Chapter 10

# What Can Be Done to Minimize the Effects of the Global Information Ecosystem on the Risk of Nuclear War?

*Harold A. Trinkunas, Herbert S. Lin, and Benjamin Loehrke*

On August 11, 2017, President Trump tweeted: "Military solutions are now fully in place, locked and loaded, should North Korea act unwisely. Hopefully Kim Jong Un will find another path!"[1] This message followed months of escalating rhetoric and military posturing between the United States and North Korea. The crisis became acute enough that, near the height of tensions in July 2018, polling showed that 60 to 75 percent of Americans were worried about the possibility of war between North Korea and the United States within the following six months.[2] Tweets from President Trump often drove or narrated the crisis, adding fears that instantaneous, direct, 280-character threats could lead directly to nuclear war. As former acting undersecretary of defense for policy Brian McKeon testified at a Senate Foreign Relations Committee hearing on presidential nuclear authorities, "The statements the president makes through his Twitter account no doubt cause concern and confusion on the other side of the Pacific. . . . I'll be very worried about a miscalculation based on continuing use of his Twitter account with regard to North Korea."[3]

As this case illustrates, the new global information ecosystem may be having an important impact on the evolution of international crises. Widespread access to social media on a global scale has accelerated news cycles in traditional media and made it easier to spread misinformation and disinformation. Intemperate, ill-considered, and impulsive outbursts have become an important part of crisis dynamics. In the decade since the founding of Facebook and Twitter, social media have added new arenas to conflicts in the Persian Gulf region among Iran, Saudi Arabia, and their respective allies; among Russia, Ukraine, and NATO; between nuclear-armed India and Pakistan; and, as we have just considered, among North Korea, Japan, South Korea, and the United States.[4] If we were to include information operations meant to influence governments and publics, we could extend the list of cases to include Russian interference in elections in the United States, the United Kingdom, Germany, Spain, Italy, and France; operations by the Venezuelan government against its neighbors in South America; and operations between China and its neighbors in East Asia.[5] Some of these crises involve nuclear-armed powers. Were one of these crises to spin out of control, the outbreak of nuclear war could have a catastrophic impact on humanity. Even a modest exchange involving one hundred relatively small warheads has the potential for producing a nuclear winter with dramatic effects on global climate and the prospects for human survival.[6]

While disinformation and misinformation have always been part of conflict, the chapters in this volume outline how the new global information ecosystem has created conditions for the spread of disinformation, misinformation, and other malign information in ways that threaten crisis stability, even nuclear crisis stability. Scholars of crisis stability have had well-established frameworks with which to analyze deterrence, decision making, and the role of public opinion in foreign policy. These approaches principally rest on rational actor models. While they acknowledge that misperception and miscalculation can have an impact on crisis stability, they tend to assume that leaders will make policy decisions rationally and analytically, based on the best available evidence and with the national interest foremost in mind.[7]

Social media and their disruptive effects are cause to reassess how existing analytical and theoretical frameworks for understanding crisis stability might be affected by the evolution of today's information ecosystem. This volume fills a gap on whether, when, and how social media could contribute to international conflict—including deterrence failure and nuclear war. In particular, it makes four contributions.

First, it incorporates findings from cognitive psychology and decision analysis into analyses of how leaders and publics receive, process, and act on information, misinformation, and disinformation in the emerging global ecosystem. It highlights how social media have an impact on how much information individuals receive, how they receive it, and, in turn, how these factors affect and may increase the likelihood of engaging in heuristic thinking (i.e., intellectual shortcuts) to manage the overwhelming volume of information available.

Second, the authors in this volume examine how cyber-enabled influence operations may be deliberately conducted via the new tools made available in the present information environment to take advantage of human cognitive biases and affect the perceptions, preferences, and decisions of both publics and leaders in times of crisis.

Third, this volume examines how the intersection of human propensity to heuristic thinking and cognitive bias may have a dangerous impact on international crisis stability. Such mental shortcuts are common to decision making. The emerging global information ecosystem, combined with deliberate influence operations designed to affect leader and public perceptions, could further wear on leaders during crises—potentially even those involving major nuclear powers and the risk of war.

And fourth, this volume assesses the limits of what adversaries may actually be able to accomplish in the present information environment, including the risk that influence operations may cause blowback on the perpetrators. In addition, public preferences may actually be fairly resilient in the long run in the face of deliberate attempts to influence mass opinion, even if these may have an impact in the short run.

## Human Cognition, Heuristic Thinking, and Implications for Crisis Stability

Digitization and global communication technologies make generating and sharing new information possible at an unprecedented speed and scale. Social media platforms provide vehicles (in many cases tailored to take advantage of human cognitive biases) via which to maximize the impact of targeted persuasion. Each year, more people around the world are part of this information ecosystem, as mobile phone penetration globally is estimated to reach five billion users in 2019 (and there is no reason to expect this trend to slow down).[8] The transformation of the global information ecosystem is not just about speed, ease, or scale of communication. It has crucially democratized information production and information dissemination. Moreover, it is increasingly apparent that the new global communications ecosystem is producing new opportunities to influence humans by playing on traditional cognitive biases that we use to process information. Audiences could be more susceptible to such efforts when faced with time pressure, high volumes of information, and appealing post-truth narratives that are preferred by significant segments of the global public instead of evidence-based journalism and policies. Taken together, these trends call into question whether traditional models of crisis stability, which assume rational decisions made by elites based on the best available evidence, are an accurate way to understand the likely evolution of future international conflicts.

In chapter 2, Rose McDermott explores the psychology of the post-truth political environment. Applied to the political environment, post-truth denotes "circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief." Absent special mental discipline, story and narrative are more important in shaping a person's views than empirical fact or logically reasoned conclusions—and this applies both to ordinary citizens and to leaders. Importantly, McDermott argues that most people will regard a plausible story as true, whether or not it is in fact true. McDermott also points out two exacerbating factors. First, the decline of public trust in institutions and expertise has left individuals on their own to gather information and to make judgments about what to believe for themselves. Second, the rise of social media as primary information sources means that those who rely on such sources do not have the benefit of intermediaries who fact-check and place information in context. In this environment, people are far more likely to fall back on their own intuitive thinking, which places much higher value on factors such as simplicity, familiarity, consistency with prior belief, and how many other people appear to believe the same things. Analytical evidence-based thinking will struggle to keep pace.

Paul Slovic and Herb Lin consider the psychology of nuclear decision making, especially during crisis. Such decisions involve the highest possible stakes. The authors point to several psychological phenomena that affect nuclear decision making. Psychic numbing refers to a devaluation of life when large numbers of deaths are contemplated—the death of one innocent civilian is regarded as a tragedy, whereas the death of a million is merely a statistic. Indeed, in some cases, the death of millions is regarded as less tragic than the death of a few. Psychological devaluation of life likely underlies the ability of nuclear planners and decision makers to proceed in ways that they believe to be consistent with laws of war that are intended to minimize harm to innocent civilians. Tribalism reflects an "us versus them" mindset, enabling "us" to hate "them." Tribalism enables the dehumanization of the enemy and treatment of the enemy in ways that do not seem to violate the laws of war. Decision makers often avoid making trade-offs between competing values, such as the value of protecting national security versus protecting noncombatant enemy civilians. Rather than finding a common currency to evaluate trade-offs, they will often prioritize different values and focus on achieving those of highest priority. Thus, a decision maker may well favor security objectives over lifesaving objectives because the former are more defensible. Combined with the affordances of social media (such as their use of short, simple messages and evocative visual and auditory content), the existence of such psychological processes means that social media messages are more likely to be processed with fast, intuitive thought rather than with reflective, deliberate thought. The same is true of leaders and decision makers who are active social media users, and they are just as likely to be pushed by their social media usage into fast, intuitive thought. Slovic and Lin conclude that where such leaders are concerned, exposure to social media may well increase the likelihood of taking rash action and of premature use of force.

## Cyber-Enabled Influence Operations: The Impact of Disinformation on Leaders and Publics

The present revolution in the global information ecosystem has made propaganda cost effective again. Manipulating information with the intent to persuade is a tried-and-tested part of warfare, and skeptics are right to note that there is nothing new about propaganda per se.[9] But the current information environment substantially reduces barriers to the conduct of information operations not just for great powers but also for small and middle powers as well as for nonstate actors. Unlike offensive cyberoperations—which require substantial investments in sophisticated cybercommands, recruitment of scarce hacking talent, and maintenance of up-to-date cyberweapons based on fresh exploits—information operations are much more affordable.[10] As we learned from the investigation into Russian targeting of US elections, influence operations may cost millions of dollars, but they need not cost tens or hundreds of millions of dollars.[11] Moreover, operations can be conducted on platforms made available largely for free by major social media platforms, designed to be used by the general public with the most minimal training. Lowering costs along all dimensions enables a wide array of states, great and small, and nonstate actors such as political parties and civil society organizations to conduct influence operations cheaply. In addition, states traditionally seem to treat influence operations as falling short of the threshold of armed conflict (more akin to subversion), which means that even great powers have avoided responding to such attacks by other state actors with military force. Since costs are low, both in financial terms and in terms of the likelihood of retaliation, we should expect the widespread use of influence operations intended to affect the behavior of leaders and publics, even against the great powers and even by weaker actors in the international system.

Misinformation and disinformation on social media have the potential to contaminate information flows, which could affect behavior during crises, as Mark Kumleben and Samuel Woolley show in chapter 4. People increasingly turn to social media for information during emergency situations, which creates an opening for nefarious actors to exploit that information ecosystem. For example, during a military crisis, an adversary could use a variety of computational propaganda techniques to interrupt and confuse information flows on social media in order to encourage publics and leaders to behave in a way that suits the adversary's interests. Kumleben and Woolley explain some of the more important of those techniques and give an overview of how they have been used in political conflicts. The cases that the authors use illustrate the potential effects of misinformation and disinformation during military crises. The 2018 false missile alert in Hawaii is a useful hypothetical on how computational propaganda could provide an adversary with a cost-effective means to erode a target state's civil defenses and interrupt its ability to mobilize resources. Political leaders might also be susceptible to digital information operations during crises. The microtargeting of Jeremy Corbyn by members of his own 2017 Labour Party campaign staff shows that disinformation on social media could affect political decision making. By showing how computational propaganda has the power to affect behavior, Kumleben and Woolley highlight the strategic importance of the information ecosystem during crises.

State and nonstate actors are already engaged in information operations designed to affect interstate relations, as Kate Starbird outlines in chapter 5 in this volume. Using the techniques analyzed by Kumleben and Woolley, these actors are conducting influence operations online to influence political discourse and generate false information, most likely with the intention of generating confusion and mistrust among their adversaries and competitors. Starbird's work outlines how deliberate efforts by state actors, such as those aligned with Russia, can influence broader online conversations and activism among sympathetic audiences. In the case of NATO, both alt-right and fringe conservative voices and international far-left activists converged on a shared anti-alliance message that was influenced and driven in part by state-sponsored online actors working via social media. There is a pattern of state actors and state-backed trolls infiltrating authentic online and social media–based activist communities on both the right and the left to reshape their activities so that they unwittingly support state-sponsored messages and objectives, in this case Russia's anti-NATO activities. The long-term impact of these activities remains to be seen, but they are already shaping conversations about and among major international actors, in this case NATO, possibly shaping the future strategic environment in ways that could undermine popular support for alliance activities to deter Russia.

## The Risks to International Crisis Stability from the Global Information Ecosystem

During the Cold War, government leaders of the major nuclear powers received information from military and intelligence services that, while of course vulnerable to many errors, was nonetheless subject to a process designed to produce verifiable data on which leaders could base decisions. Publics received information via gatekeepers, whether in the form of official or private media, that also subjected information to a vetting process, admittedly not always designed to produce truth but at least to produce consistency and a consensus view of reality among audiences.

Publics and leaders are today exposed to masses of unverified information produced at high speed and distributed at high volume for next to no cost. It is much easier to produce polarization in target populations, to spur storms of public opinion to influence enemy leaders, to leak information deleterious to adversaries, and to conduct influence operations designed to target the psychology of enemy publics.

Moreover, the same techniques, as Kristin Ven Bruusgaard and Jaclyn Kerr suggest, can target leaders, affecting perceptions of crises and of adversaries' intentions. We already know that major government officials pay attention to social media, and they are also subject to the same effects from the global information ecosystem as the publics they lead. This raises the real possibility that influence operations may become an additional contributing factor to growing crisis instability in the world today.

In fact, the deployment of post-truth information during crises may contribute to escalation dynamics in dangerous and unpredictable ways. In the current information environment and given human propensity for heuristic thinking, deployment of convenient half-truths, rumors, or "extra-factual information," as Kelly Greenhill argues, is attractive because it is a powerful mobilizer of public opinion and can magnify signals of resolve in international crisis. But precisely because it is so powerful and provocative, it can lead adversaries to escalate rather than back down. It can alarm public opinion among adversaries, putting opponents in the position of having to resort to their own escalation and provocation or else appear weak. In addition, as Jeffrey Lewis also documents in chapter 8, there is the possibility that both the general public and elites in the provoking country will come to believe extra-factual information, making it difficult to build off-ramps from international crises for fear of appearing weak or losing face. It may become difficult or impossible to "walk back" or discredit extra-factual information in a global information environment too prone to magnifying human heuristic thinking and spreading information that is appealing even if untrue.

## The Limits of Disinformation and Influence Operations

This volume has painted a grim picture of the future of a global information ecosystem increasingly awash in large volumes of unverified misinformation and disinformation, with the attendant impact on leaders and publics—and potentially even on crisis stability. However, there are some likely limits on what information alone can achieve.

The first limit on the impact of the evolving information ecosystem on the likelihood of interstate conflict is the underlying material distribution of capabilities among states. The findings in this volume are relevant to the dimensions of international conflict that relate to misperception, miscalculation, and the risk of inadvertent war. In other words, even though the global information ecosystem now makes new capabilities available to both great and small powers, and even if it increasingly exposes global publics and leaders to misinformation, disinformation, and post-truth, the great powers remain materially more capable and are thus more able to impose their preferences on others. Smaller powers are vulnerable to international pressure in ways that great powers are not, and this may be part of the eventual solution to this threat if and when great powers begin to retaliate coercively against information operations that strike too close to home. The "mouse that roared," in which a weaker power is able to dissuade or persuade a larger state's employment of its material capabilities to achieve the smaller power's preferences, may still fall into the realm of fiction.

Another limit is the possibility that those conducting influence operations may "lose control" of the disinformation or propaganda they are using and that it will "blow back" on their own population or leaders. Lewis in this volume documents several instances in which information operations went awry, infecting the debate on issues related to deterrence, nuclear deployments, and nuclear doctrine in the Soviet Union, later Russia, and possibly the United States. This is of course more of a concern for those attempting to use influence operations to achieve particular effects than for those who simply intend to sow chaos or promote polarization—which, as has been suggested by recent Russian influence operations, may be a goal in itself. But to the extent that those conducting information operations become more aware of this possibility (i.e., if an operation goes badly wrong), this may in the future lead states to self-deter from using this capability.

There is also cause to be more contingent in asserting what effects social media might have. Ben O'Loughlin in his chapter stresses that researchers first need to answer whether social media play a new or different role in public opinion. He notes that individuals perceive the world around them through established narratives they hold about how the world works, the actors in it, and the problems at hand. Changing opinions by dislodging those narratives through political communication is extremely difficult, and it is unclear if social media are an effective means for that. O'Loughlin provides a valuable cautionary note by describing a paradox that this situation presents. While social media have enabled a new and cheaper means to influence politics—at home and abroad—he believes there is not enough evidence that political communication on social media is any better at persuasion than traditional media. It is unclear if information operations on social media would change public opinion or simply help make more apparent the opinions of certain constituencies and their long-held views. Gaining more insight into and gathering evidence on such questions would better show whether social media significantly affect public opinion and help explain what roles information operations on social media might have during international crises.

## Future Trends in Crisis Stability and Avenues for Further Research

We already live in an era in which international crisis stability is being undermined by the actions of great powers. Crisis stability has traditionally derived from, in the most limited sense, the major nuclear powers having secure second-strike capabilities that assured the destruction of adversaries even in the event of a surprise attack. Such capabilities greatly diminished the incentive to strike first. In a broader sense, it has meant a different kind of stability produced by the efforts of major nuclear powers to limit arms races, facilitate crisis communication, and promote an international environment that limits the likelihood that crises will become nuclear.[12] Neither of these conditions is as true as it was in the 1970s, when both the United States and the Soviet Union were actively engaged in efforts that tended to promote crisis stability.

In the nuclear domain, the United States and Russia are recapitalizing nuclear arsenals, investing in substrategic nuclear weapons, and floating trial balloons regarding possible limited first use or use of low-yield weapons to respond to nonnuclear threats. The United States continues to invest in strategic defense against nuclear missiles, traditionally thought of as undermining crisis stability. China refuses to participate in nuclear arms-control negotiations, which is being used as an excuse by both Russia and the United States to sunset existing arms-control treaties.[13]

In addition, the nuclear weapons, conventional weapons, and associated early-warning and command-and-control systems of the major powers are becoming increasingly entangled. Emerging military technologies such as conventional long-range precision strike systems, cyberwarfare, and antisatellite weapons pose threats to the sensor and warning networks that are useful for conducting both conventional and nuclear operations. James Acton argues that this may pose a risk to crisis stability because attacks on early-warning and command-and-control systems to degrade conventional capabilities of a nuclear-armed adversary may be perceived as the preliminary moves of a nuclear first strike, encouraging the targeted nation to preemptively attack. In addition, a nuclear power engaged in a conventional war may come to believe that attacks on its long-range sensor networks in the course of military operations may degrade its ability to conduct damage limitation attacks designed to reduce the impact of an adversary's nuclear arsenal should the conflict escalate, therefore encouraging a first strike with nuclear weapons.[14]

Technological progress is also contributing to declining crisis stability by providing states with new capabilities with which to undermine the integrity and survivability of nuclear arsenals. Artificial intelligence and machine learning, combined with ubiquitous sensors, have the increasing potential to reveal the locations of once hidden second-strike capabilities such as ballistic missile submarines and ground-mobile missile launchers. These second-strike systems depend for their survival on being hard to locate.[15] There remains a lurking concern that emerging powers with small numbers of nuclear weapons may find their arsenals and their production establishments vulnerable to the use of emerging technologies, such as offensive cyberweapons to disarm them. This may lead them to favor first use or "fail-deadly" nuclear doctrines. There is even concern that the information systems of major nuclear powers are vulnerable in ways that might contribute to crisis instability.[16]

In this context of destabilizing strategic trends, it is important as ever for decision makers to think carefully and cautiously during crises. But the changes wrought by social media to the information ecosystem are making that more difficult, as tightening decision windows are met with the relentless speed and volume of information.

There are no indications that the role of the global information ecosystem in promoting crisis instability will decline in the short to medium term. There is no evidence yet that human beings are likely to become cognitively more resistant to misinformation and disinformation, nor are the platforms on which the global information ecosystem is built addressing the risks posed by human cognitive biases. For the private companies that build and deploy social media platforms, increasing consumer interaction with their products is part of their monetization strategy. This means both extending the reach of social media to new consumers, many of whom may not be on guard against online misinformation, and crafting products designed to increase the "dwell time" of existing users on platforms. Under present conditions, companies have few incentives to adjust the algorithmically selected data streams displayed via their platforms in ways that would improve the accuracy and validity of information provided but that consumers might find disagreeable. In fact, all incentives point toward algorithmically selecting experiences for platform consumers that they find agreeable and unchallenging, creating what is known as filter bubbles, rather than ones that foster reasoned thinking (or slow thinking, as discussed in chapter 3 by Slovic and Lin).

In addition, deliberate influence campaigns conducted in the present global information environment seem likely to continue to proliferate. As many as forty-eight countries have already been detected as engaging in some form of computational propaganda, according to the Oxford Internet Institute.[17] Although the rewards may not always be high, for reasons earlier discussed they are cheap and low risk, accessible to even small and middle powers. As private social media companies expand the reach of the global information ecosystem, new targets are becoming available for influence operations. And few countries have thus far retaliated against information operations, not even the United States. Under such circumstances, the incentives all point toward a continued expansion of influence operations.

But many unknowns remain, and much research has yet to be done. Here we suggest five possible research agendas:

1. What is the relationship between social media and heuristic reasoning? Popular business and journalistic narratives seem to assume there is one, suggesting that social media tend to encourage System 1, or fast, thinking, in which consumers are more prone to impulsive behavior. There is some initial evidence that this is the case, but academic studies of the relationship between social media and heuristic reasoning are still few and far between. If such a relationship is borne out by additional studies, it would support the argument that the global information ecosystem as it has currently evolved contributes to the risk of crisis instability.
2. A related question is how engagement with social media actually affects decision making in high-stakes scenarios. Some research suggests that individuals are more inclined to slow, reflective thinking when stakes are high and the individuals involved have a personal interest in the matter at hand. How and to what extent might such an inclination moderate the pressures for fast thinking induced by engagement with social media in crisis?

3. What kinds of information operations are being conducted and by whom? Increasing numbers of reports document the proliferation of influence operations by state and nonstate actors. However, data are only episodically available and are usually incomplete. More focused and systematic study of influence operations would help illuminate the boundaries between disinformation and misinformation, as well as help analysts further examine the relationship with crisis stability. Unfortunately, in the short term we will need to navigate the impasse between social media platforms and social science researchers in the wake of Cambridge Analytica's role in the 2016 US election.[18] The appropriation and misuse of large amounts of Facebook data by Cambridge Analytica for electoral purposes led to a crackdown on data sharing by social media companies which has in turn inhibited legitimate social science research on information operations globally.
4. Has mass political participation on social media affected the role of public opinion in foreign policy making? Social media have increased the velocity of information and public participation with it. For decision makers, to what degree has this caused them to become more sensitive to these information flows or to more aggressively filter out information? For publics, has this significantly changed constituent influence in foreign policy making? In some ways, public opinion is the fulcrum of an argument that social media intensify public pressure on decision makers in ways that increase risks to crisis stability. Further research into how the current information ecosystem might be changing interactions between publics and decision makers could provide better understanding of the implication for international conflict.
5. More research is needed on how societies adapt to the proliferation of technologies that democratize access to information production and distribution. The present global information environment is not the first in which traditional authorities and gatekeepers have become alarmed at technology-aided jumps in the speed of information flow and the incorporation of new users into the ecosystem. The spread of the printing press in Europe, which interacted with the Protestant reformation, so greatly alarmed the Catholic Church that it devised a new and

deliberate countermessaging strategy and organization under the rubric of the Sacra Congregatio de Propaganda Fides (Congregation for the Propagation of the Faith) in 1622. This effort by the Catholic Church to proselytize among its faithful has become known as the origin of the term *propaganda*.[19] The telegraph similarly provided a leap in availability of information to users, as eventually did radio and television. In each case, societies navigated the impact of new technology and arrived at a solution in which a means of verifying and validating ever more widely available information became available. This has not yet happened in the present global information environment.[20]

## Policy Recommendations

Publics and some political leaders are increasingly aware of the role of malicious manipulation and influence operations. This is in part because of the results of the US elections in 2016, but it is also because of news of such operations involving both domestic politics—elections in India, Mexico, France, and Germany in 2017 and 2018, for example—and international crises such as India-Pakistan border clashes or Saudi Arabia and the UAE's cold war with Qatar. However, many remain unaware of the full scope of influence operations currently at work around the globe: the actors, their true intentions, cascading consequences, and implications on international security and crisis stability.

In addition, states have so far been reluctant to devise and implement policies to curtail the negative effects of influence operations in the global information ecosystem. This volume has described a number of causes for state reticence on this issue. These include the prospect that limiting influence operations may involve restrictions on speech that would run counter to the norms and laws of democratic states. Also, foreign influence operations may in fact be caught up within a state's domestic politics, benefiting one political party over others and leading the victors to be reluctant to take actions that might damage their prospects of future electoral success. The enterprise of distinguishing "good" from "bad" information and normal campaigning and advertising from malicious influence operations may be simply too political to be handled by a neutral governance or regulatory body. Indeed, there may not be much difference between some influence operations and ordinary political campaigning in a democracy. Finally, in cases raising international security concerns, influence operations have so far been seen as falling short of the threshold of armed conflict. State leaders still have not found a consensus on appropriate ways to deter such attacks or retaliate against them. In fact, they may want to avoid setting a precedent via such a retaliation to protect their own states' ability to conduct influence operations abroad.

However, there are still some things that states can do to limit the prospect of influence operations contributing to worsening international crises, particularly those involving nuclear powers. First, the social media platforms themselves may need to change. American jurisprudence suggests that regulation of speech content on social media channels is inconsistent with the First Amendment's guaranteeing freedom of speech, although legal precedents in the European Union may provide some leverage. It may prove more feasible to regulate or otherwise influence the business model rather than the content per se. For example, improved transparency and attribution of sources may be vehicles for allowing users to assess the validity of content they are receiving via social media platforms. Although social media companies are likely to resist regulation, they may welcome uniform standards that relieve them of some liability and the reputational damage inflicted on them now by the recurring scandals related to how companies handle user information. Social media companies have optimized their business models to maximize revenues, and it is these very business models that undergird the information ecosystem of today. A key research problem in this domain is to find profitable business models that are consistent with efforts to reduce the volume and velocity of malign information spread across social media.

A second lesson from this volume is the need for decision makers to engage in clear-headed and deliberative thinking when contemplating decisions about the use of nuclear weapons. Even before the emergence of the present global information ecosystem, there were reasons to be concerned about the impact of time pressure on decision making. These pressures seem to have increased. One countermeasure may be to increase the availability of sufficient time for deliberation. Since it is the half-hour timeline for the flight of Russian ICBMs toward the United States that is most stressing for US decision makers, policy attention should be devoted to extending that timeline. This could include modernizing command-and-control systems and processes to improve the time for decisions and the quality of information available to leaders. A great deal of the time pressure derives from the belief that decisions must be made about the employment of the land-based missile force, the leg of the US nuclear triad most vulnerable to degradation by a major first strike. Essentially, it is viewed by some as a "use it or lose it" element of the US nuclear arsenal, thereby encouraging not only decision making under time pressure (when humans are more vulnerable to heuristic thinking) but also a posture of "launch on warning."

By removing requirements for launch-on-warning capability, eliminating the US silo-based ICBM force, or adopting a less vulnerable ICBM basing mode such as mobile launchers, US presidents would no longer face the same time pressure to launch on warning.[21] There would be theoretically more time to ride out an initial attack and decide how and when to retaliate. Moreover, US adversaries would know this, minimizing their incentive to try to launch a sudden attack to degrade the land-based component of the US nuclear arsenal. Similarly, other nations with nuclear weapons could take steps to increase decision time. Steps may entail changes in doctrine, force structure and deployments, or early-warning capabilities.

A third possible area for policy innovation lies in altering how decisions are made about the employment of nuclear weapons. Of course, states have different approaches to making decisions around nuclear weapons use, but the evolution of the present global information environment suggests that it is time to step away from systems that place this responsibility in the hands of a single individual. Human beings vary in their propensity for "thinking fast" or heuristic reasoning. They also vary in their susceptibility to influence operations.

Such variation suggests that a higher quality of nuclear decision making would be possible if the concurrence of multiple individuals were needed to order the use of nuclear weapons. This would reduce the likelihood that a single decision maker would act impulsively in the face of time pressure, commit cognitive errors in assessing a crisis, or fall under the effects of an influence operation.[22] For example, in the case of the United States, Richard Betts and Matthew Waxman have proposed requiring the concurrence of the secretary of defense (to certify that a nuclear weapons use order is a valid military necessity) and the attorney general (to certify that a US nuclear weapons use order is legal) before a president could initiate a nuclear strike.[23]

A fourth possible area for policy innovation lies in how information is processed during crisis within the national security apparatus of states. Almost all states have intelligence communities (or something similar) that are designed to collect, process, evaluate, and analyze data about the world, presumably with the objective of providing a somewhat accurate and verified picture of the world to their leadership. In many states, this is coupled with an executive apparatus that is designed to elaborate policy proposals for decision makers to consider and to follow up on implementation of approved proposals. For example, in the United States the intelligence community would collect, verify, and analyze information for use by the National Security Council staff and other government departments to prepare policy recommendations for vetting through the interagency process. Ideally, this process should by itself minimize the impact of disinformation and misinformation through subjecting intelligence analyses and policy recommendations to vigorous questioning and evaluation. However, in the modern global information ecosystem, it is clear that new information and policy ideas can enter the decision-making process very close to the top of a decision chain and very close to the end of the process, i.e., in the final decision-making settings, even in a state leader's office. This suggests that information assessment teams should be assigned to senior decision makers to help them evaluate information inflows from outside the normal decision-making process, such as from social media, contemporaneously to those decisions being made. Such teams would be trained to understand the tactics of information warfare perpetrators (and their allies, witting or unwitting) and the psychological mechanisms that social media leverage. They would be tasked with helping senior decision makers to understand the context of new data that they are receiving and to retain the appropriate perspective and distance from their personal information feeds. So while shielding the mass of the population from influence operations may prove to be too political or trigger accusations of partisanship in many democracies, protecting senior decision makers may in the end prove to be more feasible and practical.

Overall, the analysis presented in this volume suggests that the global information ecosystem, because of the way it interacts with human cognitive biases and because of the new abilities it affords state and nonstate actors to conduct influence operations, is a potentially important threat to crisis stability. While it is difficult to imagine developing useful countermeasures at this stage of our understanding of the phenomenon, some aspects of the problem to be addressed are clear. Human cognition is unlikely to change significantly on anything less than an evolutionary scale, so that means the information ecosystem needs to be modified to minimize the impact of bad information on crisis decision making, given current human propensity to heuristic thinking. To avoid the possibility that "fast thinking" (or System 1 thinking) may lead policy makers to poor decisions, more time for deliberation needs to be built into international crises, particularly ones among nuclear powers that have the most potentially catastrophic effects. In addition, to minimize the possibility that bad information or deliberate influence operations will lead state leaders to make cataclysmic decisions involving nuclear weapons during international crises, decision-making authority should be spread out among multiple senior leaders, serving as a check on the possibility of any single individual precipitating a nuclear exchange. Finally, senior decision makers will likely need support to evaluate and curate the data flows they receive from outside the normal governmental process for providing intelligence analyses and policy recommendations. That support should likely sit as close to them as possible.

## Notes

1. Donald J. Trump, Twitter, August 11, 2017, 4:29 a.m., https://twitter.com/realdonaldtrump/status/895970429734711298?lang=en.

2. A July 18 poll from ABC/Washington Post showed that 74 percent of respondents were concerned about the possibility of "full-scale war with North Korea." See Allison De Jong, "Distrust in Trump Deepens North Korea Concerns," ABC News, blog, July 18, 2017, https://www.langerresearch.com/wp-content/uploads/1189a3NorthKorea.pdf. In an August 15, 2017, poll from The Economist/YouGov, 60 percent of respondents were worried that North Korea will take military action against the United States, https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/8binbopoey/econTabReport.pdf.

3. *Authority to Order the Use of Nuclear Weapons*, *Senate Foreign Relations Committee*, 115th Cong. 1, November 14, 2017 (testimony of Brian McKeon).

4. Jack Stubbs and Christopher Bing, "How Iran Spreads Disinformation around the World," Reuters, November 30, 2018, https://www.reuters.com/article/us-cyber-iran-specialreport-idUSKCN1NZ1FT; Tom Hundley, "India and Pakistan Are Quietly Making Nuclear War More Likely," Pulitzer Center, April 2, 2018, https://pulitzercenter.org/reporting/india-and-pakistan-are-quietly-making-nuclear-war-more-likely; Neha Thirani Bagri, "When India and Pakistan Clashed, Fake News Won," *Los Angeles Times*, March 15, 2019, https://www.latimes.com/world/la-fg-india-pakistan-fake-news-20190315-story.html.

5. Larry Diamond, *Ill Winds: Saving Democracy from Russian Rage, Chinese Ambition, and American Complacency* (New York: Penguin Press, 2019).

6. Seth Baum, "The Risk of Nuclear Winter," *Federation of American Scientists* (blog), May 29, 2015, https://fas.org/pir-pubs/risk-nuclear-winter.

7. Robert Jervis, "Deterrence and Perception," *International Security* 7, no. 3 (Winter 1982/83): 3–30; Robert Jervis, *Perception and Misperception in International Politics*, new edition (Princeton, NJ: Princeton University Press, 2017).

8. Kyle Taylor and Laura Silver, "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally," Pew Research Center, February 5, 2019, https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally.

9. Philip M. Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day* (Manchester, UK: Manchester University Press, 2003).

10. Max Smeets, "How Much Does a Cyber Weapon Cost? Nobody Knows," *Net Politics* (blog), Council on Foreign Relations, November 21, 2016, https://blogs.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows.

11. Adrian Chen, "The Agency," *New York Times*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html; Samantha Bradshaw and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," Oxford Internet Institute, Oxford University, July 2018.

12. Joshua H. Pollack, "Is Crisis Stability Still Achievable?" APS Forum on Physics & Society, July 2017, https://www.aps.org/units/fps/newsletters/201707/crisis.cfm.

13. Steven Pifer, "With US-Russian Arms Control Treaties on Shaky Ground, the Future Is Worrying," Brookings Institution, April 25, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/04/25/nuclear-security-arms-control-and-the-us-russia-relationship.

14. James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (August 2018): 56–99, https://doi.org/10.1162/isec_a_00320.

15. Edward Geist and Andrew Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" Santa Monica, CA: RAND Corporation, 2018, https://doi.org/10.7249/PE296.

16. Andrew Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons* (Washington, DC: Georgetown University Press, 2018).

17. Bradshaw and Howard, "Challenging Truth and Trust."

18. Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *New York Times*, March 17, 2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

19. Taylor, "Munitions of the Mind."

20. It is true that to a certain extent these technologies lent themselves to economies of scale that tended to facilitate the role of gatekeepers and regulators. So far, this has not been the case with the latest wave of information technology.

21. William J. Perry, "Why It's Safe to Scrap America's ICBMs," *New York Times*, September 30, 2016, https://www.nytimes.com/2016/09/30/opinion/why-its-safe-to-scrap-americas-icbms.html.

22. See Herbert Lin, "A Two-Person Rule for Ordering the Use of Nuclear Weapons, Even for POTUS?" *Lawfare* (blog), November 9, 2016, https://www.lawfareblog.com/two-person-rule-ordering-use-nuclear-weapons-even-potus.

23. Richard K. Betts and Matthew Waxman, "Safeguarding Nuclear Launch Procedures: A Proposal," *Lawfare* (blog), November 19, 2017, https://www.lawfareblog.com/safeguarding-nuclear-launch-procedures-proposal.