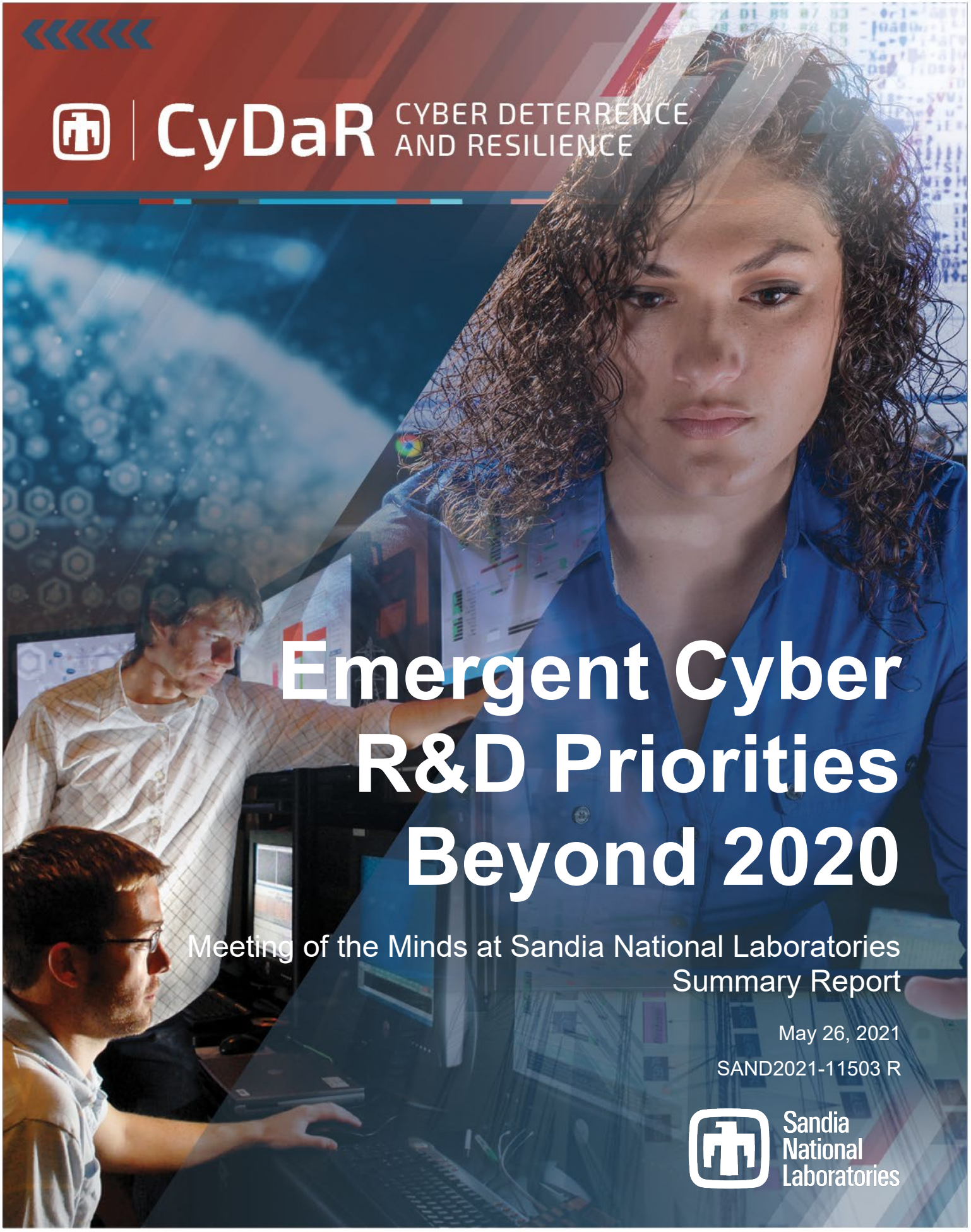


Emergent Cyber R&D Priorities Beyond 2020

Meeting of the Minds at Sandia National Laboratories Summary Report

May 26, 2021

SAND2021-11503 R

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.

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/

This page left blank.

SUMMARY REPORT

Emergent Cyber R&D Priorities Beyond 2020

Meeting of the Minds, Sandia National Laboratories

May 26, 2021

Prepared by: Mathias Boggs, Michael F. Minner, and Eva C. Uribe

TABLE OF CONTENTS

ACRONYMS

Abbreviation	Definition
AI	Artificial Intelligence
CIKR	Critical Infrastructure and Key Resources
COVID-19	Coronavirus-19
ICT	Information and Communication Technology
IoT	Internet of Things
MFA	Multi-factor Authentication
ML	Machine learning
NCF	National Critical Function
R&D	Research and Development
ROI	Return on investment
SBOM	Software Bills of Materials
SDK	Software Development Kits
SNL	Sandia National Laboratories
SQL	Structured Queried Language
U.S.	United States

EXECUTIVE SUMMARY

On May 26, 2021, Sandia National Laboratories (SNL) convened a diverse group of experts spanning private industry, academia, the United States military and federal government, and the national laboratories, and hosted a series of panels to gain their insight on critical emergent research and capability development needs to support national cyber strategy objectives. Two panelists of experts presented their prepared remarks, followed by open discussion from over 250 audience members. The overarching questions guiding each discussion were:

1. How might we advance cybersecurity in the public interest through strategic research and development (R&D) investments?

2. In an increasingly complex and integrated digital world, how do we make progress on the two intractable problems of secure, low-defect software and the authentication of trusted users?

This summary report incorporates ideas shared by participants, both panelists and audience members, without attribution. Where appropriate, our team added some additional analysis or context to expand on these ideas. The ideas summarized here are not presented in chronological order but have been reorganized to better emphasize themes from across all discussions during the meeting. Key themes include:

Panel 1

- Emerging Technologies in Context of Global Economy and Integrated World
- Cyber Physical Risks to the Nation's Critical Infrastructure and Key Resources
- Combatting Ransomware as a National Priority
- Getting Ahead of These Problems

Panel 2

- Increasing Complexity Results in Poor Security
- The Need for New Cybersecurity Paradigms
- Providing Useful Tools for Developers
- Changing Adversary Cost-benefit Analysis
- Incentivizing and Democratizing Secure Software
- Transparency in Software Development
- A Holistic Approach

AGENDA & PANEL TOPICS

Introduction Jen Gaudioso

Panel #1: R&D Priorities in the New National Cyber Strategy

Moderator: Michael Minner

Panelists: Melissa Hathaway, Brian Gattoni, Guy Walsh, Scott Aaronson, Bobbie Stempfley

Overarching Question:
How might we advance cybersecurity in the public interest through strategic R&D investments?

Specific questions:

1. Which R&D investments do you see as most critical for enabling you (or the U.S. government) to achieve strategic goals? Are there areas you think are overlooked or overhyped?
2. What critical gaps do you see in U.S. capabilities as compared to China, Russia, and the rest of the world? How might R&D investments diminish or "leap" the gaps?
3. Who has primary interests in driving forward critical R&D to meet national strategic goals? What might be done to promote coordination and partnership across siloed R&D communities?

Panel #2: Challenges of Solving Systemic Weaknesses

Moderator: Zachary Benz

Panelists: Eugene Spafford, Heather Adkins, Cristin Goodwin, Michael Sikorski, Han Lin

Overarching Question:
Secure, low-defect software and the authentication of trusted users are foundational elements for any cybersecurity strategy. We rely on complex pieces of software for everything from the most critical functions to mundane tasks, yet assessing software for modification or flaws is incredibly challenging. Simultaneously, users are shifting to remote work, requiring access to resources from new devices, locations, and networks. Managing identities, establishing new access policies, and re-evaluating trust poses serious challenges for even the most capable of organizations. How can we make progress on these two intractable and increasingly complex challenges?

Specific questions:

1. What major strategic or systemic weaknesses result from an inability to trust software or users, and what is the potential impact to the public?
2. Where do you see the most opportunity for progress? What are indicators or metrics of progress?
3. What technological processes, techniques, and tools are needed to manage ongoing and future threats in software security and user access management?
4. What other uncertainties or disruptive technology trends are you tracking and how may they change the dynamics of cyber offense and defense in the future?

KEY THEMES

Panel 1. R&D Priorities in the New National Cyber Strategy

Emerging Technologies in Context of Global Economy and Integrated World

The digital transformation of our society continues with the rapid adoption of new technologies and infrastructure. Participants identified the Internet of Things (IoT), 5G networks, and advances in artificial intelligence (AI) and machine learning (ML) as examples of emerging technologies that are driving the global economy. However, this transformation poses risks to the stability and security of our digital and integrated world. An international leadership role in many of these areas requires advanced infrastructure, supportive national policy, and federal strategy that supports agility and security in adoption of emerging technologies. The United States, at present, is not positioned to provide that leadership. In many of these areas, the nation lacks essential elements required to lead. Taking 5G+ as an example, the U.S. lacks a true 5G network, policy solutions to address issues associated with 5G, and concrete plans for 6G and 7G technologies. To support future stability and security, the U.S. should identify areas it intends to lead and cede to others those areas where leadership is not essential to U.S. strategic interests.

Participants noted that today is as simple as it is ever likely to be. Technology and its novel applications will continue to evolve in ways that will challenge society. For example, the pervasive, interconnected nature of digital systems and technologies with all aspects of society has the potential to create greater concentrations of risks that are poorly understood, as seen by recent cybersecurity incidents. This interconnectedness will be compounded as decision making processes feature more automation, as underlying hardware and software grow in complexity, and as more and more data is produced. Before these new technologies are implemented, there needs to be improved understanding of how humans make decisions, the relationship between technologies and decision makers, and the risk of new technologies on an enterprise, regional, and national level.

All of these factors are contributing to the emergence of a new legal and regulatory landscape across the globe as data sovereignty clauses and digital services taxes are introduced. The explosion of data, in particular, is driving an intractable, vicious cycle of analysis, as new innovations and technologies generate more data that must be efficiently analyzed and stored. These vast stores of data can become attractive targets themselves, requiring additional security measures and perpetuating the cycle. As AI and ML are applied to new domains, concerns over assurance and uncertainty must be addressed. Decision makers need to be able to understand how information is derived from these applications, their limitations, and potential risks of the methods themselves.

Cyber Physical Risks to Nation's Critical Infrastructure and Key Resources

Ensuring the security and reliability of the nation's various Critical Infrastructure and Key Resources (CIKR) in the face of evolving cyber threats[1] is a critical challenge for public, private, and additional stakeholders to address. Due to the interconnected nature of CIKR and the compounding effects of newer risks posed by climate change, the widespread adoption of emerging technologies, and more, stakeholders should strive for unity of effort and unity of message in advancing the security posture of CIKR entities overall.

While cybersecurity is a shared responsibility across all sectors, participants highlighted the nation's energy grid when discussing foundational elements to CIKR cybersecurity. Recommendations included establishing security standards and improved posture, partnerships for testing and

[1] CISA: Significant Historical Cyber-Intrusion Campaigns Targeting ICS. https://us-cert.cisa.gov/ncas/current-activity/2021/07/20/significant-historical-cyber-intrusion-campaigns-targeting-ics

communication, and response and recovery efforts to quickly mitigate incidents. Owners and operators of CIKR can also partner with industry and other stakeholders to test new technologies and solutions prior to operational deployment. Participants stressed that current market forces do not incentivize the design of secure products for CIKR stakeholders, as large information and communication technology (ICT) companies are incentivized for speed, cost, and performance over security, while security companies are incentivized to work with, and profit from, poorly secured products. The "release first, patch later" approach is prevalent but not necessarily the best model for the cybersecurity of ICT solutions in CIKR, as CIKR owners and operators often lack the resources to refresh infrastructure to keep pace with modernization. Government-furnished equipment for consumer grade devices and applications may operate for five to seven years, and cyber-physical systems may operate for 20 or 30 years – both come with vulnerabilities out of the box that can go unaddressed for the entire lifecycle of the equipment. Participants noted that requests from owners and operators of CIKR to establish regulations to address these concerns will always be weighed against industry's concerns for the potential to stifle innovation. Additionally, participants identified a conflict in the U.S. government's continual desire for more information from CIKR stakeholders coupled with a lack of willingness to share information with these same stakeholders.

Combatting Ransomware as a National Priority

Ransomware is a form of malicious software that renders data or services on a victim's device inaccessible, often via encryption, for the purpose of extorting payment. Participants cited the increasing frequency and cost of ransomware attacks as an urgent threat to society that must be addressed. In particular, the growing criminal market for ransomware and its associated drivers, enabling technologies, and lack of consequences require broader solutions.

Participants suggested focusing conversations around securing National Critical Functions (NCFs)[2] to enable public/private partnerships in this problem space. Slowing the spread of ransomware will, in part, require entities across sectors to "do the basics" when it comes to cyber hygiene. Actors understand their targets and the most efficient ways to achieve their goals. As organizations begin to improve their cybersecurity posture overall, adversaries will adapt and begin to use more sophisticated methods to realize their objectives. Participants noted that while common compromise vectors such as phishing may appear to lack sophistication, ransomware operators have demonstrated a capacity to research and pioneer more advanced cyber tradecraft.

The impacts of ransomware spawned additional discussion about the nature of ransomware crime and whether ransom payments should be allowed. Are ransomware attacks the equivalent of terrorist attacks, or are they mostly about transnational criminal organizations making money? Some participants emphasized that the applications of ransomware that society is witnessing are not solely about the money. Instead, ransomware actors have targeted law enforcement, government, critical infrastructure, hospitals, schools, and more with the intention of imparting psychological fear and undermining trust in our institutions. However, participants did not reach a consensus to answer this question. Participants also discussed the rise in ransomware insurance, in which consumers can pay insurance companies to negotiate with ransomware actors and/or ultimately pay ransom. Participants noted that insurance companies have a significant stake in this market, and changes to insurance policies, such as increasing the cost of coverage or removing coverage for ransomware attacks, would disrupt the status quo for ransomware actors. However, insurance companies have little motivation to change their policies unless they themselves face negative financial consequences.

[2] NCFs are functions of the government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. https://www.cisa.gov/national-critical-functions

Recent high-profile ransomware incidents, including those before and shortly after this meeting, have brought additional scrutiny and attention to this threat.[3,4,5,6]

Getting Ahead of These Problems

Participants discussed many opportunities for the U.S. to get ahead of these various cybersecurity challenges, a subset of which are summarized here. First and foremost, a national vision needs to come from the White House. This would include setting an agenda for supply chain assurance, developing and deploying secure 5/6/7G infrastructure, improving identity management, and enhancing the security and resilience of CIKR to maintain the functions of government, military, and civil society.

The U.S. will need to develop tools and techniques to analyze complex software and hardware at scale, develop security architectures for emerging technologies, and learn how to maintain operations even when using networks and systems that are not trusted. Developers should strive to incorporate security principles and capabilities at the component level, earlier in the development lifecycle, rather than later in the development process. Key stakeholders will need to right-size requirements with the R&D community to incorporate future planning and set up a pipeline for innovations. Investments are needed to bring down the extended horizons for R&D to within the three to five years timeframe so that new outcomes can be incorporated in federal funding cycles. This should be coupled with research from a variety of perspectives to understand the impacts of adopting emerging technologies, including benefits of adoption, changes in attack surface, and how malicious actors will respond. For example, participants noted the potential for adversaries to poison or distract AI and machine learning-based tools in order to manipulate responses. Additional work is needed to improve the resiliency of federal, CIKR, and other networks and systems in the face of cyber threats, including resiliency metrics, operating in a degraded state, and, if needed, failing safe.

Federal and industry stakeholders need to improve how they share information. This includes separating the generation of information and intelligence from the timely dissemination and use of that information to support decision makers at mission speed. Additionally, the U.S. should foster an ecosystem for partnerships between government, industry, academia, and international allies to drive innovation and improve coordination and communication. For the private sector, the desire to protect intellectual property or to preserve corporate reputation may cause reluctance to share information needed for collective security. Additionally, a whole private industry has emerged to monetize threat intelligence; these companies may be reluctant to share information to preserve their market value. Within the government, cyber threat intelligence is often classified and not widely disseminated to key stakeholders. On all sides, there are not enough incentives to share information. Participants also emphasized the need to expand the cyber workforce and address gaps by promoting education and skill development, expanding the diversity of recruitment and outreach initiatives, and creating opportunities for users to embed with developers to improve security and usability of security features, among other efforts.

---

[3] Stop Ransomware. https://www.cisa.gov/stopransomware

[4] Second FinCEN Exhcnage on Ransomware to Take Place in August. https://www.fincen.gov/news/news-releases/second-fincen-exchange-ransomware-take-place-august

[5] Rewards for Justice – Reward Offer for Information on Foreign Mlalicious Cyber Activity Against Critical Infrastructure. https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/

[6] Ransomware Task Force Release Comprehensive Framework to Combat Ransomware. https://securityandtechnology.org/ransomwaretaskforce/

Panel 2. Challenges of Solving Systemic Weaknesses

Increasing Complexity Results in Poor Security

Participants noted that current security strategies have led to an overwhelmingly complex security environment. Experts are no longer able to understand security systems end-to-end, but instead have become increasingly specialized in their expertise. Much of this is due to what participants called the "penetrate and patch" approach to security. Because this approach to security is responsive and does not address all of the problems at once, new layers of security are continually added over time, such as firewalls, intrusion detection, outbound monitoring, and cloud security. Complexity is known to be one of the biggest factors in poor security, and with the current model, complexity is increasing all the time. Consumers purchase technology with no knowledge of how it works on a fundamental level, while vendors profit from selling systems that presume investment in security on the consumer side. Yet, not all consumers have a large operational cybersecurity budget.

Additionally, the added complexity has led to a major shortage in trained security personnel. The United States will need over a quarter of a million new security personnel to manage security, and the world will need more than 2.5 million new security personnel. There are not that many new cyber employees entering the workforce, and there is little incentive for computer network and information technology experts to go into security fields, which tend to be less lucrative. Participants identified a need to either find ways to reduce the complexity of security systems or find ways to incentivize more security personnel to take these positions.

Cybersecurity is increasingly complex, and the COVID-19 pandemic has laid bare the complexity and security negative feedback loop. As more people transition to working at home or working on-the-go, more people are connecting more of their personal and professional devices in more and more varied ways. People increasingly lack boundaries between their personal and professional lives. Individuals are targeted in their personal lives to effect consequences in the corporate or government world, and the negative consequences manifest at the individual, institutional, national, and international scale. We live in a fully connected, digital world.

The Need for New Cybersecurity Paradigms

Rather than adding to the layers of security that exist, we need to rethink the landscape and create environments that emphasize security and resiliency. Students are taught to set up systems the same way today as we did 20 years ago, but the threat environment has evolved and the current strategy continues to fail. For example, despite the millions of dollars spent on security, the SolarWinds exploitation showed that adversaries using publicly available malware were still able to avoid detection for over a year. With this failure in mind, participants noted that the solution is not to add more layers of technology for security. Instead, we need to rethink how we design and deploy systems. We need to change what we expect systems to do and what we expect users to do. An analogy was made to telephone landline usage at the turn of the century. Bell Technologies estimated that telephone usage would become so widespread that every person in the United States would be required to become a telephone operator in order to meet the demand. They adapted the technology so that people did not have to become experts in order to effectively operate a telephone, which effectively made everyone an operator.

Changing the paradigm will not be simple. It will require constant adjustments and reassessments. Developers will need to focus on security during the research and development phases of their products, not just after the product is created. But there are examples of companies changing the landscape in the past. After struggling with how to address phishing and other campaigns targeting employee passwords, Google changed their operating environment to make passwords irrelevant,

instead turning to security keys and multi-factor authentication. The challenge is one that requires a change in the cyber environment, and a focus on security throughout software development.

Participants asked how progress can be made on systemic weaknesses like software provenance without a common baseline, a common expression of return on investment (ROI), and without a common set of metrics for progress. A key problem here is that there is no broadly accepted definition of *security*, and no standardized way to measure security. We have no standard way of measuring if we are *more* secure or *less* secure after implementing a new system or protocol. As unspecified system can never be wrong or incorrect, only surprising. Our systems are not inherently insecure, wrong, or malfunctioning; they are simply surprising us.

Security may be the wrong paradigm, as a singular focus on incident prevention means that we are not designing functional systems. If we spend all of our time trying to stop an intruder from gaining access to our systems, this means we have not designed our systems to be fully functional under the range of conditions that exist. We should borrow more concepts from the reliability and safety communities, which prioritize sustaining key critical system functions under adverse conditions. When a system fails, the main objective is not to pick up the pieces, but rather to reestablish operations and prevent further failure from occurring. *Security* often excludes these key concepts.

Providing Useful Tools for Developers

One way to promote secure software at the development stage is to make useful tools free to developers. On average, there are between one and 25 vulnerabilities for every 81,000 lines of code that are written. We touch millions of lines of code every day before we even get to work. Because insecure software impacts everyone, we need to find ways to improve how software is developed. Currently, the tools that are provided to developers focus on functionality and speed. However, we also need tools that focus more on security. To do this, we need to invest in tool-chain improvements. Participants provided a number of suggestions, such as:

- Coding programs that automatically help programmers avoid mistakes and vulnerabilities;
- Codes that automatically check for buffer overflow;
- Templating libraries to generate safe code and help avoid structured queried language (SQL) injection;
- Tools that automatically check your code every day, ensuring that changes don't lead to vulnerabilities; and
- Automatic stress-testing of code with techniques such as automatic fuzzing.

These types of tools can help ensure that software is more secure from the start, detecting software vulnerabilities before they are released rather than taking the penetrate and patch approach. Participants asserted that these types of tools should be automatically included in software development programs, free for all to use. They should not be an extra component that needs to be purchased or added separately. If these tools were added to our software development programs, we could produce more secure code without added time and expense. This would be especially beneficial in reducing vulnerability of IoT devices.

Changing Adversary Cost-benefit Analysis

As the discussion focused on U.S. R&D needs, some of the discussion included threats facing the United States in cyberspace. Participants noted that adversaries and criminals have used relatively simple techniques to exploit vulnerabilities in our systems. These include phishing, password spraying, spoofing, and man-in-the-middle techniques. Our adversaries continue to use these tactics because, despite their simplicity, they are effective in enabling adversaries to achieve their goals. This highlights

the need to improve basic cyber hygiene. Accounts that have been compromised are almost always lacking multi-factor authentication, and computers that are compromised almost always have patches available but not installed. As we seek solutions for some of the more complex adversary tactics, we also must prioritize cyber hygiene and implement known security solutions where they exist. Ensuring that we patch our systems, provide identity protection, monitor our systems, and enable multi-factor authentication will go a long way in defending our organizations against current adversary methods.

However, getting rid of "low-hanging fruit" will not eliminate all of the risk. Attackers are innovators, and they will turn to new tactics to achieve their goals. While this is expected, if we can force adversaries to change to more difficult tactics, this will change their cost-benefit analysis, as these tactics will be more expensive to carry out.

Participants also noted that while improving safety and security of our systems is important, there is also a need for more disruptive actions against adversaries. There are tools that organizations can implement to mislead attackers and affect adversary communications. These tools can be helpful in protecting those organizations. There is also a continued need for the U.S. government to lead efforts against adversaries that will penalize them and make it harder and more costly for them to carry out malicious acts.

Incentivizing and Democratizing Secure Software

Another key theme of the discussion was that the market does not currently incentivize creating secure software. The current market sees consumers taking the blame for vulnerabilities and exploitation of networks and software. Participants argued that consumers are punished while producers, attackers, and cybersecurity companies all benefit from the current market structure. Producers continue to develop new software at a lower cost, patching when vulnerabilities are discovered. Attackers are able to exploit vulnerabilities for financial gains. Cybersecurity organizations have stepped in to provide security services to consumers, but they also benefit from cyber exploitations as their services are deemed more essential. In essence, producers, attackers, and security companies each benefit from the focus on inexpensive, less-secure software production. To solve the problem, there needs to be a shift that emphasizes security in software research, design, and development.

Participants discussed possible steps to incentivize software security. For example, during the development phases of new software, some companies provide rewards for discovering vulnerabilities and breaking their systems. Rewards for vulnerability discovery can create positive incentives that will ultimately test and improve the security of these products.

Better tools need to be provided to developers as well. The global democratization of coding necessitates safe, accessible, ubiquitous tools. For example, participants noted the benefits of Software Development Kits (SDKs), which have default containerized permissions. Use of these tools make it easy for people on the developer and consumer side to behave securely without having to become experts. This leads to a fundamental question: Which types of security should be free and default to consumers, and which should be optional or additional? The analogy was made to vehicle safety standards. Over the past century, vehicle standards have evolved to include built-in seat belts, air bags, roll bars, and more. Consumers do not have the option to buy a cheaper car with no seat belts. Certain security features should be default and free for all consumers. Some examples of security features that could be made default included passwordless authentication, auto-enrollment in multi-factor authentication (MFA), and digital assistants to help developers and users review, understand, and enable security features that make sense for their usage.

Regardless of the incentives, there needs to be a shift in how we approach this issue. Security can no longer be an afterthought in software development, but instead should be designed into the systems

and their environment. We have the technology and the capability to do this but need a paradigm shift that incentivizes secure products over cheap and rapid production. This will likely need to be consumer driven, with mechanisms for measuring and understanding the level of security included in software development.

Transparency in Software Development

Another possible strategy could be to incentivize security by labeling products based on their level of security, for example, through consideration of security within Software Bills of Materials (SBOMs). Labels could provide consumers with visibility into the development processes and standards of a product, allowing them to choose products based on price, quality, and security. Participants drew various analogies to food nutrition labels, drug facts, and usage warnings printed on consumer products. Security is personal in that it depends on the personal values and priorities within a given context. When choosing to purchase secure products, consumers make similar choices as when they are buying insurance, for example. Without accurate information, consumers cannot properly evaluate costs and risks appropriate for their usage of a product. Content traceability is appealing both because it helps consumers to understand what they are buying and to demand products with security that meets their needs, and because it incentivizes developers to consider what sources of code are going into their products.

Other participants argue that labels have limitations. Consumer education through labeling only works in cases where there are multiple options available to consumers. Labels are also limited by how much consumers know and understand. A food label including information about sodium in a product is only helpful to a consumer that knows that consuming too much sodium can lead to health problems like hypertension, and their individual risk health profile will then inform their purchasing decisions. There is a need to make SBOMs more inclusive of security and to help consumers bridge the knowledge gap. When consumers can identify the links between certain software components and specific risks or vulnerabilities, then they can make informed choices. Several participants also raised the potential for developers to cheat or lie on their labels.

A Holistic Approach

Throughout the discussion, it was clear that it will take a holistic approach to solve the systemic weaknesses that we face. Software producers and consumers each have a role in improving software security. Companies can do a better job monitoring systems and training personnel. Individuals can do a better job following protocol, updating devices, and demanding secure products. R&D teams can do a better job thinking through security as they design new systems and tools. Government can do a better job creating incentives and structures that encourage better security. Each of these together can lead to improvements, but only focusing on one aspect will fail to achieve the necessary changes.

One participant highlighted six necessary components to addressing these issues:

1. Technology
2. Government Influence/Legislation
3. Developer awareness
4. Software Security from the Start
5. Economic Incentive
6. Consumer Education

Along with these six points, there is a need for us to reshape the environment in ways that will allow and promote better security.

This page left blank.

SPEAKER BIOGRAPHIES

Scott Aaronson

Vice President, Security and Preparedness, Edison Electric Institute

Scott Aaronson has been with the Edison Electric Institute (EEI) since 2009 when he joined the government relations department focusing on security and several emerging technology issues, including electric grid modernization, cybersecurity policy, and telecommunications priorities. He now leads EEI's security and preparedness team where he focuses on industry security and resilience initiatives, establishing collaborative partnerships between government and electric companies—and across critical infrastructure sectors—that enhance security for the energy sector.

In addition to his role at EEI, Scott also serves as the Secretary for the Electricity Subsector Coordinating Council (ESCC). The ESCC is the primary liaison between senior government officials and industry leaders representing all segments of the sector. This partnership is held up as a model for how critical infrastructure operators can work with government, yielding dramatic improvements in security and preparedness for the electric power sector and the nation.

In these roles, Scott has provided testimony before several state legislative and regulatory bodies, both houses of the U.S. Congress, and to the United Nations Security Council. He speaks frequently with national media, is a board member of The George Washington University's Center for Cyber and Homeland Security, and has been a trusted source for policymakers on issues of critical infrastructure security, including both the Pentagon's Defense Science Board and the President's National Infrastructure Advisory Council.

Prior to joining EEI, Scott was a senior adviser to Members of Congress serving the 12th Congressional District of California, including former House Foreign Affairs Committee Chairman Tom Lantos. From 2001 to 2007, he served as an economic policy adviser to U.S. Senator Bill Nelson.

Scott received a Bachelor's Degree in journalism from the University of Colorado at Boulder for his undergraduate studies, and a Master's Degree from The George Washington University Graduate School of Political Management. He also has received continuing education in executive leadership from the University of Pennsylvania's Wharton School of Business. He lives on Capitol Hill in Washington, DC with his wife, two daughters, a mutt, and a not-so-Great Dane.

Heather Adkins

Senior Director of Information Security, Google

Heather Adkins is an 18-year Google veteran and founding member of Google's Privacy, Safety, and Security Team. As Senior Director of Information Security, she has built a global team responsible for maintaining the safety and security of Google's networks, systems and applications. She has an extensive background in practical security, and has worked to build and secure some of the world's largest infrastructure.

Adkins now focuses her time primarily on the defense of Google's computing infrastructure and working with industry to tackle some of the greatest security challenges. She is co-author of Building Secure and Reliable Systems (O'Reilly, 2020) and has advised numerous organizations on how to adopt modern

defendable architectures. She is passionate about the security of election systems, and has consulted as part of the Defending Digital Democracy project at the Belfer Center for Science and International Affairs, John F. Kennedy School of Government at Harvard University.

Zachary Benz

Senior Manager, Cyber Security, Deputy Chief Information Security Officer, Sandia National Laboratories

Zachary ("Zach") Benz is the Senior Manager for Cyber Security and the Deputy Chief Information Security Officer at Sandia National Laboratories. His team is responsible for meeting the day-to-day challenge of defending, protecting, and assuring the cyber security of all National Nuclear Security Administration (NNSA) information systems for the lab's multi-mission national security role.

Mr. Benz has over 20 years' experience in cyber systems research, analytics, data science, and system design. He is the former leader of SNL's Emulytics™ program, which is dedicated to developing quantifiable characterizations of security in complex, distributed cyber systems through the considered application of modeling and simulation. Over his career he has worked with customers across the national security landscape, to include the Department of Defense, civilian government, and the Intelligence Community.

Prior to working at SNL, Zach worked in the private sector designing embedded signal processing systems for novel noninvasive medical devices at a biotechnology startup, and at an early stage technology start-up developing an app store platform for two-way pagers.

Brian R. Gattoni

Chief Technology Officer for the Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

Brian R. Gattoni is responsible for the technical vision and strategic alignment of CISA data and mission services to manage risk to federal networks and critical infrastructure. CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

Previously, Mr. Gattoni was the Chief of Mission Engineering & Technology responsible for developing innovative analytic techniques and new approaches to technology insertion to increase the value of DHS Cyber mission capabilities. In 2015, Mr. Gattoni was named the DHS Systems Engineer of the Year. Prior to joining DHS in 2010, Mr. Gattoni served in various positions at the Defense Information Systems Agency and the United States Army Test & Evaluation Command.

Mr. Gattoni holds a Master of Science Degree in Cyber Systems & Operations Planning from the Naval Postgraduate School in Monterey, California, and is a Certified Information Systems Security Professional (CISSP).

Jen Gaudioso

Director, Homeland Security and Defense Systems Center, Sandia National Laboratories

Jen Gaudioso is the Director of the Computation and Analysis for National Security Center at Sandia National Laboratories. She is also Program Area Director for the Homeland Infrastructure Security and Resilience Program (HISR) within SNL's Energy & 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 Computation and Analysis for National Security 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 SNL's contributions to the next-generation Nuclear Command, Control, and Communications (NC3). She also coordinated an SNL-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 SNL 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 SNL 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.

Cristin Flynn Goodwin

Assistant General Counsel of the Digital Security Unit in Microsoft's Customer Security and Trust Organization

Cristin Flynn Goodwin is the Assistant General Counsel of the Digital Security Unit in Microsoft's Customer Security and Trust organization. The Digital Security Unit includes Microsoft's Threat Context & Analysis team, and the Cybersecurity Legal team.

On the threat context side, Cristin's team leads Microsoft's efforts to understand nation state attacks against its customers and the computing ecosystem and disrupt nation state attacks. The Threat Context & Analysis team tracks activity in Russia, China, Iran, and other areas, working closely with the Microsoft Threat Intelligence Center (MSTIC).

On the legal side, Cristin's team provides a focal point for addressing complex cybersecurity legal problems across Microsoft, including legal support for MSTIC and advanced incidents with the Microsoft Security Response Center (MSRC), cybersecurity law and compliance; election law and legal support for Microsoft's Defending Democracy initiatives; national security law, and support for the Government Security Program for information sharing and assurance with governments around the world.

Cristin joined Microsoft in 2006, where she initially served as policy counsel in Microsoft's Washington, DC office. Prior to joining Microsoft, Cristin worked for several telecommunications companies. She began her career as a trial lawyer in New York City, and worked in the World Trade Center – which cemented her commitment to security for the rest of her career.

Melissa Hathaway

President, Hathaway Global Strategies

Melissa Hathaway is globally recognized as a thought leader in the fields of cybersecurity and digital risk management and has relationships with the highest levels of governments and international institutions. She served in two U.S. presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. She received the National Intelligence Reform Medal, September 2009, and the National Intelligence Meritorious Unit Citation, December 2011, for her leadership. As President of Hathaway Global Strategies, Melissa brings a unique combination of policy and technical expertise, as well as board room experience that allows her to help clients better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategies in this field. Ms. Hathaway has a B.A. degree from The American University in Washington, D.C. She has completed graduate studies in international economics and technology transfer policy, and is a graduate of the U.S. Armed Forces Staff College, with a special certificate in Information Operations. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html

Han Lin

Manager, Cyber Analysis Research Development Department, Sandia National Laboratories

Han Lin is an R&D Technical Manager at Sandia National Laboratories, where he leads the Cyber Analysis Research Development Department. Han and his team have been developing cyber capabilities in the areas of modeling/simulation, secure cloud computing, virtualization technologies, software supply chain assurance, and complex systems decision analytics that were used to support national security missions in collaboration with colleagues at other U.S. Department of Energy national laboratories, the Department of Defense, and the Department of Homeland Security.

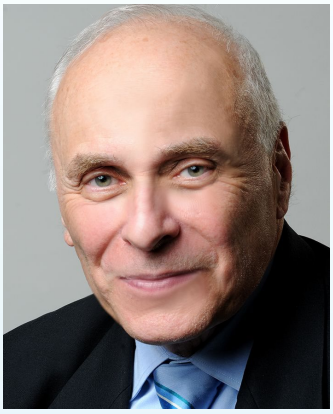
Michael F. Minner

Senior Systems Research Analyst, Sandia National Laboratories

Michael F. Minner is a senior systems research analyst at Sandia National Laboratories. His current work focuses on cybersecurity issues related to emerging technologies, national strategy, cyber deterrence, and emergency preparedness. Prior to joining SNL, Michael obtained his Ph.D. in Mathematics from Drexel University in 2016. His dissertation research focused on Compressive Sensing, addressing applied and theoretical questions related to its use in Multiple-Input-Multiple-Output radar systems. He graduated from Temple University in 2010 with a B.S. in Mathematics and Physics. Michael was also an intern with SNL for two summers before joining full time in 2016.

Michael Nacht

Professor, University of California, Berkeley



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.

Michael Sikorski

Vice President, FireEye Mandiant

Michael Sikorski is the leader of Mandiant Advantage Labs and the FLARE team at FireEye Mandiant. As one of the top enclaves of reverse engineers, threat analysts, and security researchers in the world, they recently helped uncover the SolarWinds supply chain compromise. Michael is an industry expert in malware analysis and wrote the book, "Practical Malware Analysis." He came to FireEye through its acquisition of Mandiant, where he performed incident response. Prior to Mandiant, he conducted research at MIT Lincoln Laboratory and graduated from a technical development program at the National Security Agency. He loves teaching his students to reverse engineer malware at Columbia University.

Eugene H. Spafford

Professor of Computer Sciences, Purdue University

Eugene H. Spafford is a professor of Computer Sciences at Purdue University. He is also the founder and Executive Director Emeritus of the Center for Education and Research in Information Assurance and Security. He has been working in computing as a student, researcher, consultant and professor for 43 years. Some of his work is at the foundation of current security practice, including intrusion detection, firewalls, and whitelisting. His most recent work has been in cyber security policy, forensics, and future threats.

Dr. Spafford is a Fellow of the American Academy of Arts and Sciences (AAA&S), the Association for the Advancement of Science(AAAS), the Association for Computing Machinery (ACM), the Institute of Electrical and Electronic Engineers (IEEE), and the International Information System Security Certification Consortium $(ISC)^2$; a Distinguished Fellow of the Information Systems Security Association (ISSA); and a member of the Cyber Security Hall of Fame — the only person to ever hold all these distinctions. In 2012 he was named as one of Purdue's inaugural Morrill Professors -- the university's highest award for the combination of scholarship, teaching, and service. In 2016, he received the State of Indiana's highest civilian honor by being named as a Sagamore of the Wabash.

Among many other activities, he is chair of ACM Publications Ethics & Plagiarism Committee and is editor-in-chief of the journal Computers & Security.

More information may be found at http://spaf.cerias.purdue.edu/narrate.html

Bobbie Stempfley

Executive Leadership, Dell Technologies

Bobbie Stempfley is currently serving in an executive leadership role at Dell Technologies overseeing the Dell efforts to secure its products and services. Ms. Stempfley has served in executive leadership roles in the Department of Homeland Security and Department of Defense where she led efforts to engage with critical infrastructure, the U.S. Government Department and Agencies, and industry to raise awareness, reduce risks, and prepare and respond to cyber events as the Assistant Secretary for Cybersecurity and Communications. Previously, Ms. Stempfley served as the chief information officer (CIO) of the Defense Information Systems Agency, with responsibility for the digital transformation of a major defense agency to improve the speed and efficacy of the capabilities put in the hands of war fighters and their mission support organizations. She currently serves on the board of the Center for Internet Security, an operating not-for-profit organization providing cybersecurity services for state, local, tribal and territorial governments, adjunct faculty at the Heinz School at Carnegie Mellon University and on an advisory board at the Pacific Northwest National Laboratory.

Eva C. Uribe

Senior Systems Research Analyst, Sandia National Laboratories

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.

Guy M. Walsh

Executive Director, National Security Collaboration Center

Guy M. Walsh is the founding executive director of the National Security Collaboration Center (NSCC). The NSCC, a core initiative at the University of Texas, San Antonio's (UTSA) Downtown Campus expansion, will advance research, education and workforce development in cybersecurity, data analytics, Artificial Intelligence and cloud computing while anchoring the creation of an emerging high-tech corridor to support San Antonio's future.

Walsh brings a wealth of experience in building strategic alliances between federal and state government, academia and industry partners. He is among the nation's foremost leaders in national security as the first strategic initiatives lead for U.S. Cyber Command, one of the Department of Defense's newest

Combatant Commands, which is co-located with the National Security Agency (NSA) at Fort George Meade, Md. His expertise includes cybersecurity operations, international affairs and partnerships, risk mitigation and crisis response, strategic planning and execution, and local and state emergency management.

In 2011, Walsh was hand picked by the NSA's director and commander of the U.S. Cyber Command to operationalize cyber as the newest combat organization in the Department of Defense. His strategic vision led to the creation of Cyber Command's Guard and Reserve Directorate in 2011, where he established numerous partnership and policy initiatives in collaboration with senior officials on the national security staff, Office of the Secretary of Defense, National Guard Bureau, National Governors Association, Department of Homeland Security and Department of Justice.

In 2015, Walsh was a founding member and deputy director of the Capabilities Development Group, charged with integrating USCYBERCOM's prioritized cyberspace capability development to rapidly deliver joint operational products and services required for generating, facilitating and monitoring effects in and through cyber space. He was also a founding member, co-developer and champion for CYBER GUARD, a Tier 1 level exercise to develop a "whole of nation" (federal, state and private sectors) response to cyber threats to U.S. critical infrastructure and key resources.

In addition to his national security expertise, Walsh has significant military operational experience. A career A-10 Close Air Support pilot, Walsh graduated from the United States Air Force Academy, serving as a flight, squadron and group commander prior to his appointment as the commander of the Air Force's 175th Wing, part of the Maryland National Guard. While overseeing the Maryland group's war fighting and emergency readiness from 2002 to 2009, Walsh led the Maryland Air National Guard response to support Hurricane Katrina operations in Louisiana and Mississippi.

In June 2009, Walsh was appointed by President Obama and the Secretary of the Air Force to serve as the inaugural commander of the 451st Air Expeditionary Wing (AEW) in Kandahar, Afghanistan. As the senior Air Force commander delivering airpower for U.S and NATO combat operations in Afghanistan, the 451st Wing was composed of 1,400 personnel charged with conducting full-spectrum combat air operations in support of 100,000 U.S. and coalition forces. Under his leadership, the 451st AEW provided close air support, intelligence, surveillance and reconnaissance, tactical airlift and airdrop, aero medical evacuation, command and control and combat search and rescue operations throughout Afghanistan.

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.