2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report

Brandon Valeriano
Donald Bren Chair of Military Innovation
Marine Corps University
Quantico, VA, USA

Benjamin Jensen
Professor
School of Advanced Warfighting
Marine Corps University
Quantico, VA, USA

Abstract: Crafting a national cyber strategy is an enormous undertaking. In this article we review the process by which the Cyberspace Solarium Commission generated the Solarium Commission Report, developed the strategy of layered cyber deterrence, and strategized for legislative success in implementing its recommendations. This is an article about the development of a whole-of-nation strategy. Once the production of the strategy of layered cyber deterrence is explained, the article goes on to elaborate on implementation strategies, the challenge of escalation management, and future efforts to ensure that the work of the Solarium Commission becomes entrenched in U.S. national cyber strategy and behavior. We review the work left undone by the Solarium Commission, highlighting the enormous effort that went into the process of building out a strategy to defend a nation.[1]

Keywords: *cyber strategy, deterrence, coercion, escalation*

1 It takes a village; we thank the entire Solarium Commission team, as their efforts generated the final Commission Report and the legislative successes that followed. In some ways, this article seeks to chronicle the process of building a strategy that was developed through the efforts of hundreds of people. This work reflects the process that we went through to construct the Solarium Commission report, which is particular to our experience; others may have had different recollections of the events under consideration. Brandon Valeriano is also a Senior Fellow at the Cato Institute and a Senior Advisor to the Cyberspace Solarium Commission. Benjamin Jensen is also a Scholar in Residence at American University and the Research Director for the Cyberspace Solarium Commission.

1. INTRODUCTION

Established in the fiscal year 2019, the John S. McCain National Defense Authorization Act (NDAA) created the Cyberspace Solarium Commission to evaluate competing approaches of cyber strategy and seek a consensus comprehensive strategy to defend the United States in cyberspace against significant attacks. This article will review the process of developing the report of the Cyberspace Solarium Commission (hereafter, Solarium Commission) (Montgomery, Jensen et al. 2020) and the strategy of layered cyber deterrence (Jensen 2020).

The challenge of "develop[ing] a consensus on a strategic approach" is immense (Congress 2017–2018, 132 STAT. 2141). The Fiscal Year 2019 NDAA tasked the Solarium Commission with considering the options of "deterrence, norms-based regimes, and active disruption of adversary attacks through persistent engagement" (Congress 2017–2018, 132 STAT. 2143). These options became overlapping layers, mimicking the original Eisenhower Solarium Commission's strategy of engagement with the Soviet Union combined with aspects of containment and deterrence (Gallagher 2015). Rather than viewing strategic approaches as mutually exclusive, the team viewed them as complementary, creating an overall denial-based effect on adversary decision-making.

The central idea behind layered cyber deterrence is to alter the cost-benefit calculations of the adversary to threaten U.S. interests in cyberspace yet also take into account the global reliance private sector networks have on the new digital commons. No action will stop all cyber activity by state and non-state actors engaged in political warfare, espionage, military operations, or criminal activity. Rather, the goal is to alter the cost-benefit calculation to reduce the severity and frequency of cyber activity.

The first layer became "shape behavior," encompassing the development of normative regimes to govern cyberspace in collaboration with international partnerships. Shaping behavior also seeks to leverage non-military instruments such as regulations and legal regimes to produce a cyber environment that favors stability. Entanglement (Nye 2017), another term for shaping the international environment, includes not only norm generation but also the inclusion of various structures that could facilitate progress in cyber security to shape the environment in ways that are conducive to global security. The second layer became "deny benefits," which encompasses some traditional aspects of deterrence but focuses on resiliency and defense in depth (Valeriano and Jensen 2019). This effort includes securing elections, protecting critical infrastructure, and ensuring the continuity of the economy and government. By hardening the defense targets, the U.S. can enable deterrence and forestall digital violence.

The third layer became "impose costs," which sought to generate cyber capabilities and capacity.[2] The goal was to flesh out the concept of persistent engagement (Fischerkeller and Harknett 2017; Healey 2019). Persistent engagement suggests that imposing costs was an outgrowth of the strategy, not the means (Fischerkeller and Harknett 2020). To orchestrate a whole-of-nation approach to defending the nation through forward action and cost imposition, the Solarium Commission recommended enabling the United States to leverage cyber power to achieve effects, but with an eye towards preserving privacy, the resilience of global networks, and the proper delegation of authorities, consistent with international law and existing legal regimes.

In this paper we review how the strategy of layered cyber deterrence was constructed and how the background research and wargames helped the Solarium Commission staff generate the final report (Montgomery, Jensen et al. 2020), released in March 2020. We will then evaluate the successes and the challenges of the Solarium Commission, highlighting potential criticisms and outlining a path forward as the Biden administration takes the reins in national policy.

Developing and implementing a strategy for defending a nation-state in cyberspace is a difficult proposition given all the agencies, interests, and fixed positions of those operating in the defense and cyber policy ecosystem. By valuing originality, empirical research and seeking to achieve a bipartisan goal of developing a comprehensive national strategy, the Solarium Commission Report is an example of a progressive method of generating a national strategy to defend the nation against adversaries. This article will explain the process by which the Solarium Commission strategy was built while also considering the challenge of escalation risk management.

2. THE CHALLENGE OF CREATING A NATIONAL CYBER STRATEGY

A. Building a National Strategy

There are few manuals on how to draft a national strategy. Academics tend to be better at judging other people's strategies than they are at developing organized, deliberative processes to generate policy recommendations and clear tasks for government agencies. Yet policymakers tend to see the domain of crafting strategy as – to paraphrase Hobbes – a nasty, brutish, and short battle of ideas rooted as much in gaining positional or transactional bureaucratic leverage as it is in analytical clarity and logical consistency (Jensen 2018).

2 The Solarium Commission did not develop methods to impose costs on the adversary; instead, the task was to enable the U.S. government to able to impose costs by setting it up for action. This came in the form of enabling workforce development and strategic assessments within the DoD to providing recommendations for the evolution of the State Department.

Absent a guiding process to evaluate ideas and test assumptions, strategy formation devolves into a competition between competing bureaucratic interests. Policy entrepreneurs compromise in pursuit of an agenda (Kingdon and Stano 1984; Durant and Diehl 1989; Mintrom 1997). The result is a "garbage can" full of ideas – some good, others bad, many irrelevant to the problem at hand (Cohen, March et al. 1972). The process by which one develops a strategy is as important, if not more important, than the resulting blueprint for aligning limited resources in pursuit of national objectives, given fixed preferences and risk considerations (Klimburg 2012). A clear, deliberative process can guard against some of the agenda-setting dynamics as well as check other common sources of bias. The goal is to make the process transparent and open to periodic checks with a larger set of stakeholders. Careful attention to process and risk mitigation provides decision-makers with a venue for understanding their own preferences and inherent tradeoffs in any policy selected.

Building the Team of Strategists

Concern for creating a marketplace of ideas guided the early stages of building a team and process for the Solarium Commission. Starting in early spring 2019, a small team began to meet with Executive Director Mark Montgomery (retired rear admiral and former policy director for the Senate Armed Services Committee), and his chief of staff, Deborah Gray (retired colonel, U.S. Army), to develop a plan of action.

The NDAA had already specified the research lines of effort, and the Solarium Commission started deliberating, staffing the task force leads, and hiring support staff. Dr. Erica Borghard, an academic, led Task Force One. John Costello, an appointee detailed from the Department of Homeland Security (DHS), led Task Force Two. Val Colfield, a senior official from the FBI, led Task Force Three. Cory Simpson, a lawyer with recent experience at U.S. Cyber Command (USCYBERCOM), organized and led a general support element dubbed the Fourth Directorate. Dr. Benjamin Jensen served as senior research director and lead author, organizing the process to develop the strategy, crafting deliberative mechanisms including the Red Team and Solarium event, and creating the core strategy: layered cyber deterrence.[3]

Next, the Commission built out its staff at the direction of the Task Force leads and Commission members, interviewing and hiring Commission team staffers from Capitol Hill offices, think tanks, and academia. After key hires and detailed personnel were in place, the executive director, task force leads, and senior research director, to use military jargon, "planned the plan," mapping out a timeline, key deliverables, and the overarching process to evaluate each task force effort and to build the final strategy with the commissioners.

3 The full list of staff and contributors is accessible at https://www.solarium.gov/about/staff and in the Solarium Commission Report.

In spring 2019, the appointed members of the Commission began to meet for progress reviews. The executive director used these meetings to update the Commission on progress and timelines and to solicit any additional input. The general format was that the staff products were briefed to Commission members who then would follow up and consult individual teams on their activities, shaping the report and recommendations in collaboration between Commission staff and Commission members.

B. The Process of Building a Strategy

To initiate the strategic formation process, the senior research director built on the original Eisenhower Solarium effort. The purpose was not to carbon-copy the effort but to use it as a lens through which to develop a deliberative strategy formation process. The idea was to progress from task force research to Commission approval and ultimately legislative or executive branch action based on the proposed policies.

This effort started by briefing each task force on the original Solarium effort and illustrating how competitive teams in that process organized their reporting. The senior research director distributed declassified copies of the original Solarium reports and used them to work with task force leads on the structure of their submission. Figure 1 provides a sample product used during this phase, showing the task forces' different report structures and internal logics used in the 1953 effort.

FIGURE 1: TASK FORCE PLAN FOR EISENHOWER SOLARIUM

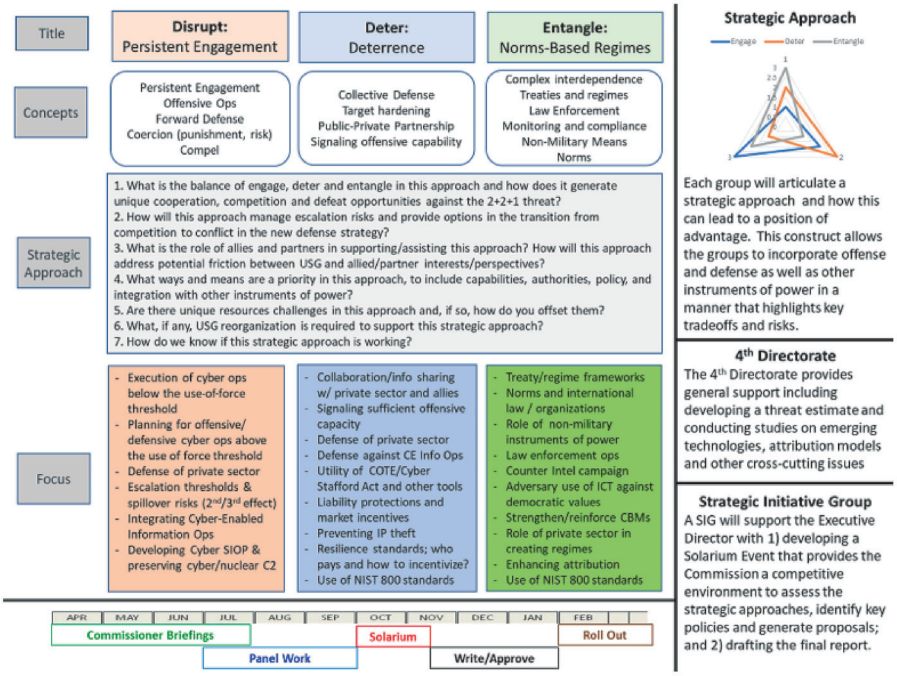
Task Force A July 1953
I. The Task
II. The Situation Before the United States
III. Courses of Action for U.S. Policy A. Maintenance of U.S. Strength B. Maintenance of the Economy C. Maintenance of Free Political Institutions D. Strengthening the Free World (general, Europe, Asia, Middle East, North Africa) E. Prevention of Soviet Expansion F. Reduction of Soviet Power G. Establishment of International Order
IV. Costs
V. Review of Conclusions in Light of Three Alternative Lines of Soviet Action
VI. Comments Regarding Questions in Section III.2 of Project Paper
VII. Summary and Concluding Statements

Task Force B July 1953
I. The Situation which the United States and the Free World Must Meet
II. Recommended National Policy A. Statement of the Policy B. Clarification of Policy C. Rejected Alternative Lines D. Rejection of the "Two Worlds" Concept
III. Summary of Advantages A. Enumeration of Principal Advantages B. Effectiveness of Alternative "B" in Meeting Possible Soviet Lines of Action
IV. Analysis of Implications A. Military Implications of Alternative "B" B. Political and Psychological Implications of Alternative "B" C. Economic Implications D. Probable Soviet Reactions to Alternative "B"
V. Weakness of Alternative "B" A. Introduction B. Soviet Capabilities and Intentions C. Effects of Other Free World Countries D. Support of the Policy by the American People
VI. Implementation A. General Considerations B. Specific Proposals
Enclosures 1. The Role of General War Under Alternative A, B, and C 2. Possible Implications of Measures
Annexes A. Examination of Alternative "B" in the Memorandum on Basic Issues B. U.S. Commitments in Regard to the Defense of Countries Subject to Armed Attack by the Soviet Bloc

Departing from the original Solarium, the Cyberspace Solarium effort opted to have each task force submit not just a strategic approach but a formal workplan organized around key questions. The reason for organizing around questions, as opposed to exclusively around policy approaches, was to ensure a more open research phase. While each task force used a common approach in the form of a workplan, the Fourth Directorate served more as general support. This group developed the threat assessment narrative and explored topics, like artificial intelligence and elections, that emerged during the research phase.

With the workplans in place, the teams initiated a compressed six-month process of conducting research and using the insights to refine their initial strategic approach and policy recommendations. During this time, the Commission held progress review meetings, in which the executive director would have various task force leads and staff brief key findings and initial perspectives based on their workplan. These meetings helped the Commission identify more contentious areas and collect additional concerns that would need to be addressed during the Solarium event. In addition, the executive director, Mark Montgomery, held a series of meetings with different Commission staff weekly to identify additional issues and concerns. It was not uncommon for Commission staff, especially the task force leads and senior research director, to meet privately with elected officials and senior appointees across government. To summarize this approach, the staff used the placemat in Figure 2 to aid in outlining the task force organization, logic, and timeline.

FIGURE 2: THE STRATEGY FORMATION PROCESS PLACEMAT

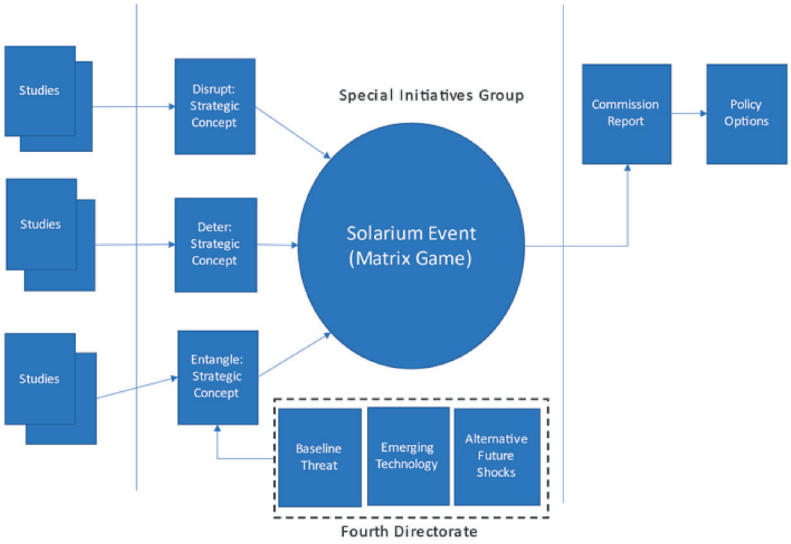


The research phase was extensive, involving over 300 interviews and reviewing over 30 submissions from academics and thought leaders in cyber security. The staff also traveled, attending meetings with officials involved in cyber policy and the private sector at events like the DEF CON hacking conference in Las Vegas and to Europe, with a particular focus on the United Kingdom, Estonia, and Israel. There were targeted trips with multiple events and meetings to San Francisco (Silicon Valley), New York City (financial sector), and Boston to consult with cyber security experts.

Towards the end of summer, the teams began to transition to panel work, essentially triaging the various answers they found through research to the core and derivative questions referenced in the workplan. The result was a task force strategy and linked policy recommendations. Each task force approached this phase slightly differently. Some took a more top-down approach, crafting ideas and then socializing them. Others divided their task force into teams focused on areas or worked each issue collaboratively. The executive director kept an open-door policy to hear any emerging concerns and used a weekly meeting to check progress. During these progress reviews, alongside the larger meetings with the Commission, the senior research

director worked to finalize the deliberative mechanisms the commissioners would use to evaluate each task force: 1) a Red Team and 2) the Solarium event.

FIGURE 3: THE SOLARIUM COMMISSION ROAD MAP



C. The Emerging Strategy and Solarium Event

From October 21 to 23, 2019, the task forces submitted their initial strategic approaches, based on their research and answers to the questions in the workplan, to a Red Team. Red teams are a common military, intelligence, and business community mechanism to identify critical assumptions and evaluate alternative perspectives by acting as the "enemy" (Zenko 2015). Applied to the Solarium Commission, the Red Team engaged predominantly in challenge activities, forcing each team to clarify their logic (e.g., theory of victory, principles) and the way policy recommendations related to core problems the task force identified. Members of the Red Team included retired flag officers, former senior National Security Council officials, and leading cyber experts from industry.[4] After the Red Team review, task forces used October 24 to prepare for the Solarium Event.

The Solarium event combined elements of red teaming, matrix wargames, and stress tests to create a deliberative environment for commissioners to evaluate each task force. The senior research director developed two scenarios linked to the baseline threat and issues previously identified by the commissioners. These scenarios, *Slow Burn* and *Break Glass*, used hypothetical countries and incorporated a wide range of both previously observed cyber incidents and more catastrophic possibilities. These

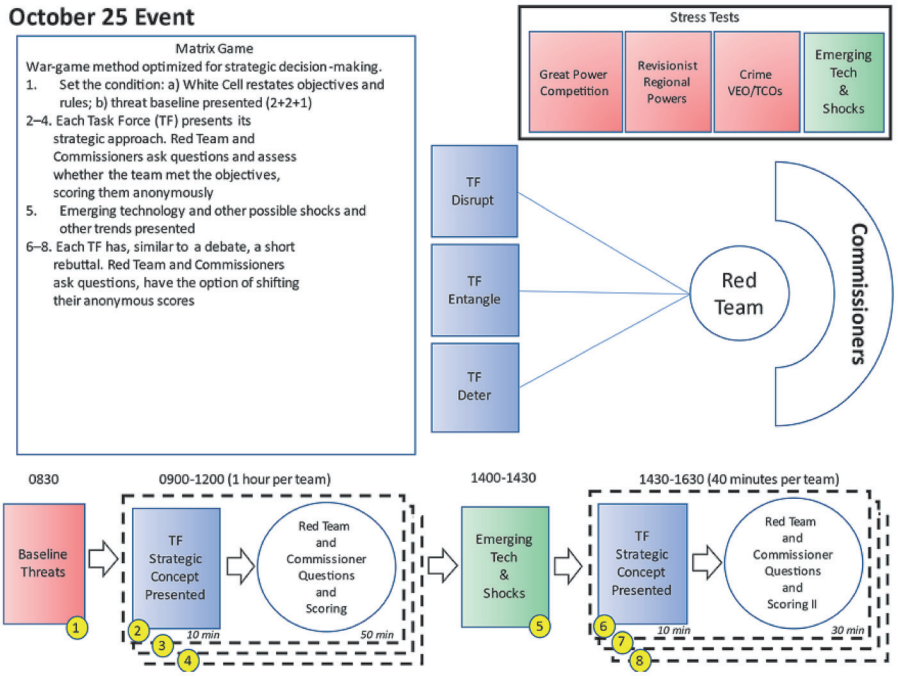
4 The complete Red Team list is available at: https://www.solarium.gov/.

scenarios, as stress tests, allowed the task forces to outline how their approach would do three things: 1) prevent the hypothetical cyber crisis; 2) provide options to respond to the cyber crisis; and 3) support the government and private sector in mitigating the consequences of the cyber crisis. As seen in Figure 4, the day was organized into four sessions. First, the baseline threat estimate was briefed to the commissioners. Second, the task forces responded to the first of two scenarios. The senior research director served as the moderator, ensuring each task force had an opportunity to outline its answers to the three questions. After the initial response, the Red Team asked questions and opened the floor to the commissioners for any follow-up questions.

The scenarios functioned as both stress tests and a modified matrix game. While there was no opponent per se, the task force leads had to account for how well their underlying strategy and linked recommendations would address the cyber crisis. While commissioners listened to the responses, they filled out their evaluation of the underlying policy recommendations using a rank-ordered system. Each commissioner privately rated each recommendation from 1 to 5, with 5 being the highest rating. They were also allowed to assign a relative weight, indicating how important the recommendation was to them. This system allowed the staff to identify areas of convergence and divergence between the commissioners. This approach proved critical in that it allowed the staff to quantitatively show the commissioners what they agreed on, thus maximizing time for debate in future meetings.

After the Solarium Event, the Commission deliberated from November to January. These sessions benefited from the ranked weighting system and the wide range of perspectives offered by the Red Team. Concurrently, the staff worked to narrow the range of recommendations (initially there were over 100 recommendations), while the senior research director, in consultation with the task force leads, developed a larger strategic logic based on the commissioner feedback: layered cyber deterrence.

FIGURE 4: THE SOLARIUM EVENT



D. Layered Cyber Deterrence

The strategy of layered cyber deterrence emerged after months of work on an accelerated timeline. The Commission staff engaged hundreds of thought leaders, government officials, and stakeholders in the cyber security field. The outcome was a strategy encompassing three layers. Recognizing that we are in a period of neither war nor peace, layered cyber deterrence seeks to apply all levers of national power to the challenge of cyber conflict. The concept is consistent with the emergence of literature on competition in national security circles over the last 10 years, captured in the 2018 *Joint Concept for Integrated Campaigning* and the 2019 *Competition Continuum* (JD-19). The goal or victory condition of the strategy is to ensure that the connectivity required by modern society remains stable despite the cyber operations that target U.S. networks. Another goal is to reduce the severity of attacks below the threshold of armed conflict. Enabling this process depends on a new version of deterrence that moves us past the nuclear deterrence developed during the Cold War. Applying multiple instruments of power to ensure both survival and stability requires new ways to apply coercion in cyberspace.

Layered cyber deterrence relies on strong public-private collaboration to ensure that U.S. national cyber strategy does not remain siloed in the Department of Defense (DoD). The goal is to change the cost-benefit calculus of the adversary. The three layers provide overlapping visions of networked cyber strategy to protect the nation as it confronts new methods of digital warfare. The end state is to reduce the overall severity and frequency of cyber operations of significant consequence (Jensen 2020). The structure of the system and views of a persistent enemy do not dominate planning; rather, the strategy focuses on the interconnections built out through society that can enable security (Maoz 2010; Cleveland, Jensen et al. 2018).

The first layer is an outgrowth of entanglement strategies, meant to consider the global conditions critical for the development of cyber stability (Hurwitz 2012; Grigsby 2017; Nye 2017). The Solarium Commission seeks to create a plausible scenario that would enable allies to work together to create norms, institutions, and regulations that encourage responsible action in cyberspace. Excluding adversaries from this process creates bifurcated institutional systems that will hamper the development of cyber norms. Institutions can serve to facilitate agreements with allies and antagonists alike.

The development of norms is an often-theorized aspect of international relations, yet few have sought to understand what conditions create norms in the system (Finnemore and Hollis 2016). There has been a fruitful discussion of how to create legal norms (Schmitt and Vihul 2014), but engagement on the global institutional front is often stymied by geopolitical posturing (Grigsby 2017). Shaping the environment for action is critical, as digital connectivity depends on global networks and international collaboration to create a rules-based social order (Raymond 2021). In addition to negative aspects of coercion, the international environment can also enable positive methods of coercion that seek to change behavior through inducement rather than negative externalities (Baldwin 2020).

Recognizing that the United States cannot go on the offense until the home front is secure, the second layer advocates for denial strategies that ensure that the United States will be resilient in the face of inevitable cyber actions directed against the state (Gisladottir, Ganin et al. 2017; Valeriano and Jensen 2019). Deterrence by denial and target hardening will protect the networks from the most severe consequences of cyber actions (Denning 2014). Defense in being (mimicking the idea of a fleet in being) and defense in depth are both concepts that can be applied to cyber security (Hattendorf 2014). Only by enabling the defense can forward action take place, because then the homefront is not held at risk.

Finally, the third layer develops cost imposition as a strategy for the cyber domain. The imposition of costs is a critical method of applying force to coerce in cyberspace

and needed restoration after it was eliminated in persistent engagement. To prevent violations of critical thresholds and actions that seek to punish the civilian populations (Dev 2015), the United States must signal a strategy that will align consequences with deviant action. Signaling is a critical but often-forgotten aspect of international strategic positioning (Jervis 1970). In the layered cyber deterrence strategy, it became a critical mechanism enabling the means to achieve ends.

To enable cost imposition, the U.S. government will need to have its capabilities maintained and ready through proper force construction. The resource allocation dimensions of cyber security are often ignored, yet justifying how forces are arranged is critical in balancing the offense with the defense. There is also the possibility and potential for application of reserve forces in cyberspace to get beyond resource constraints (Hannan 2015). This became Recommendation 6.1.7, housed in the DoD given the current constraints of the Cybersecurity and Infrastructure Security Agency (CISA). The United States must ensure the cyber workforce can handle both the job of defensive and offensive action in and through cyberspace to harden targets and apply costs when needed.

Layered cyber deterrence does not seek to create a new paradigm for cyber security; rather, the strategy itself seeks to correctly apply a connection between the means and the ends to achieve clear victory conditions in cyber security. Rovner (2020) wonders critically just what the Solarium Commission rejects. The answer is limited strategies that seek to engage singular departments (USCYBERCOM and the DoD) that fail to conceive of a means to an end in strategy. These are explicitly rejected in favor of an end state that seeks overall U.S. stability and the reduction of attacks of consequence that hold the U.S. population at risk. We now move to evaluating the implementation of strategy, which is just as critical as the logical underpinnings of a strategy.

3. LEGISLATIVE SUCCESSES AND NATIONAL CYBER STRATEGY

A. The Legislative Strategy

The key task of the Solarium Commission was to enable reform. Commissions can be powerful venues for national security change (Tama 2011). As the Solarium Commission Report notes, "While cyberspace has transformed the American economy and society, the government has not kept up, and existing government structures limit cyber policymaking processes, dampen government action, and impede cyber operations" (Montgomery, Jensen et al. 2020, 2). Enabling success is critical, and it must come through action, not reports that tend to cycle throughout the U.S. government system. Almost every decade included a comprehensive evaluation of

cyber strategy with a series of recommendations for action, including the Ware Report (1970), the Cyberspace Policy Review (2009), and the Cyber Moonshot initiative (2018).

Overall, the Solarium Commission prioritized two tracks of effort to move past the failures of past efforts. One task was to build out and support the national cyber strategy of layered cyber deterrence. The second, and perhaps more important, task was to translate the specific legislative recommendations in the Solarium Report into law. In all, 52 legislative proposals made it into the report in Appendix B.[5] These proposals were extensively researched, supported by legislative analysis, and then distributed to the various committees and subcommittees in Congress. The goal was to find natural bipartisan support for each proposal as they became fully fleshed out and implementable law or directives to be included in legislation.

The Solarium Commission was able to get 25 of the 52 legislative recommendations written into the Fiscal Year 2021 National Defense Authorization Act (FY21 NDAA). In the end, 27 recommendations (two proposals were split) became law on January 1, 2021, after a veto override. Once the FY21 NDAA was signed into federal law, it became evident that the cyber security provisions included in the overall NDAA represent "the most comprehensive and forward-looking pieces of national cybersecurity in the nation's history."[6]

Some legislative recommendations failed to become law because either there was not enough time to develop the recommendations into full legislative proposals or there was no natural sponsor of legislation. The FY21 NDAA (Section 1714) authorized the Solarium Commission to continue its work for one more year to push through some recommendations that seek to improve cyber expertise in government (workforce), increase institutional cyber engagement (support the State Department), and enhance cyber reliance (in particular, to create a cyber recovery fund and develop breach notification law).

B. Evaluating the Legislative Successes

The two main successful legislative efforts sought either to enhance the power of existing cyber entities in the U.S. government or to create new structures to support the generation of a strategy to maintain security in cyberspace. While there is a need for a new cabinet-level organization to manage cyber security and information/data across the U.S. government, there is not much initiative to create such an organization due to the problems that developed after the creation of the DHS including complications at the border (Birkland 2009).

5 More than 150 proposals were considered for the report; many of these were eliminated after the wargame.

6 Statement by Solarium co-chairs Senator Angus King (I-Maine) and Representative Mike Gallagher (R-Wisconsin). https://www.king.senate.gov/newsroom/press-releases/solarium-co-chairs-welcome-26-recommendations-in-2021-national-defense-authorization-act.

The Commission therefore focused on enabling the functions of the U.S. government that could support cyber security efforts, with a focus on CISA, DoD, and USCYBERCOM. For example, Solarium Commission Recommendations 6.1 and 6.1.3 direct the DoD to conduct a force structure assessment of the Cyber Mission Force to ensure that USCYBERCOM has the resources needed to conduct operations that seek to impose costs (Section 1706 in the FY21 NDAA). The Solarium Commission also proposed that the DoD conduct an evaluation for the requirements needed to establish a cyber reserve force (Section 1730 and Recommendation 6.1.7) to support cyber mission forces.

To enable defensive operations, the Solarium Commission recommended vulnerability assessments to command-and-control functions of the DoD, including nuclear and conventional weapons systems (CSC Recommendation 6.2b and FY21 NDAA Section 1712). Another recommendation (CSC Recommendation 6.2.1 and 6.2.2) supported the need for the Defense Industrial Base (DIB) to participate in threat-intelligence-sharing programs (Section 1737) and threat-hunting on US networks (Section 1739). The Commission also enabled CISA to conduct threat-hunting investigations on US networks (Section 1705 of the FY21 NDAA and CSC Recommendation 1.4) and granted subpoena power to the organization (Section 1716 of the FY21 NDAA and CSC Recommendation 5.1.3).

C. National Cyber Director

Perhaps most importantly, the Commission recommended the creation of the position of a National Cyber Director (NCD) (hereafter, Recommendation 1.3), which became Section 1752 in the FY21 NDAA. The NCD position is meant to restore and to elevate a coordinator for all U.S. government efforts to establish a coherent whole-of-nation strategy for cyber security and to marshal incident response for major cyber breaches. Vesting such a position outside of the DoD and National Security Council, the NCD allows for the freedom of action to coordinate all sources of U.S. power towards the cyber domain, including the Department of Justice (indictments), the State Department (cyber diplomacy), and DHS (internal resilience).[7]

The Senate-confirmed position reporting directly to the president demonstrates the importance of the NCD coordinator position. Without such an office, the organizational seams (Chaudhary, Jordan et al. 2018) evident in the U.S. government will only continue to proliferate, endowing a disparate and uncoordinated cyber capability. Tasked with developing the overall U.S. cyber strategy, the NCD can help broaden how the U.S. considers cyber security as more than the domain of the U.S. military. Coordinating defensive efforts to respond to and survive a major cyber action highlights the importance of the position. The strategy of layered cyber deterrence

7 An National Security Council-housed cyber coordinator has limited ability to organize government responses and mainly focuses on ongoing threats, not the development of strategy and defenses to avoid attacks in the first place.

could become problematic if the layers end up working at cross purposes with each other. For example, the State Department's efforts to create viable norms can conflict with DoD offensive cyber impulses. Yet having a powerful NCD who can deconflict these issues and streamline processes is a critical task of this new role.

Even as some reject the need for reorganization of government (Rovner 2020), the Commission sought to focus on this key challenge to reform national strategy and process, preferring to not let bureaucratic divisions impede effective strategy. There was intense pushback on the NCD position from the Trump administration, because the bureaucratic power centers that developed during the administration were vested in those who sought to eliminate the White House cyber coordinator role in the first place. While the Biden administration has its own concerns about the NCD position, the main issue at this point is funding the organization and staff required to maintain a NCD position.

Finally, cyber security is a whole-of-nation challenge, not a whole-of-government problem. Most cyber resources, capabilities, and targets all reside beyond the control of the U.S. government. The NCD would be the point of contact for all private sector cyber stakeholders, ensuring there was an office that would be receptive to the needs of the private sector. In order to implement a national strategy, there needs to be one office that is responsible for coordination and strategic development that thinks beyond the bureaucratic demands of the specific cabinet-level branches.

4. PRESSURE POINTS AND MANAGING RISK

A. Cost Imposition and Enabling Defend Forward

Two early criticisms of the strategy of layered cyber deterrence are that it improperly returns the U.S. back to a deterrence strategy and that it revives the notion of the need to impose costs on the adversary. Persistent engagement is purposely framed as a natural evolution away from deterrence (Fischerkeller and Harknett 2017). Yet it is difficult to discard the concept of deterrence, given the demands of the policy community and a near-reflexive dependence on deterrence. The policy community tethers itself to deterrence as a process it knows and understands; there is a clear belief that nuclear deterrence has maintained stability during and after the Cold War.

The concept of layered deterrence is not about binary outcomes (cyber attack/no cyber attack). Rather, it is the mechanism to alter how states compete in cyberspace and the cascading effects cyber actions can have on global commerce given the dependence on connectivity. Layered cyber deterrence is a framework for competition more than it is a carbon copy of first-wave nuclear deterrence theory (Jervis 1978). Following the

original Solarium Commission model – not discarding it, as Rovner (2020) incorrectly charges – is a highlight of the deliberative process the Solarium Commission built to achieve consensus on cyber strategy.

In the cyber domain, there is a need to move past conventional notions of deterrence and rebuild the concept around the frames that are likely to enable cyber stability. Deterrence as articulated in the nuclear domain is the theory of preventing an action from happening through the threat of retaliation enabled by the ability to survive a first strike (Jervis 1978). Under this concept, cyber deterrence will never work because of the near constant probes and espionage attacks witnessed in cyberspace. Deterring cyber espionage, just like conventional espionage, is nearly impossible and too costly in relation to the benefits.

The goal instead is to reduce the severity and frequency of cyber activities. A state will never stop spying; what the target can do is make it harder for adversaries to spy on them, altering the expected value of the information they steal, and taking actions in the shadows that cause them to reconsider the logic of consequence associated with covert operations. This idea builds on new literature that finds that states use covert action to signal (Yarhi-Milo 2014; Carson and Yarhi-Milo 2017; Yarhi-Milo, Kertzer et al. 2018; Carson 2020). Layered cyber deterrence should therefore alter how states compete and deter attacks in the cyber domain above and below the threshold of armed conflict, including any provocative or disruptive actions that will inhibit the maintenance of information and command coordination capabilities. This can be done by creating the conditions in the system for the stable expectation of norms (shaping entanglement), denying attack surfaces to the opposition and enabling resilience in defense (denial), and by making clear, credible commitments to leverage consequences for deviant action (imposing costs).

As Fischerkeller and Harknett (2020) have noted in the past, "cost imposition is best understood as an effect resulting from the casual mechanism associated directly with a strategy of persistent engagement." In the hope of moving beyond coercion, persistent engagement discards cost imposition as a casual mechanism. A previous work of ours (Valeriano, Jensen et al. 2018) has suggested that coercion does not work in cyber competition; this finding has often been cited as evidence for the inability of coercion to achieve effects in cyberspace. That interpretation misunderstands the point of our work; it is not that coercion is impossible in cyberspace, but it is unlikely (Borghard and Lonergan 2017). This is often because the side that imposes costs does not clearly signal costs and has no credible commitment to follow through. Cyber operations are also better thought of as having a complementary and additive effect (Valeriano and Jensen 2021). Prior work demonstrates, when combining cyber operations data with event data on instruments of power, that all successful episodes of cyber coercion

occurred alongside a broader range of diplomatic, military, and economic inducements and threats (Valeriano, Jensen et al. 2018). Cyber operations are the icing, not the cake.

Persistent engagement had no clear identified causal mechanism connecting the ends and means because there is no clear end state. In failing to understand that the imposition of costs was not an outcome, but a feature of deterrence, persistent engagement has significant limits as a theory because it does not have a method of applying force against the adversary beyond friction (Fischerkeller and Harknett 2020). Without the imposition of costs, there is no conception of how to achieve an end (strategic stability through counter cyber operations) through a means (hunting forward). Friction is a useful method to confuse the adversary and distract their operations, but it is not a clear means to achieve an end because it depends on second- and third-order effects. The imposition of costs (along with resilience and entanglement) is the key element that makes the strategy of layered cyber deterrence effective. The remaining challenge is how to measure effectiveness and avoid escalation.

B. The Danger of Cyber Escalation

The prime risk associated with cyber security is the danger of a major cyber war that might destroy the economy, harm civilians, and disrupt critical infrastructure (all exaggerated fears but fears nonetheless) (Clarke and Knake 2014). This is a classic example of a low-probability, high-consequence risk, which, consistent with work on complex systems, could quickly evolve from a limited event to a systemic crisis. These dramatic actions would occur only after the confrontation between the entities engaged in serial competition escalates into violence. Understanding what escalation is and minimizing the risk of increasing intensity in cyber conflict was a task the Solarium Commission was not able to address through legislative recommendations, although it did study ways to minimize the risk. While layered cyber deterrence, if implemented, should stabilize cyber competition, there is still a systemic risk left to be addressed by future cohorts of academics, policy-makers, and activists.

The modern study of crisis escalation emerges during the Cold War through studies examining the process of bargaining during a foreign policy crisis (Schelling 1960; Schelling 1966). Kahn (1968) is the exemplar in the study of escalation, with his view that escalation results when one side tries to demonstrate resolve by increasing directed efforts in the diplomatic, military, information, or economic domains.

Escalation is defined as an increase in the intensity of conflict (vertical escalation) or to spread of the conflict to new venues (horizontal escalation). To escalate, Actor B (the target) must react with increased intensity after Actor A makes the first move. In cyberspace, this entails either reacting with more costly means of response using cyber options or by leveraging conventional operations to punish the initial

violation (Borghard and Lonergan 2019). Cyber escalation is an interactive process of increasing hostility and intensity over a series of interactions that occur in cyberspace. Libicki focuses on two factors: increasing the intensity of cyber operations (deeper, longer lasting effects) or finding more extensive cyber response options (striking new targets) (Libicki 2016).

Borghard and Lonergan (2019) argue that there is little logic behind the idea that cyber operations will provoke escalatory reactions, primarily because of the limited nature of the weapons, the uncertain effects, and the lack of costs imposed by cyber operations, meaning that the target often does not have to respond. Valeriano et al. (Valeriano, Jensen et al. 2018; Valeriano and Jensen 2021) go further by pointing out that cyber operations are ambiguous signals, used mostly as tools of espionage, that offer limited methods of coercion. Cyber operations can actually provide de-escalation pathways if utilized during a crisis to substitute for conventional operations (Valeriano and Jensen 2021).

Overall, the community has no clear idea about escalation patterns in cyberspace at this point because there is a limited availability of interactive data between adversaries. There is no data, as of yet, to establish a baseline of operations to understand how often operations fall above normal levels and demonstrate an increase in intensity. Empirically, there is evidence that escalation is rare in cyberspace, but these findings are based on data between rival actors (Valeriano, Jensen et al. 2018; Valeriano and Jensen 2019), wargames (Jensen and Banks 2018; Jensen and Valeriano 2019; Kreps and Schneider 2019), and surveys (Jensen and Valeriano 2019).

C. Managing the Risk of Cyber Escalation

Given the uncertainty we have on the probability of cyber escalation and what conditions provoke cyber dilemmas, it would be unwarranted to dismiss the possibility of escalation in the cyber domain. Thinking that offensive operations will not provoke retaliation seems to be prudent based on the evidence, but this evidence is limited.

The Obama administration era view of cyber strategy was focused on restraint to avoid "unintended damage and uncontrollable escalation" (Fischerkeller and Harknett 2017, 389). Observing that escalation is rare in the cyber domain – counting only two such incidents but without identifying the corpus of data – Fischerkeller and Harknett (2019) argue that states will establish a method of interaction based on agreed competition and avoid escalation.

Following this logic, some current U.S. cyber strategists seem to dismiss escalation concerns. Representatives of USCYBERCOM recently wrote: "Cyber Command takes these concerns seriously, and reducing the risk is a critical part of the planning

process. We are confident that this more proactive approach (persistent engagement) enables Cyber Command to conduct operations that impose costs while responsibly managing escalation" (Nakasone and Sulmeyer 2020). Confidence in managing the possibility of escalation does little to allay concerns that there will be escalation in the cyber domain due to provocative actions leveraged against an adversary.

The challenge is that managing escalation requires awareness of the dangers of escalation, clarity of national strategy, ability to signal intent to the opposition, data to observe risks, and institutions built to create a collaborative environment for problem solving. Therefore, the Solarium Commission submitted Recommendation 1.1.1, "Develop a Multitiered Signaling Strategy." The Commission Report notes, "Rather, the United States must signal capability and resolve, as well as communicate how it seeks to change adversary behavior and shape the strategic environment. Signaling is essential for escalation management so that actions taken in support of defend forward are not unintentionally perceived as escalatory" (Montgomery, Jensen et al. 2020, 33).

The signaling strategy should contain not only overt means of communication, including leveraging public diplomacy efforts and establishing clarity in national strategy, but also covert communications that seek to make clear the costs of deviant action in cyberspace. Proper communication is key to avoiding cyber disasters. No policy on signaling U.S. strategy was adopted by legislative recommendation, but a key task of the NCD (Section 1752) is to provide strategic leadership in cyber security, including coherently signaling cyber policy.

There is also a need to gather information and data on offensive cyber interactions to understand how these operations are received by the opposition. We know little about perceptions of U.S. action by adversaries. Do they understand U.S. strategy? Are there clear red lines in their estimation that forestall escalation? More intelligence would support better estimates of adversary perceptions. A breach notification law (Recommendation 4.7.1) would enable the collection of data on attacks on U.S. targets, helping strategies determine the impact of our operations on changing the behavior of the adversary.

Fostering more wargames in the cyber security community might help us understand the process of escalation better. This leads to Solarium Recommendation 3.3.4, which was the expansion of coordinated cyber exercises, gaming, and simulations. The FY2021 NDAA contains Section 1744, which establishes a biennial National Cyber Exercise. The goal of exercises is not to understand adversary reactions to U.S. strategy but to develop U.S. government agencies, private stakeholders, and international partners' experiences and processes when dealing with cyber threats. There needs to be a better concept of what metrics would be useful in establishing

the effectiveness strategy as it is implemented. Right now, we are flying blind and moving guideposts at will with no conception of benchmarks or methods to establish baselines.

5. THE CHALLENGE OF SOLARWINDS

A. What Was SolarWinds?

When the Solarium Commission tested its cyber strategies with a wargame, it developed two scenarios. Scenario 1 was *Slow Burn*, where a series of minor actions built up to create a crisis that demanded action from all U.S. government operations. The SolarWinds hack (Sanger, Perlroth et al. 2020) is exactly the sort of massive cyber operation that the Commission envisioned.

The SolarWinds operation targeted IT management software called Orion operated by the company SolarWinds. A supply-side vulnerability was exploited to insert malicious code that enabled hacker groups the Russian SVR or APT29 Cozy Bear (Sanger, Perlroth et al. 2020) to maintain a presence on U.S. networks and extract information at will. The complete fallout of the operation is still unknown.

The SolarWinds operation represents the future of digital political warfare, where rival states employ cyber operations to conduct limited operations meant to degrade or disrupt the capabilities of the opposition (Valeriano, Jensen et al. 2018). As a weak form of coercion, the espionage operation highlights the weaknesses in both the defenses and offensive capabilities of the United States as it operates in cyberspace.

B. The Failure of Persistent Engagement?

Some suggest the response to SolarWinds should include more persistent engagement operations. Harknett (2020), one of the original authors of the persistent engagement strategy (Fischerkeller and Harknett 2017), notes that "the United States must accelerate its adoption of the doctrine of persistent engagement across the entirety of its intergovernmental space…. Had the doctrine been in place fully and comprehensively, the form of this attack and its consequences may have been different."

Harknett (2020) notes that the USCYBERCOM mission set is limited to protecting the Defense Information Network. As Corn (2021) notes, "as for allegations that Cyber Command failed to defend forward in this instance, the charge presumes without public evidence that, among other things, the Defense Department and Cyber Command were provisioned with the authority to disrupt SolarWinds." By implication, the suggestion is that USCYBERCOM needs to implement more defend-forward operations and needs more legal authorities to do so to fulfill its mission.

If the U.S. loses the initiative, Russia might dictate the pace of cyber operations and place a constant stress on U.S. defense, which would lead to U.S. failure, according to Harknett (2020). Instead, the SolarWinds operation highlights the limitations of persistent engagement as the operationalization of defend forward (Nakasone 2019). There is a clear role for defend forward operations in cyberspace, but as the sole form of forward operations, said strategies can be self-defeating, because we lack a conception of how the opposition will receive such operations. In fact, they will likely provoke counter and proportional operations that use the same strategy against the defender, which might be exactly how the Russians conceive of the SolarWinds operation. A poorly signaled strategy may well encourage them precisely to counter defend forward operations with their own forward operations.

Persistent engagement lacks a strategy of imposing clearly signaled costs on the opposition, so the opposition has freedom of movement. National strategy needs to be clarified to impose costs and create normative/legal restraints for violations like SolarWinds. Forward maneuver doctrines can only be sustained with strong defenses and a clear strategy of imposing costs on the adversary for deviant actions.

C. The Failure of the Defense?

There is also the need to truly conceptualize what defend forward means in operation. As Borghard and Schneider (2020) note, "we see [defend forward] as two types of activities: The first is information gathering and sharing with allies, partner agencies, and critical infrastructure by maneuvering in networks where they operate." By establishing more entangling partnerships in the international system and facilitating more cooperation with the private sector (Raymond and DeNardis 2015), the U.S. government should be better able to enable the protection of its networks through information-sharing. Forward operations require not only threat-hunting but also creating the overall conditions conducive to denial operations.

In the future, a deeper focus on denial-based strategies outlined in Layer 2, "deny benefits," is critical. Enabling CISA to launch internal threat-hunting would foster an environment for innovation where the continuous monitoring systems could be updated to be more proactive against unknown threats. Utilizing subpoena authority now granted to CISA, the U.S. government can more effectively implement defensive operations.

Making espionage activities more costly and difficult is the goal. The attacker is then limited in their options and must expend added effort to succeed, which thereby decreases the severity and frequency of attacks. By focusing on more than the offense, under the coordination of the NCD, the U.S. can seek to implement a cyber strategy that carefully considers the utility of defensive operations alongside hunting forward.

6. PATH FORWARD

The Solarium Commission will likely endure as a singularly effective effort to construct a roadmap for national cyber strategy. By basing the Solarium Commission Report on research, evidence, and data, the Solarium Commission sought to develop a unique strategy that considers the offense, defense, and systemic constraints at the same time, moving beyond the monocausal strategies developed in the past.

The other key innovation was thinking of cyber strategy in an integrated-network sense. The Solarium Commission began by developing a whole-of-nation strategy that sought to include both public and private stakeholders in seeking to defend the nation. This pushes the cyber security community to think more about how network connectivity is both a strength and a weakness for society. In short, the entire nation needs to be involved in the effort of cyber security, because attack surfaces in the United States are so vast.

The Solarium Commission was successful in getting a majority of its recommendations enacted into law, putting a force behind the ideas it developed that seek to ensure that cyber strategy becomes a continual and evolving process. The U.S. needs to build on its successes and avoid developing a new strategy for every new administration. The Solarium Commission will continue its work for the rest of 2021 to support the Biden administration in implementing its recommendations. Hopefully, the next Commission or strategy review does not have to repeat the effort again in five years.

The development of strategy needs to move beyond the impulses of particular departments (like the DoD) or administrations, because bureaucratic political considerations can become the enemy of progress and fail to engage the marketplace of ideas. People and organizations fall in love with their ideas over time and fail to think about the evaluation of strategies, because they become doctrinal. Policy is often the art of compromise; the Solarium Commission process was as different as it was similar to the original Eisenhower Solarium effort, because it valued bipartisan compromise, academic research, community advice, and empirical verification. If anything, the process was more inclusive and academically rigorous, providing hope that the community can avoid repeating past arguments and debates.

What remains is how the achievements of the Solarium Commission, including the NCD position, will evolve over time. Other countries can take this process as a model for their own strategic reform or, possibly, a model to avoid if the U.S. continues to fall into the trap of the pathologies of the past (not enabling cost imposition, weak defenses, or not shaping the norms and regulations that guide the system). Only time will be the judge.

REFERENCES

Baldwin, D. A. 2020. *Economic Statecraft*. New edition. Princeton University Press.

Birkland, T. A. 2009. "Disasters, Catastrophes, and Policy Failure in the Homeland Security Era." *Review of Policy Research* 26, no. 4: 423–438. https://doi.org/10.1111/j.1541-1338.2009.00393.x.

Borghard, E. D., and S. W. Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26, no. 3: 452–481. https://doi.org/10.1080/09636412.2017.1306396.

Borghard, E. D., and S. W. Lonergan. 2019. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* 13, no. 3: 122–145. https://www.jstor.org/stable/26760131.

Borghard, E. D., and J. Schneider. 2020. "Russia's Hack Wasn't Cyberwar. That Complicates US Strategy." *Wired*, December 17. Accessed April 24, 2021. https://www.wired.com/story/russia-solarwinds-hack-wasnt-cyberwar-us-strategy/.

Carson, A. (2020). *Secret Wars: Covert Conflict in International Politics*. Princeton University Press.

Carson, A., and K. Yarhi-Milo. 2017. "Covert Communication: The Intelligibility and Credibility of Signaling in Secret." *Security Studies* 26, no. 1: 124–156. https://doi.org/10.1080/09636412.2017.1243921.

Chaudhary, T., J. Jordan, M. Salomone, and P. Baxter. 2018. "Patchwork of Confusion: The Cybersecurity Coordination Problem." *Journal of Cybersecurity* 4, no. 1: 1-13. https://doi.org/10.1093/cybsec/tyy005.

Clarke, R. A., and R. K. Knake. 2014. *Cyber War*. Old Saybrook, CT: Tantor Media.

Cleveland, C., B. M. Jensen, A. David, and S. F. Bryant. 2018. *Military Strategy for the 21st Century: People, Connectivity, and Competition*. Cambria Press.

Cohen, M. D., J. G. March, and J. P. Olsen. 1972. "A Garbage Can Model of Organizational Choice." *Administrative Science Quarterly* 17, no. 1 (March): 1–25. https://doi.org/10.2307/2392088.

Congress. 2017–2018. H.R. 5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019. U. S. Congress. Washington, DC: U.S. Government Printing Office. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

Corn, G. 2021. "SolarWinds is Bad, but Retreat From Defend Forward Would Be Worse." *Lawfare*, January 14. Accessed April 24, 2021. https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.

Denning, D. E. 2014. "Framework and Principles for Active Cyber Defense." *Computers and Security* 40: 108–113. https://doi.org/10.1016/j.cose.2013.11.004.

Dev, P. R. 2015. "Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response." *Texas International Law Journal* 50: 381.

Durant, R. F., and P. F. Diehl. 1989. "Agendas, Alternatives, and Public Policy: Lessons from the US Foreign Policy Arena." *Journal of Public Policy* 9, no. 2: 179–205.

Finnemore, M., and D. B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110, no. 3: 425–479.

Fischerkeller, M. P., and R. J. Harknett. 2017. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3: 381–393. https://doi.org/10.1016/j.orbis.2017.05.003.

Fischerkeller, M. P., and R. J. Harknett. 2019. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." *Cyber Defense Review* (special issue): 267–287. https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.

Fischerkeller, M. P., and R. J. Harknett. 2020. “Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect.” *Lawfare*, February 6. Accessed April 24, 2021. https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

Gallagher, M. J. 2015. “Intelligence and National Security Strategy: Reexamining Project Solarium.” *Intelligence and National Security* 30, no. 4: 461–485. https://doi.org/10.1080/02684527.2014.885203.

Gisladottir, V., A. A. Ganin, J. M. Keisler, J. Kepner, and I. Linkov. 2017. “Resilience of Cyber Systems with Over and Underregulation.” *Risk Analysis* 37, no. 9: 1644–1651. https://doi.org/10.1111/risa.12729.

Grigsby, A. 2017. “The End of Cyber Norms.” *Survival* 59, no. 6: 109–122. https://doi.org/10.1080/00396338.2017.1399730.

Hannan, N. K. 2015. “Use of Reserve Forces in Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches.” *RUSI Journal* 160, no. 5: 46–51. https://doi.org/10.1080/03071847.2015.1102543.

Harknett, R. J. 2020. “SolarWinds: The Need for Persistent Engagement.” *Lawfare*, December 23. Accessed April 24, 2021. https://www.lawfareblog.com/solarwinds-need-persistent-engagement.

Hattendorf, J. B. 2014. “The Idea of a ‘Fleet in Being’ in Historical Perspective.” *Naval War College Review* 67, no. 1: 42–60. https://digital-commons.usnwc.edu/nwc-review/vol67/iss1/6/.

Healey, J. 2019. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” *Journal of Cybersecurity* 5, no. 1: https://doi.org/10.1093/cybsec/tyz008.

Hurwitz, R. 2012. “Depleted Trust in the Cyber Commons.” *Strategic Studies Quarterly* 6, no. 3: 20–45. https://www.jstor.org/stable/26267260.

Jensen, B. M. 2018. “The Role of Ideas in Defense Planning: Revisiting the Revolution in Military Affairs.” *Defence Studies* 18, no. 3: 302–317. https://doi.org/10.1080/14702436.2018.1497928.

Jensen, B., and D. Banks. 2018. *Cyber Operations in Conflict: Lessons from Analytic Wargames*. Center for Long-Term Cybersecurity, UC Berkeley. https://cltc.berkeley.edu/2018/04/16/cyber-operations-conflict-lessons-analytic-wargames/.

Jensen, B., and B. Valeriano. 2019. *Cyber Escalation Dynamics: Results from War Game Experiments*. International Studies Association, Annual Meeting, Toronto, Ontario, Canada. http://web.isanet.org/Web/Conferences/Toronto%202019-s/Archive/71e7820c-e61c-4187-ab8c-28de83dfd660.pdf.

Jensen, B., and B. Valeriano. 2019. *What Do We Know about Cyber Escalation? Observations from Simulations and Surveys*. Atlantic Council. Accessed April 24, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyber-escalation-observations-from-simulations-and-surveys/.

Jensen, B. 2020. “Layered Cyber Deterrence: A Strategy for Security Connectivity in the 21st Century.” *Lawfare*, March 11. https://www.lawfareblog.com/layered-cyber-deterrence-strategy-securing-connectivity-21st-century.

Jervis, R. 1970. *The Logic of Images in International Relations*. Princeton, NJ: Princeton University Press.

Jervis, R. 1978. “Deterrence Theory Revisited.” *World Politics* 31, no. 2: 289–324.

Kahn, H. 1968. *On Escalation: Metaphors and Scenarios*. Transaction Publishers.

Kingdon, J. W., and E. Stano. 1984. *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown.

Klimburg, A. 2012. *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defense Center of Excellence. https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

Kreps, S., and J. Schneider. 2019. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics.” *Journal of Cybersecurity* 5, no. 1: https://doi.org/10.1093/cybsec/tyz007.

Libicki, M. 2016. *Cyberspace in Peace and War*. Naval Institute Press.

Maoz, Z. 2010. *Networks of Nations: The Evolution, Structure, and Impact of International Networks, 1816–2001*. Cambridge University Press.

Mintrom, M. 1997. “Policy Entrepreneurs and the Diffusion of Innovation.” *American Journal of Political Science* 41, no. 3 (July): 738–770. https://doi.org/10.2307/2111674.

Montgomery, M., B. Jensen, E. D. Borghard, J. Costello, V. Cornfeld, C. Simpson, and B. Valeriano. 2020. *Cyberspace Solarium Commission Report*. Washington, DC. https://www.solarium.gov/report.

Nakasone, P. M. 2019. “A Cyber Force for Persistent Operations.” *Joint Force Quarterly* 92: 10–14. http://cs.brown.edu/courses/csci1950-p/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf.

Nakasone, P. M., and M. Sulmeyer. 2020. “How to Compete in Cyberspace.” *Foreign Affairs*, August 25. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

Nye, J. S., Jr. 2017. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3: 44–71. https://doi.org/10.1162/ISEC_a_00266.

Raymond, M. 2021. “Social Practices of Rule-Making for International Law in the Cyber Domain.” *Journal of Global Security Studies* 6, no. 2: https://doi.org/10.1093/jogss/ogz065.

Raymond, M., and L. DeNardis. 2015. “Multistakeholderism: Anatomy of an Inchoate Global Institution.” *International Theory* 7, no. 3: 572–616. https://doi.org/10.1017/S1752971915000081.

Rovner, J. 2020. “Did the Cyberspace Solarium Commission Live Up to Its Name?” *War on the Rocks*, March 19. Accessed April 24, 2021. https://warontherocks.com/2020/03/did-the-cyberspace-solarium-commission-live-up-to-its-name/.

Sanger, D. E., N. Perlroth, and E. Schmitt. 2020. “Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit.” *New York Times*, December 14. Accessed April 24, 2021. https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

Schelling, T. 1960. *The Strategy of Conflict*. Harvard University Press.

Schelling, T. C. 1966. *Arms and Influence*. New Haven: Yale University Press.

Schmitt, M. N., and L. Vihul. 2014. “The Nature of International Law Cyber Norms.” *Tallinn Papers* (no. 5). https://ssrn.com/abstract=2543520.

Tama, J. 2011. *Terrorism and National Security Reform: How Commissions Can Drive Change During Crises*. Cambridge University Press.

Valeriano, B., B. M. Jensen, and R. C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.

Valeriano, B. G., and B. Jensen. 2019. “The Myth of the Cyber Offense: The Case for Cyber Restraint.” *Cato Institute Policy Analysis* (no. 862). https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint.

Valeriano, B., and B. Jensen. 2021. “De-Escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War.” In *Cyber Peace*, edited by S. Shackelford. Cambridge University Press.

Yarhi-Milo, K. 2014. *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations*. Princeton University Press.

Yarhi-Milo, K., J. D. Kertzer, and J. Renshon. 2018. "Tying Hands, Sinking Costs, and Leader Attributes." *Journal of Conflict Resolution* 62, no. 10: 2150–2179. https://doi.org/10.1177%2F0022002718785693.

Zenko, M. 2015. *Red Team: How to Succeed by Thinking Like the Enemy*. Basic Books.