Brief No. 14.1

Coordinated Chaos

Synchronized Cyberwarfare and Disinformation Attacks

Lucas Hauser

P | I | P | S

Please direct inquiries to:
The Project on International Peace and Security
Global Research Institute
The College of William & Mary
427 Scotland Street
Williamsburg, VA 23185
pips@wm.edu

Electronic copies of this report are available at www.wm.edu/pips

Coordinated Chaos

Synchronized Cyberwarfare and Disinformation Attacks

Lucas Hauser

MAY 2022

P | I | P | S

The Project on International Peace and Security
Global Research Institute
College of William & Mary

Coordinated Chaos:
Synchronized Cyberwarfare and Disinformation Attacks

In the future, adversaries will conduct complex attacks against the United States that synchronize cyberattacks with disinformation operations to manufacture political crises. Cyberattacks trigger the crisis, while tailored disinformation manipulates the public response. The coordinated attack intensifies domestic divisions, encourages conflict and violence, and cripples the government's ability to act, thus endangering the United States' ability to respond to crises. The U.S. national security community often views cyberwarfare and disinformation as independent threats, creating a vulnerability to coordinated cyber-disinformation attacks. This unpredictable threat requires a coordinated response from all levels of government. To understand this threat, the United States government should hold a series of interagency and federal and local tabletop exercises and wargames so relevant actors can begin to prepare for this complex form of attack.

Introduction

In 2007, the Estonian government sought to move a statue commemorating the Red Army named "The Liberators of Tallinn" from the center of the capital city to the local military cemetery.[1] False Russian-language reports claimed that the statue was to be destroyed. Russian-speaking Estonians rioted to defend their beloved statue. The unrest was followed by weeks of cyberattacks targeting Estonian banks, media publications, and government websites. No direct links to the Russian military were found, although many attacks originated from Russia.

The Estonian attack previews a new threat to the United States: a coordinated cyber-disinformation operation, where an adversary synchronizes cyberattacks and disinformation campaigns to provoke domestic dissension in the target. Cyberattacks create a crisis, while disinformation campaigns frame and magnify the social and political impact of the attack.

The spectrum of potential outcomes of coordinated attacks is broad, ranging from localized disruptions to widespread unrest and violence. These attacks can occur during combat operations, disrupting command and control or targeting soldiers' morale to damage an opponent's war-fighting capacity. Coordinated cyber-disinformation attacks also can exploit existing cleavages in the United States to achieve political objectives, heighten divisions, and create chaos in local politics.

The United States is not prepared for a coordinated cyber-disinformation attack. Government structures manage cyberwarfare and disinformation as independent threats. This arrangement will stymie Washington's ability to detect and respond to coordinated attacks that cross agency jurisdictions. The wide range of potential targets—from town councils to national elections—combined with the unpredictable outcomes of coordinated attacks requires an interagency

response. Federal, state, and local authorities should explore how to best respond to coordinated cyber-disinformation attacks through interagency tabletop exercises and wargames.

The Coordinated Attack: A Cyber and Disinformation Threat

Adversaries will likely attack the United States in the future using coordinated cyber and disinformation campaigns. Cyberattacks generate a real crisis around which a disinformation campaign can be designed. Disinformation disseminators create false and misleading narratives on social media platforms to appeal to and infiltrate online communities, in order to maximize confusion.[2] Thus, a coordinated attack uses cyberattacks and disinformation to damage and divide the United States. A coordinated cyber-disinformation attack would likely follow a three-step model: (1) long-term preparation, (2) cyberattack, (3) tailored disinformation (see Figure 1).

Figure 1: A Coordinated Cyber-Disinformation Attack

- **Step One: Long-term preparation.** Disinformation can shape political attitudes, sowing the seeds of division and distrust that adversaries can later exploit. Purveyors of foreign disinformation develop a following on social media to spread inflammatory rhetoric on events to drown out reputable news and gain credibility in partisan online communities. These actions prime the information environment, shaping the domestic political discourse in preparation for a coordinated attack. Cyberattacks can also gather information to develop the future tailored disinformation campaign in this period.

- **Step Two: Cyberattack.** After deepening domestic divisions, cyberattacks are launched at an opportune moment, such as before an election or during a political scandal. Cyberattacks can damage computer networks, physical infrastructure, and devices, creating a chaotic environment for tailored disinformation to exploit.

- **Step Three: Tailored disinformation.** A new wave of tailored disinformation seizes on the cyberattack to heighten the chaos. During and immediately following the cyberattack, disinformation channels promote inflammatory false information to amplify confusion and polarization, drowning out the truth. This disinformation also encourages

violent responses to the cyberattack to increase its impact. The process of priming the information environment and then striking with a synchronized cyber-disinformation attack maximizes the impact of both types of attack.

These attacks would aim to weaken political cohesion and social trust in the United States. Disunity at home could prompt Washington to turn inward or limit the ability of the United States to conduct foreign policy. While the United States is distracted by internal turmoil, U.S. adversaries will have a freer hand to pursue their international aims.

Combining Cyber and Disinformation Magnifies Their Impact

Cyberattacks and disinformation are an effective combination for a coordinated attack. There are three main reasons why cyberattacks can enhance a disinformation campaign:

- **Cyberattacks are cost-effective and flexible.** Cyberwarfare is a less costly tool than conventional or nuclear weapons as a means of attack. The interconnectivity of the internet allows cyberattacks and disinformation campaigns to be launched from almost anywhere in the world.

- **Cyberattacks create confusion.** Cyberattacks are disruptive because their damage and the immediate anonymity of perpetrators create confusion.[3] These attacks may or may not cause physical damage to networks, systems, or infrastructure. Attacks on networks are more difficult to detect, and their consequences are difficult to measure.

- **Cyberattacks are in the gray zone.** Cyberwarfare, especially information warfare, is often perceived as a form of combat below the threshold of war—in the gray zone.[4] By operating in the gray zone, these coordinated attacks provide rival powers with the ability to weaken the United States without firing a shot. These attacks target U.S. politics, shaping U.S. behavior without resorting to war. Russia, China, and Iran, in particular, espouse doctrines, such as "hidden war," "political warfare," and "soft war," that emphasize achieving objectives without armed attacks, like cyber-disinformation attacks.[5]

Cyberwarfare and disinformation thus give adversaries the opportunity to undermine the United States by manipulating public opinion and weakening the political system. Since cyberattacks and disinformation are both tools to achieve these effects, their combination and synchronization in coordinated attacks is a logical next step. Indeed, we have already seen them combined in a military setting, with Russia employing cyberattacks alongside disinformation campaigns in Georgia in 2008 and in Ukraine in 2014 and 2022.[6]

The Scale of Coordinated Cyber-Disinformation Attacks

The following scenarios aim to depict the range of potential coordinated cyber-disinformation attacks (see Figure 2). These attacks can be effective at a smaller scale: aiming to manufacture

localized disruptions that are difficult to detect. Coordinated attacks can have larger goals as well: chaos and violence on a national scale.

Figure 2: Goals and Outcomes for a Coordinated Attack

Scenario 1: An attack on the judicial system

Russian operatives aim to erode institutional trust and create political dysfunction through a coordinated attack that harasses local judicial officials, who often enjoy positions of special trust in American communities. Over time, Russian actors tasked with spreading disinformation develop trusted fake accounts and sites, embedding themselves in radical online communities. Next, intelligence operatives identify a local judge who has made a ruling unfavorable to Russia's interests. Disinformation disseminators spread sensational stories about his alleged corrupt rulings against these radical groups.

Hackers then steal personal information about the judge to then leak his identity, residence, travel patterns, and office location online to the violent groups, inciting the spread of deepfakes, inflammatory disinformation, and violent calls to arms. The harassment of a local judge would likely not be material for national news—being seen as merely cyber-crime or cyber-harassment by activists—allowing Russian operatives to repeatedly target a variety of public officials without provoking a U.S. government response.

Scenario 2: An attack to stoke racial divisions

Beijing aims to weaken U.S. social cohesion and expose its system as inferior to the Chinese model through a coordinated attack that encourages racial conflict. Chinese operatives identify an American metropolitan area with tense racial relations. China-backed disinformation accounts and channels continually expose users to racially charged rhetoric that villainizes those with dissimilar racial identities, pitting black and white groups against each other. Long-term disinformation campaigns plant seeds of division in anticipation of the coordinated attack.

Hackers then identify important infrastructure for a community, like power lines and local schools, and begin launching cyberattacks. Subsequently, Chinese disinformation operatives feed into existing racially charged messaging by casting blame for the disruptions on racially stereotyped scapegoats. The choice of target would confirm the lies spread in the initial disinformation campaign, making the messaging after the attack more believable to each audience.

Scenario 3: A catastrophic strike on Election Day fuels polarization, violence

Russian hackers aim to subvert the U.S. electoral process through a coordinated attack that casts doubt on the outcome of a major election. Russian disinformation actors insert themselves in online communities across the United States and on both sides of the political spectrum over many months. Targets for future deepfakes are identified, such as political figures and scapegoats for the attack, and their data is stolen.

Russian hackers launch a series of crippling cyberattacks to cause rolling electrical blackouts in the key swing state of Pennsylvania on Election Day. Simultaneously, disinformation disseminators circulate partisan messaging. For the right, disinformation agents play into fears of the "deep state" stealing the election, creating a deepfake of a leaked cell phone video of a DNC executive telling intelligence officers, "we're going to shut down the power and steal the votes." A fake map shows overlaps between blackout zones and concentrations of Republican voters. To stoke outrage on the left, disinformation disseminators attribute the attack to GOP operatives planning to suppress liberal votes. As Americans see these messages and create new disinformation, Russian accounts amplify these grassroots false narratives.

The disinformation dominates the online news environment. Deepfakes of trusted journalists are posted to partisan media. Spoofs of reputable websites are used to enhance the credibility of fake articles and images distributed to followers. Hackers even breach mainstream news sources and temporarily alter their content. Within radical groups, every Russian-operated account begins sounding the alarm. Disinformation accounts make calls to arms and encourage vigilante justice to seize control of the election.

These scenarios demonstrate an array of potential coordinated cyber-disinformation attacks. This dynamic threat is difficult to counter. Therefore, the United States cannot pursue a one-size-fits-all approach to coordinated cyber-disinformation attacks. In response, the United States will need a level of coordination and sophistication that reflects the unpredictability of coordinated attacks.

America the Vulnerable: Preparing for Coordinated Attacks

Coordinated cyber-disinformation attacks exploit U.S. vulnerabilities. To counter this threat, the United States will need an interagency response. Tabletops and wargames provide an avenue to explore the nature of this threat and prepare for future attacks.

Why is the United States at High Risk?

The United States is particularly vulnerable to coordinated cyber-disinformation attacks for three key reasons:

- **Responsibility is 'stove-piped' within the government**. The U.S. national security community often views cyber and disinformation as distinct threats. Accordingly, the government has different management for cybersecurity and disinformation. The Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) forefronts cybersecurity.[7] However, the monitoring and management of the domestic information environment lack a leading agency, although the Global Engagement Center (GEC) at the U.S. State Department monitors disinformation specifically from foreign sources.[8] The separation of cyber and disinformation creates "stove-pipes," or distinct channels that do not interact, of responsibility that will hinder the government's identification of and response to the multidimensional threat of a coordinated cyber-disinformation attack.

- **Disinformation subverts an open information environment.** In the United States, protection of free speech and a free press has resulted in an open flow of information online. Malign actors exploit these freedoms by spreading disinformation. The U.S. government has little authority to limit online disinformation.[9]

- **Attacks are difficult to trace.** Coordinated attacks are cheaper than conventional conflict for adversaries and require no physical military capabilities.[10] Adversaries can launch cyberattacks and inundate U.S. information ecosystems with disinformation from anywhere in the world with an internet connection. Virtual private networks (VPNs) make tracing these attacks difficult, especially in real time.[11] VPNs also subvert boundaries of control, blurring the lines between regional commands and whether a threat is foreign or domestic in origin.

To better prepare for both dimensions of a combined attack, the United States should continue investments in its cybersecurity capabilities and centralize responsibility under CISA or another designated agency. The United States should also make greater investments into combatting disinformation by building trust in democratic institutions and reducing the sway dis- and misinformation have in the U.S. media ecosystem, particularly on social media.

These tasks are neither simple nor quick. As such, the United States should prepare for these attacks to mitigate their impact. Washington must take a proactive approach to preventing the damage of coordinated cyber-disinformation attacks. The dynamic nature of a coordinated cyber-disinformation attack requires innovative interagency responses to mirror the complexity of coordinated attacks.

Coordinated Cyber-Disinformation Attacks Require an Interagency Response

It is not possible to prepare for every potential coordinated attack. Therefore, it is essential to prepare strategies to limit their damage. Coordinated cyber-disinformation attacks are likely to fall outside the purview of a single government agency or organization. Indeed, adversaries could seek to exploit institutional fault lines when designing an attack. The complexity of the threat means that a response requires cooperation among actors across the government and private sector.

An interagency response is the best answer to a coordinated cyber-disinformation attack. Interagency simulations, tabletop exercises, and wargames offer avenues for generating effective cooperation strategies prior to an attack. For example, in Scenario 2 outlined above, a number of actors would need to be involved after the attack. Education departments, health and medical offices, utility companies, departments of energy and transportation, and law enforcement agencies would all play a role in repairing the institutional damage from sporadic cyberattacks. To restore public trust, the same organizations would need to work with local government, civil society, social media companies, public relations firms, and groups that monitor disinformation in majority-minority communities. We see with this scenario that interagency cooperation is integral to identifying a coordinated attack and synchronizing responses—even if the attack fails to make national headlines.

An interagency response to coordinated cyber-disinformation attacks would minimize damage in several ways:

- Responses to attacks will occur more quickly, limiting their impact.
- Lines of authority will be clear and prevent unnecessary duplicative efforts.
- Actors at all levels and across all sectors will be aware of the potential for coordinated cyber-disinformation attacks, increasing detection and respondence to these attacks.

Interagency Response Blueprint: Simulations, Tabletops, and Wargames

An interagency response requires preparation and coordination. Through this preparation, government officials will gain a better understanding of how the threat can manifest and potential roadblocks to cooperation across agencies and levels of government.

An effective interagency response can be formulated through exercises that simulate coordinated cyber-disinformation attacks to generate avenues for communication and planning during an actual crisis. In a tabletop or wargame environment, representatives of different government agencies and private sector actors can practice crafting an interagency response, learning how to best deploy their joint capabilities. These exercises will illuminate effective standard operating procedures for future interagency operations following coordinated cyber-disinformation attacks.

Such exercises require thoughtful design. Effective tabletops and wargames to develop a blueprint for interagency cooperation should follow these guiding principles:

- **Representative members.** Effective tabletops and wargames could incorporate players across the government and civil society to avoid "stove-piping." A diversity of institutional perspectives and capabilities would enable the wargames to fully explore the implications of a range of coordinated attacks. The recommendations produced from such exercises would also be more creative because the process of considering alternative perspectives encourages innovation.

- **Scenario realism.** More believable scenarios with greater stakes can help participants design and execute scenarios that realistically capture the uncertainties of a coordinated cyber-disinformation attack and help identify critical decision points when seeking to limit the damage. These games should incorporate real computer networks and systems rather than insulated clones of relevant pieces of systems to maintain scenario realism.

- **A dedicated red team.** A red team can explore how adversaries might exploit U.S. weaknesses in coordinated cyber-disinformation attacks. This process could tease out the varied and even unexpected ways that cyberattacks and disinformation can work in unison. A dedicated group that considers these questions over multiple games can offer insights into what adversaries might attempt.

- **Participation by senior leadership.** Involvement by senior leadership can reveal the layers of complexity at and between different levels of government during a coordinated cyber-disinformation attack. As part of a simulation, players could brief higher ranked participants, receive instructions, and return to their games. This exercise can help uncover how barriers to communication and coordination among agencies could be exploited and how to overcome these challenges.[12]

Such exercises would produce the building blocks for future interagency responses. Participants could craft protocols for responding to the range of coordinated attack types, memorandums of understanding between agencies about responsibilities and divisions of labor, and basic communication procedures following an attack.

These efforts can build on existing (but independent) initiatives that fight cyberwarfare and combat disinformation. The Department of Homeland Security issued a report in October 2019, entitled "Combatting Targeted Disinformation," that brought together members of government, the private sector, and the academy to discuss the threat of tailored disinformation campaigns.[13] At DHS, CISA conducts wargames for cyber threats.[14] Building on these types of initiatives could form the basis of an interagency response to a coordinated attack.

The United States has approached previous emerging challenges similarly. To prepare responses to nuclear attacks, the Department of Defense created Strategic Command (STRATCOM) in 1992.[15] STRATCOM took the lead in coordinating immediate strategic responses to nuclear attacks, which otherwise would have fallen between the jurisdictions of geographical and functional commands.[16] STRATCOM led wargames to improve intergovernmental cooperation, reducing response times in a crisis. STRATCOM takes the lead in bringing resources across agencies together to create rapid, coordinated reactions.[17] The United States can adopt such an approach in preparing for coordinated cyber-disinformation attacks.

Conclusion

The coordination of cyberattacks and disinformation offers unique advantages to U.S. adversaries. Cyberattacks create chaos that tailored disinformation can seize upon and magnify. Both

cyberattacks and disinformation attacks can be executed and synchronized from a distance via an internet connection. Both also are difficult to detect and react to because they operate below the conventional threshold of war.

Coordinated attacks are likely. At the local and national level, coordinated cyber-disinformation attacks encourage polarization, chaos, and violence, undermining the American political system and paralyzing the U.S. government.

The United States can prepare for this threat through interagency tabletops and wargames. These exercises will allow U.S. policymakers to explore the dangers posed by coordinated cyber-disinformation attacks and develop procedures for how to respond when they occur. In this way, the United States can craft reactions that are as innovative and nimble as the coordinated cyber-disinformation attacks themselves.

Acknowledgments

I am extremely grateful to Avah Dickinson for her extensive assistance, without which this paper would not have been possible. I would also like to recognize the invaluable assistance of my military fellow, Lt. Colonel Gregory Tomlin, for his guidance and feedback throughout the process. I must also thank Mitchell Croom for all of his help and for serving as a mentor for this project. I would also like to thank Kathryn Floyd, Maureen Fromuth, Daveed Gartenstein-Ross, Lisa Kaplan, Major Joseph Littell, Captain Margaret Smith, and Jimmy Zhang, whose feedback significantly improved the paper. I would like to pay my special regards ti Lt. Colonel Nathan Finney for helping me form the idea for this paper and providing feedback throughout the PIPS process. I am also grateful to the entire 2021-2022 PIPS team, who inspired me every week and made the three-hour meetings the highlight of my week every time. I also have to thank Nitya Labh for first bringing me into the PIPS community last year and making me feel at home. I would like to extend my deepest gratitude to Professors Amy Oakes and Dennis Smith for their tireless efforts to support me from start to finish—this project would not be what it is without them. Finally, I cannot begin to express my thanks to my friends, family, and colleagues who supported me throughout the project.

[1] Damien McGuinness. "How a Cyber Attack Transformed Estonia." *BBC*, April 27, 2017. https://www.bbc.com/news/39655415.
[2] Chris Meserole. "How Misinformation Spreads on Social Media—And What to Do About It." *Brookings Institution*, May 9, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it/.
[3] Panayotis A. Yannakogeorgos. "Strategies for Solving the Cyber Attribution Challenge." Air University Press, 2016. https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF.
[4] François Delerue. "The Threshold of Cyber Warfare: From Use of Cyber Force to Cyber Armed Attack." In *Cyber Operations and International Law*. Cambridge Studies in International and Comparative Law. Cambridge University Press, 2020. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/18EED20277D22CAE25E71F63A27C8009/9781108490276c6_273-342.pdf/the-threshold-of-cyber-warfare-from-use-of-cyber-force-to-cyber-armed-attack.pdf; James Andrew Lewis. "Thresholds for Cyber War." *Center for Strategic and International Studies*, October 1, 2010. https://www.csis.org/analysis/thresholds-cyberwar; Michael N. Schmitt. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017. doi:10.1017/9781316822524. Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016) 163.
[5] Kyle Genaro Phillips. "UNPACKING CYBERWAR: The Sufficiency of the Law of Armed Conflict in the Cyber Domain." *Joint Force Quarterly*, no. 70, 3rd Quarter 2013 (2013): 70–75. 73.; Arsalan Bilal. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." *NATO Review*, November 30, 2021. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.; Hallvard Notaker. "In the Blind Spot: Influence Operations and Sub-Threshold Situational Awareness in Norway." *Journal of Strategic Studies*, February 20, 2022.; Sarah Jacobs Gamberini. "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns." *Joint Force Quarterly*, no. 99 (November 19, 2020). https://wmdcenter.ndu.edu/Portals/68/Documents/jfq/jfq-99/jfq-99_4-13_Gamberini.pdf?ver=Yoes_BQSvex7rNRLXvI08Q%3d%3d. Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines between War and Peace* (Washington, DC: Georgetown University Press, 2019); Dennis Poindexter, *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests*, 2nd ed. (Jefferson, North Carolina: McFarland & Company, Inc., 2018); Blout, Emily. "Iran's Soft War with the West: History, Myth, and Nationalism in the New Communications Age." *The SAIS Review of International Affairs* 35, no. 2 (Summer-Fall 2015): 33–44.
[6] Georgia: Peter Dickinson. "The 2008 Russo-Georgian War: Putin's Green Light." *Atlantic Council*, August 7, 2021. https://www.atlanticcouncil.org/blogs/ukrainealert/the-2008-russo-georgian-war-putins-green-light/.; Paulo Shakarian. "The 2008 Russian Cyber-Campaign Against Georgia." *Military Review*, January 2011. https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia. https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.
Ukraine 2014: Natalia Zinets. "Ukraine Hit by 6,500 Hack Attacks, Sees Russian 'Cyberwar.'" *Reuters*, December 29, 2016. https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC.; Adrian Croft and Peter Apps. "NATO Websites Hit in Cyber Attack Linked to Crimea Tension." *Reuters*, March 15, 2014. https://www.reuters.com/article/us-ukraine-nato/nato-websites-hit-in-cyber-attack-linked-to-crimea-tension-idUSBREA2E0T320140316.; Andy Greenberg. "How an Entire Nation Became Russia's Test Lab for Cyberwar." *Wired Magazine*, June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine; Elīna Lange-Ionatamišvili. "Analysis of Russia's Information Campaign Against Ukraine." NATO Strategic Communications Centre of Excellence, 2015. https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf.
Ukraine 2022: Jessica Brandt and Adrianna Pita. "How Is Russia Conducting Cyber and Information Warfare in Ukraine?," n.d. https://www.brookings.edu/podcast-episode/how-is-russia-conducting-cyber-and-information-warfare-in-ukraine/.; Zulfikar Abbany. "Ukraine: Cyberwar Creates Chaos, 'It Won't Win the War.'" *Deutsche Welle*, March 3, 2022. https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197.; Stephanie Stamm and Hanna Sender. "Cyberattacks, Hacks and Misinformation: The Many Fronts of Russia's Hybrid War in Ukraine." *Wall Street Journal*, February 26, 2022. https://www.wsj.com/articles/cyber-attacks-hacks-

and-misinformation-the-many-fronts-of-russias-hybrid-war-in-ukraine-11645871401.; David E. Sanger, Julian E. Barnes, and Kate Conger. "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War." *The New York Times*, February 28, 2022. https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.

[7] Cyber Security & Infrastructure Security Agency. "ABOUT CISA," n.d. https://www.cisa.gov/about-cisa.

[8] "Global Engagement Center." Functional Bureau Strategy, October 2, 2018. https://www.state.gov/wp-content/uploads/2019/01/FBS_GEC_UNCLASS-508.pdf.

[9] Philip Seib, *Information at War: Journalism, Disinformation, and Modern Warfare*, 1st ed. (Polity, 2021)

[10] Frank C. Sanchez, Weilun Lin, and Kent Korunka. "Applying Irregular Warfare Principles to Cyber Warfare." *JFQ*, Quarter 2019. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_15-22_Sanchez-Lin-Korunka.pdf.

[11] Panayotis A. Yannakogerorgos."Strategies for Resolving the Cyber Attribution Challenge." *Air Force Research Institue*, Perspectives on Cyber Power, December 2013. https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF.

[12] The chain of command, through the National Security Council, cabinet secretaries, and the White House, should drive the scenarios. An initial event could lay out the scenario and solicit input from experts and government leaders. Following that, an event could be held for lower-level action officers, who work through a scenario. That event could lead to an ultimate event with senior leaders, who would produce decision memos, memos of understanding, protocols to be approved in an NSC meeting, or a briefing with the White House. Senior leadership involvement through stair-step actions allows for future interagency responses that can move up and down the chain of command.

[13] 2019 Public-Private Analytic Exchange Program. "Combatting Targeted Disinformation Campaigns." Department of Homeland Security, October 2019. https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

[14] "Critical Infrastructure Exercises: CISA Tabletop Exercises Packages." CISA, n.d. https://www.cisa.gov/cisa-tabletop-exercises-packages.

[15] "History." U.S. Strategic Command, January 2018. https://www.stratcom.mil/About/History.

[16] Fontenot, Jon M Fontenot. "A New Era: From SAV to STRATCOM." Marine Corps Command and Staff College, May 23, 1995. https://spp.fas.org/eprint/fontenot.htm.

[17] James E Cartwright. The Posture of the U.S. Strategic Command (USSTRATCOM), § Strategic Forces Subcommittee of the Committee on Armed Services (2007). https://www.govinfo.gov/content/pkg/CHRG-110hhrg37317/html/CHRG-110hhrg37317.htm; U.S. Strategic Command. "USSTRATCOM & U.S. Naval War College Conducted DEGRE Series of Wargames." *USSTRATCOM Public Affairs Office*, April 16, 2021. https://www.stratcom.mil/Media/News/News-Article-View/Article/2575852/usstratcom-us-naval-war-college-conducted-degre-series-of-wargames/; Steve Liewer. "On 9/11, as StratCom Played War Game, The Ugly Reality of Terror Arrived." *Omaha World-Herald*. September 7, 2021. https://omaha.com/news/local/on-9-11-as-stratcom-played-war-game-the-ugly-reality-of-terror-arrived/article_d6bbd088-0aa8-11ec-a674-73859242f2c2.html.