Political Warfare and Propaganda
An Introduction

James J. F. Forest, PhD

Abstract: The digital age has greatly expanded the terrain and opportunities for a range of foreign influence efforts. A growing number of countries have invested significantly in their capabilities to disseminate online propaganda and disinformation worldwide, while simultaneously establishing information dominance at home. This introductory essay provides a brief examination of terms, concepts, and examples of these efforts and concludes by reviewing how the articles of this issue of the *Journal of Advanced Military Studies* contribute to our understanding of political warfare and propaganda.
Keywords: information operations, digital influence, political warfare, psychological warfare

In 1970, Canadian media theorist Marshall McLuhan predicted that World War III would involve "a guerrilla information war with no division between military and civilian participation."[1] More than 30 years later, in their 2001 groundbreaking book *Networks and Netwars: The Future of Terror, Crime, and Militancy*, John Arquilla and David Ronfeld described how

> the conduct and outcome of conflicts increasingly depend on information and communications. More than ever before, conflicts revolve around "knowledge" and the use of "soft power." Adversaries are learning to emphasize "information operations" and "perception management"—that is, media-

James J. F. Forest is a professor at the School of Criminology & Justice Studies, University of Massachusetts Lowell and a visiting professor at the Fletcher School, Tufts University. He has published more than 20 books in the field of international security studies, most recently *Digital Influence Warfare in the Age of Social Media* (2021) and *Digital Influence Mercenaries* (2021).

> oriented measures that aim to attract or disorient rather than coerce, and that affect how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries. Psychological disruption may become as important a goal as physical destruction.[2]

How prescient these observations seem today, particularly given how malicious actors—both foreign and domestic—are now weaponizing information for the purpose of influencing political, economic, social, and other kinds of behavior.

This issue of the *Journal of Advanced Military Studies* addresses the intersection of political warfare and the digital ecosystem. To frame the contributions that follow, this introduction to the issue reviews the broad landscape of terms and concepts that refer to the weaponization of information, and then provides a small handful of historical and modern examples that reflect the goals and objectives pursued through influence efforts. The discussion then turns to describe how the articles in this issue contribute to our understanding of political warfare and propaganda in the digital age, before concluding with some thoughts about the need for research-based strategies and policies that can improve our ability to defend against foreign influence efforts and mitigate their consequences.

A Diverse Landscape of Terms and Concepts

The past several centuries have largely been defined by physical security threats, requiring a nation's military to physically respond with whatever means they have available. But as explained by Isaiah Wilson III—president of Joint Special Operations University—today we face "compound security threats," which include physical security threats as well as "communication and information operations that scale with the speed of a social media post that goes viral, as well as cyber warfare, hacking and theft by our adversaries, both state and non-state actors."[3] These compound security threats can exploit cybersecurity vulnerabilities as well as psychological and emotional vulnerabilities of targets, using modern internet platforms to reach targets worldwide.

Terms like *information operations* or *information warfare* have been frequently used in military doctrine to describe computer network attacks (often by highly trained military units) like hacking into databases to observe or steal information, disrupting and degrading a target's technological capabilities, weakening military readiness, extorting financial ransoms, and much more. These terms have also referred to operations intended to protect our own data from these attacks by adversaries. Computer network attacks like these can also be used to send a message (e.g., about a target's vulnerabilities and the attacker's capabilities), and in that way could be a means of influencing others. Cyberattacks are seen as compound security threats because they can have implications

for multiple dimensions of a nation's well-being, including politics, economics, technology, information security, relations with other countries, and much more.

Today's digital influence attacks also have implications for these same multiple dimensions and are likewise seen as compound security threats. The goals of digital influence attacks can include disrupting and degrading a target's societal cohesion, undermining confidence in political systems and institutions (i.e., democratic elections), fracturing international alliances, and much more. Tactics used in such attacks include various forms of deception and provocation, from deepfake videos and fake social media accounts to gaslighting, doxing, trolling, and many others. Through social media and other internet technologies, attackers can incentivize and manipulate interactions directly with citizens of a foreign population, bypassing government efforts to insulate their citizens from an onslaught of disinformation.[4] These types of attacks exploit human vulnerabilities more than technological attacks and capitalize on psychological and emotional dimensions like fear, uncertainty, cognitive biases, and others.

A variety of terms are used to describe these attacks, sometimes leading to confusion rather than clarity. The term *political warfare* was used by the legendary diplomat George Kennan in 1948 to describe "the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert and can include various kinds of propaganda as well as covert operations that provide clandestine support to underground resistance in hostile states."[5] Paul A. Smith describes political warfare as "the use of political means to compel an opponent to do one's will" and "its chief aspect is the use of words, images, and ideas, commonly known, according to context, as propaganda and psychological warfare."[6] Carnes Lord notes a "tendency to use the terms psychological warfare and political warfare interchangeably" along with "a variety of similar terms—ideological warfare, the war of ideas, political communication and more."[7] And the U.S. Department of Defense has used the term *military information support operations* to describe efforts to "convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."[8]

In a 2019 research report published by Princeton University, Diego A. Martin and Jacob N. Shapiro illustrate how "foreign actors have used social media to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation."[9] The researchers define *foreign-influence efforts* as: 1) coordinated campaigns by one state to impact one or more specific aspects of politics in another state, 2)

through media channels, including social media, and by 3) producing content designed to appear indigenous to the target state.[10] The objective of such campaigns can be quite broad and to date have included influencing political decisions by shaping election outcomes at various levels, shifting the political agenda on topics ranging from health to security, and encouraging political polarization.[11] Similarly, research by Philip N. Howard describes "countries with dedicated teams meddling in the affairs of their neighbors through social media misinformation."[12] And social media platforms—most notably Facebook—are now using the term *information operations* when referring to deliberate and systematic attempts to steer public opinion using inauthentic accounts and inaccurate information.[13]

A recent book by Carl Miller describes how "digital warfare has broken out between states struggling for control over what people see and believe."[14] Other terms used in the literature include "new generation warfare," "ambiguous warfare," "full-spectrum warfare," and "non-linear war."[15] Scholars have also described these security challenges as forms of hybrid warfare, encompassing a combination of political warfare, psychological operations, and information operations (including propaganda). Similar terms in this broad landscape include *public diplomacy* and *strategic communications*. Further, some states are portrayed as pursuing "information dominance" over the populations of other states through a combination of computer network operations, deception, public affairs, public diplomacy, perception management, psychological operations, electronic countermeasures, jamming, and defense suppression.[16]

Whatever we want to call it, there are clear examples of aggression, attackers, targets, defenders, tactics, strategies, goals, winners, losers, and innocent victims. And this is not something that only states do to other states: non-state actors are increasingly engaged in these kinds of activities as well.[17] The author's own work has used the term *influence warfare* to describe the kinds of activities in which the focus is not the information but on the *purposes* of that information.[18] This conceptual approach views the implicit goal of spreading propaganda, misinformation, disinformation, and so forth as shaping perceptions and influencing behavior of a specific target (or set of targets). Further, influence warfare strategies and tactics—particularly as we have seen online—also involve more than just manipulation of information; they can include behavior signaling (e.g., swarming or bandwagoning), trolling, gaslighting, and other means by which the target is provoked into having an emotional response that typically overpowers any rational thought or behavior.[19] Clickbait, memes, and ragebait (for example) are not really seen as forms of information operations as traditionally conceived, but they are certainly ways of influencing others via the internet. This leads us to the term *digital influence warfare,* which will be used variably throughout this introduction

as a catchall phrase representing the broadly diverse terrain of political and psychological warfare in the digital age.[20]

Strategic Goals and Tactics of Influence Warfare

The "weaponization of information" in order to obtain power and influence is of course not new. The principles of influence warfare are based on an ancient and much-repeated maxim, attributed to the Chinese general and military theorist Sun Tzu, paraphrased as "to win one hundred victories in one hundred battles is not the highest skill. To subdue the enemy without fighting is the highest skill."[21] When the thirteenth-century Mongols were rolling across Eurasia, they deliberately spread news of the atrocities they perpetrated on cities that did not surrender, the obvious goal being what Sun Tzu argued was the ultimate victory: to defeat the enemy before a single shot has been fired. As Marc Galeotti explains, fear is a powerful emotion, and in this instance it was used to coerce the behavior of cities the Mongols had in their sights, preferring that they surrender instead of having to spend valuable resources conquering them through force.[22] Mongol hordes would also drag branches behind their horses to raise dust clouds suggesting their armies were far larger than reality—an early and effective form of deception and disinformation.

The previous century saw a wide variety of efforts involving the weaponization of information for strategic purposes. During the Chinese Civil War (1945–49), both the Communist and Nationalist (Kuomintang, or KMT) armies spread false information to sow discord in enemy-controlled areas, spreading rumors about defections, falsifying enemy attack plans, and stirring up unrest in an effort to misdirect enemy planning. After the Nationalist government relocated to Taiwan in 1949, the influence efforts continued as the two sides flooded propaganda and disinformation into enemy-controlled territories to affect public opinion and troop morale.[23] Various forms of influence warfare also played a major role in both World Wars. For example, the Committee on Public Information was created during World War I by U.S. president Woodrow Wilson to facilitate communications and serve as a worldwide propaganda organization on behalf of the United States.[24]

Influence warfare was increasingly prominent throughout World War II, especially the massive amounts of propaganda disseminated by Joseph Goebbels and the Nazi regime. In response, U.S. president Franklin D. Roosevelt established the Office of War Information in 1942, responsible for (among other things) undermining the enemy's morale—often through various psychological and information operations—as well as for providing moral support and strengthening the resolve of resistance movements in enemy territories. The Voice of America (VOA) was also established in 1942 as the foreign radio and television broadcasting service of the U.S. government, broadcasting in English,

French, and Italian. Years later, the United States Information Agency (USIA) was created in 1953 as a primary conduit for enhancing our nation's strategic influence during the Cold War.[25] The director of USIA reported to the president through the National Security Council and coordinated closely with the secretary of state on foreign policy matters.

Meanwhile, when Radio Moscow began broadcasting in 1922, it was initially available only in Moscow and its surrounding areas, but by 1929, the Soviets were able to broadcast into Europe, North and South America, Japan, and the Middle East using a variety of languages.[26] By 1941, the Union of Soviet Socialist Republics (USSR) was able to broadcast in 21 languages and, 10 years later, had a program schedule of 2,094 hours.[27] But radio and television broadcasting were just the visible tip of the iceberg for what became a multidimensional influence effort during the Cold War involving an array of covert influence tactics, particularly through the spread of disinformation. As Thomas Rid notes, "Entire bureaucracies were created in the Eastern bloc during the 1960s for the purpose of bending the facts."[28] The Soviets used disinformation "to exacerbate tensions and contradictions within the adversary's body politic, by leveraging facts, fakes, and ideally a disorienting mix of both."[29]

In the first academic study of the Soviet-era active measures program, Richard H. Shultz and Roy Godson explain how the Soviets cultivated several different types of so-called "agents of influence . . . including the unwitting but manipulated individual, the 'trusted contact,' and the controlled covert agent."[30] As they explain,

> The agent of influence may be a journalist, a government official, a labor leader, an academic, an opinion leader, an artist, or involved in a number of other professions. The main objective of an influence operation is the use of the agent's position—be it in government, politics, labor, journalism or some other field—to support and promote political conditions desired by the sponsoring foreign power.[31]

Forged documents—including faked photographs—have also been a part of influence warfare for more than a century. For example, during the 1920s the Soviet Cheka (secret police) used elaborate forgeries to lure anti-Bolsheviks out of hiding, and many were captured and killed as a result.[32] During the Cold War, as Shultz and Godson note, many "authentic-looking but false U.S. government documents and communiqués" could be categorized mainly as either "altered or distorted versions of actual US documents that the Soviets obtained (usually through espionage)" or "documents that [were] entirely fabricated."[33] Examples include falsified U.S. State Department documents ordering diplo-

matic missions to sabotage peace negotiations or other endeavors, fake documents outlining U.S. plans to manipulate the leaders of Third World countries, or even forged cables from an American embassy outlining a proposed plan to overthrow a country's leader.[34]

In one case, an authentic, unclassified U.S. government map was misrepresented as showing nuclear missiles targeting Austrian cities. A fabricated letter ostensibly written by the U.S. defense attaché in Rome contained language denying "rumors suggesting the death of children in Naples could be due to chemical or biological substances stored at American bases near Naples," while no such substances were stored at those bases.[35] Even a fake U.S. Army Field Manual was distributed, purportedly encouraging Army intelligence personnel to interfere in the affairs of host countries and subvert foreign government officials and military officers.[36] Through these and other types of information operations, the Soviets tried to influence a range of audiences, and the lessons to be learned from this history—both successes and failures—can inform the influence warfare efforts of many countries today.

Influence Opportunities in the Digital Age

While the primary strategies and goals of influence warfare have remained fairly constant, the operational environment in which these efforts take place has changed significantly during the past two decades. The rise of the internet and social media companies, whose profit model is based on an attention economy, has been a game changer. Within the attention economy, the most valued content is that which is most likely to attract attention and provoke engagement, with no regard to whether it is beneficial or harmful, true or untrue. New tools have emerged for creating and spreading information (and disinformation) on a global scale. Connectivity in the digital realm is now much easier, and yet the emergence of hyperpartisan echo chambers has sequestered many online users into separate communities who reject the credibility and merits of each other's ideas, beliefs, and narratives.

Unlike conventional cyberattacks, the goal of a digital influence warfare campaign is not about degrading the functional integrity of a computer system. Rather, it is to use those computer systems against the target in whatever ways might benefit that attacker's objectives. Often, those objectives include a basic divide and conquer strategy—a society that is disunited will fight among themselves over lots of things, instead of coming together in the face of a threat that only some of them believe is there. Many influence activities are meant to shape the perceptions, choices, and behaviors of a society—and in some cases, the goal may in fact be making the target dysfunctional as a society. This is not simply propaganda, fake news, or perception manipulation. It is a battle over

what people believe is reality and the decisions that each individual makes based on those beliefs. The victors in this battle are the attackers who have convinced scores of victims to make decisions that directly benefit the attackers.

Digital influence warfare involves the use of persuasion tactics, information and disinformation, provocation, identity deception, computer network hacking, altered videos and images, cyberbullying, and many other types of activity explored in this issue of the *Journal of Advanced Military Studies*. The attacker (or "influencer") seeks to weaponize information against a target in order to gain the power needed to achieve the goals articulated in their strategic influence plan. Some goals may involve changing the target's beliefs and behaviors, prompting the targets to question their beliefs in the hopes that once those beliefs have been undermined, the targets may change their minds. Other goals may include manufacturing uncertainty to convince the target that nothing may be true and anything may be possible.[37] In other instances, the goals of an influence strategy could include strengthening the target's certainty, even their commitment to believing in things that are actually untrue.

The central goal of influence attacks is—according to a recent report by Rand—"to cause the target to behave in a manner favorable to the influencer."[38] The influencer may seek to disrupt the target's information environment—for example, interrupting the flow of information between sources and intended recipients of an organization, or on a broader level, between the target's government and its citizens. Similarly, the influencer may also seek to degrade the quality, efficiency, and effectiveness of the target's communication capabilities, which may involve flooding channels of communication with misinformation and disinformation. The overall goal here involves undermining the perceived credibility and reliability of information shared among the adversary's organizational members (government or corporate) or between the target's government and its citizens.[39] Attackers in the digital influence domain can organize swarms of automated social media accounts ("bots") alongside real accounts, coordinated to amplify a particular narrative or attack a specific target. Government (or corporate) leaders can hire technically skilled mercenaries and contractors (from large so-called social media influence corporations to lone hackers) to do the dirty work for them.[40]

Based on whatever goals the attacker wants to achieve, they will need to identify the targets they want to influence. When conducting research on their targets, the attackers will seek to answer specific questions like: What do they already believe about their world and/or their place within it? What do they think they know, and what are they uncertain about? What assumptions, suspicions, prejudices, and biases might they have? What challenges and grievances (economic, sociopolitical, security, identity, etc.) seem to provoke the most emotional reactions among them? Throughout the history of influence warfare,

this information has been relatively easy to identify in open liberal democracies of the West. In more closed or oppressed societies, an additional step may be needed to determine how the target audience's perceptions compare to the discourse in the public domain—for example, what the news media (often owned and controlled by the government) identify as important topics and acceptable views within that society may not fully reflect the reality.

Influence efforts should always be guided by data on potential targets. An attacker should never waste their resources on target audiences that are already well-armed to repeal the influence efforts; better instead to identify vulnerable targets to exploit. For example, if the goal is to sow division and increase political polarization within a society, the United States offers a prime target for achieving that goal. Research by the Oxford Internet Institute in 2019 has found that people in the United States share more junk news (i.e., completely fabricated information disguised to look like authentic news) than people in other advanced democracies such as France, Germany, and the United Kingdom.[41] A study by the Pew Research Center in 2017 found that 67 percent of U.S. adults received news through social media sites like Twitter and Facebook.[42] Further, analysis of Russian influence efforts by the Atlantic Council's Digital Forensic Research Lab in 2018 found that Americans were vulnerable to a distinct type of troll accounts that used "carefully crafted personalities" to infiltrate activist communities and post hyperpartisan messages in order to "make their audiences ever more radical."[43]

These research studies reflect another important dimension of influence efforts: after gathering enough quality information about the target, the attacker will then seek to establish a foothold in the information environment preferred by that target. They must establish a credible presence among an audience of like-minded social media users before attempting to influence or polarize that audience. A common approach involves initially posting some messages that the target audience is likely to agree with. The convention of "like" or "share" facilitated by social media platforms can draw the target toward recognition of an acceptable persona (the "like-minded, fellow traveler").[44] Once established within the target's digital ecosystem, the persona can then begin to shape perceptions and behavior in ways that will benefit their influence strategy.

Perhaps the most well-known example of this in the public arena today is called disinformation or fake news. Essentially, these are forms of information deception, and there are several variations to consider. According to researcher Claire Wardle, some of the most "problematic content within our information ecosystem" includes:

- False connection: when headlines, visuals, or captions do not support the substance or content of the story itself;

- Misleading content: misleading use of information to frame an issue or individual;
- False context: when genuine content is shared with false contextual information;
- Imposter content: when genuine sources are impersonated;
- Manipulated content: when genuine information or imagery is manipulated to deceive (altered videos and images, including deepfakes, are the most prevalent examples of this); and
- Fabricated content: new content is 100 percent false and designed to deceive and do harm.[45]

Each of these forms of "problematic content" has a role to play in achieving an influence warfare strategy. Further, in many cases the most effective means of using these types of information (or disinformation) involves a careful integration between fake details and accurate details that the target already accepts as true. In the field of education, teachers often refer to the concept of *scaffolding* as a strategy to foster learning by introducing material that builds on what the student already understands or believes. For the purposes of an influence strategy, as Thomas Rid explains, for disinformation to be successful it must "at least partially respond to reality, or at least accepted views."[46]

Additional examples of deceptive digital influence tactics include identity deception (e.g., using fake or hijacked social media accounts) and information source deception (e.g., rerouting internet traffic to different sources of information that seem legitimate but relays false information to the viewers). As with the other forms of deception, a primary intent of these tactics is for the influencer to make the target believe what is not true. Similarly, the influencer may also spread disinformation through the target's trusted communication channels to degrade the integrity of their decision making and even their perception of reality.

Of course, deception is only one of several digital influence strategies. Another, which we have seen in use frequently in recent years, is to encourage engagement—especially by provoking emotional responses—using information that may in fact be all or partially accurate. Unlike disinformation and deception, the primary focus here is less on the message than on provoking people to propagate the message. Effective targets for this approach are those who have higher uncertainty about what is true or not but are willing to share and retransmit information without knowing whether it is untrue (and often because they want it to be true). And it is widely understood that fear is an exceptionally powerful emotion that can lead people to make a wide variety of (often unwise) decisions.

There are many kinds of influence goals that can be achieved by inten-

tionally provoking emotional responses, usually in reference to something that the target already favors or opposes. The tactic of provoking outrage can be particularly effective here against a target audience—as Sun Tzu wrote, "Use anger to throw them into disarray."[47] With the right sort of targeting, message format, and content, the influencer can use provocation tactics to produce whatever kinds of behavior they want by the target (e.g., angrily lashing out at members of an opposing political party or questioning the scientific evidence behind an inconvenient truth). And an additional type of influence warfare involves attacking the target directly—threatening or bullying them, calling them derogatory names, spreading embarrassing photos and videos of them, and so forth.

One of the most well-known earlier forms of digital influence warfare was North Korea's attack against Sony. In the summer of 2014, Sony Pictures had planned to release a comedy, *The Interview*, featuring a plot in which two bumbling, incompetent journalists score an interview with Kim Jong-un, but before they leave they are recruited by the Central Intelligence Agency (CIA) to blow him up.[48] An angered North Korea responded by hacking into Sony's computer networks, destroying some key systems and stealing tons of confidential emails that they later released publicly in small, increasingly embarrassing quantities. Details about contracts with Hollywood stars, medical records, salaries, and Social Security numbers were also released. But unlike other well-reported cyberattacks of that era, this was—in the words of David E. Sanger—"intended as a weapon of political coercion."[49] As with many other examples of this hack and release tactic, the strategic goals are fairly straightforward: for example, to weaken an adversary by undermining its perceived credibility. This same script was followed by Russia during the 2016 U.S. presidential election, when they hacked into John Podesta's email account and released (via WikiLeaks) a stream of embarrassing messages (as detailed in the investigation report by former Federal Bureau of Investigation [FBI] director Robert S. Mueller III).[50]

Today, states are engaged in these kinds of digital influence activities with increasing regularity and sophistication. As a July 2020 report by the Stanford Internet Observatory explains:

> Well-resourced countries have demonstrated sophisticated abilities to carry out influence operations in both traditional and social media ecosystems simultaneously. Russia, China, Iran, and a variety of other nation-states control media properties with significant audiences, often with reach far beyond their borders. They have also been implicated in social media company takedowns of accounts and pages that are manipulative either by virtue of the fake accounts and suspicious domains involved, or by way of coordinated distribution tactics

> to drive attention to certain content or to create the perception that a particular narrative is extremely popular.[51]

China in particular has significantly ramped up its digital foreign-influence efforts, to include disrupting Twitter conversations about the conflict in Tibet and meddling in Taiwanese politics.[52] In fact, public opinion warfare and psychological warfare are closely intertwined in Chinese military doctrine. According to a recent Pentagon report, China's approach to psychological warfare "seeks to influence and/or disrupt an opponent's decision-making capability, to create doubts, foment anti-leadership sentiments, to deceive opponents and to attempt to diminish the will to fight among opponents."[53] A primary objective, as Laura Jackson explains, is "to demoralize both military personnel and civilian populations, and thus, over time, to diminish their will to act . . . to undermine international institutions, change borders, and subvert global media, all without firing a shot."[54]

China's "Three Warfares" doctrine is focused on: (1) public opinion (media) warfare (*yulun zhan*); (2) psychological warfare (*xinli zhan*); and (3) legal warfare (*falu zhan*).[55] In their conception of public opinion warfare, the goal is to influence both domestic and international public opinion in ways that build support for China's own military operations, while undermining any justification for an adversary who is taking actions counter to China's interests.[56] But this effort goes well beyond what Steven Collins refers to in a 2003 *NATO Review* article as "perception management," in which a nation or organization provides (or withholds) certain kinds of information to influence foreign public opinion, leaders, intelligence agencies, and the policies and behaviors that result from their interpretation of this information.[57] According to the Pentagon report, China "leverages all instruments that inform and influence public opinion . . . and is directed against domestic populations in target countries."[58] As Laura Jackson explains, "China's extensive global media network, most notably the Xinhua News Agency and China Central Television (CCTV), also plays a key role, broadcasting in foreign languages and providing programming to stations throughout Africa, Central Asia, Europe, and Latin America."[59] In turn, Western media outlets then repeat and amplify the spread of messages to a broader international audience, lending a perception of legitimacy to what is in fact Chinese state-directed propaganda.[60]

Similarly, Russia has also engaged in a broad, multifaceted influence warfare campaign involving all of the former tools and tactics of its active measures program along with a flurry of new technological approaches. Media outlets like Sputnik and RT (formerly Russia Today) view themselves—according to Margarita Simonyan, chief editor of RT—as equal in importance to the Defense Ministry, using "information as a weapon."[61] And like many other au-

thoritarian regimes, Russia has invested heavily in online troll farms, armies of automated bot accounts, cyber hacking units, and other means by which they can pursue their foreign influence goals using the most modern tools available to them.[62] While the "agent of influence" of the Cold War may have been a journalist, a government official, a labor leader, or an academic (among many other examples), today the agent is more likely to be a social media user with enough followers to be considered a potential "influencer."[63]

According to a report by the Stanford Internet Observatory, both China and Russia have "full-spectrum propaganda capabilities," including prominent Facebook pages and YouTube channels targeting regionalized audiences.[64] Both have military units dedicated to influencing foreign targets and also encourage and incentivize citizen involvement in those efforts.[65] They gather extensive information about their targets and manage an array of fake Facebook pages and Twitter personas that are used for eroding the international perception and domestic social cohesion of its rivals.[66] And as detailed in many reports by congressional committees, think tanks, and academics, Russia has been particularly aggressive during this past decade in its online efforts to influence democratic elections in the United States, Europe, Africa, and elsewhere, as well as to sow confusion and encourage widespread societal polarization and animosity.[67]

Meanwhile, other countries are also increasingly engaging in their own forms of digital influence warfare. In October 2019, Facebook announced the deletion of 93 Facebook accounts, 17 Facebook pages, and 4 Instagram accounts "for violating our policy against coordinated inauthentic behavior. This activity originated in Iran and focused primarily on the US, and some on French-speaking audiences in North Africa."[68] According to the announcement, "the individuals behind this activity used compromised and fake accounts—some of which had already been disabled by our automated systems—to masquerade as locals, manage their Pages, join Groups and drive people to off-platform domains connected to our previous investigation into the Iran-linked 'Liberty Front Press' and its removal in August 2018."[69] Facebook also removed 38 Facebook accounts, 6 pages, 4 groups, and 10 Instagram accounts that originated in Iran and focused on countries in Latin America, including Venezuela, Brazil, Argentina, Bolivia, Peru, Ecuador, and Mexico. The page administrators and account owners typically represented themselves as locals, used fake accounts to post in groups and manage pages posing as news organizations, as well as directed traffic to other websites.[70] And that same month, Microsoft announced that hackers linked to the Iranian government targeted an undisclosed U.S. presidential campaign, as well as government officials, media outlets, and prominent expatriate Iranians.[71]

In short, older strategies, tactics, and tools of influence warfare have evolved to encompass a new and very powerful digital dimension. By using massive

amounts of internet user data, including profiles and patterns of online behavior, microtargeting strategies have become a very effective means of influencing people from many backgrounds. The strategies, tactics, and tools of digital influence warfare will increasingly be used by foreign and domestic actors to manipulate our perceptions in ways that will negatively affect us. According to a 2018 United Nations Educational, Scientific and Cultural Organization (UNESCO) report, the danger we face in the future is "the development of an 'arms race' of national and international disinformation spread through partisan 'news' organizations and social media channels, polluting the information environment for all sides."[72]

Tomorrow's disinformation and perceptions manipulation will be much worse than what we are dealing with now, in part because the tactics and tools are becoming more innovative and sophisticated. As a 2019 report by Rand notes, "Increasingly, hostile social manipulation will be able to target the information foundations of digitized societies: the databases, algorithms, networked devices, and artificial intelligence programs that will dominate the day-to-day operation of the society."[73] The future evolution of digital influence tools—including augmented reality, virtual reality, and artificial intelligence (AI)—promise to bring further confusion and challenges to an already chaotic situation, offering a new frontier for disinformation and perceptions manipulation.[74] For example, in the not-too-distant future we will see a flood of fake audio, images, messages, and video created through AI that will appear so real it will be increasingly difficult to convince people they are fakes.[75] Technology already exists that can be used to manipulate an audio recording to delete words from a speech and then stitch the rest together seamlessly, or add new words using software that replicates the voice of the speaker with uncanny accuracy.[76] Imagine the harm that can be done when in the future, digital influencers have the ability to clone any voice, use it to say anything the influencer wants, and then use that audio recording to persuade others.[77]

Creating deepfake images and video is also becoming easier, with increasingly realistic results becoming more convincing. One particularly sophisticated AI-related approach involves a tool known as generative adversarial networks (GANs). These involve integrating a competitive function into software, with one network seeking to generate an item, such as an image or video, while the other network judges the item to determine whether it looks real. As the first network continues to adapt to fool the adversarial network, the software learns how to better create more realistic images or videos.[78] Over time, according to Michael Mazzar and his colleagues at Rand, "As technology improves the quality of this production, it will likely become more difficult to discern real events from doctored or artificial ones, particularly if combined with the advancements in audio software."[79] If the target of such deepfake disinformation holds

true to the old adage of "hearing and seeing is believing," the long-term harmful effects of this technology are quite obvious. Technological advances will make it increasingly difficult to distinguish real people from computer-generated ones, and even more difficult to convince people that they are being deceived by someone they believe is real.

And, of course, we can fully expect that digital influence warfare attacks against democratic elections will continue and will likely involve new and innovative tactics. For example, there are concerns that in the future malicious hackers could use ransomware to snatch and hold hostage databases of local voter registrations or cause power disruptions at polling centers on election day. Further, as one expert noted, "with Americans so mistrustful of one another, and of the political process, the fear of hacking could be as dangerous as an actual cyberattack—especially if the election is close."[80] As Laura Rosenberger observes, "You don't actually have to breach an election system in order to create the public impression that you have."[81] The future will likely bring darker influence silos that no light of truth can penetrate, resulting in heightened uncertainty and distrust, deeper animosity, more extremism and violence, and widespread belief in things that simply are not true. This is the future that the enemies of America's peace and prosperity want to engineer. The United States must find ways to prevent them from succeeding. The research and analysis provided in this issue contributes to that important goal.

The Issue of *JAMS* on Political Warfare and Propaganda

Each of the contributions to this issue addresses the central theme of influencing perceptions and behavior. First, Daniel de Wit draws lessons from a historical analysis of the Office of Strategic Services (OSS), America's intelligence and special operations organization in World War II. In addition to its efforts to collect intelligence on the Axis powers and to arm and train resistance groups behind enemy lines, the OSS also served as America's primary psychological warfare agency, using a variety of "black propaganda" methods to sow dissension and confusion in enemy ranks.[82] As noted earlier, psychological warfare plays a significant role in the conduct of today's military operations, so de Wit's research offers important historical lessons for contemporary campaign planners.

Next, Kyleanne Hunter and Emma Jouenne examine the uniquely troubling effects of spreading misogynistic views online. Their analysis of three diverse case studies—the U.S. military, the incel movement, and ISIS—reveals how unchecked online misogyny can result in physical behavior that can threaten human and national security. Glen Segell then explores how perceptions about cybersecurity operations can have positive or negative impacts on civil-military relations, drawing on a case study of the Israeli experience. Lev Topor and Alexander Tabachnik follow with a study of how Russia uses the

strategies and tactics of digital influence warfare against other countries, while continually seeking to strengthen its information dominance over Russian citizens. And Donald M. Bishop reveals how other countries do this as well, including China, North Korea, Iran, Cuba, and Venezuela. Each is engaged in these same kinds of efforts to control the information that circulates within their respective societies, while using various forms of propaganda against other countries to strengthen their influence and national power.

Phil Zeman's contribution to this issue looks at how China and Russia are trying to fracture American and Western societies through information, disinformation, economic coercion, and the creation of economic dependencies—in many cases capitalizing on specific attributes and vulnerabilities of a target nation to achieve their strategic objectives. Through these efforts, he concludes, China and Russia hope to prevent the will or ability of American or Western states to respond to an aggressive act. Next, Michael Cserkits explains how a society's perceptions about armed forces can be influenced by cinematic productions and anime, drawing on a case study comparison of Japan and the United States. And finally, Anthony Patrick examines how social media penetration and internet connectivity could impact the likelihood that parties within a conventional intrastate conflict will enter negotiations.

As a collection, these articles make a significant contribution to the scholarly research literature on political warfare and propaganda. The authors shed light on the need for research-based strategies and policies that can improve our ability to identify, defend against, and mitigate the consequences of influence efforts. However, when reflecting on the compound security threats described at the beginning of this introduction—involving both cyberattacks and influence attacks—a startling contrast is revealed: we have committed serious resources toward cybersecurity but not toward addressing the influence issues examined in this issue. We routinely install firewalls and other security measures around our computer network systems, track potential intrusion attempts, test and report network vulnerabilities, hold training seminars for new employees, and take many other measures to try and mitigate cybersecurity threats. In contrast, there are no firewalls or intrusion detection efforts defending us against digital influence attacks of either foreign or domestic origin. Government sanctions and social media deplatforming efforts respond to influence attackers once they have been identified as such, but these efforts take place after attacks have already occurred, sometimes over the course of several years.

The articles of this issue reflect an array of efforts to influence the perceptions, emotions, and behavior of human beings at both individual and societal levels. In the absence of comprehensive strategies to more effectively defend against these efforts, the United States risks losing much more than military advantage; we are placing at risk the perceived legitimacy of our sys-

tems and institutions of governance, as well as our economic security, our ability to resolve social disagreements peacefully, and much more.[83] Further, many other nations are also facing the challenges of defending against foreign influence efforts. As such, the transnational nature of influence opportunities and capabilities in the digital age may require a multinational, coordinated response. In the years ahead, further research will be needed to uncover strategies for responding to the threat of digital influence warfare with greater sophistication and success.

Endnotes

1. Marshall McLuhan, *Culture Is Our Business* (Eugene, OR: Wipf and Stock Publishers, 1970), 66.
2. John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: Rand, 2001), 1, https://doi.org/10.7249/MR1382.
3. Isaiah Wilson III, "What Is Compound Security?: With Dr. Isaiah 'Ike' Wilson III (Part 2 of 4)," YouTube, 26 February 2021, 16:48; and Isaiah Wilson III and Scott A. Smitson, "The Compound Security Dilemma: Threats at the Nexus of War and Peace," *Parameters* 50, no. 2 (Summer 2020): 1–17.
4. Wilson, "What Is Compound Security?"; and Wilson and Smitson, "The Compound Security Dilemma."
5. Max Boot and Michael Doran, "Political Warfare," Council on Foreign Relations, 28 June 2013.
6. Paul A. Smith, *On Political War* (Washington, DC: National Defense University Press, 1989), 3.
7. Carnes Lord, "The Psychological Dimension in National Strategy," in *Political Warfare and Psychological Operations: Rethinking the US Approach*, ed. Carnes Lord and Frank R. Barnett (Washington, DC: National Defense University Press, 1989), 16.
8. *Military Information Support Operations*, Joint Publication 3-13.2 (Washington, DC: Joint Chiefs of Staff, 2014).
9. Diego A. Martin and Jacob N. Shapiro, *Trends in Online Foreign Influence Efforts* (Princeton, NJ: Woodrow Wilson School of Public and International Affairs, Princeton University, 2019), 3.
10. Martin and Shapiro, *Trends in Online Foreign Influence Efforts.*
11. Martin and Shapiro, *Trends in Online Foreign Influence Efforts.*
12. Philip N. Howard, *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives* (New Haven, CT: Yale University Press, 2020), 75.
13. Caroline Jack, *Lexicon of Lies: Terms for Problematic Information* (New York: Data & Society Research Institute, 2017), 6.
14. Carl Miller, *The Death of the Gods: The New Global Power Grab* (London: Windmill Books, 2018), xvi.
15. Mark Galeotti, *Russian Political War: Moving Beyond the Hybrid* (Abingdon, UK: Routledge, 2019), 11.
16. Michael V. Hayden, *The Assault on Intelligence: American National Security in an Age of Lies* (New York: Penguin Press, 2018), 191.
17. In addition to terrorists and insurgents using these tools of digital influence for political purposes, we also see various kinds of individuals and marketing firms engaged in profit-seeking activities as described in James J. F. Forest, *Digital Influence Mercenaries: Profit and Power Through Information Warfare* (Annapolis, MD: Naval Institute Press, 2021).

18. James. J. F. Forest, ed., *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas* (Westport, CT: Praeger Security International, 2009).
19. While Arquilla and Ronfeldt initially defined *swarming* as a "deliberately structured, coordinated, strategic way to strike from all directions," in this context the term is used to describe a collection of social media accounts that converges on a single target like a swarm of bees. See John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: Rand, 2000); Ali Fisher, "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence," *Perspectives on Terrorism* 9, no. 3 (June 2015): 3–20; and *bandwagoning* is a term from social psychology used to describe a type of cognitive bias and collective identity signaling that leads people to adopt the behaviors or attitudes of others. This can be observed in political campaigns, support for a winning sports team, fashion trends, adoption of new consumer electronics, and many other arenas of daily life.
20. James J. F. Forest, *Digital Influence Warfare in the Age of Social Media* (Santa Barbara, CA: ABC-CLIO/Praeger Security International, 2021).
21. Specifically, chapter 3, "Attack by Strategem" reads: "Supreme excellence consists in breaking the enemy's resistance without fighting." Sun Tzu, *The Art of War* (New York: Fall River Press, 2015), 54.
22. Galeotti, *Russian Political War*, 10.
23. Russell Hsiao, "CCP Propaganda against Taiwan Enters the Social Age," *China Brief* 18, no. 7 (April 2018).
24. W. Phillips Davison, "Some Trends in International Propaganda," *Annals of the American Academy of Political Science and Social Science* 398, no. 1 (November 1971): 1–13, https://doi.org/10.1177/000271627139800102.
25. Daniel Baracskay, "U.S. Strategic Communication Efforts during the Cold War," in *Influence Warfare*, 253–74.
26. James Woods, *History of International Broadcasting*, vol. 2 (London: IET, 1992), 110.
27. Woods, *History of International Broadcasting*, 110–11.
28. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Strauss and Giroux, 2020), 4.
29. Rid, *Active Measures*, 7.
30. Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (New York: Pergamon Brassey's, 1984), 133.
31. Shultz and Godson, *Dezinformatsia*, 133.
32. Shultz and Godson, *Dezinformatsia*, 149.
33. Shultz and Godson, *Dezinformatsia*, 150–51.
34. Shultz and Godson, *Dezinformatsia*, 152–53.
35. Shultz and Godson, *Dezinformatsia*, 155.
36. Shultz and Godson, *Dezinformatsia*, 157.
37. This is a cornerstone of Russia's digital influence warfare program and the title of an important book. See Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia* (New York: Public Affairs, 2014).
38. This section of the discussion significantly amplifies and paraphrases a report by Eric V. Larson et al., *Understanding Commanders' Information Needs for Influence Operations* (Santa Monica, CA: Rand, 2009), Appendix B: Task List Analysis, 71–73, which cites several Department of the Army documents and 1st Information Operations Command (Land), Field Support Division, "Terminology for IO Effects," in *Tactics, Techniques and Procedures for Operational and Tactical Information Operations Planning* (Washington, DC: Department of the Army, 2004), 23.
39. Larson et al., *Understanding Commanders' Information Needs for Influence Operations*, 71–73.
40. For details, see Forest, *Digital Influence Mercenaries.*
41. Howard, *Lie Machines*, 99–100. *Junk news* was defined by the Oxford Internet Institute as being articles from outlets that publish "deliberately misleading, deceptive or incorrect information." See Ryan Browne, " 'Junk News' Gets Massive Engagement on Facebook Ahead of EU Elections, Study Finds," CNBC, 21 May 2019.

42. Elisa Shearer and Jeffrey Gottfried, "News Use Across Social Media Platforms 2017," Pew Research Center, 7 September 2017.
43. Ben Nimmo, Graham Brookie, and Kanishk Karanm, "#TrollTracker: Twitter Troll Farm Archives, Part One—Seven Key Take Aways from a Comprehensive Archive of Known Russian and Iranian Troll Operations," Atlantic Council's Digital Forensic Research Lab, 17 October 2018.
44. For the purpose of this discussion, a "like-minded fellow traveler" is described as someone who sees the world in much the same way you do and is moving intellectually and emotionally in a direction that you approve of.
45. Claire Wardle, "Fake News. It's Complicated," First Draft, 16 February 2017.
46. Rid, *Active Measures*, 5, with a direct quote from famous Soviet defector Ladislav Bittman, author of the 1972 book *The Deception Game* (Syracuse, NY: Syracuse University Research Corp, 1972).
47. Various interpretations of this classic work use different phrasing. For example, "If your opponent is of choleric temper, seek to irritate him." Sun Tzu, *The Art of War*, 49 (passage 1.22); and "When their military leadership is obstreperous, you should irritate them to make them angry—then they will become impetuous and ignore their original strategy." Sun Tzu, *The Art of War*, trans. by Thomas Cleary (Boston, MA: Shambhala Pocket Classics, 1991), 15 (passage 1.12).
48. For a detailed examination of this event, see David E. Sanger, *The Perfect Weapon: Sabotage and Fear in the Cyber Age* (New York: Crown Publishing, 2018), 124–43.
49. Sanger, *The Perfect Weapon*, 143.
50. Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vol. 1 (Washington, DC: Department of Justice, 2019).
51. Renee DiResta et al., *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives* (Stanford, CA: Stanford Internet Observatory and Hoover Institution, Stanford University, 2020), 3.
52. Howard, *Lie Machines*, 77; Jonathan Kaiman, "Free Tibet Exposes Fake Twitter Accounts by China Propagandists," *Guardian*, 22 July 2014; and Nicholas J. Monaco, "Taiwan: Digital Democracy Meets Automated Autocracy," in *Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media*, ed. Samuel C. Woolley and Philip N. Howard (New York: Oxford University Press, 2018), 104–27, https://doi.org/10.1093/oso/9780190931407.003.0006.
53. Stefan Halper, *China: The Three Warfares* (Washington, DC: Office of the Secretary of Defense, 2013), 12.
54. Halper, *China.*
55. Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle Barracks, PA: United States Army War College Press, 2014), 29–30. Note: according to Wortzel, a direct translation of *yulun* is "public opinion"; thus, in many English translations, the term "public opinion warfare" is used. In some People's Liberation Army translations of book titles and articles, however, it is called "media warfare."
56. Wortzel, *The Chinese People's Liberation Army and Information Warfare.*
57. Steven Collins, "Mind Games," *NATO Review* (Summer 2003).
58. Halper, *China,* 12–13.
59. Laura Jackson, "Revisions of Reality: The Three Warfares—China's New Way of War," in *Information at War: From China's Three Warfares to NATO's Narratives* (London: Legatum Institute, 2015), 5–6.
60. Jackson, "Revisions of Reality."
61. Ben Nimmo, "Question That: RT's Military Mission," Atlantic Council's Digital Forensic Research Lab, 8 January 2018.
62. *Statement Prepared for the U.S. Senate Select Committee on Intelligence Hearing, 115th* Cong. (30 March 2017) (statement of Clint Watts on "Disinformation: A Primer in Russian Active Measures and Influence Campaigns"), hereafter Watts statement.
63. Watts statement.
64. Watts statement.
65. For details on the efforts of both China and Russia, see Ross Babbage, *Winning With-*

out Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail, vol. 1 (Washington, DC: Center for Strategic and Budgetary Assessments, 2019); Esther Chan and Rachel Blundy, " 'Bulletproof' China-backed Site Attacks HK Democracy Activists," Yahoo News, 1 November 2019; John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives 13 (Washington, DC: National Defense University Press, 2018); Joanne Patti Munisteri, "Controlling Cognitive Domains," *Small Wars Journal*, 24 August 2019; Austin Doehler, "How China Challenges the EU in the Western Balkans," *Diplomat*, 25 September 2019; Keoni Everington, "China's 'Troll Factory' Targeting Taiwan with Disinformation Prior to Election," *Taiwan News*, 5 November 2018; "Hong Kong Protests: YouTube Shuts Accounts over Disinformation," BBC News, 22 August 2019; Paul Mozur and Alexandra Stevenson, "Chinese Cyberattack Hits Telegram, App Used by Hong Kong Protesters," *New York Times*, 13 June 2019; and Tom Uren, Elise Thomas, and Jacob Wallis, *Tweeting through the Great Firewall: Preliminary Analysis of PRC-linked Information Operations on the Hong Kong Protests* (Canberra: Australian Strategic Policy Institute, 2019).

66. DiResta et al., *Telling China's Story.*
67. *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution* (Washington, DC: Office of the Director of National Intelligence, 2017); Ellen Nakashima, "Senate Committee Unanimously Endorses Spy Agencies' Finding that Russia Interfered in 2016 Presidential Race in Bid to Help Trump," *Washington Post*, 21 April 2020; Jane Mayer, "How Russia Helped Swing the Election for Trump," *New Yorker*, 24 September 2018; Philip N. Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012–2018* (Oxford, UK: Programme on Democracy & Technology, 2018); and Nike Aleksejeva et al., *Operation Secondary Infektion: A Suspected Russian Intelligence Operation Targeting Europe and the United States* (Washington, DC: Atlantic Council Digital Forensic Research Lab, 2019).
68. Nathaniel Gleicher, "Removing More Coordinated Inauthentic Behavior from Iran and Russia," Facebook Newsroom, 21 October 2019.
69. Gleicher, "Removing More Coordinated Inauthentic Behavior from Iran and Russia."
70. Gleicher, "Removing More Coordinated Inauthentic Behavior from Iran and Russia."
71. "Hacking Group Linked to Iran Targeted a U.S. Presidential Campaign, Microsoft Says," *Los Angeles (CA) Times*, 4 October 2019.
72. Cherilyn Ireton and Julie Posetti, *Journalism, "Fake News" and Disinformation* (Paris: UNESCO, 2018), 18.
73. Michael J. Mazarr et al., *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment* (Santa Monica, CA: Rand, 2019), 65–66, https://doi.org/10.7249/RR2714.
74. For instance, see Rob Price, "AI and CGI Will Transform Information Warfare, Boost Hoaxes, and Escalate Revenge Porn," Business Insider, 12 August 2017; and Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 87.
75. Will Knight, "Fake America Great Again: Inside the Race to Catch the Worryingly Real Fakes that Can Be Made Using Artificial Intelligence," *MIT Technology Review* 17 August 2018; for some examples of realistic Instagram memes created by powerful computer graphics equipment combined with AI, see "the_fakening," Instagram, accessed 6 April 2021.
76. Avi Selk, "This Audio Clip of a Robot as Trump May Prelude a Future of Fake Human Voices," *Washington Post*, 3 May 2017; Bahar Gholipour, "New AI Tech Can Mimic Any Voice," *Scientific American*, 2 May 2017; and Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 85–86.
77. "Imitating People's Speech Patterns Precisely Could Bring Trouble," *Economist*, 20 April 2017; and Mazarr et al, *The Emerging Risk of Virtual Societal Warfare*, 86.
78. "Fake News: You Ain't Seen Nothing Yet," *Economist*, 1 July 2017; Faizan Shaikh, "Introductory Guide to Generative Adversarial Networks (GANs) and Their Promise!,"

Analytics Vidhya, 15 June 2017; and Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 88.

79. Mazarr et al., *The Emerging Risk of Virtual Societal Warfare*, 91.
80. Matthew Rosenberg, Nicole Perlroth, and David E. Sanger, " 'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020," *New York Times*, 10 January 2020.
81. Rosenberg, Perlroth, and Sanger, " 'Chaos Is the Point'."
82. Howard Becker, "The Nature and Consequences of Black Propaganda," *American Sociological Review* 14, no. 2 (April 1949): 221, https://doi.org/10.2307/2086855. " 'Black' propaganda is that variety which is presented by the propagandizer as coming from a source inside the propagandized."
83. For a discussion of strategies to counter foreign influence threats from Chinese and Russian malign influence efforts, see Thomas G. Mahnken, Ross Babbage, and Toshi Yoshihara, *Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare* (Washington, DC: Center for Strategic and Budgetary Assessments, 2018).