improve, reducing the ability to detect foreign context through grammar mistakes and misuse of colloquialisms. Cheapfakes spread at a rate faster than automated detection and content moderators can respond. Media literacy and civics education may prove to be more worthwhile long-term investments to make a population resilient against foreign influence.[99]

7. **Greater coordination between Russia and China on influence operations would pose significant challenges for the United States and its allies and partners.** Given growing similarities in information-based and narrative manipulation tactics between the two countries (even if, at present, this is mostly tacit alignment rather than express cooperation),

PHOTO SOURCE: THE WHITE HOUSE VIA GETTY IMAGES influence perpetrators may find utility in cooperating directly or indirectly to amplify the other's influence campaigns, weaken alliance cohesion, and cast doubt on Western values and systems of governance. At a minimum, Russia, China, and other U.S. adversaries will learn from one another to refine influence efforts and gain a stronger understanding for situations in which they can create tactical or strategic advantage. For example, if Russian influence efforts (including their operational concepts, employment of digital influence technologies, and perhaps even objectives) prove effective in the context of Ukraine, it may inform strategies chosen by China in a Taiwan Strait crisis. More formal cooperation between Russia and China—particularly on sensitive influence operations—may prove more challenging.

RECOMMENDATIONS

1. **Gaming and exercising by the U.S. government and nongovernmental organizations (NGOs) are essential tools to anticipate potential influence operations and recognize attendant escalation and crisis management risks.** Exercising these scenarios can help decisionmakers better understand the risks, identify techniques for escalation management, pre-position essential capabilities to detect and attribute such campaigns, and share required information with the public, government leaders, and foreign partners. Interagency bodies such as the National Security Council would be well suited to carry out such exercises.

2. **The United States and its allies should create a "crisis playbook" standardizing coordination procedures to synchronize responses to short-term tactical information operations.** This should include coordination with the NGO community and other mainstream sources of information. Such preparation would involve developing shared terminology and establishing channels to proactively disseminate authoritative information. The United States should use the process of creating this "playbook" to spark conversations with allies about longer-term adversary influence operations and how to counter them. The forum for such discussions may vary depending on the ally. For example, NATO may be an appropriate starting point for the United States and many European allies; for other alliances in East Asia, bilateral relationships and interagency teams led by the U.S. Department of State may be more appropriate.

3. **The National Science Foundation (NSF) and Defense Advanced Research Projects Agency (DARPA) should direct research investment into digital defense technologies that can enable timely and accurate detection of dangerous AI-created content such as deepfakes and forged or false information.** While content detection and removal are not the sole solutions, rapid detection and attribution of false content is an essential component of a comprehensive strategy to address disinformation and misinformation online. Targeted countries need to break the viral cycle and expose false content and its originators quickly.

4. **The U.S. intelligence community, in cooperation with the Departments of Homeland Security and Defense, should invest in capabilities to monitor the information environment in real time and build the capacity to disseminate information and coordinate across agencies and departments quickly.** While some U.S. government organizations are investing in monitoring capabilities, efforts are frequently siloed to special units.[100] Given the speed at which influence operations take hold in the digital era, both robust monitoring capabilities and responsive coordination mechanisms are necessary to quickly identify operations, disseminate information to stakeholders, and coordinate responses.

5. **The United States should synchronize its understanding of adversary information operations with allies, as well as clarify the risks and benefits of different approaches to deterring, combating, or countering such efforts.** There are risks of incongruity in conceptual understandings of how to define and address the information challenge. Identifying and addressing any differences before a conflict is key to better coordination during a conflict. Again, the forum in which this takes place will depend on the relationship: it may be led by the Department of State, Department of Defense, the intelligence community, or some combination thereof.

6. **The Office of the Director of National Intelligence (ODNI) and Department of Homeland Security Cybersecurity and Infrastructure Security Agency**

(CISA) should implement public-private partnerships to create emergency coordination mechanisms and disinformation containment actions when public health, security, or safety is at stake. The equivalent of a Wall Street "circuit breaker" but for mainstream social media could be one approach. Covid-19 and rampant disinformation associated with the source of the outbreak, the efficacy of public health measures, and the safety of vaccines have spurred a willingness among social media giants such as Facebook and Twitter to finally engage disinformation on their platforms more aggressively. These efforts should provide a basis on which to develop more effective coordination mechanisms.

7. **The executive branch and Congress should prioritize initiatives to enhance societal and institutional resiliency.** Enhanced education and preparedness—through training, exercises, and establishment of clear protocols—are essential to improving crisis management and decisionmaking. The United States and its allies will also be more capable of dissuading the use of these sub-conventional tactics and operations if they demonstrate that such operations can be effectively detected, attributed, and countered. Enhanced recognition and awareness of foreign manipulation of information, including digital content, cannot just be the responsibility of the government or media institutions. An informed citizenry is essential. Digital disinformation defense must become a routine element of being online, much the same way that internet safety and cybersecurity practices are staples of the digital workplace today. The diverse array of agencies and authorities involved would make the National Security Council an ideal organization to coordinate such an effort.

Appendix A

RUSSIA-FOCUSED SCENARIOS

Scenario 1

NATO EXTORTION CAMPAIGN

INTENSITY OF CONFRONTATION
Competition/Relative Peace

Background Context

It is 2030, and NATO-Russia tensions are rising in Eastern Europe. In recent years, high-profile instances of attempted Russian interference in Ukrainian elections have renewed calls within Ukraine to seek NATO membership. Many NATO members along the alliance's eastern periphery, with strong encouragement from several prominent U.S. politicians, are seeking a clearer commitment from both the United States and the NATO alliance to oppose Russian aggression in the region. But a growing chorus of member states, quietly supported by Germany and France—both of which have elected left-leaning governments—are pushing for a more conciliatory, cooperation-based agenda with Russia and renewal of the NATO-Russia Council.

Key Events Timeline

- In the last two weeks, three senior officials from the United States, United Kingdom, and Germany stationed at the NATO mission in Brussels have publicly revealed that they have been targeted with highly aggressive digital bribery and blackmail attempts from an anonymous activist group that calls itself "Europeans for a Peaceful NATO." The perpetrators have demonstrated that they have access to detailed personal information, including security clearance investigations as well as private email and WhatsApp communications.

- The individuals report being inundated by cryptic direct messages to personal accounts on Twitter and Facebook revealing personal information and internal communications, as well as an uptick of spam-like messages and follow requests from AI-enabled bots. In the following days, damaging and detailed personal information associated with the officials who came forward begins trickling out. Despite the strong potential that this information is false or misleading and deliberately "leaked," traditional and social media coverage raises questions about the integrity of NATO personnel. This discourages others who were targeted from coming forward about similar extortion attempts.

- In the immediate aftermath of the revelations, several stories across traditional news outlets in Europe and the United States discuss the alleged perpetrator, "Europeans for a Peaceful NATO," before evidence emerges of more comprehensive state-connected activity.

- A preliminary investigation suggests the problem runs much deeper, stemming from a massive cyber intrusion by a Russian Foreign Intelligence Service (SVR) unit that enabled Russian access to hundreds of government and private networks, including classified NATO networks. The investigation further suggests that the access and apparent activities of the intruders could have led to the creation of comprehensive digital profiles of several prominent

U.S. and NATO officials. The full scope of the intrusion and extent of compromise among national delegations and the international staff is not yet known.

- NATO has condemned Russia for its actions and launched an investigation in an attempt to understand who has been targeted and where such targeting efforts might have succeeded. It is still unclear how much information was compromised, for how long, and how many individuals have experienced similar microtargeting operations. Multiple national-level investigations are now underway as well.
- Senior Russian officials asked about the intrusion have denied any involvement while commending the work of "peace-loving Europeans unwilling to stand idly by in the face of NATO aggression."
- An emergency meeting of the United States, United Kingdom, France, and Germany is currently underway in London. Early reports suggest that the meeting is not going well. The United States, United Kingdom, and Germany have proven reluctant to fully share details of their internal investigations. In heated discussions, U.S. and British representatives have suggested that calls by prominent French and German officials in Brussels for greater cooperation with Russia could be the result of compromise or bribery.
- An emergency meeting of the North Atlantic Council is scheduled for later this week to discuss the cyber intrusion and escalating tensions in Ukraine.

Critical Decision Points

- Should the Russian activities be classified as an intelligence operation or an attack? Did the cyber intrusion cross a red line, or was it the theft and use of the information? Does the attack, if proven to be perpetrated by Russia, rise to the level of an Article 5 response?
- Should the results of the U.S. investigation into the Russian intrusion, including the extent of U.S. compromise, be shared with allies and NATO staff? To what extent should that information be made public?
- In addition to condemning Russia's operation, what collective steps should NATO undertake immediately?
- Should the United States undertake unilateral measures in addition to or in place of NATO action? For example, should it impose sanctions on involved Russian entities or increase its military assistance to Ukraine?
- How should targeted individuals be investigated and treated? Should they be allowed to remain in their posts while investigations are ongoing? Should responsibility fall to individual nation states or to the alliance system collectively?

Scenario 2

PROMOTING EXTREMISM

INTENSITY OF CONFRONTATION
Competition/Relative Peace

Background Context

It is April 2030, and Vladimir Putin has won a sixth term in office. International election watchers, as well as the United States and European Union, condemn the government for alleged ballot stuffing, disqualification of key opposition candidates, lack of press freedom, and the continued imprisonment of vocal Putin critics. In recent weeks, large protests have erupted across major Russian cities. State-aligned media and senior Russian decisionmakers allege Western governments are stoking the unrest. Russian claims of foreign interference dominate state-affiliated media outlets, joined by a growing chorus of opinion writers sympathetic to Russia's views, who suggest that the United States lives in a "glass house" and should tend to its own internal human rights and social justice problems.

Key Events Timeline

- A recent spate of hate-inspired vandalism targeting Jewish communities and communities of color across the United States has prompted outrage among politicians and renewed national-level protests across several major American cities. At the same time, propaganda by "white power" groups and their supporters—including several dramatic "call to action" videos—have proliferated across niche platforms such as Parler, Gab, and 8-Chan; specialized media outlets; private groups on Facebook normally out of sight from mainstream view; and encrypted end-to-end messaging apps.

- A variety of social justice and anti-hate groups have called for a March on Washington in opposition to the rise of domestic hate-based crimes and threats across the United States. The FBI has discovered widespread calls by far-right figures on various online messaging apps proposing a counter-call to action against "foreign-inspired socialists." These calls have been amplified by—and in some cases appear to have originated from—AI bots of unclear origin and Twitter accounts geotagged in foreign countries.

- In recent weeks, similar events have occurred in Hungary, Poland, Germany, and France. Work stoppages, strikes, and traffic disruptions allegedly coordinated and publicized in part by foreign organizers and social media accounts have prompted a violent backlash. Protests from ideologically opposed organizations on the far right and far left were frequently held on the same date and time and in close physical proximity, amplifying the risk of violence. Investigations by intelligence and law enforcement organizations in these countries have revealed that publicity campaigns for both the violent right-wing protests and workers' protests had in fact been organized by foreign nationals posing as citizens and not by members of the respective organizations in those nations.

- Interviews with some protesters in Europe reveal highly specific instructions to protest and commit violent acts, as well as a widespread belief of elaborate far-right conspiracy theories that are largely untraceable on public platforms—likely a result of increasing reliance on end-to-end encrypted messaging apps to organize rallies and disseminate information. While some accounts calling for physical violence are being removed once reported, the groups continue to grow and proliferate quickly.

- Facebook and Twitter announce internal investigations and reveal that foreign, state-sponsored actors may be behind the initial uptick in online hate activity and that at least some materials in circulation have been digitally doctored, including deepfake videos showing incendiary and suggestively racist statements made off the record by leadership currently in government. A combination of verified accounts of far-right media members and unverified accounts (including both real people and inauthentic profiles), amplified by reposts and likes from automated bot accounts, have also been reposting and sharing inflammatory material. Social media accounts that have spent months growing their following before the crisis, ranging from 500 to 10,000 followers, pose as grassroots activists on the far right and far left to further inflame tensions. Facebook and Twitter are in the process of identifying and suspending accounts on the grounds of platform manipulation, but the investigation is ongoing.

- The FBI and Interpol also report a broader increase in online hate activity on other platforms and are increasingly concerned about the risk of domestic terrorism. They suspect that organization is occurring primarily through private end-to-end encrypted messaging apps, such as WhatsApp, Telegram, and Signal, and closed Facebook groups, based on the extremely limited law enforcement visibility into said networks through informants or undercover agents.

- On public social media networks, Russian intelligence uses network mapping techniques to understand the connections and relationships among individuals within and between these groups (both on the far left and far right). They use this information to identify influential individuals within groups for cultivation, with some evidence that they are also receiving direct funding and materiel support.

- With hate speech on the rise, particularly in information environments prone to an echo-chamber dynamic, a truck is driven into a crowd of protesters in southern France. The driver appears inspired by an anti-Semitic conspiracy theory, which was itself potentially bolstered by Russian disinformation. Threats of violence are on the rise across Europe and the United States. In the United States, the Capitol, Supreme Court, and White House have gone into lockdown following reports of potentially violent demonstrations.

- The domestic political debate—how to respond to the shooting, the rise in vandalism and violence, and the uptick of hate speech and disinformation occurring in a vacuum guarded from public view—is heating up rapidly. Calls on the president to stand up against Russian interference, doubling down on objections to Russian human rights violations and undemocratic behavior while also holding it accountable for any role in the uptick in violence, are growing. At the same time, investigations into ongoing hate crime activity suggest that Moscow may not be solely to blame and that such posturing simply serves as a distraction from real and present threats of domestic extremist violence.

Critical Decision Points

- Should the United States publicly blame Russia for attempting to incite violence in Europe and the United States?

- What should the U.S. position be on protests in Russia? Should the United States respond by increasing its support—including via its own covert influence operations—to pro-democracy groups in Russia and seek to bolster pro-democracy narratives?

- Given Russia's involvement in inciting the violence, does this constitute an armed attack? At what point would it constitute such an attack? What redlines, if any, should the United States and its allies draw?

- Should the United States seek to share information and coordinate a response with Hungary, Poland, France, and other European partners to deal with this level of domestic interference? Is there a role for NATO? How can they coordinate and share information while protecting civil liberties?

Scenario 3

NUCLEAR CRISIS OF CONFIDENCE

INTENSITY OF CONFRONTATION

Competition/Acute Crisis

Background Context

It is 2031, and despite pushback and initial delay, the Ground Based Strategic Deterrent (GBSD) has reached initial operational capacity and is now in the process of deployment as the land-based intercontinental ballistic missile (ICBM) force. In addition, Russia's own nuclear modernization is ongoing as it fields several novel systems, claiming a need to counter U.S. missile defenses. New START, which expired in February 2026, has not been replaced. Meanwhile, the International Campaign to Abolish Nuclear Weapons (ICAN) is gaining steam in Europe and Asia. Particularly in NATO countries, citizens are increasingly mobilizing to put pressure on their governments to renounce nuclear weapons and sign the Treaty on the Prohibition of Nuclear Weapons (TPNW). Anti-nuclear advocates have highlighted the risk that current dynamics could lead to intentional or accidental nuclear war. Recent reports of lax safety standards at nuclear weapons storage sites in Europe have been used by anti-nuclear weapons advocates to bolster their claims.

Key Events Timeline

- For months, high-level Russian officials, including President Vladimir Putin, have raised concerns about "reckless" U.S. behavior and the danger that a false alarm could trigger a U.S. launch of a nuclear weapon before realizing its systems had erred.
- Against this backdrop, an alleged correspondence from a senior military officer assigned to U.S. Strategic Command is leaked. The document appears to notify a U.S. Department of Defense official of a cyber vulnerability in the nuclear command, control, and communications (NC3) system supporting the launch control facilities. After 24 hours, top officials publicly explain that the document is a forgery with the intent of reducing domestic and allied trust in the U.S. nuclear deterrent and its ICBM force in particular.
- A series of stories based on the "leak" proliferate across various Russian-connected outlets. Major news outlets acknowledge questions about authenticity but still report on the controversy, raising public awareness. Russian media outlets and state-linked bloggers begin publishing related content in "data voids," ensuring that misleading information appears at the top of search engine results during the crisis.
- Additional leaks spread across less-established news outlets claiming the United States is undertaking a comprehensive review of the integrity of its NC3 communications, with immediate amplification across social media. Twitter accounts claiming to be freelance reporters cite unnamed former U.S. government-contracted engineers who claim to have raised flags about issues with NC3 integrity in the past and the potential that certain issues may even be carrying over to modernized systems.
- Members of Congress, particularly those on the House and Senate Armed Services Committees, are inundated with real and likely fake "constituent calls" (fabricated AI-generation audio bots that appear extremely lifelike) expressing concerns about the control

of U.S. nuclear weapons and accidental war and questioning the need to modernize U.S. nuclear weapons. Appearing to believe the forged leaks (or using them as an opportunity to advance preexisting policy preferences), several members of Congress have already come forward on Twitter to express strong concern, calling for congressional investigations into the stories.

- The nongovernmental community comments extensively on Twitter. Though not taking the stories at face value, several prominent think tank experts include tweets along the lines of: "If true, ..."
- While initial leaks seem to have originated from Russian-affiliated accounts, far-left-leaning European, Canadian, and Australian influencers have seized on the controversy and insist that the United States is stifling a whistleblower with information about poor U.S. NC3 practices. ICAN and TPNW advocates in Europe have seized on the situation and called for major protests across Europe. Several European parliaments have raised concerns and expressed a willingness to reconsider TPNW membership in light of the growing controversy.
- Some European nations are engaging through NATO to promote changes to U.S. declaratory policy in the alliance with relation to no-first-use. Germany and the Netherlands are under significant political pressure to stop participating in NATO nuclear sharing. A block of nonaligned countries has asked to put the NC3 issue on the agenda at the Conference on Disarmament.
- Even as it becomes apparent in official quarters that the leaks were forged, the direct effects of the coordinated disinformation efforts appear to be having an outsized impact on public debate, especially in Europe. Sensationalized mainstream reporting—initially on the substance of the leaks (before government actors could weigh in to deny their authenticity), and now on the foreign influence efforts themselves—seems to have exaggerated the effects of the broader influence operation and raised it to the level of a major crisis, seeking to undermine public confidence in nuclear force posture and policy.

Critical Decision Points

- Should the U.S. secretary of defense or president call their counterparts in Europe to assure them of U.S. NC3 integrity and reaffirm support for NATO's nuclear mission?
- Should the United States actively lobby its European partners against the TPNW?
- How should the United States respond to Russian actions? Should the United States release incriminating information about Russian behavior? Should it impose sanctions or other penalties on Russia? What response is likely to deter future attempts to discredit U.S. command and control systems?
- Should the United States share further details about its NC3 systems and processes with the U.S. public and allies to assure them of its reliability and restore confidence?
- Should the United States seek to block any attempt at negotiations at the Conference on Disarmament? Should it refuse to discuss NATO consideration of policy changes vis-à-vis the TPNW and declaratory policy?

Scenario 4

DECONFLICTION BREAKDOWN

INTENSITY OF CONFRONTATION
Acute Crisis/Conflict

Background Context

It is 2030, and relations are worsening between U.S. allies and partners and Russia, exacerbated by reciprocal NATO and Russian military exercises in close proximity to each other's Arctic territory in the span of two weeks. Unsafe and provocative behavior in the High North between NATO and Russian aircraft and vessels are is also occurring with increasing frequency, particularly over the last six months. Last week, a Norwegian F-16 pilot was participating in a routine patrol off of its coast—tasked with identifying an aircraft that entered the patrol area in international airspace—when a Russian MiG fighter darted in front of the Norwegian fighter. The ensuing events ultimately resulted in a crash, forcing both pilots to eject. However, neither survived long in the ocean awaiting rescue, resulting in the death of both pilots.

Key Events Timeline

- RT and other Russian state-connected media outlets immediately release doctored video that appears to be recorded from the MiG's own camera, depicting aggressive maneuvers from the Norwegian fighter that did not occur and implicating Norway in the dangerous behavior that resulted in the deaths of both pilots.
- Deconfliction communications have broken down as Moscow repeats the false information to Western military counterparts. U.S. and NATO partners have called for an immediate safety stand-down. Norway has called for an emergency North Atlantic Council meeting. The U.S. Department of Defense is considering deployment of additional air patrol assets to the North Atlantic, though a decision to reallocate assets has not been made. Canada has placed air defense assets on alert.
- While media outlets are generally under pressure to generate web traffic, RT and large media publications find that the public's interest in the circumstances surrounding the pilots' death has resulted in a significant uptick in web traffic to the sites. They use sentiment analysis to assess how users interact with social media posts about the events and adapt content marketing accordingly to further generate interest, resulting in further spread of the false video.
- Human-like computational propaganda bots as well as personal social media accounts owned by real people are actively posting on Twitter and the comment sections of Facebook posts, YouTube videos, and online news articles, specifically with the intention of convincing the U.S. audience that Norway is at fault in an attempt to decrease support for a U.S. diplomatic or military response. While American and Norwegian government officials—and nongovernment technology experts—claim the Russian video is doctored, the Russian version of events had spread for days unaddressed through social media networks before an official "debunking" report is put together and cleared through the U.S. interagency and declassification process.

- Where recommendation engines assign priority by publication date, the continued generation of news stories around the issue keeps the Russian narrative at the top of search results and present in social media news feeds as the speculation continues to drive interest (similar to the intense speculation that followed the disappearance of Malaysia Airlines Flight MH370 in March 2014).
- The Norwegian prime minister summons the Russian ambassador to Norway for a meeting and conveys regret at the loss of life but demands the Russians stand down on the disinformation campaign and refrain from further provocative and unsafe behavior. The Russian ambassador insists that the Russian government is not involved and that they cannot control the actions of private news networks.
- An open-source investigative outlet issues a major report that proves the video is false but also implicates officials in several European countries in a bribery scandal, alleging they were paid to make statements supporting the Norwegian accounts (implying that portions of the Russia narrative are plausible). The report calls for continued NATO investigation.
- While some NATO members—the United States, Norway, France, and United Kingdom—are in favor of taking immediate action in response, Germany and others are instead pushing for de-escalation and the conclusion of investigations before evaluating if additional action is necessary.

Critical Decision Points

- Should the United States take immediate action to support Norway, or instead pursue a collective response through NATO, where opposition to Russia among some members is weakening under the pressure of Russia's campaign of plausible deniability?
- Should NATO increase its air patrols in the High North to deter future unsafe Russian air activities?
- How should the United States deal with sensitive classified information that counters the Russian narrative if disclosure could compromise valuable sources and methods? Should the United States endorse or remain silent on the open-source analysis published on the internet that comports with its assessment of events?

Appendix B

CHINA-FOCUSED SCENARIOS

Scenario 1

COUNTERINFLUENCE CAMPAIGN

INTENSITY OF CONFRONTATION
Competition/Relative Peace

Background Context

It is 2030 and a bombshell investigative report from a Western NGO and several follow-on stories published by prominent newspapers detail extensive human rights abuses, forced assimilation, destruction of cultural sites, and, in at least two instances, killings perpetrated by Chinese paramilitary forces in Tibet. Leaks of authoritative Chinese Communist Party (CCP) Central Documents, which hail the importance of "ideological work" and detail the full extent of centrally directed cultural cleansing (including one document outlining a briefing given to Xi Jinping on the party's efforts), are making it increasingly untenable for Western countries and democratic governments in Asia to ignore the ongoing situation. The reports lead to widespread condemnation outside of China, as well as renewed momentum in the United States and partner countries (e.g., Australia, Canada, and states in the European Union) to sanction specific Chinese nationals, government entities, and businesses. Two Canadian and New Zealander journalists who coauthored reports from inside China on the situation have been detained. The governments of Canada and New Zealand are seeking assistance from the United States and Europe.

Key Events Timeline

- In response to the many statements and reports detailing and criticizing Chinese behavior, CCP officials have issued a series of statements that "anti-China forces" are seeking to instigate unrest in China by spreading lies and trying to "erode national unity."
- As progress toward sanctions on CCP-connected officials gains steam, state media outlets and other nationalistic Chinese citizens begin encouraging boycotts of certain Western and American brands (the so-called "blacklist" treatment).
- Elites in the Chinese diaspora, including celebrities, businesspeople, and diplomats, begin creating and amplifying narratives of U.S. and European hypocrisy on human rights, receiving strong engagement on social media.
- CCP-linked United Front organizations in both Europe and the United States (e.g., the China-U.S. Exchange Foundation), their funding recipients (e.g., high-profile public relations firms and lobbying organizations), and sympathetic politicians are mobilized to advance CCP propaganda and advocate in favor of a conciliatory approach to China. Russia-linked social media accounts and bots amplify claims of U.S. hypocrisy, perceiving an opportunity to advance U.S.-Europe discord.
- In recent days Chinese surrogates and state media outlets have engaged in targeted attempts to discredit and coerce journalists and NGO operatives investigating Chinese human rights violations. Personal attacks are launched across social media, including doxing, creation of fake videos, and threats against family members of the detained journalists and close associates, both in China and in Canada and New Zealand.
- China blacklists certain EU, Canadian, and New Zealander officials, with the possibility of further action based on future statements and actions.

- In response, officials from the European Union, Canada, and New Zealand are lobbying the United States for assistance, specifically advocating for the coordinated withdrawal of diplomats from Beijing and additional multilateral sanctions.
- The U.S. Congress begins drafting bipartisan legislation that would require sanctions against Chinese officials and companies with any links to human rights abuses or their cover-up—creating the potential for massive U.S. sanctions against high-profile people and organizations.
- Through a combination of observational and computational techniques, China-linked actors use comprehensive human network analysis (using publicly available information from Facebook, Twitter, LinkedIn, and other sources) to identify a list of influential EU parliamentarians who have historically been critical of U.S. foreign policy and who are well positioned within social networks to sway other legislators and politicians. The China-linked actors use this information to direct a campaign targeting the lawmakers, their staffs, and people with online social connections to their staffs to spread news of U.S. human rights abuses abroad and other disinformation to discredit stories of China's wrongdoing.
- Geofenced targeting of the Congress and the House and Senate office buildings, as well as the European Parliament in Brussels, is also used to circulate advertisements in favor of China and Beijing-based companies. Social media testing and sentiment analysis allows the state-linked advertisers to adapt and refine their campaign based on audience engagement.
- Multiple China-sympathetic lawmakers in the United States and Europe, many of whom were targeted by China-linked influence efforts, have raised questions about the credibility of initial NGO reporting in Tibet, cautioning against the United States intervening in the internal affairs of other countries. A verbal altercation between two lawmakers on the Senate floor goes viral, raising the public salience of the crisis and prompting dozens of other lawmakers to take sides.

Critical Decision Points

- Should the United States publicly identify China's role and activities and attempt to disrupt them? Some of the detection and attribution information that confirms China's involvement involves sensitive sources and methods—how should this be shared with allies and partners to ensure common cause in opposing this behavior? Should the United States warn its allies that specific political figures and their staffs are the target of adversary influence efforts?
- Should the United States agree to requests by allies to coordinate the withdrawal of diplomats—and perhaps even ambassadors—from Beijing?
- Should the president support draft sanctions legislation in Congress? Should the executive branch impose additional sanctions as well, and if so, what should they target and why—what is the strategic message?
- The United States has the ability to carry out a cyberattack to disable the China-affiliated social media accounts and actors targeting the journalists—should it do so?
- Should the United States reach out to NGOs (private and nonprofit) to counter China's influence operations? When should it approach these organizations and what should it ask?

Scenario 2

CROSS-STRAIT ENCROACHMENT

INTENSITY OF CONFRONTATION
Acute Crisis

Background Context

It is June 2029, and over the last three months, PLA aircraft and vessels have been encroaching into Taiwan's territorial waters and airspace with increasing frequency. What began with a smaller number of fishing vessels and transport aircraft entering Taiwan's air defense identification zone (ADIZ) has ramped up in recent weeks, with PLA fighter jets and ships now engaging in more assertive "cognitive warfare" and entering Taiwan's airspace and territorial waters on a nearly daily basis in increasingly larger numbers. The Democratic Progressive Party-led government in Taiwan is publicly and privately calling on the United States to provide more diplomatic and military support.

Key Events Timeline

- A forged Taiwan Ministry of National Defense policy paper is leaked to Taiwan press that advocates for asking the United States to forward deploy a range of additional capabilities to Taiwan, including tactical nuclear weapons. The suspected goal of the forgery is to force the United States to reject such a move, leading Taiwan to call into question the U.S. security commitment.

- Official Chinese government Twitter accounts denounce the actions described in the cable as an unacceptable and aggressive move, calling on the United States to avoid a "clear escalation of an internal matter." In what appears to be a coordinated move, unofficial state-linked accounts begin responding by reposting the cable with undoctored but old photos of U.S.-Taiwan attaché activity in Taipei, designed to create the appearance of ongoing military-to-military coordination. Still, the origins of the leak are unclear—whether centrally directed by China, released by an independent actor operating within China, or coming from a different source altogether.

- The U.S. intelligence community is divided on assessments of PLA intent, with some arguing that the intensified activity constitutes the early stages of a move to reclaim Taiwan.

- Several U.S. congressional China hawks make repeated media appearances praising the plans in the cable—whether fake or not—and calling for action. The media clips are circulated by Chinese news organizations and CCP-linked accounts, calling out the supposed U.S. and Taiwanese aggression.

- Official PLA statements, CCTV segments, and social media accounts run by the PLA ramp up efforts to target citizens in Taiwan, broadcasting images and videos of PLA operations in the Taiwan Strait and interjecting divisive commentary into discussions on the incursions across Facebook, as well as on Taiwanese platforms such as PTT. These broadcasts seek to blame PLA operations on the assertiveness by the Taiwanese military and the growing popularity of separatist sentiment within Taiwan. A chorus of patriotic influencers within China, outside of direct government control, issues a series of highly inflammatory warnings against further Taiwanese moves toward independence.

- Meanwhile, Taiwan begins mobilizing its advocates in the United States to advance its agenda of strong diplomatic and military support; its extensive lobbying arm as well as members of the Congressional Taiwan Caucus and a chorus of pro-Taiwan think tank experts begin vocally advocating for clear signals of support, including moving a carrier group into the Taiwan Strait and providing written statements in support of Taiwan.

- As incursions into Taiwan's airspace continue to increase in frequency, senior U.S. Department of Defense officials are seeking permission to ramp up working-level security, intelligence, and defense consultations with Taiwanese government officials. The ongoing interagency debate is leaked to the press, further heightening domestic pressure for a White House response to the crisis.

- Taiwan is conveying to the United States its desire to execute a cyber operation against Chinese social media companies to temporarily disable a set of the Chinese-affiliated social media accounts targeting its citizens, but it cannot guarantee that major government media organizations will not be affected as well.

- Deepfake audio of Taiwanese officials is "leaked" portraying conversations in which leaders argue for (1) a more assertive posture toward China and (2) efforts to entangle the United States in any potential ratcheting up of tensions. In fact, these depictions were sophisticated forgeries using computational manipulation that spliced existing audio from the officials taken out of context. Though targeting the U.S. public, several members of Congress against assertive U.S. action seize on the videos as further reasoning to oppose direct U.S. military assistance in the crisis.

Critical Decision Points

- Should the United States publicly disavow the forged Taiwan Ministry of National Defense memo? If so, should it indicate what steps it is taking, if any, to aid Taiwan? Should it attempt to assign blame for the forgery?

- Should the United States counter this disinformation campaign with an information offensive of its own?

- Should the United States respond favorably to Taiwan's request to execute cyber countermeasures on the Chinese-affiliated accounts?

- Given escalating tensions and Taiwan's desire for U.S. support, should the United States send a carrier strike group to the region?

- Should the United States share its assessment on the forged memo and audio with Congress, even though doing so may reveal sensitive sources and methods?

Scenario 3

ALLIANCE COHESION IN ASIA

INTENSITY OF CONFRONTATION
Conflict

Background Context

It is June 2030, and amid intensifying U.S.-China competition, South Korea remains conflicted between its economic dependence on China and its close security cooperation with the United States. U.S. attempts to rejuvenate Japanese-South Korean relations have resulted in progress on bilateral and trilateral (U.S.-Japan-South Korea) security cooperation focused on North Korea, intelligence sharing, and military exercises. However, it is clear that Beijing believes the moves are a pretext to coordination against China. After a trilateral meeting of senior defense officials in Tokyo two weeks ago, China démarched all three capitals regarding anti-China military collusion and threatened sanctions. A week later near the Senkaku/Diaoyu Islands, a PLA detachment disguised as commercial shipping vessels advanced on a Japanese naval vessel in a region where the PLA denies having a military presence. The vessels engaged in gunfire, leading to a small number of casualties on each side. A second altercation occurred 48 hours later—a Chinese naval vessel intercepted a Japanese vessel, causing the Japanese vessel to abruptly change course, and a Japanese Air Self-Defense Force aircraft harassed a Chinese surveillance patrol.

Key Events Timeline

- Seeking to drive a wedge between Japan and South Korea to inhibit a coherent trilateral response to escalating tensions, statements by the Chinese Foreign Ministry, in addition to state media outlets, allege they have uncovered evidence of a high-level cover-up by Japanese officials of a mass grave of Korean "comfort women" victims that does not actually exist.

- Such statements immediately proliferate across social media in the increasingly large global network of official Twitter accounts connected to China (e.g., ambassadors) and on the accounts of officials from other aligned countries, such as Venezuela, as elite intermediaries and celebrities abroad express solidarity with World War II victims and their families. Chinese intelligence officers who provided the materials for the influence operation track engagement with and user sentiment of the posts and refine the content to boost engagement and ensure its continued spread.

- Having spent months gradually building an audience on Korean social media sites, sleeper cells consisting of both bot networks and human-operated accounts (put in place to build social media history in advance of activation during a crisis in which it would serve Beijing to inhibit a coherent trilateral U.S.-South Korean-Japanese response) aim to instigate further South Korea-Japan historical animosity from World War II atrocities. They infiltrate private survivors and solidarity groups on these sites (groups that have previously lobbied the government to demand reparations and other punitive actions), which have in turn renewed pressure on their government to demand reparations from Japan.

- In an approach designed to sideline South Korea from a coordinated response to the current crisis, PLA intelligence uses network analysis computational techniques and human intelligence from within the solidarity networks to identify influential individuals within the groups. Targeted engagement and messages highlight stories of Chinese comfort women atrocities and other instances of imperial

Japan's human rights crimes in an effort to build solidarity with South Korea against Japan. The intelligence operatives engage directly with those select individuals to ensure the spread and influence of anti-Japan messages.

- Solidarity groups in South Korea and Japan gain traction in the mainstream as the sleeper cells shift their messaging focus to gaining broader support throughout the general populations. Mass protests in South Korea and Japan, coordinated in part by foreign actors acting as community organizers, have the potential to overshadow maritime confrontations, distract the Japanese and South Korean publics, and decrease the ability of the United States, Japan, and South Korea to respond trilaterally.
- Beijing is privately threatening harsh economic penalties against South Korea, including bans on exports and tourism, should Seoul not stay neutral on the island dispute. The Global Times also releases an op-ed seemingly making the threat publicly.
- Even as false claims of the cover-up are disproven, rallies have continued for several days and are growing in intensity. Meanwhile, South Korean officials have told the United States that they are not willing to publicly support Japan in the ongoing crisis.
- Japan has requested U.S. assistance in the Senkaku/Diaoyu Islands, concerned that a third altercation could lead to a wider conflict. The CCP media releases doctored satellite images of the conflict on the islands suggesting provocative military actions were initiated by and continue on the part of the Japanese. The photos also depict a build-up of Japanese military installations and forward positioning of equipment and materiel. Several public pieces with the doctored photos provide sympathetic coverage before U.S. intelligence sources and the NGO community publicly call out the fake.

Critical Decision Points

- Should the United States do joint patrols with Japan near the Senkaku/Diaoyu Islands where the Japanese vessels were harassed and attacked?
- Should the United States attempt to work as an intermediary between South Korea and Japan to resolve the recent flare-up stemming from the controversy over the faked mass grave, or should it stay uninvolved in the hopes the controversy and anger subsides?
- Should the United States attempt to pressure South Korean leaders to reverse their decision with regard to supporting Japan in the current crisis?
- Should the United States propose countering disinformation as a central focus of future U.S.-South Korean-Japanese dialogues?

Scenario 4

LINE OF ACTUAL CONTROL BORDER TENSIONS

INTENSITY OF CONFRONTATION
Conflict

Background Context

It is February 2029, a few months before Indian general elections. Tensions are rising again in multiple locations across the China-India border area—across the Himalayas from Ladakh to Sikkim. Tens of thousands of Indian and Chinese troops have mobilized along the contested border, massing artillery and fighter aircraft on both sides. For weeks, minor face-offs have been met with Indian criticism, blaming PLA forces for instigating the incident. Chinese officials have called on India to refrain from escalatory actions, while China's state-affiliated news organizations have denied the clashes entirely. A few days ago, however, a border incident led to dozens of soldiers being killed or captured on both sides.

Key Events Timeline

- While India alleges PLA troops moved past the Line of Actual Control (LAC) and started the violence, Chinese officials blame India. Both states have released videos that appear to confirm their claims, but that are contradictory when taken together. While current U.S. intelligence suggests that PLA troops did in fact cross and remain on the Indian side of the LAC, it is unclear which country instigated the confrontation. India is appealing to its security partners in the Quad—the United States, Australia, and Japan—to confirm its version of events.
- Chinese officials have also released fabricated satellite imagery showing wide-scale Indian mobilization in the region and AI-generated audio of Indian military officials admitting blame. Within 24 hours, the audio has circulated across WhatsApp to thousands of Indian citizens and continues to spread quickly.
- China is also circulating actual footage of Indian soldiers maneuvering aggressively in the border region, combining the real information with the fake video of Indian soldiers firing shots at PLA troops in a manner that complicates efforts to debunk the claims.
- Despite Indian forces having been directed to leave all personal devices in garrison prior to deployment, PLA forces are able to acquire multiple personal mobile phones from Indian soldiers that have been captured along the border. As part of a psychological warfare campaign, the PLA sends dozens of families of Indian troops false text notifications that they have died. Detachments of PLA troops carry the stolen devices through the region to generate location data showing Indian troops in locations that contradict official Indian statements on troop movements, casting doubt on the veracity of official Indian statements.

- Indian military sources have released their own version of events. U.S. sources cannot corroborate the events as described by either side. The Indian defense minister has issued a fiery speech blaming China for the march to war and a dangerous crisis between two nuclear-armed states.
- An aggressive disinformation campaign, the origins of which are not immediately clear, is launched across Facebook, Twitter, and other social media sites, portraying the border confrontation as a deliberate attempt by the Indian government to rally its citizens around the Bharatiya Janata Party (BJP) and boost domestic support before an election. Seeing an opportunity to paint the BJP as overly militant, thousands of Indian National Congress (INC) volunteers operating the party's social media campaign for the elections unwittingly spread the claims, ultimately reaching millions of social media users and resulting in protests against the BJP government in several major cities.
- Though an attempt to push decisionmakers in New Delhi to capitulate, the campaign appears to embolden the Indian leadership, which in turn claims that the INC opposition is deliberately or tacitly colluding with China to undermine Indian security and embarrass the country on the global stage.
- Pressure is also building in Washington, with some senior officials and members of Congress advocating for action that communicates unequivocal support for India, and others pushing for a more neutral approach. Australian officials want the Quad to issue a joint statement that is supportive of India's position and notes the apparent use of disinformation by China; Japanese officials are more cautious and want to take a more balanced approach that calls for both sides to stand down.
- In private communications between New Delhi and Washington, the Indian government asserts it cannot stand down from the situation, less it risk the political damage associated with appearing to admit fault or "back down." Separately, U.S. intelligence indicates India is preparing to mobilize its forces to push China back across the LAC—developments China is also likely aware of—and which analysts assess could spark a major conventional war between these two nuclear-armed states.

Critical Decision Points

- With inconclusive evidence, should the United States blame an aggressor in the situation? Should it do so unilaterally or only with support of the Quad? If the decision is to wait, what type of evidence would be decisive?
- Should the United States publicly release imagery and intelligence that it has to support the version of events put forward by India, an important security partner, or instead aim to diffuse tensions?
- Should the United States privately warn—or encourage—India and China not to raise the alert levels of their nuclear forces or otherwise introduce nuclear threats into the equation? How should the United States respond if either side begins bringing the threat of nuclear weapons into the standoff?
- A key tenet of U.S. foreign policy to this point has been an "alliance of democracies" to compete against China and push back on problematic and coercive behavior. While the United States and India have no formal alliance, given the risks that China may successfully occupy a part of Indian—a key democratic partner—territory, should the United States provide any further commitments or aid to India, either in the form of intelligence, military assistance, or security and defense commitments?

ABOUT THE AUTHORS

Rebecca Hersman is director of the Project on Nuclear Issues (PONI) and senior adviser with the International Security Program at the Center for Strategic and International Studies (CSIS). A leading expert on nuclear, chemical, and biological weapons policy; global health security; and crisis management, Ms. Hersman leads the preeminent national program designed to develop next generation nuclear expertise. An author of numerous studies and reports on nuclear and chemical weapons policy, emerging technologies and strategic stability, and crisis management and decisionmaking, Ms. Hersman also co-chairs the CSIS U.S./UK/France Trilateral Dialogues on Nuclear Issues and has served as a commissioner on the CSIS Commission on Strengthening America's Health Security. Ms. Hersman joined CSIS in April 2015 from the Department of Defense (DOD), where she served as deputy assistant secretary of defense for countering weapons of mass destruction since 2009. In this capacity, she led DOD policy and strategy to prevent WMD proliferation and use, reduce and eliminate WMD risks, and respond to WMD dangers. She was a key leader on issues ranging from the elimination of Syria's chemical weapons, nuclear response and mitigation during the Fukushima crisis, and WMD interdiction policy and response. Ms. Hersman led DOD engagements on WMD issues with NATO, South Korea, Japan, and others, and also served as DOD's principal policy advocate on WMD arms control, nonproliferation, and threat reduction. Prior to joining DOD, Ms. Hersman was a senior research fellow with the Center for the Study of Weapons of Mass Destruction at the National Defense University from 1998 to 2009. Ms. Hersman previously held positions as an international affairs fellow at the Council on Foreign Relations, a special assistant to the undersecretary of defense for policy, and a member of the House Armed Services Committee professional staff. She holds an MA in Arab studies from Georgetown University and a BA from Duke University.

Eric Brewer is deputy director and senior fellow with the Project on Nuclear Issues at CSIS. He specializes in nuclear proliferation, Iran, and North Korea. Prior to joining CSIS, Mr. Brewer was a 2018–2019 Council on Foreign Relations International Affairs fellow at the Center for a New American Security. From 2017 to 2018, Mr. Brewer served as the director for counterproliferation at the National Security Council (NSC), where he was responsible for coordinating U.S. policy to prevent and reverse the spread of nuclear weapons, their delivery systems, and related technologies. While at the NSC, Mr. Brewer played a lead role implementing elements of U.S. North Korea policy. From 2014 to 2017, Mr. Brewer served as deputy national intelligence officer for WMD and proliferation at the National Intelligence Council. In that capacity, he led the intelligence community's (IC) analysis of foreign nuclear weapons capabilities and intentions, proliferation trends, and over-the-horizon proliferation threats. This included IC assessments on Iran's nuclear program during U.S. nuclear negotiations with Iran and monitoring the implementation of the Joint Comprehensive Plan of Action. He also represented the IC in White House meetings and briefings to Congress. From 2008 to 2014, Mr. Brewer held several positions at the Defense Intelligence Agency (DIA), including senior intelligence analyst for Iran. Before joining DIA, Mr. Brewer worked at the National Nuclear Security Administration. Mr. Brewer is the author of several reports, including most recently *Toward a*

More Proliferated World? The Geopolitical Forces that Will Shape the Spread of Nuclear Weapons. He has authored op-eds and articles in outlets such as the *Washington Post*, the *Washington Quarterly*, *Foreign Affairs*, the Bulletin of the Atomic Scientists, and *The Atlantic*. He received an MA in security policy studies from the George Washington University, an MS in strategic intelligence from the National Intelligence University, and a BA in international relations from the University of San Diego.

Lindsey Sheppard is a former fellow with the International Security Program at CSIS, where she focuses on the nexus of emerging technologies and national security for the United States and allied and partner nations. Her research areas include artificial intelligence, machine learning, autonomous systems, defense innovation policy, and technology ecosystems. Ms. Sheppard contributes expertise in computational modeling and simulation, system architecture and design, and GPS-denied operations from her prior experience in defense research and development. Before joining CSIS in March 2018, she was a member of the technical staffs at the Charles Stark Draper Laboratory and the Georgia Tech Research Institute. During this time, she was the programmatic and technical systems engineering lead on various software development projects. Ms. Sheppard's work supported U.S. Air Force and U.S. Army procurement and technology development efforts to support operations in contested environments. She holds an MS and a BS in aerospace engineering from the Georgia Institute of Technology.

Maxwell Simon is a former program coordinator and research assistant with the Project on Nuclear Issues in the International Security Program at CSIS. He graduated from Harvard University with a BA in government and history. Prior to joining CSIS, he held positions as a junior research fellow at the Tony Blair Institute in London and as a legislative intern in the United States Senate.

ENDNOTES

Project Objective and Scope

1 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

2 Department of the Army, *The Conduct of Information Operations* (Washington, DC: October 2018), 1, Glossary-3, https://fas.org/irp/doddir/army/atp3-13-1.pdf.

3 Herb Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," Lawfare, September 6, 2018, https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations.

4 Kathleen Hicks et al., *By Other Means Part I: Campaigning in the Gray Zone* (Washington, DC: CSIS, July 2019), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf.

5 Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (October 2012): 5–32, doi:10.1080/01402390.2011.608939.

Influence Tactics, Techniques, and Trends

6 Rid, *Active Measures*.

7 Ibid.

8 In 1974, John Barron, a *Readers Digest* investigative journalist, collaborated extensively with the CIA to release *KGB: The Secret Work of Soviet Secret Agents*, which became an international bestseller and revealed the names of hundreds of KGB and GRU officers operating around the world. See John Barron, *KGB: The Secret Work of Soviet Secret Agents* (New York: Reader's Digest Press, 1974); and John M. Crewdson and Joseph B. Treaster, "The C.I.A.'s 3-Decade Effort to Mold the World's Views," *New York Times*, December 25, 1977, https://www.nytimes.com/1977/12/25/archives/the-cias-3decade-effort-to-mold-the-worlds-views-agency-network.html.

9 Michael Schwirtz, "Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say," *New York Times*, October 8, 2019, https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html.

10 Matt Schrader, *Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries* (Washington, DC: German Marshall Fund Alliance for Securing Democracy, April 22, 2020), https://securingdemocracy.gmfus.org/friends-and-enemies-a-framework-for-understanding-chinese-political-interference-in-democratic-countries/.

11 Nathan Beauchamp-Mustafaga and Michael S. Chase, *Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations* (Washington, DC: Johns Hopkins School of Advanced International Studies Foreign Policy Institute, 2019), https://www.fpi.sais-jhu.edu/borrowing-a-boat-out-to-sea-pdf; Wang Jichang, "Main Experience of Russia's Military Operations in Syria," *China Military Science* 3 (2016): 119–126; Zhu Ningning, "An Analysis of Russia's Unfolding of Media Warfare Tactics Amid the Turbulent Political Situation in Ukraine," *Military Correspondent*, 2014; and Kuang Xiaoqin, "Analysis on the Coping Strategies for Social Media Information Warfare: Taking Russia's Approach to the Ukraine Crisis as an Example," *Military Correspondent*, August 2018, http://www.81.cn/jsjz/2018-08/22/content_9260460.htm.

12 Laura Rosenberger, "China's Coronavirus Information Offensive: Beijing Is Using New Methods to Spin the Pandemic to Its Advantage," *Foreign Affairs*, April 22, 2020, https://www.foreignaffairs.com/articles/china/2020-04-22/chinas-coronavirus-information-offensive.

13 Jessica Brandt and Bret Schafer, "Five Things to Know About Beijing's Disinformation Approach," Alliance for Securing Democracy, March 30, 2020, https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/; and Edward Wong, Matthew Rosenberg, and Julian 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.

14 Lachlan Markay, "China increases spending 500% to influence America," Axios, May 11, 2021, https://www.axios.com/china-foreign-influence-spending-317a9be4-8ead-4abf-8ac4-3f27974d7a9d.html.

15 United States v. Internet Research Agency LLC, 1:18-cr-00032, (United States District Court for the District of Columbia, 2018), 7, https://www.justice.gov/file/1035477/download.

16 Sean Edgett, "Update on Results of Retrospective Review of Russian-Related Election Activity," Written Statement to the U.S. Senate Committee on the Judiciary, January 19, 2019, 5, https://www.judiciary.senate.gov/imo/media/doc/Edgett%20Appendix%20to%20Responses.pdf.

17 Rid, *Active Measures*.

18 Anne Gearan, Phillip Rucker, and Abby Phillip, "DNC chairwoman will resign in aftermath of committee email controversy," *Washington Post*, June 24, 2016, https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html.

19 "Who's who in the CIA," *Los Angeles Free Press*, March 28, 1969, http://jfk.hood.edu/Collection/White%20%20Files/Security-CIA/CIA%200224.pdf.

20 Rid, *Active Measures*.

21 Adam Satariano and Amie Tsang, "Who's Spreading Disinformation in U.K. Election? You Might Be Surprised," *New York Times*, December 12, 2019, https://www.nytimes.com/2019/12/10/world/europe/elections-disinformation-social-media.html.

22 Schrader, *Friends and Enemies*; and Alex Joske, "The Party Speaks for You: Foreign Interference and the Chinese Communist Party's United Front System," Australian Strategic Policy Institute, *Policy Brief* 32, (2020), https://www.aspi.org.au/report/party-speaks-you.

23 Sheera Frankel, "How a Fake Group on Facebook Created Real Protests," *New York Times*, August 14, 2018, https://www.nytimes.com/2018/08/14/technology/facebook-disinformation-black-elevation.html.

24 Ibid.

25 Alex Newhouse, "Far-right activists on social media telegraphed violence weeks in advance of the attack on the US Capitol," *The Conversation*, January 8, 2021, https://theconversation.com/far-right-activists-on-social-media-telegraphed-violence-weeks-in-advance-of-the-attack-on-the-us-capitol-152861.

26 Rid, *Active Measures*.

27 Nick McKenzie, Bethany Allen-Ebrahimian, Zach Dorfman, and Fergus Hunter, "Beijing's Secret Plot to Infiltrate UN Used Australian Insider," *Sydney Morning Herald*, November 11, 2018, https://www.smh.com.au/world/asia/beijing-s-secret-plot-to-infiltrate-un-used-australian-insider-20181031-p50d2e.html.

28 Adam Klasfeld. "Ex-UN General Assembly Heads Tied to Bribery Scheme," Courthouse News Service, December 1, 2018, https://www.courthousenews.com/ex-un-general-assembly-heads-tied-to-bribery-scheme/; and "In the UN, China Uses Threats and Cajolery to Promote Its Worldview," *The Economist*, December 7, 2019, https://www.economist.com/china/2019/12/07/in-the-un-china-uses-threats-and-cajolery-to-promote-its-worldview.

29 Zeyi Yang, "The Anatomy of a Chinese Online Hate Campaign," Protocol, April 9, 2021, https://www.protocol.com/china/chinese-online-hate-campaigns.

30 Joby Warrick and Anton Troianovski, "Agents of Doubt: How a Powerful Russian Propaganda Machine Chips Away at Western Notions of Truth," *Washington Post*, December 10, 2018, https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/.

31 Schrader, *Friends and Enemies*.

32 Damien McGuineess, "How a Cyber Attack Transformed Estonia," BBC, April 27, 2017, https://www.bbc.com/news/39655415.

33 Ivo Juurevee and Mariita Mattiisen, *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict* (Tallinn: International Centre for Defence and Security, 2020), https://icds.ee/wpcontent/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf.

34 Alison Brennan, "Microtargeting: How campaigns know you better than you know yourself," CNN, November 5, 2012, https://www.cnn.com/2012/11/05/politics/voters-microtargeting/index.html.

35 Barbara Ortutay and Amanda Seitz, "How microtargeted political ads are wreaking havoc on our elections," *Los Angeles Times*, February 1, 2020, https://www.latimes.com/business/technology/story/2020-02-01/how-microtargeted-political-ads-are-wreaking-havoc-on-our-elections.

The Information Ecosystem and Digital Influence Technologies

36 Sarah Jacobs Gamberini and Amanda Moodie, "Governing a Pandemic: China's Authoritarian Approach to COVID-19 in the Context of Great Power Competition," Inkstick Media, May 7, 2020, https://inkstickmedia.com/governing-a-pandemic/.

37 Conor Sen, "The 'Big Five' Could Destroy the Tech Ecosystem," Bloomberg, November 15, 2017, https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem; and Farhad Manjoo, "Tech's 'Frightful 5' Will Dominate Digital Life for Foreseeable Future," *New York Times*, January 20, 2016, https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html.

38 Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout so Far," *New York Times*, April 4, 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

39 Christopher H. Sterling and John Michael Kittross, *Stay Tuned: A History of American Broadcasting*, 3rd ed. (Mahwah, NJ: LEA, 2002), https://www.routledge.com/Stay-Tuned-A-History-of-American-Broadcasting/Sterling-Kittross/p/book/9780805826241.

40 David Tewksbury and Jason Rittenberg, *News on the Internet: Information and Citizenship in the 21st Century* (Oxford University Press, 2012), doi:10.1093/acprof:osobl/9780195391961.001.0001.

41 Chris Anderson, *The Long Tail: How Endless Choice is Creating Unlimited Demand* (New York: Random House Business Books, 2006).

42 In 2020, 53 percent of Americans reported getting news on social media "often" or "sometimes." See Elisa Shearer and Amy Mitchell, "News Use Across Social Media Platforms in 2020," Pew Research Center, January 12, 2021, https://www.journalism.org/2021/01/12/news-use-across-social-media-platforms-in-2020/.

43 W. Lance Bennett and Shanto Iyengar, "A New Era of Minimal Effects? The Changing Foundations of Political Communication," *Journal of Communication* 58, no. 4 (2008), doi:10.1111/j.1460-2466.2008.00410.x.

44 Christina Nemr and William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (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.

45 Michael J. Mazarr et al., *Hostile Social Manipulation: Present Realities and Emerging Trends* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2713.html.

46 Goldman Sachs Global Investment Research, *The Internet of Things: Making Sense of the Next Mega-Trend* (New York: September 2014), http://www.goldmansachs.com/our-thinking/pages/internet-of-things/iot-report.pdf.

47 "The Internet of Everything," Cisco, 2013, http://perma.cc/Y4LQ-633J?type=live.

48 Patricia Moloney Figlola, *The Internet of Things: Frequently Asked Questions*, CRS Report No. R44227 (Washington, DC: Congressional Research Service, 2015), https://sgp.fas.org/crs/misc/R44227.pdf; Janna Anderson and Lee Raine, "The Internet of Things Will Thrive by 2025," Pew Research Center, https://www.pewresearch.org/internet/2014/05/14/internet-of-things/; Agnes Szolnoki and Andras Nabradi, "Economic, Practical Impacts of Precision Farming—With Especial Regard to Harvesting," *Applied Studies in Agribusiness and Commerce* 8, no. 2–3 (2014): 141–46, doi:10.22004/ag.econ.202892; Special Committee on Aging, "Roundtable: Harnessing the Power of Telehealth: Promises and Challenges?," U.S. Senate, 2014, http://www.aging.senate.gov/hearings/roundtable-harnessing-the-power-of-telehealthpromises-and-challenges; James Manyika et al., *The Internet of Things: Mapping the Value Beyond the Hype* (San Francisco: McKinsey and Company, June 2015), https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.pdf; and Matthew Cuddy et al., *The Smart/Connected City and Its Implications for Connected Transportation* (Washington, DC: Department of Transportation, October 2014), http://www.its.dot.gov/itspac/Dec2014/Smart_Connected_City_FINAL_111314.pdf.

49 National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things* (Washington, DC: November 2014), https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

50 Kolla Bhanu Prakash, ed., *Internet of Things: From the Foundations to the Latest Frontiers in Research* (Boston: De Gruyter, 2020), https://www.degruyter.com/document/doi/10.1515/9783110677737/html?lang=en.

51 Dipayan Ghosh and Ben Scott, *Digital Deceit: The Technologies Behind Precision Propaganda on the Internet* (Washington, DC: New America, January 2018), https://www.newamerica.org/pit/policy-papers/digitaldeceit/.

52 Rid, *Active Measures*, 13.

53 Alina Polyakova, *Weapons of the weak: Russia and AI-driven asymmetric warfare* (Washington DC: Brookings Institution, November 2018), https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

54 Mazarr et al., *Hostile Social Manipulation*.

55 Ghosh and Scott, *Digital Deceit*.

56 Britt Paris and Joan Donovan, *Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence* (New York: Data & Society, September 18, 2019), https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf.

57 Kasey Panetta, "Gartner Top Strategic Predictions for 2018 and Beyond," Gartner, Inc., October 3, 2017, https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/.

58 "Deepfakes, shallowfakes, speech synthesis: tackling audiovisual manipulation," European Science-Media Hub, December 4, 2019, https://sciencemediahub.eu/2019/12/04/deepfakes-shallowfakes-and-speech-synthesis-tackling-audiovisual-manipulation/.

59 Paris and Donovan, *Deepfakes and Cheap Fakes*.

60 "A Beginner's Guide to Generative Adversarial Networks (GANs)," Pathmind, https://wiki.pathmind.com/generative-adversarial-network-gan.

61 For examples of deepfake images of human faces see: https://thispersondoesnotexist.com/.

62 Patrick Tucker, "A Better Way to Spot Deep-Faked Satellite Imagery," Defense One, April 23, 2021, https://www.defenseone.com/technology/2021/04/better-way-spot-deep-faked-satellite-images/173586/.

63 James Vincent, "Tom Cruise deepfake creator says public shouldn't be worried about 'one-click' fakes," The Verge, March 5, 2021, https://www.theverge.com/2021/3/5/22314980/tom-cruise-deepfake-tiktok-videos-ai-impersonator-chris-ume-miles-fisher.

64 Ibid.

65 "Old photos circulated in misleading social media posts about Pfizer-BioNTech Covid-19 vaccine trial volunteers developing facial paralysis," AFP Hong

Kong, December 18, 2020, https://factcheck.afp.com/old-photos-circulated-misleading-social-media-posts-about-pfizer-biontech-covid-19-vaccine-trial.

66 Michael Yankoski, Walter Scheirer, and Tim Weninger, "Meme Warfare: AI countermeasures to disinformation should focus on popular, not perfect, fakes," Bulletin of the Atomic Scientists, May 13, 2021, https://thebulletin.org/premium/2021-05/meme-warfare-ai-countermeasures-to-disinformation-should-focus-on-popular-not-perfect-fakes/.

67 Michael Garbade, "A Simple Introduction to Natural Language Processing," Becoming Human AI, October 15, 2018, https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32.

68 Kyle Wiggers, "How Google is using emerging AI techniques to improve language translation quality," Venture Beat, June 3, 2020, https://venturebeat.com/2020/06/03/how-googleis-using-emerging-ai-techniques-to-improve-language-translation-quality/.

69 Tom B. Brown et al., "Language Models are Few Shot Learners," arxiv, July 22, 2020, https://arxiv.org/pdf/2005.14165.pdf.

70 Will Douglas Heaven, "OpenAI's new language generator GPT-3 is shockingly good—and completely mindless," *MIT Technology Review*, July 20, 2020, https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/.

71 Ben Buchanan, Andrew Lohn, Micah Musser, and Katerina Sedov, *Truth, Lies, and Automation: How Language Models Could Change Disinformation* (Washington, DC: Center for Security and Emerging Technology, May 2021), https://cset.georgetown.edu/publication/truth-lies-and-automation/; and Alex Tamkin, Miles Brundage, Jack Clark, and Deep Ganguli, "Understanding the Capabilities, Limitations, and Societal Impact of Large Language Models," arxiv, February 4, 2021, https://arxiv.org/pdf/2102.02503.pdf.

72 Rid, *Active Measures*, 17–32.

73 Marc A. Smith et al., "Mapping Twitter Topic Networks: From Polarized Crowds to Community Clusters," Pew Research Center, February 20, 2014, https://www.pewresearch.org/internet/2014/02/20/mapping-twitter-topic-networks-from-polarized-crowds-to-community-clusters/#:~:text=Network%20maps%20are%20created%20by,a%20particular%20subject%20are%20plotted.

74 Jeff Tollefson, "Tracking QAnon: how Trump turned conspiracy-theory research upside down," Nature, February 4, 2021, https://www.nature.com/articles/d41586-021-00257-y.

75 "Making Ugandan Community Radio Machine-readable Using Speech Recognition Technology," UN Global Pulse, 2016, https://www.unglobalpulse.org/project/making-ugandan-community-radio-machine-readable-using-speech-recognition-technology/.

76 "Bots," Imperva, 2021, https://www.imperva.com/learn/application-security/what-are-bots/.

77 Karen Hao, "How Facebook got addicted to spreading misinformation," *MIT Technology Review*, March 11, 2021, https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/.

78 Ghosh and Scott, *Digital Deceit*.

79 Casey Newton, "Here's how Twitter's new algorithmic timeline is going to work," The Verge, February 6, 2016, https://www.theverge.com/2016/2/6/10927874/twitter-algorithmic-timeline.

80 Kiran Garimella, Gianmarco De Francisci Morales, Aristides Gionis, and Michael Mathioudakis, "Political Discourse on Social Media: Echo Chambers, Gatekeepers, and the Price of Bipartisanship," WWW '18: Proceedings of the 2018 World Wide Web Conference, April 2018, 913–922, doi:10.1145/3178876.3186139.

81 Hao, "How Facebook got addicted to spreading misinformation"; and Jessica Dawson, "Microtargeting as Information Warfare," *Cyber Defense Review* 6, no. 1 (Winter 2021): 63–79, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2537110/microtargeting-as-information-warfare/.

82 Hao, "How Facebook got addicted to spreading misinformation"; and Jeff Horwitz and Deepa Seetharaman, "Facebook Executives Shut Down Efforts to Make the Site Less Divisive," *Wall Street Journal*, May 26, 2020, https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

83 Kirsten Grind et al., "How Google Interferes with its Search Algorithms and Changes Your Results," *Wall Street Journal*, November 15, 2019, https://www.wsj.com/articles/how-google-interferes-with-its-search-algorithms-and-changes-your-results-11573823753; and "8 major Google algorithm updates, explained," Search Engine Land, October 13, 2020, https://searchengineland.com/8-major-google-algorithm-updates-explained-282627.

84 Soroush Vosoughi, Deb Roy, and Sinan Aral, "The spread of true and false news online," *Science* 359, no. 6380 (March 2018), https://science.sciencemag.org/content/359/6380/1146.

85 Louise Matsakis, "Facebook's Targeted Ads Are More Complex Than It Lets On," *Wired*, April 25, 2018, https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/.

86 Ibid.

87 Nicholas Confessore, "Cambridge Analytica and Facebook."

88 Elisa Shearer, "Social media outpaces print newspapers in the U.S. as a news source," Pew Research Center, December 10, 2018, https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/.

89 Giovanni Luca Ciampaglia and Filippo Menczer, "Biases Make People Vulnerable to Misinformation Spread by Social Media," *Scientific American*, June 21, 2018, https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media; and Michael J. Mazarr et al., *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment* (Santa Monica: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2714.html.

90 Nathaniel Gleicher et al., *Threat Report: The State of Influence Operations 2017-2021* (Menlo Park, CA: Facebook, May 2021), https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf.

Exploring the Connection between Influence Operations and Escalation Risk

91 Hicks et al., *By Other Means Part II*. See also Kelly M. Greenhill, "Of Wars and Rumors of Wars: Extra-Factual Information and (In)advertent Escalation," 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: Hoover Institution Press, 2020); and Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review* 3, no. 4 (2020), doi:10.26153/TSW/10962.

92 Martin C. Libicki, "Correlations Between Cyberspace Attacks and Kinetic Attacks," in *20/20 Vision: The Next Decade*, edited by T. Jančárková, L. Lindström, I. Signoretti, and G. Visky Tolga (Tallinn, Estonia: NATO CCDCOE Publications, 2020), 201, https://ccdcoe.org/uploads/2020/05/CyCon_2020_11_Libicki.pdf; and Benjamin Jensen and Brandon Valeriano, *What Do We Know About Cyber Escalation? Observations from Simulations and Surveys* (Washington, DC: Atlantic Council, November 2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf.

93 Healey and Jervis, "The Escalation Inversion."

94 Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review* 3, no. 3 (2020), doi:10.26153/tsw/10220.

95 While the existing body of research, such as the March 2020 edited volume *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict*, is beginning to explore how disinformation and extra-factual information may impact crisis stability, scholars have yet to explore and probe specific escalation pathways.

96 For example, see, Soroush Vosoughi et al., "The Spread of True and False News Online," *Science* 359, no. 6380 (March 2018), doi:10.1126/science.aap9559; and Gordon Ramsay and Sam Robertshaw, *Weaponizing News* (London: Policy Institute King's College London, January 2019), https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf.

97 The scenario set is better thought of as vignettes as they capture a limited point in time and lack the road to war, staging, and time-phasing associated with more fully developed scenarios.

98 Healey and Jervis, "The Escalation Inversion."

Key Findings and Recommendations

99 Reid Standish, "Why Is Finland Able to Fend Off Putin's Information War?," *Foreign Policy*, March 1, 2017, https:// foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/; and Michael Yankoski, Walter Scheirer, and Tim Weninger, "Meme Warfare: AI countermeasures to disinformation should focus on popular, not perfect, fakes," Bulletin of the Atomic Scientists, May 13, 2021, https://thebulletin.org/premium/2021-05/meme-warfare-ai-countermeasures-to-disinformation-should-focus-on-popular-not-perfect-fakes/.

100 Analyst Exchange Program, *Combatting Targeted Disinformation Campaigns: A whole-of-society issue*, (Washington, DC: Department of Homeland Security, 2019), 22, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

COVER PHOTO GREG BAKER/AFP/GETTY IMAGES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**

ROWMAN &
LITTLEFIELD

Lanham • Boulder • New York • London

4501 Forbes Boulevard
Lanham, MD 20706
301 459 3366 | **www.rowman.com**

ISBN 978-1-5381-4046-8
90000
9 781538 140468