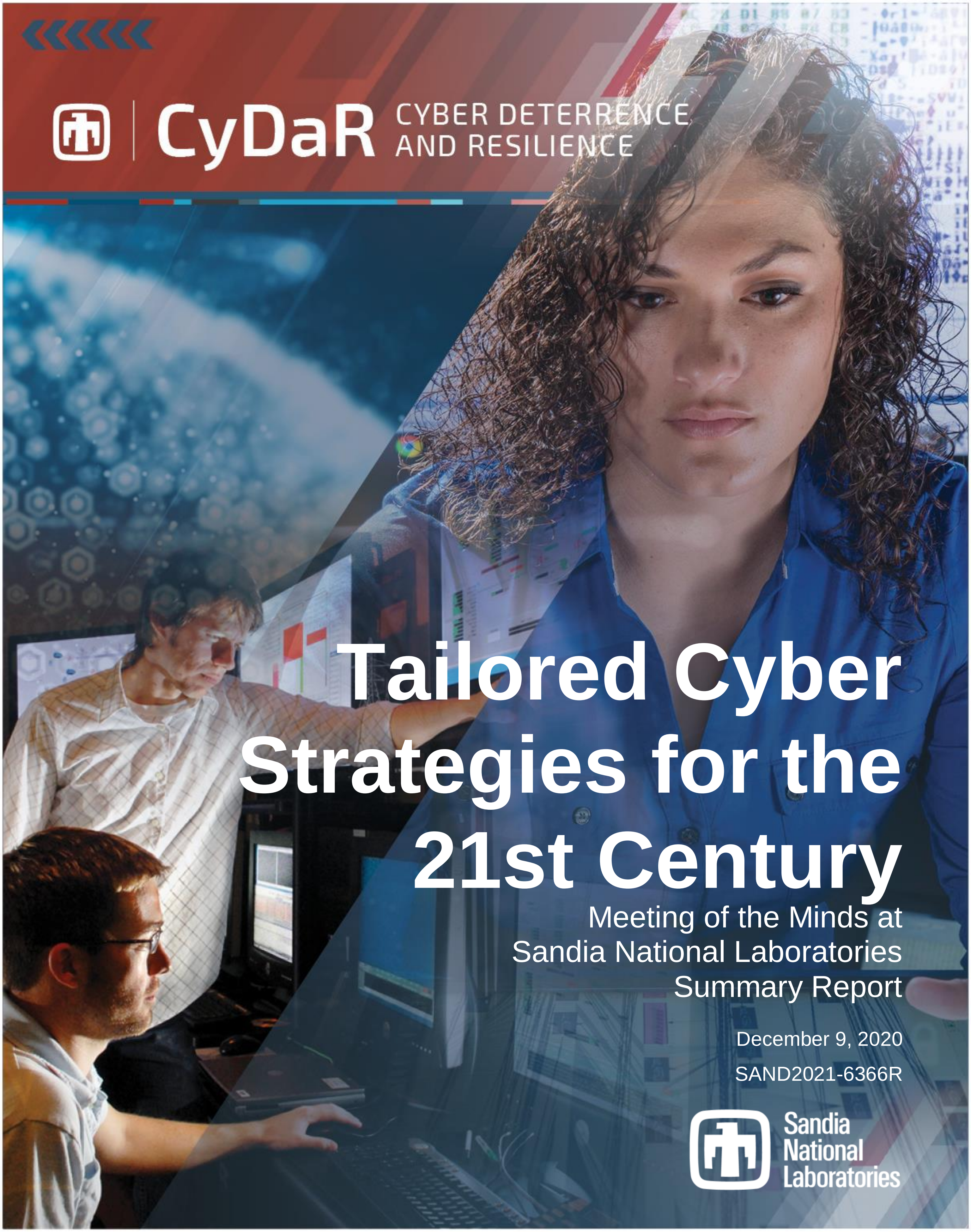

CyDaR CYBER DETERRENCE AND RESILIENCE

Tailored Cyber Strategies for the 21st Century

Meeting of the Minds at Sandia National Laboratories Summary Report

December 9, 2020

SAND2021-6366R

Sandia
National
Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

CONTENTS

SUMMARY REPORT

Tailored Cyber Strategies for the 21st Century

Meeting of the Minds, Sandia National Laboratories

December 9, 2020

Prepared by: Eva C. Uribe, Mathias Boggs, Michael Minner, Bryn Stuart, and Nerayo P. Teclemariam

The views summarized here are those of the meeting participants and should not be attributed to Sandia National Laboratories, National Technology and Engineering Solutions of Sandia, LLC (NTESS), or any other organization.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
CIA triad	Confidentiality, Integrity, Availability
CISA	Cybersecurity and Infrastructure Security Agency
CSC	Cyberspace Solarium Commission
CYBERCOM	United States Cyber Command
DF/PE	Defend forward/persistent engagement
DIE	Distributed, immutable, ephemeral
DOD	Department of Defense
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
IP	Intellectual property
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NRMC	National Risk Management Center
NSPM	National Security Presidential Memorandum
NTESS	National Technology and Engineering Solutions of Sandia, LLC
SNL	Sandia National Laboratories
U.S.	United States
USG	United States Government

EXECUTIVE SUMMARY

On December 9, 2020, Sandia National Laboratories (SNL) convened a diverse set of voices from across the federal government, the United States (U.S.) military, the private sector, and national laboratories to understand current and future trends affecting our national cyber strategy, and to illuminate the role of Federally Funded Research and Development Centers (FFRDCs) in contributing to national cyber strategy objectives.

The event featured two sets of panelists who provided prepared remarks followed by open discussion. The overarching question posed to the panelists were:

- What progress has been made in defining U.S. cyber strategy and policy, and what are the primary forces driving future evolution?
- What is necessary to implement and operationalize strategic theory and policy on cyber conflict and competition? What barriers must be overcome?

The first set of panelists discussed the evolution of U.S. cyber strategy and policy, providing insight into how the U.S. has thought about cyber in the past, how adversaries are utilizing cyber, and what interests and forces are driving U.S. cyber policy and strategy changes. The second panel debated alternative cyber strategies that the U.S. could pursue, considering theory, the unique characteristics of cyber competition, and measurements of success in assessing these strategies. These two panels provided important opportunities to discuss complex cyber topics with a wide range of participants. There were a number of key themes that were discussed in this event.

One of the primary points of discussion was the change in U.S. perceptions of cyberspace. Panelists noted that U.S. thinking about cyber has been in constant change over the past two decades. The U.S. has been primarily concerned with terrorist threats during these two decades, but cyber presents a different type of threat. While terrorism tends to be opportunistic, adversaries use cyber in strategic ways, targeting U.S. priorities to achieve strategic gains. As these characteristics of cyber conflict became clearer, the Obama administration sought to provide calculated responses to cyber operations in an effort to avoid escalation. The Obama administration maintained a close hold on the use of U.S. cyber capabilities, and focused on international collaboration and norms development. The Trump administration took a much different approach, worrying less about escalation and instead prioritizing flexibility and initiative by U.S. Cyber Command (CYBERCOM) and the Department of Defense (DOD). While policy has changed across administrations, the growing understanding of cyber as a critical domain has remained constant, bridging partisan divides and becoming a whole of nation priority.

In addition to how the U.S. Government (USG) has thought about cyber, there was considerable debate among the panelists regarding the theory and frameworks that should be drawn upon in cyber strategy. Panelists presented various ways of thinking about cyber competition, comparing it to intelligence campaigns, information warfare, conventional conflict, nuclear deterrence, or eschewing these comparisons altogether and asserting the uniqueness of cyber conflict. Panelists also discussed what U.S. goals should be in cyberspace and what strategies best accomplish those goals. However, there were also multiple panelists that noted there is no "end state" in cyberspace, and that the domain is constantly evolving. As the domain changes, the U.S. must actively play a role in shaping the "rules of the game" in cyber competition.

Establishing rules and norms in cyberspace will require the U.S. to utilize its strong partnerships, both internationally and domestically. Panelists noted that the U.S. has more allies than our adversaries, and that it should use this asymmetric advantage to shape the future of cyber competition. However, not all allies have the same capabilities or even the same interests. As the U.S. works with international partners, it should identify tiers of cooperation, such as those states that have the capabilities to conduct joint operations with the U.S., those who can work on defensive missions, those who are trying to keep their networks secure, and then others who are seeking partnership but may have limited capabilities. Similar tiers of partnerships could be developed with private sector partners, where some companies participate in joint operations with the USG, while others simply seek to improve security. Regardless of the levels of our partners, the U.S. should continue to utilize these relationships to strengthen our position in cyberspace.

Another point of discussion among panelists was the challenge associated with setting standards and performing assessments. Panelists noted that standards and assessments often turn into checklists, rather than risk-informed decisions. Because "what gets measured gets done," there is tension between establishing metrics and allowing flexibility and assessment tailored to specific organizations. However, organizations need to identify risks and priorities in order to appropriate allocate resources.

This Meeting of the Minds brought a diverse set of panelists together to assess U.S. cyber strategy, current and future trends, and opportunities for improvement throughout the USG and private sector. The discussion provided insight on implementation and coordination of cyber strategy, as well as budget and policy considerations. This, and future similar events, will illuminate the challenges and opportunities for future cyber strategy.

AGENDA & PANEL TOPICS

Introduction Jen Gaudioso

Panel #1: Current and future U.S. cyber initiatives

Moderator: Michael Nacht

Panelists: Bob Kolasky, David White, Robert Morgus, Thomas Wingfield, Jacquelyn Schneider

Overarching Question:
What progress has been made in defining U.S. cyber strategy and policy, and what are the primary forces driving future evolution?

Specific questions:

1. What are the core interests of the U.S. in cyberspace?
2. What cyber policies and initiatives did the Trump administration inherit, and what actions has it taken?
3. What is or will be the impact of the Cyberspace Solarium Commission Report on cybersecurity programs and initiatives across federal agencies and the private sector?
4. What are the primary forces driving future change in U.S. cyber policy?
5. What is the role of an FFRDC (and Sandia in particular) in achieving national cyber strategy objectives?

Panel #2: Debating alternative cyber strategies

Moderator: Ben Bonin

Panelists: Eva Uribe, Emily Goldman, Mark Montgomery, Joshua Rovner, Jay Healey, Sounil Yu

Overarching Question:
What is necessary to implement and operationalize strategic theory and policy on cyber conflict and competition? What barriers must be overcome?

Specific questions:

1. What are the primary or archetypical cyber threats to our national security? How will these evolve in the next 5-10 years?
2. What are the desired outcomes or end states for each type of threat? (e.g. defeat, deter, engage persistently, prevail in protracted competition, establish resiliency, establish norms, or other?) What is needed to achieve these end states from a practical or operational perspective?
3. Are cyber operations elements of intelligence competitions or precursors to armed conflict?
4. How do we go beyond cyber strategy that is reactive to risks towards one driven by seizing opportunities?

Conclusion & Discussion

Discussants: Len Napolitano, Jason Reinhardt, Jon Lindsay, Jen Gaudioso

KEY THEMES

A Dynamic Global Security Environment

Attendees discussed the shifting security environment towards one characterized by strategic cyber risk and great power competition. Following the terrorist attacks of 9/11, when the Department of Homeland Security (DHS) was first established, the primary goal was to defend against foreign terrorist threats, which are characterized by opportunism. The threats facing our nation now are strategic. Adversaries are intentional in using cyber attacks to attack our strategic priorities. When an actor behaves strategically, we have to defend strategically. This means we must shift our defensive posture to manage strategic cyber risk, to reduce the risk facing the nation from cyber attacks. In cyberspace, our long-held geographic advantage no longer exists; we must actually defend ourselves now. Long-term strategic competition requires that we take a more proactive approach in cyber and to integrate our capabilities here in the U.S. and with our international partners.

Attendees emphasized offensive advantage in cyberspace. Defenders are often trying to figure out how to prevent or defend against the last attack that happened. Attackers do not often deploy the same methods of their last attack. We should not be surprised by the latest breach (e.g., SolarWinds) announced by FireEye and others. It is not uncommon for nation state cyber adversaries to employ new techniques that have never been seen before.

Other attendees observed a shift in strategic focus over the past decade, from a concern over network breaches to include information integrity in general. There is a bifurcation globally between those who would use the Internet for democratic purposes and those who would use it for authoritarian purposes, and whoever achieves technology dominance has the upper hand in this battle. Cyberspace is evolving and will continue to evolve. As an example, Netflix takes up more than one third of the bandwidth of the Internet on any given night. That is a huge surface area to defend. It is growing exponentially and with no sign of stopping. Our response to this rapid change is fragmented. Our government is not structured to respond to rapid change, but to evoke change only slowly and deliberatively. Congress, by design, is not agile nor flexible enough to confront these changes. The Department of Homeland Security still reports to 24 different Senate and House Committees after 20 years.

Evolution of U.S. Cyber Policy and the Role of the Department of Defense

U.S. cybersecurity strategy and policy have evolved with and adapted to this dynamic security environment. Participants provided an overview of U.S. defense cyber policy over the past several administrations. In the Obama administration, the focus within the DOD was to respond to cyber incidents and deter cyber attacks. The administration prioritized interagency coordination among the DHS, Federal Bureau of Investigation (FBI), and State Department for coordinating cyber operations over the DOD. U.S. military offensive cyber capabilities have been guarded very closely and restrained at the highest levels of government. This restraint stemmed from concerns about the potential for offensive cyber operations to escalate conflict or precipitate crises. By the end of this administration, there was frustration over this degree of restraint, which can be seen in the 2018 Command Vision for U.S. Cyber Command.[1] However, strong leadership during the Obama administration resulted in progress on key areas, particularly on interagency coordination, and a clear articulation of norms, including the norm against attacking critical infrastructure. The Obama administration focused on specific activities, such as the taskforce on intellectual property (IP) theft, which coordinated across multiple agencies to address a particular threat.

[1] https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

During the Trump administration, there was less concern about cyber operation resulting in conflict escalation, and a shift towards more risk-accepting policies and more decentralized authorities. U.S. CYBERCOM was elevated to a combatant command in 2018 and received more authority and more autonomy over operations with National Security Presidential Memorandum 13 (NSPM-13). General Paul M. Nakasone, Commander of U.S. CYBERCOM, is an operationally-focused leader. With these new authorities, the past four years have seen extraordinary operational innovation, including the public release of malware and hunt forward activities, along with the use of task forces to confront scoped and carefully-defined problems, such as election security. A lack of strategic vision and oversight at the highest levels of government may have allowed for experimentation and operational innovation. The Cyberspace Solarium Commission recommended the need for strategic vision along with operational innovation at lower levels and across agencies.

Participants commented on priorities for the new administration. The vacuum in strategic vision over the last four years was detrimental to the national security cyber mission. The coordinated U.S. response needs to continue to move from being reactive towards shaping the playing field to our own advantage. The new administration needs to build a strategy from the top down, leaning more heavily on the State Department, followed by the DOD. These two entities have to work together to signal and propagate norms of acceptable behavior. The new administration should clearly articulate the role of the DOD. We have seen new concepts introduced, including persistent engagement and defend forward, but what do these mean? We should clearly articulate what it is the DOD will do and what they will not do. One panelist advocated for better articulation of our existing declaratory policy of restraint at the strategic level, arguing that the DOD has exercised significant restraint, but often is not credited with being a norm propagator.

Cyber capabilities alone are insufficient without a proper focus on authorities. A foundational and critical step is defining and clarifying our strategies, procedures, plans, and authorities. The DOD now has appropriate authorities to execute its mission in cyberspace with speed and agility, but it was necessary to get the bureaucratic paperwork right first. The 2018 DOD Cyber Strategy[2] guides development of our forces and our deterrent posture. This strategy focuses on five key pillars:

1. Ensuring the U.S. military can continue to fight in the face of adversary activity
2. Strengthening the U.S. military through integration of cyber capabilities
3. Defending critical infrastructure
4. Securing DOD information
5. Strengthening our partnerships around the world to counter cyber threats

The DOD strategy prioritizes expanding cyberspace cooperation with three categories of partners, including U.S. interagency counterparts (such as DHS, FBI, and the State Department), private sector industry, and international allies and partners.

Allies and Partners are a Strategic Advantage

Our allies and partners are a strategic force multiplier that underlies all pillars of our national security and is at the heart of our DOD and national cyber strategy. We have relied on close partnerships to counter cyber threats. Our alliances and partnerships provide a durable, asymmetric, strategic advantage that is unmatched by our rivals. We must work with our partners and allies to secure supply chains and infrastructure. We want to advocate for responsible behavior in peace time, press our global partners to act within those norms, and hold accountable those who do not.

[2] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

The United States has more friends and allies than its competitors. We should fully engage the strategic and asymmetric advantage of our robust relationships with friends and allies abroad to achieve our national security objectives. We have different categories of allies and partners, organized in concentric circles. Our closest allies are those with whom we share intelligence and conduct offensive missions. We conduct defensive missions with a larger number of allies and partners. A third category are nations who we are confident exercise sovereignty over their own cyberspace. Beyond that, there is grey space. We want to bring more countries out of that grey space and into alignment with those first three circles; we want confidence that they can see what is going on in their cyberspace and they can respond with defensive measures appropriately.

This same onion layer structure can apply to the private sector as well. Some private sector partners have successfully defended themselves, and others face major challenges. There are certain private sector partners with whom the U.S. government or U.S. military might conduct joint operations; others with whom they would conduct joint defense operations; and others who are asked to defend their own space. A new strategy must be built on engaging, encouraging, and, when necessary, enforcing guidelines.

A Compliance-Based Approach versus a Risk Management Approach

The federal government is pivoting from defending the internet to defending our core critical assets. Will our weapon systems work, based on past attacks? Are there pre-positioned capabilities on our grid or weapons systems that compromises them? As we pivot away from defending the internet, we incorporate operational technology more. Rapid innovation by cyber attackers makes a compliance-based or checklist-based approach flawed from the outset. Tools like the National Institute of Standards and Technology's (NIST) Risk Management Framework that are initially designed to help us evaluate risks and make decisions eventually devolve into a set of checklists. Instead, we should adhere to principles of risk management, relying on individualized, threat-informed information for each individual entity. Audits should be based on the credibility of how threat-informed decisions are being made, not on checklists they adhere to. Many agree that the best thing companies can do to secure their networks is to hire the best people.

Multiple panelists emphasized the importance of viewing national cybersecurity strategy as a risk management problem. The Cybersecurity and Infrastructure Security Agency (CISA) is the nation's risk advisor. The National Risk Management Center (NRMC) within DHS focuses on reducing the risk of cyber attack to the nation and ensuring continuity of critical operations. In April 2019 they published a list of 55 national critical functions to help rewrite critical defense national security strategy. These functions align with a strategic approach and give us language to prioritize sources of risk.

An example of a critical function is elections. A strategic risk management approach looks systematically at how voting is done, all the way from voter registration to certification of the results. What are the sources of risk? Which cyber operations are capable of disrupting these functions? Cybersecurity of our elections became a top national priority in 2016. Protection of the 2020 elections was successful because the USG took a risk-based strategic view, and developed channels to share information. This is an example of a unique, coordinated, national effort. DHS/CISA brought together different capabilities and authorities to secure the election. The key to that success was creating teams, bringing people together, and collaborating with the private sector across capabilities and authorities.

At an institutional level, risk management is often used to prioritize mitigations. We focus on which vulnerabilities are most critical and which ones need to be addressed first. In cybersecurity, is it meaningful to prioritize vulnerabilities? This is an incredibly complex problem. Only organizations that truly understand their systems (few do) can triage their vulnerabilities this way. Everyone has limited security budgets. Risk is not just vulnerability, but a product of vulnerability, threat, and consequence. Threat and consequence often provide important context beyond just hardware and software security.

Key Recommendations from the Cyberspace Solarium Commission Report

Panelists discussed some of the key recommendations from the Cyberspace Solarium Commission (CSC) Report.[3] The report includes recommendations that are easily achievable within the short term, as well as medium-term and long-term recommendations that would require broader change.

National cyber defense is a shared responsibility between government and the private sector, which owns, operates, and has primary agency over most of our critical infrastructure. The USG must mature to be a full partner to ensure security and resiliency of national cybersecurity efforts. CISA has not been adequately resourced to achieve this mission. Therefore, in the near-term, the report recommends elevating CISA's resources and authorities so that it becomes a fully operational agency within DHS.

Cybersecurity is an increasingly important facet of national security. The CSC Report recommends, and the 2021 National Defense Authorization Act (NDAA) creates a National Cyber Director role within the White House, to coordinate efforts across the federal government and private sector. Without leadership at the highest levels, we remain uncoordinated and inefficient. The purpose of creating this post was to elevate cyber policy as an issue within the White House.

The Cyberspace Solarium Commission makes key recommendations on increasing our national resilience. First, we must prioritize the most important critical functions that must be maintained, define expectations, and provide government support for these. Second, we need to create and strengthen sector specific agencies, which constitute the complex system of partnership between the U.S. government and the private sector. Empowering DHS/CISA to align and strengthen these networks is important. Third, we need a process for ensuring continuity of the economy, which is a major element of our national power. This effort will involve mapping our economy across systemically important critical infrastructure, mapping dependencies, and preparing to reconstitute or restart those critical systems in case of disruption.

Deterrence in Cyberspace

Participants debated the merits of applying traditional concepts of deterrence to cyber conflict. Strategic deterrence in the nuclear context is often not relevant to the type of cyber conflict and competition seen today, which tends to be tailored to fall below agreed-upon thresholds of armed conflict, in order to avoid rather than provoke escalation. Nonetheless, the idea of influencing or shaping adversary behavior over time, to dissuade unwanted behavior, to impose unacceptable costs to breaking norms, and to remove obvious incentives for attack, such as poorly protected critical infrastructure, remains a staple within U.S. national security strategy documents. Cyber conflict has many similarities with sub-strategic conventional conflict, in which denial tactics are used to convince adversaries that quick wins are impossible. As Michael Gerson notes, "deterrence is best served when the attacker believes that his only alternative is protracted war." Broadly conceived to include cost imposition and denial, *deterrence* can include cybersecurity defense; forward defense to raise operational costs; threats of military, economic, or diplomatic retribution; and fostering systemic resilience for critical infrastructure. When it comes to cyber conflict, is deterrence the forest or a tree? Is it a primary

[3] https://www.solarium.gov/report

outcome that all elements of our national strategy should be driving towards, or is it merely one constitutive part of a broader strategy? This is an ongoing and unresolved debate.

The Cyberspace Solarium Commission Report**Error! Bookmark not defined.** recommends *layered cyber deterrence* as a theoretical concept that helps define and measure a desired end state. Layered cyber deterrence includes shaping behavior, denying benefits, and imposing costs in cyberspace. Deterrence by denial is the anchor of this approach. However, most critical infrastructure is owned and operated by the private sector, and there is extreme inconsistency in how well these entities are defended. Deterrence by denial cannot be the sole responsibility of the government. The private sector not only owns and operates a majority of critical infrastructure, but also has primary agency and decision-making authority over how much risk is acceptable and how many resources should be dedicated to security and resilience. The private sector has to be incentivized to defend itself. An example is data monetization. Critical infrastructure companies are incentivized to act proactively against the threat of ransomware because they want to protect their data, their operations, and ultimately their customers.

What is the private sector view on deterrence of cyber activity? Private industry relies on clear legal frameworks. There is no clearly communicated and agreed-upon framework for cyber deterrence. The Cyberspace Solarium Commission did not necessarily provide a legal framework that would make private sector partners comfortable. Furthermore, anyone who has watched Stanley Kubrick's film *Dr. Strangelove* knows that deterrence is the art of producing in the mind of the enemy the fear to attack. While we have seen innovation in offensive cyber operations, it is not clear how this fear of attack is being manifested. Instead, we see clear red lines being crossed – for example, attacks against hospitals and research centers during a pandemic. This clearly violates norms we wish to uphold, but what has been the response? Deterrence requires clear communication of credible threats, and carrying through on those threats. We need to show some action when norms are violated. Yet other participants observed that for decades we have observed significant attacker advantages in cyberspace. Few if any security controls can stop a dedicated red team. Rather than focus on deterrence, we should shift our focus to make defense better than offense.

Another view presented is that cost imposition is more likely to be successful when both parties agree that the adversary is the aggressor and not the defender. If there is disagreement about which party threw the first punch, and thus which party is being deterred, the stakes and motives are ambiguous, and that makes deterrence more difficult. Who are really the actors who are defending the status quo, and who are those trying to disrupt the status quo? There is not universal agreement here.

Yet another view presented on the subject of deterrence of cyber adversaries is that while deterrence is a stated mission of the DOD, we should not use it as a universal metric by which to judge all other aspects of cybersecurity. Deterrence is a theory only, a causal prediction that if we take an action, it will lead to other national security outcomes. An example of a different causal prediction is the *security dilemma*: If one party gets tremendous weapons, then their adversary will get tremendous weapons as well. Robert Jervis wrote in 1978 that the security dilemma is especially dangerous when offense cannot be distinguished from defense. If we see someone with a weapon, we do not know if they are defending themselves or preparing to attack us. Can we distinguish espionage from preparing the battlefield? Therefore, actors should be cautious about brandishing their awesome cyber capabilities. Deterrence requires transparency to some degree about one's capabilities; however, in doing so, we may invite our adversaries to develop more fearsome capabilities of their own. This is different than building a moat, which is purely defensive.

Ultimately, participants in this meeting did not generate consensus on the question of whether deterrence is a useful strategy or set of concepts for cyberspace, but rather demonstrated the lively debate around this topic. One observer pointed out that deterrence during the Cold War was as complex and poorly understood as it is today. During the Cold War, there was similarly a lot of innovation, operations, capability demonstration, secrecy, intelligence operations, and withholding of information to keep tools in reserve. When we focus on the practice of deterrence during the Cold War, we observe a lot of continuity with today. Deterrence is not one concept, but a plethora of concepts that includes stability, certainty, credibility, and efficiency without resorting to war – all of which are good goals but may have difficult tradeoffs. Coherent strategy requires prioritization of end states. There is no shortcut to strategy – critical thinking must be done every time.

Defend Forward and Persistent Engagement

Participants argued that strategic frameworks must map to the realities of the strategic environment. Characteristics of cyberspace induce an imperative for persistent activity. Cyberspace is an operational space in which costs are contestable, in that one can defend or design around attacks and intrusions. In the nuclear domain, costs are incontestable and defense is not possible. States are already engaging one another persistently in cyberspace. Deterrence is based on operational restraint and coercive threats of response – this is inconsistent with an environment where constant operational engagement is rewarded. If the cost/benefit calculation is a given, no one can change it.

The primary threat space we are concerned with is nation-states because they have the potential to have the most strategic impact. For too long we have relied on the concept of *deterrence* to contend with strategic threats. Strategic threats erode national sources of power. These can take the form of kinetic power above the threshold of armed attack, or they can take the form of integrated campaigns of events that occur over time, all below the threshold of armed attack. Deterrence concepts do not apply equally well across this spectrum. Rather than asking which end states we should be driving towards, we should be asking, *What is the strategic space I am operating in, and what is required?* Deterrence applies to cyber attacks equivalent to armed attacks. Below the threshold of armed attack, persistent engagement seeks to disrupt activity rather than to signal, shape decision calculus, or coerce. Defend forward and persistent engagement emerged in response to the frustration within policy communities and Congress that our previous approaches to conflict in cyberspace, based upon operational restraint and the desire to deter cyber adversaries, was not working. A key barrier to making additional progress here is getting stuck in our old ways of thinking. We should not equate *defend forward* with *forward defense*. Defend forward is not about signaling through force posture and disposition, but is about seizing the initiative – defending forward in time, not position. It focuses on the question *how we secure* and not *how we deter*.

The Cyberspace Solarium Commission Report**Error! Bookmark not defined.** calls for incorporating defend forward into our national strategy. There is a clear role for DOD in defending forward and hunting forward operations. Defend forward concepts can be applied across other elements of power from the rear. The vast majority of defending forward is from the rear. Currently, we do not apply a consistent approach broadly across economic, law enforcement, diplomatic, and military elements of power. We lack clear coordination in the interagency, or at least we do not acknowledge this coordination if it exists, and this results in a lack of clear declaratory policy. Participants called for enhancing and enabling defend forward across all elements of power. Clear articulation of a national cyber strategy led by a new National Cyber Director is essential to this effort.

There was considerable debate amongst panelists whether or not defend forward/persistent engagement (DF/PE) constitutes deterrence below the threshold of armed conflict. DF/PE creates friction, increases the adversary's cost of doing business, all of which results in cost imposition or deterrence by denial, and long-term shaping of behavior. Others disagree and argue that deterrence has become a term that is too broadly used. *Deterrence* means a threat of prospective action in order to change decision calculus. A strategy of deterrence is premised on the belief that we cannot adequately defend and must resort to fear in the minds of our adversaries. Persistent engagement is not about changing adversaries' decision calculus, but rather actively disrupting their operations. This could achieve a deterrence *effect* over time, but it is not a strategy of deterrence. Deterrence as a strategy must be distinguished from deterrence effects. A strategy of deterrence has many different things that DF/PE does not have. The same is true when we discuss defense in the context of deterrence by denial. One can only use defense to deter by denial if one can attrit. If attrition is not possible, we will never convince our adversaries that they won't be able to get through. We have not yet achieved this – adversaries are continuing to try to get through. Therefore, our actions are more properly categorized as defense, not deterrence by denial.

The Threshold of Armed Conflict

Yet another viewpoint represented was that deterrence of certain behaviors in cyberspace is currently U.S. policy, but that frameworks for operationalizing these goals are lacking. In 2018 the Office of the Coordinator for Cyber Issues articulated two desired end-states for cyber deterrence efforts, including a continued absence of cyber attacks that constitute a use of force against the U.S. and its allies, and a significant, long-lasting reduction in destructive, disruptive, or destabilizing cyber activities against U.S. interests that fall below the threshold of the use of force. The "use of force" threshold may be problematic. Clear delineation between cyber activity above and below the use of force may be impossible or inadvisable. Nations have thus far not agreed on what types of cyber activities constitute a use of force within the Law of Armed Conflict. Participants argued for the need for additional open source analysis to understand how geopolitical context influences the strategic nature of cyber conflict and competition. The suitability of deterrence concepts may depend more heavily on specific geopolitical context and specific aspects of the relations between actors than it does on thresholds that lack consensus from the international community.

Assuming the use of force threshold is a valid organizing principle for cyberspace, our observation that state actors use cyberspace to undermine our strategic interests below the threshold of armed conflict means we need to both strengthen deterrence above this threshold and reestablish deterrence below this threshold. Cyber conflict and cyber competition are different. Cyber attacks above use of force threshold must be distinguished from cyber activity below this threshold. Most cyber attacks do not result in significant property damage or loss of life, but may have other significant effects over time (e.g. systematic intellectual property theft). Deterrence has largely been successfully held above the use of force threshold. We have not seen many cyber activities above the threshold. Layered cyber deterrence takes into account this distinction and aims to strengthen deterrence above the threshold of armed attack and reestablish deterrence below this threshold.

Moreover, as we continue to debate alternative cyber strategies, the imperative question remains, what are the key challenges and opportunities as we move beyond making strategy into implementing and operationalizing an integrated strategy across federal, state, and local governments, the private sector, and our international allies and partners?

Deterrence versus Resilience

Determined adversaries will find a way in, so deterrence is a less relevant concept than resilience. Resilience is a core, strategic interest of our nation. We will never be able to deter against all of the small attacks, that ultimately surmount to a strategically significant or catastrophic outcome. The Cyberspace Solarium Commission Report$^{\text{Error! Bookmark not defined.}}$ envisions a role for deterring higher level activities, and acknowledges the difficulty of deterring smaller operations that amount to major problems. The best way to manage those lower level activities is through resilience. Private industry has no power, authority, or tools to participate in deterrence. These tools are concentrated in the hands of the government and military. Private industries do have control over the defense and resiliency of their systems.

There are no borders within cyberspace. Our efforts to strengthen defense and resilience must expand beyond U.S. borders. The DOD cyber strategy pillars are intended to counter adversaries and create norms. We seek to develop information sharing methods that will increase our cyber defense posture. Cyber actors will be increasingly disruptive in the future. The level of risk is growing at an increasing rate. First we must strengthen our cyber defenses and resilience, so that we can ultimately deter and defeat our adversaries. Defending forward and countering adversaries outside of U.S. networks is an important part of this strategy.

New Principles for Resiliency

While we tend to think of security and resilience together, there are potential tradeoffs. We should strive to achieve one or the other, not both. A useful analogy for distinguishing systems that we want to secure versus systems that we want to make resilient is pets versus cattle. We care about pets – we give them names, become emotionally attached to them, take them for medical care when they get sick. Our Social Security numbers and personal laptops are pets. If they are lost or compromised, we experience a high degree of loss. For pets, we have a very low tolerance for acceptable loss. Cattle are different. We give them an obscure name or simply a number. Each individual cow is dispensable. The tolerance for acceptable loss is very high. For pets we need to maintain security, confidentiality, integrity, and availability (known as the CIA triad). For cattle, we want to practice resiliency, but we should not seek to apply CIA principles. Instead, we should seek to make these systems distributed, immutable, and ephemeral (DIE). Creating more cattle instead of more pets would give us a higher loss tolerance, and provides a buffer for those systems whose security we really care about.

Of course, reality is more complex than this analogy. In reality systems have pet-like properties or cattle-like properties. To defend ourselves better and make ourselves more secure, we should strive to maximize those systems that are cattle-like. This is a continuous goal. When we are unable to do so, then we use CIA security best practices on a smaller portion of our systems. This allows us to dedicate more of our security resources where they truly matter. Our greatest problem is not insufficient protection for our pets, but rather that we have too many pets.

What does this look like in the real world? What do cattle look like? How do we build defensible infrastructure? For cattle-like systems, the best defense is business-driven change and rapid innovation. The best defense is when we displace our dependency on legacy components that are less defensible. Private industry does not just "own and operate" – it creates new products and invents new ways of doing things. The best defense is to constantly change the rules, so that potential adversaries have to play on our playing field and play by our rules rather than their own. The best way to create defensible infrastructure is to enable continuous change and innovation.

Unlike in other industries, in cybersecurity, we are lacking a framework to understand the "margin of safety." The DIE framework for resiliency principles presents some advantages over the CIA triad for measuring cybersecurity. It is difficult to measure or quantify *confidentiality*. It is an easier problem to measure or quantify the number of pets versus cattle we own. Using the DIE triad provides an easier framework around which to define a margin of safety for our cyber systems.

Is Cyber Conflict Escalatory?

Under what conditions are cyber actions escalatory or de-escalatory? A decade ago, we had very little data for answering this question empirically. Scholars were confined to theory, and many assumed that cyber operations were inherently escalatory. Now we have a lot of data, and many scholars have conducted empirical work on this question. For example, see work by Jacquelyn Schneider, Ryan

Maness, Brandon Valeriano, Ben Jensen, and Nadiya Kostyuk. To summarize this extensive body of work, there is no evidence that cyber conflicts escalate to violence. Nadiya Kostyuk has investigated the use of cyber on the battlefield in the Russia/Ukraine conflict, and found no evidence between the use of cyber operations and conflict escalation. Jacquelyn Schneider has conducted experimental wargaming, some in which cyber operations are even used to generate nuclear effects. She has shown that within the American public there are statistically significant differences in our reluctance to retaliate against cyber attacks compared to a kinetic attack where effects where held equal. The academic work has shown no evidence that cyber operations have created escalatory dynamics.

The majority of cyber operations do not achieve the same kind of damage that kinetic operations do; therefore, they do not elicit the same kinds of retaliatory responses. Most cyber operations do not cause physical damage. The causes and effects of operations are often obscured, and people are often uncertain about the true stakes involved. This makes coercion difficult in cyberspace; however, it reduces the risks of escalation. If a cyber actor does not purport to impose serious costs, then their actions are less likely to provoke a serious conflict. The natural corollary to consider is, can we make strategic use of cyber activity for conflict de-escalation? Cyber operations can provide a release valve for conflict, similar to the way states have previously used covert operations as an alternative to warfighting. States have a long history of using covert operations to de-escalate ongoing conflict and reduce dangers during a crisis.

Some participants conversely observed that relying on empirical data causes us to focus on what has happened rather than on what could or will happen, and furthermore constrains us to studying the last several decades, which have been relatively peaceful. Rather than answer the question, *are cyber operations escalatory or de-escalatory?,* we should understand the conditions under which cyber operations may be escalatory or de-escalatory. Which geopolitical pressures and constraints lead to escalation of cyber operations into armed conflict? During times of relative peace, when competitors both want to keep the peace, cyber operations may de-escalate. But "pressure release" is not the only use case for cyber activity. An actor may also want to use cyber actions to provoke. Jason Healey and Robert Jervis provide a framework for various conditions leading to stability or instability in cyber conflict in their paper, "The Escalation Inversion and Other Oddities of Situational Cyber Stability."[4] In addition to *pressure release*, they describe how cyber operations can act as a *spark* in which cyber conflict directly leads to armed conflict in other domains. They also describe how the threat of armed conflict during an acute geopolitical crisis may result in riskier behavior generally that leads to more unrestrained use of cyber operations (a situation they call *pull out the big guns*), as well as situations where states are incentivized to use these capabilities first and early in a crisis to gain asymmetric advantage (*escalation inversion*). Several participants observed that uncertainties and ambiguities within the cyber domain make it potentially more prone for mistake and miscalculation that could lead to escalation during acute geopolitical crises. Escalation in cyberspace is a very active area of research and scholarly exploration. Select additional references brought up during this discussion are listed below.

Cyber War versus Cyber Realities: Cyber Conflict in the International System, Brandon Valeriano and Ryan C. Manness, Oxford University Press, 2015

Nadiya Kostyuk and Yurk M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution*, 63 (2), 2019

Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly*, 13 (3), 2019

[4] https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/

Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, 2019

Austin Carson, *Secret Wars: Covert Conflict in International Politics*, Princeton University Press, 2018

Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies,* 22 (3), 2013

Jacquelyn Schneider, Benjamin Schechter, and Rachael Shaffer, "Navy-Private Sector Critical Infrastructure War Game," *United States Naval War College*, 2017

Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity*, 5 (1), 2019

Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review*, Vol 3, Issue 4, Fall 2020, 30–53

Healey, Jason, "The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities" (June 15, 2016), https://dx.doi.org/10.2139/ssrn.2836206

Cyber Competition is an Intelligence Contest

One perspective elucidated by participants is that cyber conflict and competition is an intelligence contest over information dominance, rather than a competition for alliances or new territory. While it is taking place within a new domain, intelligence contests are not new and have been ongoing for thousands of years. In intelligence contests, actors hold information close. Deception and obfuscation are primary objectives rather than clear signaling and declaratory policy. Knowing where you stand with respect to others is difficult or impossible. When we ask for cyber strategy assessment, we are asking USCYBERCOM to measure the results of an intelligence competition. Assessment is difficult because true assessment relies on knowing how you affect the other side, how you have prevented them from taking actions against you. Strategy assessment is a difficult task that must be approached with humility.

Cyberspace competition is an information duel. Actors seek to collect, exploit, and corrupt information – the coin of the realm. All things equal, we want superior information to our rivals – more reliable and higher quality. This is unlike other types of competition, including war and arms races. Other forms of competition require transparency. In a war, you have to compel or coerce your adversary, to show them they cannot win, and that continuing in their course of action is futile. In intelligence contests, you obscure in order to induce uncertainty in your adversary.

The question about desired end states for certain types of cyber conflict and competition is misguided. There is no end state for international politics. There is no end state for espionage and intelligence contests. What we want to achieve is a situation where communications are reliable, but nobody can ever declare victory. Analogies to conventional war and military strategy fail us here. A better analogy may be counterterrorism. We will never achieve a great and lasting victory over terrorism. Rather, we seek to arrive at political decisions about how much risk we can live with in our daily lives. The same principle applies in cyberspace. We are not going to deter intelligence gathering; the task before us is to decide which secrets are the most important to protect. Another useful analogy is private sector competition. The private sector competes, and this competition does not end, but is persistent. They must continually understand who their competitors are to gain a strategic advantage over them. Obtaining this advantage, gaining the initiative, is a temporary and fleeting state. It is not a strategy of coercion or trying to change others' behavior, but rather a strategy of exploitation. We want to be able to do this in an anticipatory way to achieve anticipatory resilience.

The Role of U.S. Cyber Command

USCYBERCOM has been tasked with implementing and operationalizing strategic theory. They have faced a multitude of barriers – bureaucratic, doctrinal, authority, conceptual – and have made progress in each of these areas. The proactive efforts demonstrated to protect U.S. elections in 2018 and 2020 demonstrated this progress. Defending forward had to be built up conceptually and has been integrated into strategy. The doctrine of persistent engagement had to be established. USCYBERCOM has been granted authorities through the 2019 NDAA, which clarifies the status of military cyber operations as traditional military operations exempt from the oversight required for other covert actions. Notable successes of the past five years include gaining public support for hunt forward operations, and successfully defending the 2018 and 2020 U.S. elections. However, other aspects of critical infrastructure are much more integrated with the Internet and are therefore more vulnerable than our electoral systems, which are largely isolated from the Internet.

The Challenge of Cybersecurity Metrics

How do we measure the operational successes of the last four years? How do we measure effectiveness? Metrics are inherently difficult in cybersecurity because often we do not know when we have been compromised. Applying "standardized" metrics across the board results in the kind of checklist, compliance-based approaches that are ineffective against complex threats. Decades of investigation by academics in cybersecurity technical fields have failed to reach a conclusion on measures of effectiveness.

A potential alternative is security based on threat analysis. Organizations would conduct individualized threat assessments, and the compliance checklist would be based on qualities of the threat assessment and what was done to respond, as opposed to a standard set of check boxes that are supposed to apply to all in every situation. System modeling is an important capability here. Across all domains, it is difficult to know how any individual operation or system impacts overall strategic objectives. If we can prove that we can model an environment with a provable degree of fidelity and accuracy, then we can conduct repeatable experiments. This helps us move away from a checklist-based approach. With a model, we can show with some confidence where the highest risks are and which investments will have the most impact.

Another way to think about cybersecurity metrics is through the concept of *acceptable losses*. In cyberspace, what are we willing to declare as an acceptable loss? We have lost Social Security numbers and SF-86 information for millions of Americans. This loss is clearly not acceptable, yet because it has already occurred, it has become acceptable to us. In retail and the financial sector, we have notions of shrinkage, fraud, and degrees or threshold of acceptable losses. Defining these are a key part of developing a cybersecurity strategy.

Ongoing Systemic Challenges

- *Software security*. We are more and more aware of challenges in the hardware supply chain, which remains a priority. Dominance in cyberspace requires getting into the lowest possible position, getting into the hardware, and controlling the atoms. In war, we need to get to the higher point. In cyber, we have to get to the lowest point. The next big, untenable, technological challenge is inherent trust of our software supply chain. At a national level, we are doing almost nothing to address the difficult problem of software provenance. We get our software from everywhere. In the cloud, you can get thousands of pieces of software in one application. This increases the surface area of attack. Adversaries can go to third, fourth, or fifth parties (or more) to insert their malicious code. They can do multiple hops to get to a single, strategic target. The most recent breach is an example. This is an insidious problem that requires a national wakeup call and a national response.

- *Confronting nation-state cyber threats*. Interagency task forces work best when they are targeted towards a well-defined problem. How does this translate to developing strategies to manage strategic competitor at the nation-state level?
- *Recruiting talent*. We have a dearth of qualified cybersecurity specialists. This is why we are often forced to resort to checklist or compliance-based security approaches. As a nation, we should make better use of the reserves, encourage engagement with academia, and reduce barriers to allow more people to rotate through academia and government.

Select Suggested Readings

The following references have helped to shape the CyDaR team's thinking about cyber strategy, deterrence, and resilience. They provide context for our discussion today. This list is not intended to be comprehensive.

Policy Documents

Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command, March 2018

Cyberspace Solarium Commission Report, March 2020

DoD Cyber Strategy and Cyber Posture Review – Sharpening our Competitive Edge in Cyberspace, unclassified public fact sheet, 2018

Federal Cybersecurity Research and Development Strategic Plan, prepared by the Cyber Security and Information Assurance Interagency Working Group, National Science & Technology Council, December 2019

National Cyber Strategy of the United States of America, The White House, September 2018

U.S. Department of Homeland Security Cybersecurity Strategy, May 2018

Books and Academic Works

Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*, Penguin Books, 2019

Cyber Analogies, Emily O. Goldman and John Arquilla, Eds., *Naval Postgraduate School,* 2014

Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," Foreign Policy Research Institute*, Orbis*, Vol. 61, Issue 3, 2017, pp 381-393

Michael S. Gerson, "Conventional Deterrence in the Second Nuclear Age," *Parameters,* Autumn 2009, pp 32-48

Emily O. Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy," *Texas National Security Review,* Special Issue: Cyber Competition, Fall 2020

Jason Healey and Neil Jenkins, "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing," *11th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2019

Jason Healey, "The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities" June 2016, http://dx.doi.org/10.2139/ssrn.2836206

Robert Jervis and Jason Healy, "The Dynamics of Cyber Conflict," Columbia School of International and Public Affairs, August 2019

Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-based Logics," *Journal of Cybersecurity*, Vol. 5, Issue 1, 2019

Martin Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009

Herb Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts" *Hoover Institution*, 2016

Herb Lin and Amy Zegart, Eds., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, The Brookings Institution, Washington, D.C., 2018

Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-scale Intelligence Problem," *Intelligence and National Security*, DOI:10.1080/02684527.2020.1840746, 2020

Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack," *Journal of Cybersecurity*, 1(1), pp 53-67, 2015

Jon R. Lindsay and Erik Gartzke, "Cross Domain Deterrence, from Practice to Theory," in *Cross Domain Deterrence: Strategy in an Era of Complexity,"* Jon R. Lindsay and Erik Gartzke, Eds., Oxford University Press, 2019

Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17) pp 44-17

Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" Strategic Studies Quarterly 5(4): 18-38, 2011

Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, September 2019

Joshua Rovner, "What is an Intelligence Contest?" Texas National Security Review, *Policy Roundtable, Cyber Conflict as an Intelligence Contest*, Robert Chesney and Max Smeets, Chairs, September 2020

David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing, New York, 2018

Jacquelyn G. Schneider, "Deterrence in and through Cyberspace," in *Cross Domain Deterrence: Strategy in an Era of Complexity,"* Jon R. Lindsay and Erik Gartzke, Eds., Oxford University Press, 2019

Jacquelyn Schneider, Benjamin Schechter, and Rachael Shaffer, "Navy-Private Sector Critical Infrastructure War Game 2017 Game Report," Naval War College, 2017

Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies*, Vol. 40, No. 1-2, pp 92-117, 2017

Eva C. Uribe. Benjamin J. Bonin, Michael F. Minner, Jason C. Reinhardt, Ann E. Hammer, Nerayo P. Teclemariam, Trisha H. Miller, Ruby E. Booth, Robert D. Forrest, Jeffrey J. Apolis, Lynn I. Yang, "Why Does Cyber Deterrence Fail, and When Might it Succeed? A Framework for Cyber Scenario Analysis," Sandia National Laboratories, 2020; SAND-2020-5016

SPEAKER BIOGRAPHIES

Ben Bonin

Ben Bonin has been with Sandia National Laboratories since 2005. He currently supports Systems Research and Analysis programs for Sandia California, with a recent focus on national security challenges in cyberspace. This includes developing methods and tools for evaluating cyber risks to critical infrastructure for the Department of Homeland Security and supporting an internal strategic initiative on the role of deterrence in defending critical infrastructure against cyber threats. Ben's past experience includes international outreach on arms control and nuclear security, facilitating engagement and training programs in the Middle East, Africa, Eastern Europe, and Asia. He is an Associate Alumni of the Near East South Asia Center for Strategic Studies at National Defense University, and a member of the World Institute for Nuclear Security. Ben holds a Ph.D. in Political Science from the University of New Mexico; his dissertation research explored the factors influencing arms control between nuclear-armed strategic rivals.

Jen Gaudioso

Jen Gaudioso is the Director of the Homeland Security and Defense Systems Center at Sandia National Laboratories. She is also Program Area Director for the Homeland Infrastructure Security and Resilience Program within Sandia's Energy and Homeland Security Portfolio. Jen leads the Center's support of the Department of Homeland Security and other federal, state, and local government agencies in increasing our nation's resilience to natural disasters and terrorist events. She also oversees the Integrated Security Solutions Division's use of systems analysis and data science capabilities to tackle complex national security challenges. Throughout her career, Jen has demonstrated a passion for connecting basic research to critical national security missions and, ultimately, impacting operations; the Homeland Security and Defense Systems Center spans the breadth of this wide spectrum.

Previously, as Senior Manager for Global Strategic Futures, Jen led development of the Global Security Division's mission, science and technology pipeline, and mission- aligned programs. In addition to chairing the Global Security Mission Foundation's Laboratory Directed Research and Development Investment Area Team, Jen was Senior Manager Lead for Sandia's contributions to the next-generation Nuclear Command, Control, and Communications (NC3). She also coordinated a Sandia- wide emerging initiative at the interface of NA-10, NA-20, NA-80, and DOE-IN, receiving a Department of Energy (DOE) Secretary of Energy Award for the team.

Jen began her Sandia career in 2002 as a postdoctoral fellow and became a technical staff member in 2004. In 2011, she moved into management, leading the International Biological and Chemical Threat Reduction Program, which enhances U.S. and international security via innovative solutions for countering biological and chemical threats globally. Jen and her teams visited facilities in more than 40 countries to consult on biosecurity and chemical security issues. Jen's leadership established Sandia as a critical contributor to the U.S. government's response to the Ebola outbreak in West Africa. The team's ground-breaking efforts were also acknowledged with a DOE Secretary of Energy Award.

Jen served on two National Academies Committees addressing biodefense issues and has authored numerous peer-reviewed articles, book chapters, and two books. She served on the board of the Elizabeth R. Griffin Research Foundation and was an MIT Seminar XXI Fellow. She has a Ph.D. and a master's degree in physical chemistry from Cornell University and a bachelor's degree in chemistry from Bard College. Jen's time at Bard taught her to value diverse perspectives in problem-solving.

Emily Goldman

Dr. Emily Goldman serves as a strategist at U.S. Cyber Command and a thought leader on cyber policy. She was cyber advisor to the Director of Policy Planning at the Department of State, 2018-2019. From 2014-2018 she directed the U.S. Cyber Command / National Security Agency Combined Action Group, reporting to a four-star commander and leading a team that wrote the 2018 U.S. Cyber Command vision, "Achieve and Maintain Cyberspace Superiority." She has also worked as a strategic communications advisor for U.S. Central Command and for the Coordinator for Counterterrorism at the State Department. She holds a doctorate in Political Science from Stanford University, and was a professor of Political Science at the University of California, Davis, for two decades. Dr. Goldman has published and lectured widely on strategy, cyber security, arms control, military history and innovation, and organizational change.

Jason Healey

Jason Healey is a Senior Research Scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict and risk. Prior to that, he was the founding director of the Cyber Statecraft Initiative of the Atlantic Council where he remains a Senior Fellow. He is the editor of the first history of conflict in cyberspace, *A Fierce Domain: Cyber Conflict, 1986 to 2012*. A frequent speaker on these issues, he is rated as a "top-rated" speaker for the RSA Conference and won the inaugural "Best of Briefing Award" at Black Hat. He helped the world's first cyber command in 1998, the Joint Task Force for Computer Network Defense, where he was one of the early pioneers of cyber threat intelligence. During his time in the White House, he was a director for cyber policy, coordinating efforts to secure U.S. cyberspace and critical infrastructure. He created Goldman Sachs' first cyber incident response team and later oversaw the bank's crisis management and business continuity in Asia. He served as the vice chair of the Financial Services Information Sharing and Analysis Center (FS-ISAC). He is on the review board of the DEF CON and Black Hat hacker conferences and served on the Defense Science Board task force on cyber deterrence. He started his career as a U.S. Air Force intelligence officer with jobs at the Pentagon and National Security Agency and is president of the Cyber Conflict Studies Association.

Bob Kolasky

Bob Kolasky was selected to lead the Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) in 2018, at the Department of Homeland Security (DHS). As one of CISA's Assistant Directors, he oversees the Center's efforts to facilitate a strategic, cross-sector risk management approach to cyber and physical threats to critical infrastructure. The Center provides a central venue for government and industry to combine their knowledge and capabilities in a uniquely collaborative and forward-looking environment. Center activities support both operational and strategic unified risk management efforts.

As head of the National Risk Management Center, Mr. Kolasky has the responsibility to develop integrated analytic capability to analyze risk to critical infrastructure and work across the national community to reduce risk. As part of that, he co-chairs the Information and Communications Technology Supply Chain Risk Management Task Force and leads CISA's efforts to support development of a secure 5G network. He also serves on the Executive Committee for the Election Infrastructure Government Coordinating Council.

Mr. Kolasky's current position is the culmination of years of risk and resilience experience. He most recently served as the Deputy Assistant Secretary and Acting Assistant Secretary for Infrastructure Protection (IP), where he led the coordinated national effort to partner with industry to reduce the risk posed by acts of terrorism and other cyber or physical threats to the nation's critical infrastructure, including election infrastructure.

Mr. Kolasky has served in a number of other senior leadership roles for DHS, including acting Deputy Under Secretary for NPPD before it became CISA and the Director of the DHS Cyber-Physical Critical Infrastructure Integrated Task Force to implement Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, as well as Executive Order 13636 on Critical Infrastructure Cybersecurity.

He is also the former Assistant Director for the Office of Risk Management Analysis at DHS where he was responsible for developing DHS's formative policies and processes for risk management, including the DHS Risk Management Fundamentals and Risk Lexicon. Prior to joining DHS, he was a journalist and an entrepreneur. He helped start two of the first public policy web sites and served as the Managing Editor for IntellectualCapital.com.

Mr. Kolasky joined the Federal government in 2008 after six years as a management consultant. He graduated from Dartmouth College in 1994 and from the Harvard Kennedy School in 2002.

Jon Lindsay

Jon Lindsay is Assistant Professor of Digital Media and Global Affairs at the Munk School of Global Affairs & Public Policy and Department of Political Science at the University of Toronto. He is the author of *Information Technology and Military Power* (Cornell University Press, 2020) and co-editor of *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford University Press, 2015), with Tai Ming Cheung and Derek Reveron, and *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford University Press, 2019), with Erik Gartzke, as well as publications in international relations, intelligence studies, and the sociology of technology. He is currently working on a book project called "Age of Deception: Technology, Intelligence, and Control in International Relations." He holds a Ph.D. in political science from the Massachusetts Institute of Technology and an M.S. in computer science and B.S. in symbolic systems from Stanford University. He has also served in the U.S. Navy with assignments in Europe, Latin America, and the Middle East.

Mark Montgomery

Mark Montgomery serves as the Senior Advisor to the Chairmen of the Cyberspace Solarium Commission, and was the Executive Director. He is also the Director of the Center on Cyber and Technology Innovation and a Senior Fellow at the Foundation for Defense of Democracies. He previously served as Policy Director for the Senate Armed Services Committee under the leadership of Senator John S. McCain.

Mark completed 32 years as a nuclear trained surface warfare officer in the U.S. Navy, retiring as a Rear Admiral in 2017. He commanded the USS McCampbell (DDG 85) and Destroyer Squadron FIFTEEN. His flag officer assignments included Director of Operations (J3) at U.S. Pacific Command; Commander of Carrier Strike Group 5 embarked on the USS George Washington stationed in Japan; and Deputy Director, Plans, Policy and Strategy (J5) at U.S. European Command.

Robert Morgus

Robert Morgus is a Senior Director for the US Cyberspace Solarium Commission, where he directs research and analysis for Task Force Two. At the Commission, Morgus has led the development of the ecosystem pillar of the Commission's final report as well as the Pandemic White Paper and the Supply Chain White Paper. Previously, he helped build New America's Cybersecurity Initiative, where he headed the organization's international cyber policy work. While at New America, his research focused on mechanisms to counter the spread of offensive cyber capability, cybersecurity and international governance, and Russian internet doctrine.

In the past, he has authored reports on international cybersecurity norms, internet governance, cybersecurity insurance, amongst others. Morgus has spoken about cybersecurity at a number of international forums including NATO's CyCon, the Global Conference on Cyberspace at The Hague, and Cy Fy 2015 in New Delhi, India. His research has been published and recognized by the *New York Times*, *Slate*, the *IEEE*, peer-reviewed academic journals, and numerous other national and international media outlets. Morgus serves as a member of the Research Advisory

Network for the Global Commission on Internet Governance, as well as the Global Forum on Cyber Expertise, and has served as an expert advisor for the World Economic Forum.

Michael Nacht

Michael Nacht holds the Thomas and Alison Schneider Chair at the Goldman School of Public Policy, University of California - Berkeley. From 1998-2008 he was the Aaron Wildavsky Dean of the Goldman School. He is a specialist in U.S. national security policy; science, technology and public policy; and management strategies for complex organizations.

He is the author or co-author of six books and more than eighty articles and book chapters on nuclear weapons policy; regional security issues affecting Russia and China, the Middle East and East Asia; cyber and space policy; counter-terrorism and homeland security; international education; and public management. He recently co-edited and co-authored *Strategic Latency and World Power: How Technology Is Changing Our Concepts of Security* published by the Lawrence Livermore National Laboratory Center for Global Security Research.

Nacht served as Assistant Secretary of Defense for Global Strategic Affairs (2009-2010), after unanimous U.S. Senate confirmation, for which he received the Distinguished Public Service Award, the Department's highest civilian honor. Previously, he was Assistant Director for Strategic and Eurasian Affairs of the U.S. Arms Control and Disarmament Agency (1994-97), during which time he participated in five Presidential summits, four with Russian President Yeltsin and one with Chinese President Jiang Zemin.

He received a B.S. in Aeronautics and Astronautics and an M.S. in Operations Research from New York University, and a Ph.D. in Political Science from Columbia University.

Leonard M. Napolitano, Jr.

Dr. Leonard M. Napolitano, Jr., is currently a Senior Advisor for Cybersecurity and Infrastructure Resilience in the Global Security Program at Lawrence Livermore National Laboratory. He provides guidance in developing and matching Laboratory technical capabilities towards national program goals of the Department of Energy, the Department of Homeland Security, and the Department of Defense (DOD). He is also serving as a technical expert to the Defense Science Board regarding DOD Dependencies on Critical Infrastructure and New Domains of Conflict.

He retired as Chief Information Officer (CIO) and Vice President for Information Technology Services at Sandia National Laboratories in Albuquerque, New Mexico in 2017. As CIO, his major focus was to deliver an IT environment that provided mission value by transforming the way the Laboratories use, protect, and access information.

In this role, he was responsible for the vision and leadership of Sandia's computing, information technology, information management, and cyber security strategies. He led the Laboratories' push into advanced cybersecurity defenses, hybrid cloud implementation, enterprise software evolution, Internet of Things (IoT) strategy, and the management assurance processes that ensure cost, schedule, and performance in a continually changing environment.

His previous position was Director for Computer Sciences and Information Systems at Sandia National Laboratories in Livermore, California, where he managed a large organization that ranged from fundamental research and development in cybersecurity, decision analysis, large dataset manipulation and information extraction to maintaining and operating a range of computer networks and production computing and information resources.

Before that, he held a range of technical and management positions at Sandia in advanced technology development and program development for a range of US defense needs, including establishing Sandia's research foundation in bioscience.

Dr. Napolitano has undergraduate and graduate degrees from MIT and a doctorate from Stanford University.

Jason C. Reinhardt

Jason C. Reinhardt is a national security systems analyst and Distinguished Member of Technical Staff at Sandia National Laboratories. His work is focused on probabilistic analysis methods, quantitative and non-quantitative approaches for risk analysis and management. His current research is in support of the development of risk assessment and frameworks for cyber threats to critical infrastructure. He has also worked extensively with international partners on applications of systems analysis and risk methods to nuclear security challenges. Jason received his Ph.D. in Risk Analysis from Stanford University School of Engineering's Department of Management Science and Engineering. He also holds an M.S. in Electrical Engineering from Stanford University, and a B.S. in Electrical Engineering from the Purdue School of Electrical Engineering.

Joshua Rovner

Joshua Rovner is associate professor in the School of International Service at American University. In 2018 and 2019 he served as scholar-in-residence at the National Security Agency and U.S. Cyber Command.

Jacquelyn Schneider

Jacquelyn Schneider is a Hoover Fellow at the Hoover Institution. Her research focuses on the intersection of technology, national security, and political psychology with a special interest in cybersecurity, unmanned technologies, and Northeast Asia. She is a non-resident fellow at the Naval War College's Cyber and Innovation Policy Institute and a senior policy advisor to the Cyberspace Solarium Commission. Her work has appeared in *Security Studies*, *Journal of Conflict Resolution*, *Strategic Studies Quarterly*, *Journal of Cybersecurity*, *The Washington Quarterly*, *Journal of Strategic Studies* and is featured in *Cross Domain Deterrence: Strategy in an Era of Complexity* (Oxford University Press, 2019). Her current manuscript project is *The Rise of Unmanned Technologies* with Julia Macdonald (upcoming, Oxford University Press). In addition to her scholarly publications, she is a frequent contributor to policy outlets, including *New York Times*, *Foreign Affairs*, *CFR*, *Cipher Brief*, *Lawfare*, *War on the Rocks*, *Washington Post*, *Bulletin of the Atomic Scientists*, *National Interest*, *H-Diplo*, and the *Center for a New American Security*.

In 2018, Schneider was included in CyberScoop's Leet List of influential cyber experts. She is also the recipient of a Minerva grant on autonomy (with co-PIs Michael Horowitz, Julia Macdonald, and Allen Dafoe) and a University of Denver grant to study public responses to the use of drones (with Macdonald). She is an active member of the defense policy community with previous positions at the Center for a New American Security and the RAND Corporation.

Before beginning her academic career, she spent six years as an Air Force officer in South Korea and Japan and is currently a reservist assigned to U.S. Cyber Command. She has a B.A. from Columbia University, MA from Arizona State University, and Ph.D. from George Washington University.

Eva C. Uribe

Eva C. Uribe is a senior systems research analyst at Sandia National Laboratories. Her current work focuses on nuclear nonproliferation, nuclear fuel cycle safeguards, cyber systems analysis, and deterrence. Prior to joining the laboratory, she was a Stanton Nuclear Security postdoctoral fellow at the Center for International Security and Cooperation (CISAC) at Stanford University. Eva graduated from UC Berkeley with a Ph.D. in chemistry in 2016. Her dissertation research focused on development of high surface-area solid phase materials for the separation of actinides and lanthanides. She graduated from Yale University with a B.S. in 2011, with a double major in chemistry and political science. Eva was a Next Generation Safeguards Initiative intern in the Nonproliferation Division at Los Alamos National Laboratory in 2008 and 2009.

David R. White

As the Director of the Information Operations Center at Sandia National Laboratories, Dr. David R. White is responsible for overseeing the delivery of major national security programs for the U.S. government. These programs include research and development in the areas of cyber security that span from atoms to data.

Previously, David served as the Deputy Associate Lab Director for National Security Programs where he had mission assurance responsibilities for the over $500M/year portfolio of research and development programs performed for various government sponsors. During that time, he also was Sandia's Field Intelligence Element Director responsible for overseeing all high security work for Sandia. Prior to that, he served as Chief Information Security Officer, where he was responsible for identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology security risks. As Director of the Cyber Security and Mission Computing Center, he also led Sandia's cyber security, high performance computing, and mission software engineering efforts.

David has also served as Senior Manager for Sandia's Cyber Security Research and Development programs that support the U.S. Department of Defense, where he conceptualized and managed projects in cyber modeling and simulation, dynamic defense, industrial control systems, data analytics, red teaming, and supply chain risk management. David also had several other leadership positions in data science, computing support, and information systems engineering.

David received his bachelor's and master's degrees in Engineering from Brigham Young University, and his Ph.D. in Engineering with an emphasis on Computational Geometry and Computation Mechanics from Carnegie Mellon University. In 2013, David was named a National Security Fellow by Harvard University's Kennedy School of Government, where he conducted research on defending the U.S. electric grid from cyberattack. Raised in metropolitan Massachusetts and rural Utah, David now calls Albuquerque, New Mexico, home. He and his wife, Catherine, enjoy spending time hiking, reading, and all types of sporting events with their five children.

Thomas C. Wingfield

Mr. Thomas C. Wingfield was appointed the Deputy Assistant Secretary of Defense for Cyber Policy on November 25, 2019. In this capacity, he supports the Secretary of Defense and other senior Department of Defense leaders by formulating, recommending, integrating, and implementing policies and strategies to improve DOD's ability to operate in cyberspace. Prior to this appointment, Mr. Wingfield was the Acting

Chancellor and Dean of Faculty and Academic Programs at the College of Information and Cyberspace at the National Defense University in Washington, D.C.

Beginning his career as a naval officer, he served as Squadron Intelligence Officer with an F/A-18 strike fighter squadron aboard the USS Midway, based in Yokosuka, Japan. He also served as a Desk Officer at Headquarters, Office of Naval Intelligence, and then as Intelligence Liaison Officer at the Center for Naval Analyses, the Navy's principal think tank. While in Washington, he served as a White House Social Aide and completed his law degrees at Georgetown.

Upon passing the Georgia bar exam, Mr. Wingfield transitioned to the naval reserve and took a position with a defense consulting firm to advise military and intelligence community clients in the areas of treaty compliance, use of force in cyberspace, and space law. In 2003, he became a Research Fellow of the Potomac Institute for Policy Studies, providing analysis to Congress and the Administration on the legal and policy aspects of emergent national security issues.

Appointed an Associate Professor at the US Army Command and General Staff College at Fort Belvoir, Virginia, Mr. Wingfield served in the Department of Joint, Interagency, and Multinational Operations. Mr. Wingfield then deployed to Afghanistan in 2009-10 as Rule of Law Advisor for

COMISAF's Counterinsurgency Advisory and Assistance Team. He served as Professor of International Law at the George C. Marshall European Center for Strategy Studies, where he directed the Program on Applied

Security Studies, and was Professor of Law and Strategy at the newly-established United Arab Emirates National Defense College in Abu Dhabi, UAE.

Mr. Wingfield holds a B.A. in History and Russian Language (summa cum laude) from Georgia State University, and a Doctor of Laws (J.D.) and a Master of Laws (L.L.M., with distinction, International and Comparative Law) from the Georgetown University Law Center. He is the author of *The Law of Information Conflict: National Security Law in Cyberspace* and is one of the drafters of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, 2013). A former Chair of the American Bar Association's Committee on International Criminal Law, he is a member of the State Bar of Georgia, the District of Columbia Bar, and the Bar of the United States Supreme Court. His wife Kim is a Professor of Renaissance Art History, and they have two children.

Sounil Yu

Sounil Yu is currently the CISO-in-Residence at YL Ventures, where he leverages his 30+ years of industry experience to support the due diligence process, vet entrepreneurs, and evaluate startup ideas. Sounil proactively supports the ideation processes of up and coming entrepreneurs and advises them on greenfield opportunities in cybersecurity.

He is the creator of the Cyber Defense Matrix and the D.I.E. Triad, which are helping to reshape how the industry thinks about and approaches cybersecurity. He serves on the Board of the FAIR Institute and SCVX; co-chairs Art into Science: A Conference on Defense; volunteers for Project N95; contributes as a visiting National Security Institute fellow at GMU's Scalia Law School; and advises many security startups.

Previously, Sounil was the Chief Security Scientist at Bank of America, leading a cross-functional team focused on driving innovation and a thriving startup culture to meet emerging cybersecurity needs, to serve as a challenge function, and to be a change agent driving unconventional thinking and alternative approaches to hard problems in security. Prior to Bank of America, Sounil managed a practice at Booz Allen Hamilton focused on helping clients establish a security program, discover and respond to intrusions, and increase the maturity of existing security functions.

Sounil co-chaired the OpenC2 standards group, was recognized by Security Magazine as one of the most influential people in security, and has 22 granted patents. In addition to CISSP and GSEC certifications, Sounil holds a master's in Electrical Engineering from Virginia Tech and bachelor's in Electrical Engineering and Economics from Duke University.

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.