Stanley Center
FOR PEACE AND SECURITY

NUCLEAR POLICY
READOUT & RECOMMENDATIONS

Three Tweets to Midnight

Nuclear Crisis Stability and the Information Ecosystem

58th Strategy for Peace Conference
October, 2017 | Airlie Center, Warrington, VA

This Readout and Recommendations presents key discussion points and observations from a multidisciplinary roundtable convened in October 2017 at the Stanley Foundation's 58th annual Strategy for Peace Conference. The brief provides a framework for identifying such questions. It identifies several disruptive dynamics in the information ecosystem. It then looks at the psychology of decision making and asks when during the arc of a crisis the information ecosystem might have significant detrimental influence. It also recognizes that technology may be empowering new actors who have stabilizing effects on the information ecosystem and could promote accuracy and informed decisions. The brief concludes with a series of open questions deserving further examination.

How might a nuclear crisis play out in today's media environment? What dynamics in this information ecosystem—with social media increasing the volume and velocity of information, disrupting journalistic models, creating potent vectors for disinformation, opening public channels for adversaries to influence national leaders, and changing how political leaders interact with constituencies—might threaten rational decision making during crises between nuclear-armed states?

There are still many unknowns about the effects of social media on international conflict. Digital disinformation and influence campaigns have already been used by foreign adversaries to interfere in democratic elections and have played roles in low-intensity international conflicts. But leaders have not been tested in high-stakes security crises in this media environment. It is worth asking what new dynamics leaders would face and whether this affects

the likelihood that a conflict could escalate, potentially to include the threatened or actual use of nuclear weapons.

"Trending"

The Information Ecosystem and Its Malignancies

The urgent focus today on social media and "fake news" often neglects the scope and scale of the challenge.[1] A large-scale technology transition is disrupting how we communicate, thereby changing how we interact with and interpret the world around us. The resulting dynamics are destabilizing the global information ecosystem, and the effects are increasingly observable in international conflicts. The ecosystem metaphor may seem intuitive, but we will turn first to an overview of how we communicate using a systems view of communication, then explore how the

Internet and social media are disrupting that system, followed by a discussion of the malignancy of fake news.

Communication is commonly seen as the transmission of information. A more holistic perspective sees communication also as a complex social ritual through which communities can develop shared beliefs. This view of communication as a social ritual explains how community members interact with information to construct, maintain, and modify shared beliefs within that community.[2]

This view of communication as a dynamic social process hints at a larger set of interrelationships at play in an information ecosystem.[3] This is akin to a community of living organisms and the relationships between them and with the surrounding environment. There is not a common definition for what makes up an information ecosystem.[4] Internews, in its research on the concept, defined it as:

> "a loose dynamic configuration of different sources, flows, producers, consumers, and sharers of information interacting within a defined community or space."[5]

The Internet and social media technology are disrupting this information ecosystem, compelling dramatic changes in the actors and the complex interrelationships within it.[6] These shifts are still under way, but some stand out:

- It is cheaper and easier than ever to create and distribute content.

- Individuals, organizations, networks, and states can directly communicate with global audiences like never before.

- The volume and velocity of information has greatly accelerated news cycles.

- Verified information is necessarily more expensive and slower to produce than unverified information, because the latter—by definition—need not undergo a verification process that has a cost and time associated with it.

These shifts accompany other changes in the information ecosystem that warrant attention for discussions of international conflict:

- The volume and velocity of information are increasing faster than norms, policies, and institutions have evolved to manage the consequences of the information.

- The increasing volume and velocity of information could produce versions of a "CNN effect," wherein disruptive communications technology accelerates news cycles and intensifies interplay between foreign policy makers, publics, and the media.[7]

- Professional journalists' once primary roles as gatekeepers for information and privileged narrators of the world around

us have been weakened, and today they have diminished influence to counter false or misleading narratives.

- The business models of traditional journalism have been upended. Social media platforms have overtaken publishers' roles in distributing information, driving dramatic declines in advertising revenue and circulation.

- There is a crisis of public trust in institutions, particularly in print media. Trust in media recently reached historically low levels, though it may be rising, according to one recent poll.[8]

- Audiences increasingly rely on social media networks to access and interpret news, often leading them to alternative sources of information that are not subject to the same verification standards as traditional news sources.

- Using advanced algorithms, social media platforms allow precise audience segmentation for advertisers while drawing user attention toward messages that more closely conform to their existing personal, ideological, and political beliefs.[9]

- Politicians and constituencies interact in dynamic new ways in this information ecosystem. It is easier to distribute messages, segment and narrowly target messages to different groups, shape political narratives, and interpret or whip up public support.

These changes in the information ecosystem also enable the misuse of false information for political effect. There is a resurgence of misinformation, disinformation, and propaganda campaigns.[10] This has been keenly felt with recent foreign interference in democratic elections. States and malicious actors can—at low cost and with high impact—sow confusion and discord in adversaries' domestic politics through digital information campaigns.

Defending against and responding to these campaigns has proven difficult.[11] It takes more time and resources to refute or displace a falsehood than to propagate it. A lie can circulate within trusted networks long enough to be socialized as credible before fact checkers can debunk it. Such campaigns have been highly cost effective, distributed, adaptive, and deniable. Automated accounts on social media—or "bots"—can scale up the effects.[12] These problems are not necessarily new, but the new information ecosystem has made such campaigns cost effective on a scale that was difficult to achieve previously.[13]

"Engagements"

Information and International Conflict

Rapid evolution in the information ecosystem has affected domestic and international political dynamics and widened the arena for conflict. Early cases where digital disinformation and social media had effects in international crises have been few and low on the spectrum of conflict intensity. They do, however, at least

raise questions about whether countries are sufficiently resilient to such dynamics.[14]

For example, disinformation driven on social media sparked a diplomatic crisis in the Persian Gulf in May 2017. Hackers reportedly planted highly inflammatory statements attributed to the Qatari emir on the Qatar News Agency. This caused a wave of outcry, likely amplified on social media by bots, from neighboring Kuwait, Saudi Arabia, and the United Arab Emirates. Qatari officials denied the statements. Even so, Qatar's neighbors responded in protest by severing diplomatic ties with the country and cutting off air and land travel with Qatar.[15]

Disinformation driven on social media has sown confusion into the politics around chemical weapons attacks in Syria. In the hours following the Syrian regime's use of chemical weapons on April 4, 2017, a pro-Assad Web site published an article claiming the attack was a "false flag" operation. The piece was promoted by pro-Kremlin sites, caught traction in alt-right media, and went viral under the hashtag #SyriaHoax. The campaign ended up drawing in a part of President Donald Trump's political base on social and digital media to echo pro-Assad messages opposing the administration's response with missile strikes in Syria.[16]

Social media have played a prominent role in the Trump administration's management of the escalating crisis with North Korea.[17] This has caused experts and observers to publicly worry about whether the president's Twitter usage has undercut diplomatic options and raised the risk of war.[18] As Brian McKeon, former acting undersecretary of defense for policy, testified at a recent 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."[19] Such concerns are undoubtedly accentuated by the consistently expressed administration view that Trump tweets reflect official statements by the president of the United States.[20]

Crises involving the potential use of nuclear weapons are an extreme on the conflict-intensity spectrum. Given tensions in nuclear deterrent relationships today—including the NATO-Russia, US-North Korea, and India-Pakistan relationships—low-level conflicts could escalate quickly. Two roundtable participants argued that, during a conflict in this information ecosystem, it might be easier to inflame calls for war, complicate signaling, and compress decision windows. For example, in December 2016, Pakistani Defense Minister Khawaja Muhammad Asifa—apparently in response to a false news story that Israel had threatened Pakistan with nuclear weapons—tweeted, "Israeli def min threatens nuclear retaliation presuming pak role in Syria against Daesh. Israel forgets Pakistan is a Nuclear state too."[21]

A nuclear use decision—generally made by a country's sole political leader and possibly in very tight time frames—could be particularly sensitive to such new pressures. It is worth exploring how features of this information ecosystem might contribute to escalatory dynamics and the risk of deterrence failure between nuclear powers.

"Impressions"

Information, Stress, and the Phases of a Crisis

The most likely path through which the structure of today's information ecosystem—and specifically social-media-enabled disinformation campaigns—can exert significant influence on those making nuclear decisions is during the earlier phases of a crisis whose evolution and dynamics help to shape the psychology of the ultimate decision. It is of course possible that a nuclear decision maker could wake up one morning and decide to use a nuclear weapon. That scenario, however, seems far less likely than the cumulative effects of the information ecosystem influencing the mind-set and predisposition of the leader responsible for making nuclear use decisions.

Viewing crises as a phased process, and understanding the roles of information and perception throughout them, helps to identify where these cumulative effects might be most significant. According to Michael Brecher, a crisis occurs following the receipt of information about a change in the environment that creates the perception of a threat to basic values, the probability of military involvement, and a finite time in which to respond to the threat.[22] These perceptions induce feelings of stress and uncertainty, the resolution of which is the drama of a crisis.

Leaders will not necessarily behave rationally during a crisis. Stress is known to degrade leaders' cognitive performance by restricting attention, limiting receptivity to information that challenges existing beliefs, and narrowing the range of alternatives considered.[23] Moreover, leaders are not any less susceptible than other people to relying on heuristic and intuitive thinking processes when under stress.[24] These processes are subconscious mechanisms that operate in short time frames and allow individuals to make decisions without the kind of deliberation that characterizes rational thought. Such mechanisms enable individuals to minimize their cognitive load and to arrive at (or avoid) a vital decision, but such shortcuts subject leaders to cognitive biases and make them more prone to wishful thinking. For example, feeling acute domestic political or strategic vulnerabilities, leaders might fear loss and act irrationally out of desperation.[25] Prospect theory also suggests that leaders who perceive that they are in a domain of losses, as might be the case in a crisis, are more likely to be irrationally risk acceptant. Stress may also worsen decision makers' abilities to frame and interpret adversaries' signals.[26]

No human decision is more fraught than one involving the use of nuclear weapons—a decision on which rides the lives of millions of people and potentially the fate of civilization. Such a decision would be made under unfathomable stress, with imperfect information, in four minutes or less in some scenarios.[27] Heuristics and emotional thinking may well reign over rational deliberation in

this environment. Because of this, a nuclear-use decision during a crisis may largely be determined by the decision maker's perceptions of reality developed, in part, prior to the onset of a crisis.

Could the information ecosystem—over days, weeks, or years before a crisis—distort a decision maker's perception of reality? Could it change the social process through which a leader and his or her circle of closest advisers develop shared assessments and beliefs? Could malicious actors hijack such processes? It is unclear under which conditions, (if any) such influence is possible, significant, or significantly different in the current information ecosystem.[28] If such influence is significant, it is worth asking how the effects of the information ecosystem on decision makers could contribute to conflict escalation and deterrence failure.

Researching deterrence psychology and the information ecosystem, or gaming scenarios involving social media use during a crisis between nuclear-armed states, could illuminate questions for future consideration. Such questions could include:

- To what degree does the information ecosystem make it easier for a leader to use bad information, disinformation, or questionable alternative information sources to shape or buttress his or her preferred decision? How might these dynamics affect a leader's ability to identify and dismiss bad information?

- How might online belittling and humiliation (directed either at a nation or personally at an individual decision maker) affect the emotional state of that decision maker in a crisis?

- How do leaders factor messages on social media into perceptions of adversary signals? What messages on social media, and in which contexts, might be effective at signaling? How does the proliferation of message channels affect signal consistency?

- How might the information ecosystem change the likelihood that a leader gets caught in a commitment trap or is able to escape one?[29]

- How and to what extent, if any, could an online public opinion firestorm calling for war from a leader's political base predispose him or her to escalate a crisis or use nuclear weapons first?[30]

- How might a leader instigate such an online firestorm? How could an adversary, or third party, spark such a firestorm through disinformation?

"What's Happening?"

Stabilizing Effects in the Information Ecosystem
The features of the information ecosystem that let falsehoods proliferate also enable new dynamics that could have stabilizing influences on international crises. New tools for professional

journalists, the growth of citizen journalism, and new means for public diplomacy could improve the accuracy of reporting and contribute to more-informed, deliberative, and cautious policy debates and decisions.

For example, the exponential growth of digital sensors in the world has improved the timeliness of information, given actors more objective sources, and increased the resolution that analysts and journalists can achieve with reports. Consider the sensors inside a mobile phone: cameras, microphones, accelerometers, and GPS receivers. With billions of smartphones globally, these devices represent a vast sensor network that provides a dimension of data that records changes in the world. Other networked devices for personal, industrial, or public uses similarly hold data from niche applications. At global and local levels, earth-imaging satellites, meteorological sensors, and seismographic networks provide real-time data about events. Following an event, data from these sensors can quickly propagate through social media and get picked up by analysts and journalists. This allows actors in the information ecosystem near-instantaneous alerts on developing events. Looking through social media and data leading to an event provides a time machine with which to see how events transpired. Analyzing data sets also allows actors to identify and understand trends.

This data-rich environment, and the interconnectivity between actors in it, has given analysts and journalists powerful new tools with which to strengthen reporting and combat falsehoods. There is a new emphasis on how stories can use data to investigate, be enriched by data, or explain the data itself.[31] Crowdsourcing has transformed how stories can be found, developed, and shared with participating audiences.[32] The relationship between the audience and journalism is also now more dynamic, as citizen journalists have grown increasingly skilled with journalistic practice.[33] In this increasingly transparent and open source world, it is easier to identify and refute misinformation and disinformation.

Open source experts and networks of citizen journalists have increasingly innovative ways to locate, track, and analyze conflicts and events. Such activities have increased the information and analysis available to states. This has provided citizens and publics with independent sources of information on world events. The cases below illustrate this.

- Notification of crisis-provoking events—like nuclear tests or missile launches—near-instantaneously appear in social media. One roundtable participant described how, after North Korea test launched a long-range missile, he was able through live social media reports on its flight characteristics to approximate the range of the missile before its flight ended.

- Citizen journalist networks like Bellingcat have proven adept at open source investigations that combat falsehoods around Russia's involvement in the shooting down of Malaysian Air Flight 17 and the Assad regime's use of chemical weapons in Syria.[34]

- Even intelligence hard targets like North Korea are now observable by citizens. Analysts at the Center for Nonproliferation Studies apply geospatial imagery, open source data, and 3-D modeling to analyze North Korea's nuclear weapons and ballistic missile programs.[35]

Such open source capabilities are not so important to national intelligence services, whose technical means and analytical resources can achieve higher resolution with and greater confidence in their intelligence products. Rather, open source capabilities pull back the veil of secrecy that traditionally envelops intelligence collection and analysis, making it harder for national leaders to keep secrets from the interested public. In some instances, the inability to maintain secrecy (e.g., about impending military operations) may induce caution on the part of national leaders.

The information ecosystem has also opened new channels for diplomacy. One hypothesis is that digital communications (including social media) have made it easier for current and former officials to maintain relationships with peers abroad, thereby creating more networks for backchannel diplomacy. It might also be easier to conduct public diplomacy in this ecosystem. One roundtable participant argued that parties to the P5+1 negotiations for the 2015 Iran nuclear agreement tacitly coordinated communications to develop a common narrative that allowed political space to reach agreement.

Such potential stabilizing effects of the information ecosystem on decision making deserve more attention. Potential questions for future research include:

- Under what circumstances, if any, do crowdsourcing and open source intelligence analysis improve the pace and accuracy of public reporting?

- How do the ubiquity of sensors and disintermediation of intelligence affect the management of public opinion during crises?

- How, if at all, might the immediacy and directness of social media allow leaders to improve signaling or reassure publics during times of crisis?

- How and to what extent, if any, does increased connectivity of sitting or former officials create richer and more frequent opportunities for diplomatic outreach?

"Follow and RT"

Additional Open Questions
This Readout and Recommendations, and the roundtable discussion it draws on, raises more questions than it answers. This reflects a shared observation that security researchers have not fully engaged with how the information ecosystem affects foreign policy and crisis decision making.

To facilitate that examination, these are some additional open questions that are possible avenues for future research:

- What features of a state—or of deterrent relationships—might make crises between nuclear-armed states more susceptible to the negative effects of today's information ecosystem? How does the strength of communication and diplomatic ties between states affect such vulnerabilities?

- What do cases tell us about feedback loops on issues of state instability and war?

- Does the information ecosystem complicate the politics of extended deterrence arrangements? If it is easier for adversaries to manipulate domestic constituencies, is decoupling allies similarly becoming easier? What effect might this have on states' decisions to acquire nuclear weapons?

- What is the relationship between nuclear posture and doctrine and decision makers' timelines?

- What steps could be taken to increase leaders' decision time and encourage leaders during crises to "think slowly" and be more deliberative?

- Should governments attempt to manage the social media environment during a crisis?

- How does the information ecosystem influence public attitudes about the use of nuclear weapons?[36]

- How might the information ecosystem change over the next five to ten years? What lessons can be inferred today about the future roles of the information ecosystem in international conflict?

This Readout and Recommendations concludes with a sense of concern about the disruptive potential of social media and digital disinformation campaigns on public policy and international conflict. It also concludes with renewed appreciations for psychological perspectives and the dynamics of crisis decision making. It is clear that more perspectives and more original research are needed to arrive at better understandings of how conflicts, potentially escalating to involve the use of nuclear weapons, could transpire in this information ecosystem.

Until then, we are likely to experience those effects—280 characters at a time.

Endnotes

[1] There is a vibrant community working to define and understand the information ecosystem and the disruptive dynamics within it. See David Lazer et al., "Combating Fake News: An Agenda for Research and Action," Shorenstein Center on Media, Politics, and Public Policy, May 2017, *https://shorensteincenter.org/combating-fake-news-agenda-for-research/*; Giovanni Luca Ciampaglia et al., "Report on ICWSM 2017 Workshop on Digital Misinformation," International Conference on Web and Social Media, May 15–18, 2017, *https://docs.google.com/document/d/1wX-A8nr4j_CVhTVYLa-PJ3j2DwPBH4efbBV4eeQjDWfc/edit*.

[2] James W. Carey, "A Cultural Approach to Communication," in *Communication as Culture: Essays on Media and Society*, (London: Routledge, 1989), pp. 3–8.

[3] See Marie Gillespie and Ben O'Loughlin, "The Media-Security Nexus: Researching Ritualised Cycles of Insecurity," in *The Routledge Handbook of Media, Conflict and Security*, ed. Romy Frohlich, Piers Robinson, and Philip Seib (London: Routledge, 2016), pp. 51–67.

[4] This description draws on the writing of Timothy Norris and Todd Suomela, who argue that the ecosystem metaphor has its faults. See Timothy B. Norris and Todd Suomela, "Information in the Ecosystem: Against the 'Information Ecosystem,'" First Monday, Vol. 22, No. 9, 2017, *http://firstmonday.org/ojs/index.php/fm/article/view/6847/6530#11*.

[5] Internews Center for Innovation and Learning, "Why Information Matters: A Foundation for Resilience," May 2015, p. 11, *https://www.internews.org/sites/default/files/resources/150513-Internews_WhyInformationMatters.pdf*.

[6] See also Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking," Council of Europe Report, September 27, 2017, pp. 10–14, *https://shorensteincenter.org/wp-content/uploads/2017/10/PREMS-162317-GBR-2018-Report-de%CC%81sinformation.pdf?x78124*.

[7] The "CNN effect" is disputed and argued in a variety of ways. The term is used here because it is recognizable in the literature as a prominent discussion on communications technology change and foreign policy making. For a review of various studies on the CNN effect, see Eytan Gilboa, "The CNN Effect: The Search for a Communication Theory of International Relations," *Political Communication*, Vol. 22, No. 1, 2005, pp. 27–44.

[8] Frank Newport, "Americans' Confidence in Institutions Edges Up," Gallup News, June 26, 2017, *http://news.gallup.com/poll/212840/americans-confidence-institutions-edges.aspx*.

[9] Anamitra Deb, Stacy Donohue, and Tom Glaisyer, "Is Social Media a Threat to Democracy?" The Omidyar Group, October 1, 2017, *https://www.omidyargroup.com/wp-content/uploads/2017/10/Social-Media-and-Democracy-October-5-2017.pdf*.

[10] While the terms "misinformation," "disinformation," and "propaganda" are widely used, there is not a common set of definitions for them. For a discussion of practical definitions, see Claire Wardle, "Fake News. It's Complicated," First Draft, Feb. 16, 2017, *https://firstdraftnews.com/fake-news-complicated/*; Caroline Jack, "Lexicon of Liew: Terms for Problematic Information," Data & Society, August 9, 2017, *https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf*.

[11] See David Lazer et al., "Combating Fake News: An Agenda for Research and Action," Shorenstein Center on Media, Politics, and Public Policy, May 2017, *https://shorensteincenter.org/wp-content/uploads/2017/05/Combating-Fake-News-Agenda-for-Research-1.pdf?x78124*; Giovanni Luca Ciampaglia et al., "Report on ICWSM 2017 Workshop on Digital Misinformation," International Conference on Web and Social Media, May 15, 2017, *http://cnets.indiana.edu/blog/2016/12/29/icwsm-2017-misinformation-workshop/*.

[12] Samuel Woolley, "Automating Power: Social Bot Interference in Global Politics," First Monday, Vol. 21, No. 4, 2016, *http://firstmonday.org/ojs/index.php/fm/article/view/6161/5300*.

[13] David Uberti, "The Real History of Fake News," *Columbia Journalism Review*, December 16, 2016, *https://www.cjr.org/special_report/fake_news_history.php*.

[14] For a more in-depth discussion of digital disinformation in international conflict and the vulnerabilities of liberal democratic societies to it, see Herb Lin and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity*, 2018 (forthcoming), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680*.

[15] Akin Ünver, "Can Fake News Lead to War? What the Gulf Crisis Tells Us," War on the Rocks, June, 13, 2017, *https://warontherocks.com/2017/06/can-fake-news-lead-to-war-what-the-gulf-crisis-tells-us/*.

[16] Ben Nimmo and Donara Barojan, "How the Alt-Right Brought #SyriaHoax to America," Digital Forensic Research Lab, April 7, 2017, *https://medium.com/dfrlab/how-the-alt-right-brought-syriahoax-to-america-47745118d1c9*.

17 "Everything President Trump Has Tweeted (and What It Was About)," *Los Angeles Times*, accessed December 10, 2017, *http://www.latimes.com/ politics/la-pol-updates-everything-president-trump- has-tweeted-and-what-it-was-about-2017-htmlstory. html#lb-tag=north-korea*.

18 See Abigail Tracy, "Diplomats Fear Trump Is Tweeting the United States Into War," *Vanity Fair*, October 9, 2017, *https://www.vanityfair.com/news/2017/10/diplomats-don- ald-trump-twitter-north-korea*; Laura Rosenberger, "How President Trump Could Tweet His Way Into Nuclear War With North Korea," *Washington Post*, July 5, 2017, *https://www.washingtonpost.com/news/posteverything/ wp/2017/07/05/how-president-trump-could-tweet-his- way-into-nuclear-war-with-north-korea/?*.

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

20 On June 6, 2017, when asked about the president's tweets, press secretary Sean Spicer said, "The President is the President of the United States, so they're considered official statements by the President of the United States." *http:// www.cnn.com/2017/06/06/politics/trump-tweets-offi- cial-statements/index.html*. This position was repeated in response to a lawsuit filed against the Department of Justice, in which the department said on November 13, 2017, that "The government is treating the statements upon which plaintiffs rely as official statements of the President of the United States." See *https://assets.documentcloud.org/docu- ments/4200037/Trump-Twitter-20171113.pdf*.

21 Russell Goldman, "Reading Fake News, Pakistani Minister Directs Nuclear Threat at Israel," *New York Times*, December 24, 2016, *https://www.nytimes.com/2016/12/24/world/ asia/pakistan-israel-khawaja-asif-fake-news-nuclear.html*.

22 Michael Brecher, "State Behavior in International Crisis: A Model," *Journal of Conflict Resolution*, Vol. 23, No. 3, 1979, pp. 446–480.

23 Alexander George, "The Impact of Crisis-Induced Stress on Decision Making," in *The Medical Implications of Nuclear War*, ed. Fred Solomon and Robert Q. Marston (Washington, DC: National Academies Press, 1986), pp. 539–542.

24 Discussion of heuristics and biases depend on the pioneer- ing work of Amos Tversky and Daniel Kahneman. See Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

25 For a discussion of framing effects and the effects on deterrence, see Jeffrey Berejikian, "A Cognitive Theory of Deterrence," *Journal of Peace Research*, Vol. 39, No. 2, 2002, pp. 165–183.

26 Richard Ned Lebow, "Deterrence: A Political and Psychological Critique," in *Perspectives on Deterrence*, ed. Robert Axelrod, Robert Jervis, Roy Radner, and Paul Sterns (New York: Oxford University Press, 1989), pp.25–51.

27 Jeffrey Lewis, "Our Nuclear Procedures Are Crazier Than Trump," *Foreign Policy*, August 5, 2016, *http://foreignpolicy.com/2016/08/05/ our-nuclear-procedures-are-crazier-than-trump/*.

28 Ben O'Loughlin summarized this point well, with healthy skepticism, in a piece on his reflections from the roundtable. Ben O'Loughlin, "Nuclear Policy Remains a Strategic Decision, Despite Tactical Tail-Twisting on Twitter," *Global Policy Journal*, November 14, 2017, *http://www.globalpolicyjournal.com/blog/14/11/2017/ nuclear-policy-remains-strategic-decision-despite-tacti- cal-tail-twisting-twitter*.

29 Scott D. Sagan, "The Commitment Trap: Why the United States Should Not Use Nuclear Threats to Deter Biological and Chemical Weapons Attacks," *International Security*, Vol. 24, No. 4, 2000, pp. 85–115.

30 Katja Rost, Lea Stahel, and Bruno S. Frey, "Digital Social Norm Enforcement: Online Firestorms in Social Media," PLOS One, Vol. 11, No. 6, June 17, 2016.

31 Simon Rogers, Jonathan Schwabish, and Danielle Bowers, "Data Journalism in 2017: The Current State and Challenges Facing the Field Today," Google News Lab, September, 2017, p. 6, *https://newslab.withgoogle.com/assets/docs/data-jour- nalism-in-2017.pdf*.

32 Mimi Onuhoa, Jeanne Pinder, and Jan Schaffer, "Guide to Crowdsourcing," Tow Center for Digital Journalism, 2015, pp.9-12, https://academiccommons.columbia.edu/catalog/ ac:95x69p8d09.

33 The terms "citizen journalism" or "participatory journal- ism" have varied and wide interpretations. See Luke Goode, "Social News, Citizen Journalism and Democracy," *New Media & Society*, Vol. 11, No. 8, pp. 1288–1292.

34 Ben Sullivan, "Bellingcat Wants Your Help to Debunk Fake News," Motherboard, March 7, 2017, *https:// motherboard.vice.com/en_us/article/78qbqy/ bellingcat-wants-your-help-to-debunk-fake-news*.

35 See Anna Fifield, "With Technology, These Researchers Are Figuring Out North Korea's Nuclear Secrets," *Washington Post*, November 21, 2017, *https:// www.washingtonpost.com/world/asia_pacific/ with-technology-these-researchers-are-figuring-out-north- koreas-nuclear-secrets/2017/11/20/274d9786-c9e2-11e7- b244-2d22ac912500_story.html?utm_term=.39b6a3884ce5*; Jeffrey Lewis, "Applying New Tools to Nonproliferation: A

Nuclear Detective Story," *Nuclear Threat Initiative*, May 2, 2016, *http://www.nti.org/analysis/reports/apply-ing-new-tools-nonproliferation-nuclear-detective-story/.*

36 36 Scott Sagan and Ben Valentino, "Revisiting Hiroshima in Iran," *International Security*, Vol. 42, No. 1, 2017, pp. 41–79.

Participant List

CoChairs

Herbert Lin, Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation, Stanford University

Benjamin Loehrke, Program Officer, Nuclear Policy, The Stanley Foundation

Harold Trinkunas, Deputy Director and Senior Research Scholar, Center for International and Security Cooperation, Stanford University

Rapporteur

Danielle Jablanski, Program Associate, Nuclear Policy, The Stanley Foundation

Participants

James Acton, Co-Director and Senior Fellow, Nuclear Policy Program, Carnegie Endowment for International Peace

Jeffrey Berejikian, Professor, International Affairs, University of Georgia

Malfrid Braut-Hegghammer**, Associate Professor, Political Science, University of Oslo

Jennifer Erickson**, Professor, Political Science and International Studies, Boston College

Henry Farrell**, Professor, Political Science and International Affairs, George Washington University

Anya Loukianova Fink, Stanton Nuclear Security Fellow, RAND Corporation

Tom Glaisyer, Director of the Public Square Program, Democracy Fund

Robert Gorwa, Doctoral Student, Political Science and International Relations, Oxford University

Kelly Greenhill, Professor, Political Science and International Relations, Tufts University, and Research Fellow, Harvard University

Jaclyn Kerr, Postdoctoral Research Fellow, Center for Global Security Research, Lawrence Livermore National Laboratory

Ben O'Loughlin, Professor, Politics and International Relations, Royal Holloway, University of London

Anna Péczeli, Research Fellow, Centre for Strategic and Defense Studies, National University of Public Service

Keith Porter, President, The Stanley Foundation

John Scott-Railton, Senior Researcher, Citizen Lab University of Toronto, Munk School of Global Affairs, University of Toronto

Paul Slovic, Professor, Psychology, University of Oregon

Lior Tabansky, Scholar of Cyber Power, Tel Aviv University

Philip Taubman, Adjunct Professor, Center for International Security and Cooperation, Stanford University

Devon Terrill, Program Officer, Media, The Stanley Foundation

Benjamin Valentino, Associate Professor, Government, Dartmouth College

---

Affiliations are listed for identification purposes only. Participants attended as individuals rather than as representatives of their governments or organizations.

About Us
The Stanley Center for Peace and Security partners with people, organizations, and the greater global community to drive policy progress in three issue areas—mitigating climate change, avoiding the use of nuclear weapons, and preventing mass violence and atrocities. The center was created in 1956 and maintains its independence while developing forums for diverse perspectives and ideas. To learn more about our recent publications and upcoming events, please visit stanleycenter.org.