TR-1205/18

# Cybersecurity Policy and Planning

## Technologies for Keeping the Nation Safe

Abraham Wagner, Thomas Garwin, Nicholas Rostow,
Sophia d'Antoine and David Aitel

CAST
CENTER FOR ADVANCED STUDIES ON TERRORISM

The Center for Advanced Studies in Terrorism (CAST) is an independent, non-profit policy research organization that aims to improve policy and decision making for the public interest through research and analysis. CAST's publications do not necessarily reflect the opinions of its research clients and sponsors.

The research described in this report was sponsored by the Defense Advanced Research Projects Agency (DARPA) under Contract No. GS00Q10ADU108. The views expressed are those of the authors and do not reflect any policy or position of the sponsoring agency.



*www.terrorstudies.org*

# Preface

The December 2017 *National Security Strategy* and the January 2018 *National Defense Strategy* set forth the Trump Administration's plan for meeting worldwide challenges the nation faces for keeping the nation safe at a time of changing technologies employed by adversaries, whereas the February 2018 *Worldwide Threat Assessment of the US Intelligence Community* identifies increasing threats of cyberattack.

As the "birthplace" of the Internet and cyberspace the Defense Advanced Research Projects Agency (DARPA) continues to play an important role in the development of technologies that support vital national security missions including the challenges of cybersecurity. In the 1960s ARPA, as it was then known, initiated this new technology with no sense that it would evolve into the largest media revolution in history. At that time there was no need for a national strategy or policy for this resource.

Since then the world has seen radical changes never anticipated – at DARPA or anywhere else. Technology evolved into a connected world where communications and information technology across all sectors have become reliant on this infrastructure. Along with a myriad of benefits, cyberspace has also become a domain for crime, espionage, and warfare. Now there is a compelling need for national policy and strategy to address both existing and emerging cybersecurity problems.

Meeting this need, however, requires a strategy that is both consistent with current national policy guidance as well as an understanding of the threat environment and technology path. The present study grew out of a concern that a policy, strategy and plan for cybersecurity did not exist, and an effort to articulate them would be useful to those with cybersecurity responsibilities.

Members of the study team had already been working on this problem as members of the Presidential transition study, *Fixing America's Cybersecurity: A Plan for Cyber Policy and Organization* (January 2017) reflects these concern and awareness of the incoming Trump administration for this critical national policy area. Subsequently the President's May 2017 *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

reflected concerns raised during the transition and directed timely studies that would form the basis for longer-term solutions and policy.

Such an enterprise is not new or unique, but what is new is the speed at which cybersecurity problems arise and the need to respond in a timely fashion to the changing threat environment. The technology revolution that began with the ARPAnet and the Internet is being played out today in network technology, communications, and social media that were largely unanticipated, as was the rapid adoption of new technologies and applications.

Major sectors, including national security, power, finance, and others quickly adopted these technologies and became highly dependent on the commercial infrastructure enabling them. Needed investments in technology to secure this infrastructure were not made. Now vulnerabilities are more broadly recognized, and the government more committed to addressing them.

The present analysis is the work of a team including national security specialists, cybersecurity professionals, and legal experts examining the broad set of policy, technology, legal, and other issues involved. This effort recognizes the major dynamics involved, and that the world of today continues to change.

Cybersecurity issues are greater than any individual agency can address within its charter or available resources. Because these problems affect the entire Federal government and the nation, the intention here is to illuminate the context within which DARPA and others can work to meet these critical challenges and provide an innovative technology path to help in keeping the nation safe.

# Contents

# Acknowledgements

This study was made possible with support from the Defense Advanced Research Projects Agency (DARPA). We are enormously grateful to the DARPA Director, Dr. Steven Walker, as well as DARPA's Information Innovation Office (I2O) for their support, guidance and assistance with this study.

We would also like to express our gratitude to the late Dr. Paul Kozemchak, Special Assistant to the DARPA Director, for his tireless advice and counsel throughout the process until his untimely passing. This study is dedicated to his memory.

The study team has also benefited greatly from the work of several research assistants, currently students at Columbia Law School and Yale Law School, as well as insightful comments and suggestions from various individuals with extensive government and industry experience who have been generous enough to provide their counsel. Here special thanks go to Edward Doyle, Ryan Stortz, Albert Carnesale, Daniel Gallington, Col. Gary Brown (USAF, Ret.), and Anthony Cordesman.

# Executive Summary

The December 2017 *National Security Strategy,* the January 2018 *National Defense Strategy* and the February 2018 *Nuclear Policy Review* set forth the Trump Administration's approach to meeting the global challenges facing America and to keeping the nation safe at a time of changing threats and technologies employed by potential adversaries including those posed by cyberattacks. This strategy places a high priority on meeting cybersecurity goals that support deterrence and responding effectively to cyberattack and information warfare.

The digital revolution created a world where digital data has replaced analog files and other antiquated media while most of the world's communications and information technology systems have become part of a "connected world" dependent on the Internet network infrastructure. Neither government nor the private sector anticipated the speed of this technology revolution and the challenges it would pose.

Cybersecurity issues related to hacking, vulnerability, denial of service, and information warfare are now matters of great concern involving not only vital national security operations but power, finance, and other critical sectors. The concepts of defense and national security have needed to adapt, and now incorporate cyberwarfare as a major conflict domain.

Deterrence has long been fundamental to U.S. national security strategy and remains so today. Potential adversaries, including nation states and non-state actors such as terrorist groups, have been deterred from attacking the U.S. and allied nations because of the unacceptable costs from retaliation, both conventional and nuclear. As the range of possible attacks now includes cyberwarfare, policy and strategy for deterrence incorporate this new domain of espionage and warfare.

## The Challenge of American Cyber Vulnerability

National security as well as other critical sectors remain vulnerable to cyberattack while near-term prospects for eliminating these vulnerabilities are not good. Almost total dependence on commercial network infrastructure, however, complicates this task even for national security networks and

systems. A cyberattack could impede U.S. military efforts, exploiting vulnerabilities so that the U.S. would be deterred from military action by the threat of cyberattack. Such threats come not only from advanced countries such as China and Russia, but also from smaller adversaries such as Iran, North Korea, and terrorist organizations.

The President's May 2017 Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* focuses on protection at the national level, building on agency priorities for international efforts including "investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation."

Policy choices have crucially affected the evolution of the cyber domain. The Internet was not initially designed with security in mind, and many attributes that contribute to cyber vulnerabilities also favor privacy and anonymity valued by many Internet users. Unlike kinetic warfare, cyber is "unterritorial" in nature, so some concepts and strategies based on a territorial world become problematical. In the cyber world geography is irrelevant.

## The Role of Deterrence in Dealing with U.S. Cyber Vulnerability

After the U.S. became vulnerable to Soviet and Chinese nuclear attack, a nuclear standoff was widely recognized as limiting actions by all sides that affected each other's' vital interests. American strategy aimed to keep nuclear weapons relevant beyond deterring an attack on the U.S., extending deterrence to forestall coercion of allies based on local force imbalances and to prevent use of biological and chemical weapons.

National policy now recognizes that cyberattacks and cyber "weapons" have entered the domain of warfare and military strategy. The national security community has not yet achieved consensus or settled policy on applying deterrence to global challenges including the threat of cyber warfare – either by the threat of retaliation within the cyber domain or by threats of retaliation through other means.

## Continuity with Criminal Activity, Espionage and Cyberwarfare

Prior to the onset of conflict it is difficult to distinguish "cyberwarfare" from "cyberespionage" – i.e., actions that begin appearing as clandestine operations later revealed to have enabled damaging attacks equivalent to significant military operations. While the use of nuclear weapons – "the nuclear threshold" – provided a clear red line and certainly never to happen in

peacetime, cyber operations including hostile entry networks, denial of service and information operations occur frequently. Similarly concerns about proliferation of nuclear weapons to non-state actors were exactly that, while tools for costly cyberattacks are already used routinely for criminal purposes and are also in the hands of non-state actors such as terrorists.

The continuity of criminal activity and espionage with cyberattack complicates cyber deterrence but also is a reason for paying close attention to the options available for "peacetime" responses on the deterrence of serious cyber intrusions and attacks. Dealing routinely with malicious cyber intrusions offers an opportunity to think differently about deterrence and tailored responses in the cyber domain and how they might impact other domains included in overall national strategy.

### Attack Identification and Timely Attribution

A nuclear detonation is immediately obvious, and in most scenarios, attribution to a particular attacker is readily achieved based on trackable delivery technologies or radionuclide fingerprints affected by weapons design and fissile material origin. In a cyberattack, accurate and timely attribution can be highly problematic. Confidently discerning the attacker's identity and the ultimately responsible party in a timely way remains difficult. An attacker may be able to obfuscate responsibility and motivation using various techniques, such as proxies or loosely aligned groups.

Even if precise attack attribution is achieved based on secret information, the need to protect intelligence sources and methods can too easily preclude an overt response or undermine international and public support if reprisals are attempted without convincing public justification. Improving technical capabilities for timely, usable and convincing attribution is one key to effective overt response and thus to many kinds of effective deterrence. Clear attribution that cannot be used overtly raises the need to consider the possibility of effective covert responses and whether and how the prospect of covert retaliation can be effectively communicated in advance for deterrent effect.

### Variable and Uncertain Precision of Cyber Targeting

For cyber actions, both attackers and responders are affected by the possibility that cyberattacks will escape beyond the original targets and cause more widespread damage than expected. Cyber attacks can cause damage well

below that of a conventional attack that would be a clear act of war, but also may cause farther greater damage than this conventional attack threshold. Diplomatic and economic actions currently dominate U.S. responses to undesirable behavior by state actors in the cyber domain. This condition reflects the difficulty of crafting a coherent doctrine of proportional response and applying it to usually murky facts.

What are the appropriate targets for responding to attacks that may or may not have had full government authorization or reflect the will of the people? And should the response be calibrated to the intended or actual effect, even in the unlikely event that these are both known? And how should any uncertainty in the effects of our own cyber weapons be taken into account? This involved not just proportionality but also how particular responses might result in different escalatory dynamics, assuming an adversary can respond further, and how different responses would affect the robustness of deterrent perceptions of other bad actors in the future.

## Asymmetries in Digital Vulnerability

It is generally believed that the U.S. gains greater benefit from technology than most potential cyber enemies, creating an asymmetric "cyber dependence" and a corresponding asymmetric cyber vulnerability. The U.S. economy and military forces have many points of reliance on the Internet and commercial infrastructure and this larger cyber "attack surface" is further assumed to increase our vulnerability to catastrophic attack, as compared to less advanced states. Possible attacks by non-state actors serving the interests of nation state adversaries also create problematic asymmetries.

While these concerns are real, they may be offset by other characteristics. Less-advanced states may have prioritized rapid adoption of digital technologies and not emphasized protection or resilience, resulting in extreme vulnerability or fragility. Advanced states including the U.S. may have effective cyber defenses, with greater resilience and incident response capacity. Only individual and detailed net assessments can lead to judgments of relative vulnerability and advantage.

## Cybersecurity as a Mission Area

Cyber deterrence presents complexities not present in nuclear deterrence as there are far fewer bright lines and a great deal more ambiguity between acceptable and unacceptable behavior. Unlike nuclear warfare, or

even conventional warfare, because of the continuity with criminal activity and espionage, cyber defenses are tested daily and so they may be potentially more reliable than nuclear ones. Moreover, cyber operations, again unlike nuclear ones, are generally viewed as authorized both under Title 50 (intelligence authorities) as well as the Title 10 (military authorities) of the U.S. Code.

Cyberattacks on networked systems supporting military and national security operations have the potential for a system-wide debilitating effect on military capability at very low direct cost and conceivably with a degree of deniability. The U.S. must ensure that deterrence of a cyberattack prevails over enemy cyber threats aimed at constraining foreign policy.

## Deterring Cyber Attack

Deterrence by threat of retaliation, no matter how focused and improved, is unlikely to be a silver bullet for preventing cyberattack, and so reducing cyber vulnerability and improving resilience remains essential. Resilience is improved by mitigating vulnerabilities, eliminating unnecessary complexity, and reducing brittleness in IT systems supporting national security. Since deterrence relies on the enemy's cost-benefit calculation, reducing vulnerability and improving resilience also increases the effectiveness of deterrence.

It is also clear that there is a need to characterize adversary capabilities, as well as for technical and operational capabilities for active defenses and preemption utilizing cyber tools. These could be supported by kinetic attacks on communication nodes and lines if needed.

To the extent that an adversary may rely on a network of proxies it is important to consider the possibility of acting against such networks to reduce their capabilities or willingness to act. The law enforcement strategy of dynamic concentration – deterrence resulting from swift and sure consequences to those engaging in malicious activities – is relevant to controlling proxies if the cost of detection of the behavior subject to sanction is relatively low. A combination of active and passive defenses with web surveillance to achieve these conditions appears to be an optimal strategy.

## Prior Issues in Cybersecurity

The rapid evolution of cyberspace resulted from the merger of several revolutions concurrently in ways that were not imagined or anticipated, including IP and related protocols, a set of communications technologies, and

a media revolution. These technologies also gave rise to a worldwide social and cultural revolution where the use of net-connected devices has become a part of everyday life that was never imagined.

The initial ARPAnet demonstrated that packet switching was far more efficient than traditional line-switching while new communications technologies greatly increased available bandwidth. Developments in computer hardware and networking led to a new world where low cost computers proliferated throughout offices, institutions, schools, and homes. These quickly became connected to a rapidly evolving Internet.

New technologies for mobile devices and a myriad of software applications helped bring about a cultural revolution as well as falling prices for mobile devices and the explosive rise of social media made this technology base a part of everyday life. Social media also became an integral element in aspects of foreign affairs, military operations and terrorist activity.

At the same time the nature of data itself became transformed. As the era of "Big Data" evolved, the world moved from an analog to an almost entirely digital one where physical media of all kinds began to disappear rapidly and digital files on net-based systems became the norm. For its part the Government joined in the stampede into the Internet era with a rapid proliferation of internal networks all utilizing the Internet.

Major sectors including national security, power, finance and others became highly dependent on the commercial infrastructure supporting it. The speed and extent of this transition was unprecedented while the planning and budgeting processes with the government failed to meet the requirements for securing this new world of cyberspace. Adequate investments to secure this critical infrastructure were not made. Today these vulnerabilities are more broadly recognized, and the government is far more committed to their solution. Major issues include:

- *Major Threats Were Largely Ignored:* Systems supporting national security as well as critical sectors are vulnerable to debilitating cyberattack and near-term prospects for eliminating many of the recognized threats are not great.
- *The Internet is Inherently Vulnerable:* The Internet still operates on protocols developed in the 1960s that are inherently vulnerable and inadequate given the role the Internet plays in 21st century society, commerce, and national security.

- *Earlier Cyber Policy Came Without Adequate Resources:* Prior policy directives such as PDD/NSC63, PPD/20, PPD/21 and PPD/41 do not assign critical cybersecurity missions to government agencies capable of dealing with them.
- *Corporations Did Not Act to Develop and Deploy Secure Systems and Infrastructure, as Experts Assumed They Would:* National policy has been made on the incorrect assumption that industry, led by the technology sector, would address major vulnerabilities that were increasingly evident and respond to demand for increased security. The idea that "the market" would respond to demands for increased cybersecurity was a myth.
- *Government Failed to Achieve Needed Partnerships with Industry:* Solving cybersecurity problems requires a strong partnership with key industry sectors, including technology, finance, power and others. This partnership involves not only funded programs, but data sharing, security clearances and other key elements. Without a full and genuine partnership government efforts are doomed to failure.
- *Existing Statutes are Inadequate:* Laws written during and before the Cold War cannot accommodate the realities of cyberwarfare and cybersecurity. Evolution in the legal regime takes place at a glacial pace in comparison to advances in technology. Government and the courts are being asked to apply laws developed for technologies that are generations old and often simply don't make sense.
- *Strategic Information Operations Were Largely Ignored:* While most cybersecurity efforts focus on denial of service, destruction, impairment and use of malware, a major issue remains in the use of the Internet and social media for information operations related to matters ranging from politics to terrorism to geopolitical warfare. Modern media provide opportunities for manipulation of opinion and enable targeting of messages – and these threats will only worsen in the future based on "deep fake" technologies.

## National Policy Goals for Cybersecurity

The challenges of cybersecurity embrace a larger set of actors than traditional national security problems such as kinetic warfare and even intelligence operations. Following World War II, the nation undertook a major

reorganization with the National Security Act of 1947 which established the National Security Council (NSC) as the key instrument for managing the national security process. Executive Order 12333 (1981) assigned specific roles and missions to a rapidly growing Intelligence Community.

After the 9/11 terrorist attacks, efforts were made to solve apparent national security problems with the Homeland Security Act (HSA) of 2002 which created the Department of Homeland Security (DHS) and the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA), which created the Director of National Intelligence (DNI).

National policy for cybersecurity remains in need of such an organizational process, and America must face cybersecurity as it did the threat of nuclear warfare with a programmatic infrastructure capable of meeting the challenge. Specific roles and missions of the relevant agencies must be defined, with an appropriate reporting structure. Also essential is a coordination structure for both analytic, research and operational concerns. Specific policy goals for cybersecurity include:

- *Meeting the Challenge of Cyber Conflict:* National policy recognizes the major role cyber operations will play in any future conflict. This calls for a portfolio of programs as well as the ability to conduct operations where needed – or to have such capabilities available to help deter attacks by potential adversaries.
- *Securing Critical Infrastructure:* Widespread use of Internet technology has rendered critical sectors highly dependent on commercial infrastructure. Existing protocols are highly vulnerable and inadequate for 21st century security requirements. The U.S. needs a network architecture to meet the current challenges.
- *Building a Cyber Workforce:* America requires a workforce capable of confronting challenges in the cyber domain, and the national requirement for skills in the cybersecurity area will continue to grow. Education in this area requires funding for undergraduate and graduate education.
- *Building the Partnership with Industry:* The technology sector, financial sector and others are essential partners in meeting the cybersecurity challenge. DARPA created cyberspace beginning in the 1960s through contracts with industry and university research

institutions, a base which has greatly expanded and is now critical to solving the range of cybersecurity problems facing the U.S.

- *Creating a Responsive Security System:* Personnel in industry, law enforcement and others need timely access to cyber data. Unlike the SIGINT analog which is largely a one-way collection regime, these sectors also see threat data that needs to be shared. Some threat data maintained at the Top Secret and compartmented levels can be downgraded to Secret and shared on a secure network.
- *Repairing the Vulnerabilities Equities Process:* The Vulnerability Equities Process (VEP) is used to determine whether to withhold or disclose information on new software security vulnerabilities so that the software developer has a chance to fix the problem—or the government may choose to withhold the information to use it for various purposes such as intelligence collections and exploitation.
- *Approaching Internet Governance with Realism:* Lawyers and diplomats have invented the field of Internet Governance including issues that are both real and imagined, which conflates management of technical resources with discussion of content behavior. The nation needs to preserve the values and opportunities essential to ongoing Internet operations, recognizing that no government or organization owns, runs or controls the Internet.
- *Reforming Export Control to Serve America's Interests:* America's supremacy in technology is increasingly challenged by China and others while thinking about how to sustain the U.S. advantage through aggressive export control is no longer effective. The U.S. must avoid agreements that are adverse, but also put the nation in a weaker position on cyber security issues.
- *Recognizing That the World is Going Dark and Changing Policies and Programs Accordingly:* Computers, devices and applications are adopting encryption schemes to meet user demands for privacy and security. Legislation to prevent this or work around it is doomed to failure, as this is a worldwide phenomenon and a technology path that cannot be stopped. The U.S. needs to support technical programs that meet this reality.
- *Protecting Digital Privacy and Intellectual Property:* Increasing hacks and theft of data, as well as legitimate surveillance programs have

raised concerns among many Americans. New programs must meet intelligence and law enforcement requirements that also protect privacy interests. The U.S. can no longer allow other nations to steal intellectual property and must increase security against cyber attacks that enable the theft of intellectual property.

## Deterring Cyber Attack – Reducing Vulnerability with Defense

Much recent attention has focused on the vulnerability of critical infrastructure to cyberattack. Credible attack capabilities against not only national security, power, financial and other sectors could significantly damage the nation and its defense capabilities for extended periods. While government and the industry have established some procedures to improve cyber security, the level of protection is obviously imperfect.

The Department of Defense and the military services depend heavily on these key sectors. They have a major interest in ensuring strong cyber protection and deterring attacks with defensive measures that reduce vulnerability. Reducing critical infrastructure vulnerability can be viewed in terms of several types of technology-supported capabilities and interventions:

- *Generally applicable cyber prophylaxis:* Since infrastructure shares common Internet vulnerabilities using applications as entry points, technologies that enhance security at these entry points will help to protect critical infrastructure as well.
- *Mapping systemic vulnerabilities:* Meeting the cybersecurity challenge requires a thorough mapping of systemic vulnerabilities and a corresponding investment strategy for achieving greater resilience of the infrastructure to disruption from any source.
- *Enhanced monitoring of specific threats to critical infrastructure:* Monitoring of specific threats must be combined with active defenses targeted on and tailored to current, emerging, and evolving threats.
- *Strategic, operational, and tactical cyber intelligence:* A range of offensive measures responsive to cyber threats in gray zones is needed. Signatures of attack preparations can be identified to guide this approach.

Existing programs lack an effective means for centralized integration, vulnerability mapping, intelligence sharing, innovative concepts, and technical judgment to focus on the most cost-effective solutions. These investments and

preparatory activities must be accompanied by an operational focus that affords closely coordinated action among national security agencies, domestic federal agencies, corporations, state and local governments, and allied governments.

## Asymmetry in Cyber Vulnerability

Because deterrence by threat of retaliation is not a silver bullet against cyberattack, reducing cyber vulnerability and improving systemic resilience are important. Resilience is improved by mitigating vulnerabilities, eliminating unnecessary complexity, and reducing brittleness in networked systems. Since deterrence relies on the enemy's cost-benefit calculation, reducing vulnerability and improving resilience also increases the effectiveness of deterrence.

Raising uncertainty about whether vulnerabilities are real and suggesting they might be removed can strengthen deterrence and discourage enemy investment in cyberattack, though of course one needs to avoid announcing an impending reduction in vulnerability that could evoke a use-it-or-lose-it spasm in a crisis. Establishing a robust mix of defense, resilience and deterrence to head off cyber threats is critical to national security. The broad focus on deterrence vs. defense may obscure choices that are more familiar from other domains for warfare.

## Resilient Cyber Infrastructure and Networks

Key components of any cybersecurity strategy are initiatives that dramatically increase the resilience of the cyber infrastructure. Programs in this area include ones that not only aim to detect malicious cyber activity, but also seek automated remediation and response to cyberattack. They also need to focus on engineering and software tools to make the network and connected devices more secure, including resilient physical systems and infrastructure.

## Assured Engineering

Embedded and networked systems underlie much of modern technology, ranging from supervisory, control and data acquisition (SCADA) systems to medical devices, computer peripherals, communication devices, as well as vehicles including airplanes and satellites. Networked devices enable convenient access to diagnostic information, perform software updates, lower costs, and improve ease of use. At the same time these systems are vulnerable to remote attack that can cause damage while hiding the effects from monitors.

### Eliminating Vulnerability in Algorithms

As new defensive technologies make vulnerabilities difficult to exploit successfully, adversaries develop new vulnerabilities and exploits based on flawed implementations of algorithms. Once new defensive technologies make vulnerabilities based on flawed implementations more difficult to exploit, however, adversaries will turn their attention to vulnerabilities inherent in the algorithms themselves.

### Automated Repair and Adaptation of Software

As computing devices become more pervasive, the controlling software has become increasingly complex. Despite the resources devoted to making software more robust and resilient, ensuring that programs are correct remains difficult. Uncaught errors triggered during program execution can lead to major problems, runtime failure or other unintended behavior. These can have negative consequences on productivity, reliability of mission-critical systems, and operation of critical cyber infrastructure.

### Code Obfuscation

Reverse engineering of software is not difficult, often requiring no more than a debugger, a compiler and limited effort to de-obfuscate code that has been obfuscated with the best current methods. This relative ease is primarily based on "security through obscurity" strategies, typified by inserting passive junk code into a program's source code.

### Supply Chain Risk - Sensing and Detecting Malicious Behavior

All users rely upon commercial "off-the-shelf" (COTS) hardware, including mobile phones, computer workstations and others which are the product of supply chains involving vendors from many nations providing components, including software and firmware. Supply chains provide adversaries opportunities to insert malicious functionality into this software and firmware that can be exploited to accomplish malicious objectives, including data exfiltration and sabotage.

### Automated Vulnerability Remediation

A critical piece of solving the cybersecurity problem lies in an automated, scalable, capability for vulnerability detection and patching, particularly as more and more systems—from personal devices to major

military platforms—get connected to and become dependent upon the Internet. Currently the manual process of finding and countering bugs, hacks, and other cyber attacks remains antiquated.

### Binary Resilience

Rapid innovation in software and hardware has produced systems that remain vulnerable to attack. Even with less vulnerable hardware and software security improvements that diffuse into the installed base, this process can take years. One alternative is to produce cyber fault-tolerant defensive cyber technology to protect existing and planned systems without requiring major changes to the concept of operations.

### Critical Infrastructure Rapid Recovery

A major goal of national policy is the protection of critical infrastructure from cyberattack. While policy guidance from the prior administration fails to mention the Department of Defense, or assign specific missions in this area to DoD, it is evident that the entire national security community is critically dependent on the nation's critical infrastructure, such as the electric power grid. A major programmatic goal are systems that enable rapid recovery of the grid following cyberattack.

### Internet of Things Protection Using the Analog Domain

A major cybersecurity concern is posed by the rapidly evolving Internet of Things (IoT), the network of physical devices and other items embedded with electronics, software, sensors, actuators, and network connectivity. The IoT has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems.

### Data Integrity

A matter of increasing concern is the integrity of data collected by a wide range of systems as well as open-sources. For imagery the government has operated collection systems that provided imagery with assured integrity. Recently, however, consumer imaging technology such as digital cameras and mobile phones has become widespread, enabling people to take and share images and video instantaneously. Users can manipulate and distort the message of the visual media, and while some changes are benign, others are not, such as propaganda or misinformation campaigns.

## Data Privacy

Respect for privacy is a cornerstone of our democracy, and there is a growing desire to understand, control and manage the "digital contrail" of personal information – data that others could exploit. People have far less control over their personal data or what is done with it, as paper files have been replaced by digital files with data is vulnerable to "hacks," surveillance programs and commercial exploitation. Users are demanding greater privacy and security while suppliers of devices and software are meeting this demand with new products utilizing encryption and other security features. The legal regime can no longer control its application, while large scale collection and analysis of information is used to for online commerce and other applications.

## Configuration Security

Growth of the Internet-of-Things has led to connected devices with minimal security and which remain vulnerable to malware. Connected devices also provide a vast attack surface. While scope of what can now be connected, monitored, and controlled over the Internet has increased dramatically, platform diversity has decreased. It has become necessary to automatically generate, deploy, and enforce configurations of components that address vulnerabilities, minimize attack surfaces and maintaining functionality.

## Cyber Situational Awareness: Behavior and Threat Detection

Essential to cybersecurity is rapid and accurate warning of cyberattack, as well as timely and accurate attribution. Detection of these threats requires adjustments to network and host sensors at machine speed while data required to detect threats may be distributed across devices and networks while perpetrators hide their activities inside DoD and other networks. Current tools do not address the scale and speed needed to collect, share, and respond to threat intelligence. Real-time threat detection is not simply an issue of scale, but also a function of the variable nature of these malicious activities.

## Enhanced Attribution

Any response to cyberattack requires timely and accurate attribution of the attack – be it to a nation-state, non-state actor or some criminal. Malicious actors in cyberspace currently operate with little fear of being caught as it is extremely difficult, in some cases perhaps even impossible, to reliably attribute their actions, stemming in part from a lack of end-to-end accountability in the

current Internet infrastructure. Identities of malicious cyber operators are often obscured by malicious operators to evade defense.

### Social Engineering Defense

The connected world of cyberspace has enabled major advances in national security from pervasive real-time intelligence and communications to optimal logistics but with this has come the threat of cyberattacks on both military systems and critical infrastructure. Most current cybersecurity efforts are focused on computers and networks, more than 80% of cyberattacks come from efforts that exploit humans rather than computer or network security flaws. Cybersecurity therefore requires efforts to not only protect computers and networks but their human users as well.

### Gray Space Operations

Improving network security posture alone is not enough to counter major cyber threats to national security as most botnet nodes reside in neutral networks often referred to as "gray space." Malicious actors are currently able to use collections of compromised and conscripted devices owned and operated by third parties, commonly referred to as botnets with impunity for criminal, cyber espionage, and network attack purposes. The U.S. needs an ability to identify and neutralize botnets and other malware from compromised devices and networks in a scalable, timely, safe, and reliable manner, in accordance with appropriate privacy and other legal constraints.

### Supporting National Security Users

National policy now recognizes the major role cyber operations will play in any future conflict as well as their integral relationship to other aspects of modern warfare. DoD has called for investments in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations as well as major efforts to incorporate cyber operations cyberwarfare into overall planning and operations. This approach includes defensive strategies and programs as well as the ability to conduct strong offensive operations where needed.

### Proactive Cyber Defense

While many cybersecurity issues are new others evoke painful, lessons from the past. A key element of cybersecurity policy is to assess the gravity of the threats and to engage in ongoing tests of critical cyber systems by putting

them under closely managed stress. Proactive cyber defense goes by various terms including "stress testing," "white hat hacking," "red teaming" and "cyber threat hunting" among others. Operationally this may be the only experience of cyberwarfare reality seen before an actual cyber adversary shuts down critical infrastructure and looks at the disastrous results for the America.

## Competing in the Information War

The Intelligence Community recognizes the growing threat played by hostile information operations as a key concern, and the critical role that the information environment is now playing in politics, terrorism, geopolitical warfare and other important areas. In the modern world people have become increasingly dependent on their connected devices, the content they derive from them, and susceptible to the use of techniques of mass manipulation. Most cybersecurity efforts all relate to the defense of the information infrastructure, and various malicious activities that can be undertaken to disable or exploit it. They do not deal with malevolent use of the infrastructure to influence and manipulate entire populations, known as information warfare. Competing in the information war with Russia or other adversaries requires a different set of supporting technologies and operations.

## Implications for U.S. Policy

Current U.S. policy not only recognizes the prospects of cyberespionage and cyberwarfare but integrates them into the broader context of planning for future conflict across a wide spectrum. Trump Administration policy documents articulating these concepts are recent, and those responsible need to develop programs, strategies and operational plans consistent with this guidance. For cybersecurity the May 2017 Executive Order set in motion studies which will provide the basis for moving forward. It is already evident that the U.S. must take several key steps:

- *Reduce Vulnerability:* Reduce the cyber vulnerabilities of national security systems used by the military, Intelligence Community and others as well as their supporting commercial infrastructure.
- *Develop Active Cyber Defense:* Develop active defense capabilities, including tactical and operational offense, focused on adversary capabilities and forces as well as against cyberattack generally; and

- *Pursue Dynamic Deterrence:* Establish effective multi-faceted and multi-level deterrence supplementing defense and resilience with options that would impose unacceptable costs on a cyber attacker and communicating about these capabilities and the will of the U.S. to use them to dissuade potential adversaries and degrade hostile cyber capabilities over time, or at least impede their improvement.

# 1. Introduction: The Policy Context

## 1.1 The Challenge of American Cyber Vulnerability

National security and other critical infrastructure sectors are vulnerable to debilitating cyberattack, while near-term prospects for eliminating this vulnerability are not good.[1] Addressing this threat the Director of National Intelligence has recently stated:

> ***The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits.***[2]

Many U.S. Government systems are vulnerable and at the federal level the government has authority to implement solutions. Government networks and software, however, depend on civilian infrastructure and global supply chains. Government procurement rules and uncompetitive pay compared to Silicon Valley or Wall Street complicate the effort to identify and apply solutions to cyber vulnerabilities wherever located.

The 2017 Defense Science Board Task Force report on Cyber Deterrence suggests that these vulnerabilities might be severe enough to hobble an American military effort in wartime.[3] An adversary might hope to create enough concern about such vulnerabilities that the threat of cyberattack might deter the U.S. A recent *New York Times* article argues that second or third tier countries in terms of their level of overall technology, such as North Korea and

[1] The most recent statement of cyber threats can be found in Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (13 February 2018). There is much expert agreement on these propositions. See, for example, George R. Cotter, *Security in the North American Grid: A Nation at Risk* (April 8, 2015); and Daniel Wagner, "The Growing Threat of Cyber-Attacks on Critical Infrastructure," *Huffington Post* (May 25, 2017).

[2] *Worldwide Threat Assessment of the US Intelligence Community, op. cit.* p., 5.

[3] Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence,* (February 2017). This report underplays the extent that *civilian* vulnerabilities might lead U.S. leaders to forego military action they might otherwise take.

Iran, can rapidly develop effective cyber threats previously thought typical of nations that possess substantial, advanced military-industrial complexes, such as China or Russia.[4]

The President's 2017 Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* makes agency heads responsible for the security of U.S. Government networks, data and for taking steps to modernize federal government IT systems. It also focuses on "deterrence and protection" at the national level and an "engagement strategy for international cooperation in cybersecurity," building on agency priorities for international efforts including "investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation."[5]

The Department of Defense has identified information as a domain of military operations, analogous to land, sea, air, and space. Like these other domains, cyber is home to significant civilian and economic interactions. Unlike them, however, it is wholly constituted by technology, and thus technology is essential in dealing with threats in the cyber domain.[6] This new policy and vision is already being incorporated into planning at CYBERCOM.[7]

Policy choices, and sometimes the lack of explicit policy, have crucially affected the evolution of the cyber domain as the Internet was not initially designed with security in mind. Attributes that contribute to cyber vulnerability also favor privacy and anonymity that are highly valued. Unlike the land domain, cyber has no national borders, though there are protected enclaves that are more defensible, so in that sense there is some topography if

[4] https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

[5] Executive Office of the President, Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (May 11, 2017).

[6] One can argue that technology is required for access to space, air, sea, and land operations to the point that it is required for any military problem, but these domains themselves are still natural and subject to physical constraints rather than being completely the product of human creation.

[7] See United States *Cyber Command, Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, (March 2018).

not geography.[8] Most importantly, few if any key decision makers have adequate knowledge of the technologies they use and would regulate.

Contemporary military operations involve all domains – traditional and non-traditional. All branches of the U.S. and other militaries apply cyber technologies to conduct operations and win. Were the military domains to compartmentalize, hardware and software vulnerabilities would not be nearly so important. Counter-insurgency doctrine and "countering violent extremism" recognize society – not land, sea, or air, as the principal domain of warfare. Even in the realm of nation-state conflict, leaders and the civilian population, and not military forces, are often the ultimate target.

As a mission area strategic cybersecurity shares many characteristics with counter-terrorism, including the role of non-state actors and sometimes states posing as non-state actors or using them as proxies, the prevalence of threats to civilian assets and soft targets in "peacetime," continuity with law enforcement and overlaps with purely criminal enterprise, hardening civilian assets, and the need for international cooperation.

One key difference, of course, is that while terrorist attacks absent weapons of mass destruction pose little threat to the military's ability to perform major national defense missions in wartime, successful cyberattacks could severely degrade DoD's major warfare capabilities.[9] Even where secure and classified systems are involved, they are all highly dependent on commercial Internet infrastructure.[10]

---

[8] The physical carriers of the cyber domain (servers and transmission channels) do largely exist on land and are differentially subject to both physical destruction and potentially legal process or other government access based on their location. Nevertheless, the contrast with the other domains is clear and Jack Goldsmith is in principle correct in saying that in the cyber context "geography is irrelevant." Jack Goldsmith, "How Cyber Changes the Law of War," 24 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1 (2013). See also, Jennifer Daskal, "The Un-Territoriality of Data," 125 YALE LAW JOURNAL 326 (2015).

[9] Arguably IEDs and other terrorist-style attacks have dramatically affected the ability and willingness of the U.S. to perform low-intensity conflict and peacekeeping missions; but serious defense experts are concerned that cyber vulnerability could impede the ability of U.S. forces to properly execute operations – a much greater level of threat.

[10] The extent to which all government communications are almost entirely dependent on commercial infrastructure is not widely appreciated, even among professionals who should be more aware. Government users may employ secure servers, encryption and other technologies, but ultimately, they are all wired to a commercial backbone.

## 1.2 The Role of Deterrence

During the Cold War, once the American continent became vulnerable to Soviet and then Chinese nuclear attack, a nuclear standoff was recognized as limiting actions affecting each other's' vital interests. Despite the standoff strategists found ways to keep U.S. nuclear weapons relevant beyond neutralizing Soviet and Chinese nuclear weapons; nuclear deterrence was extended to forestall coercion of allies based on local conventional force superiority and to prevent use of biological and chemical weapons. Similarly, national security specialists now discuss what role deterrence can play in redressing American cyber vulnerability – either by the threat of retaliation within the cyber domain or by threats of retaliation through other means.

For over half a century the concept of deterrence has been fundamental to U.S. national security strategy. [11] Potential adversaries including superpowers and regional antagonists have been deterred from undertaking kinetic attacks on the U.S. and allied NATO nations because of the prospect of retaliation involving unacceptable costs. Formally developed with respect to nuclear weapons, deterrence theory has increasingly been applied to non-

[11] Deterrence theory is the subject of an extensive literature. The seminal work is Bernard Brodie, *Strategy in the Missile Age,* (Princeton: Princeton University Press, 1959), which grew out of a series of RAND Corporation studies by Brodie and others largely related to nuclear weapons. Another key contribution to the field is Thomas C. Schelling, "The Diplomacy of Violence," in *Arms and Influence* (New Haven: Yale University Press, 1966). Schelling argues that strategy can no longer be defined as the science of military victory, but is now more, the art of coercion, of intimidation and deterrence. To be coercive or deter another state, violence must be anticipated and avoidable by accommodation. The use of the power to hurt as bargaining power is the foundation of deterrence theory and is most successful when it is held in reserve. For a review of deterrence in the context of conventional (non-nuclear) warfare, see John Mearsheimer, *Conventional Deterrence* (Cornell: Cornell University Press, 1983). Many have attempted to adjust deterrence theory to take into account the reality that humans are not fully rational decision makers, and also the political and organizational determinants of national decision making. See for example Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1976) and Graham Allison and Philip Zelikow, *Essence of Decision*, 2nd ed., (New York: Pearson, 1999). Barbara Tuchman's study of the onset of World War I published in the year of the Cuban Missile Crisis is often read as a study of catalytic war despite a rational situation in which war should have been deterred. *The Guns of August* (New York: MacMillan, 1962). See also, Frank C. Zagare, "Reconciling Rationality with Deterrence: A Re-examination of the Logical Foundations of Deterrence Theory," *Journal of Theoretical Politics,* 16 (2) (2004), who argues that deterrence theory is logically inconsistent, and not empirically accurate. Rational choice scholars have argued for *perfect deterrence*, which assumes that states may vary in their internal characteristics and especially in the credibility of their threats of retaliation.

nuclear conflict types, including those variously characterized as "cyber," "digital," "informatics," "fifth dimension," or "fifth domain."[12] Current national policy speaks of "tailored deterrence" and "extended deterrence" and incudes the prospects of cyberattacks and cyber "weapons" as elements of modern warfare and military strategy in addition to kinetic weapons.

The possibility of strategic cyberwarfare is often compared to the use of nuclear weapons during the Cold War, although this analogy points to the role of deterrence in cybersecurity that imperfect at best.[13] Its popularity may be based on wishful thinking that deterrence would eventually make cyberwar irrelevant to the normal conduct of military operations and foreign policy, as it had often almost seemed to make nuclear weapons irrelevant. It was in the American interest to maintain the credibility of a nuclear response not just to nuclear weapons use but also to the use of other weapons of mass destruction and even to massive conventional attack, particularly by the Soviet Union and its Warsaw Pact allies against NATO but also by China and North Korea.

Extended deterrence also reduced the need for other governments to develop their own nuclear weapons, serving U.S. stability and non-proliferation goals. As the confrontation with the Soviet Union became more stable, battlefield and then other tactical weapons were deemphasized, but there was still a tension in U.S. policy which aimed overall at avoiding nuclear weapons use but also tried to maintain the viability of the nuclear threat to deter chemical, biological, and massive conventional attack.

Following the Cold War, strategists generally recognized that with the demise of the massive conventional threat on the doorstep of Western Europe

---

[12] Terminological profusion and imprecision are currently a major barrier to clear communication regarding operations, strategy, and policy in this area. As a domain, 'cyber' is unique in that – unlike land, sea, air, or space – it is not kinetic, but informatics, and, in principle, free from geography. The non-kinetic character of the cyber domain does not, however, preclude its localization within or across kinetic domains in any given theater or operational environment. *See*, e.g., Headquarters, Department of the Army (HQDA), *Cyber Electromagnetic Activities*, FM 3-38, (2014).

[13] See, Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44-71. An alternative view is provided by Rebecca Slayton, "What is the Cyber Offense-Defense Balance?" *International Security*, Vol. 41, No. 3 (Winter 2016/2017). For a comparative review of the Nye and Slayton papers see Brandon Valeriano, "What Is the Cyber-Offense-Defense Balance? Conceptions, Causes and Assessment," *H-Diplo – ISSF Article Review 83,* (July 26, 2017).

its interests had shifted to minimize the role of nuclear weapons in world affairs because it was now regional powers that were going to want nuclear weapons to offset U.S. conventional superiority. After the end of the Cold War, these strategists have generally followed Congressman Les Aspin, who articulated the notion that America's new superiority in conventional forces – what others called the unipolar moment – made the U.S. military the "equalizee" rather than a power in need of a nuclear equalizer.

Porting deterrence theory to cyber conflict presents significant challenges. As a strategic doctrine, deterrence theory was developed with high sensitivity to the uniquely cataclysmic characteristics of nuclear weapons. There are several differences between the cyber and nuclear realms that need to be considered in applying deterrence concepts to cyber interactions and attacks. Most recently the National Security Council and Department of Defense have begun to articulate this new application, but these are only some initial steps.[14]

## 1.3 Continuity with Cybercrime, Espionage and Cyberwarfare

Prior to the onset of large-scale conflict it may be difficult to distinguish "cyberwarfare" from "cyberespionage" – i.e., actions that begin appearing as clandestine penetrations that later are revealed to have created options for attacks that cause damage equivalent to significant military operations.[15] While the use of nuclear weapons – "the nuclear threshold" – was intended to be a clear red line within warfare and certainly was never to happen in peacetime, cyber operations occur including unauthorized entry into adversary networks and systems are reported to occur frequently. The U.S. engages in such activities for intelligence purposes in peacetime.[16] Similarly

[14] Three recent key documents are the December 2017 *National Security Strategy,* January 2018 *National Defense Strategy,* and the February 2018 *Nuclear Policy Review* which addresses "tailored deterrence" and "tailored assurance."

[15] This remains an ongoing quandary for the U.S., where Title 50 of the U.S. Code covers intelligence and espionage and Title 10 covers military operations. *See,* e.g., Gary D. Brown, "Spying and Fighting in Cyberspace: What is Which?" (April 1, 2016). 8 JOURNAL OF NATIONAL SECURITY LAW & POLICY (2016). See also, Geoffrey B. Demarest, "Espionage in International Law," *Denver Journal of International Law and Policy*, (1995).

[16] It could be argued that while nuclear weapons had no peacetime role other than deterrence, nuclear delivery forces were exercised constantly including in the 1950's bomber operations reported to penetrate Soviet air space, and later alert patrols by ballistic

concerns about proliferation of nuclear weapons to non-state actors were exactly that, while tools for costly intrusions and attack are already in the hands of non-state actors and are used routinely for criminal purposes.

While the barriers to entry for nuclear weapons are very significant, espionage, sabotage, and other intrusion capabilities in the cyber domain are ultimately functions of general purpose computing. There are no esoteric materials or choke-point technologies to control, and consequently no obvious supply-side solution to the proliferation of even advanced capabilities in the cyber domain. It is also a domain where international law and norms are either in an early state of evolution or simply don't exist.[17]

In the nuclear context, espionage and criminal enterprise are relevant to the question of proliferation but are not part of the operational spectrum of nation-state interactions as they are in the cyber context. Deterrence *may* be applicable to constrain the operations of nation-state espionage interactions and it deserves separate treatment from deterrence of significant cyberattack. Information gleaned during cyber operations short of war may also be useful in active defense against cyberattack. Finally, it is important that the adversary not take apparent toleration of cyber espionage and intrusions as an implicit signal that cyberattack will not meet a forceful response.

The apparent continuity of both espionage and criminal activity with cyberattack complicates cyber deterrence but also is a reason for paying close policy attention to the effects of "peacetime" responses on the deterrence of serious cyber intrusions and attacks. Dealing routinely with cyber intrusions

---

missile submarines … these operations might have been hard to distinguish from wartime operations, just as computer network incursions aimed at data exfiltration (generally a crime) can be hard to distinguish from attacks designed to do harm at that time or in the future. Throughout the Cold War a majority of U.S. intelligence resources were devoted to monitoring the force capabilities of the Soviet Union, including the types and numbers of weapons systems deployed and under development. A second critical intelligence function was to provide timely warning of a hostile Soviet attack. A U.S. response to an attack was to either launch "on warning" or "on attack" which was debated among experts at the time.

[17] See Abraham R. Wagner and Nicholas Rostow, *Cybersecurity and Cyberlaw,* (Durham: Carolina Academic Press, 2017). *See, also* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VIRGINIA JOURNAL OF INTERNATIONAL LAW 697. At best there has been some limited agreement on international cybercrime. See Council of Europe Convention on Cybercrime arts. 17-18, 32, *opened for signature* Nov. 23, 2001, S. Treaty Doc. No. 108-11 (2006), E.T.S. No. 185 (*entered into force* July 1, 2004).

in peacetime offers an opportunity to think differently about deterrence in the cyber domain.

Deterrence theory as used to analyze the criminal justice system may be more relevant than classical nuclear deterrence theory in reducing future cyber threats.[18] In addition to the traditional focus of deterrence theory on antagonistic decision makers, cyber deterrence theory needs to focus on channeling the evolution of society, including potential bad actors, toward safer equilibria, with reduced vulnerability and away from increasing capabilities that would be damaging in the hands of hostile parties.

It is also essential to recognize that espionage differs significantly from criminal enterprises in that state intelligence services maintain plausible deniability for such activities, which remains an area devoid of international law.[19] While nations can prosecute those responsible for cybercrimes, there is no corresponding ability to prosecute for espionage. Such activities remain in the domain of clandestine operations and not criminal enterprises.

## 1.4 Attack Identification and Timely Attribution

One knows instantaneously when a nuclear explosion has occurred, and, in most attack scenarios, in short order who built the device and used it in an attack.[20] None of this is necessarily true of a cyberattack. Identifying that such an attack has occurred and discerning the identity of "the attacker" and the ultimate responsible party in a timely way with high confidence remains a

[18] See Mark A.R. Kleiman, *When Brute Force Fails*, (Princeton University Press, 2009), David M. Kennedy, *Deterrence and Crime Prevention,* (Toronto: Routledge, 2009), and George Kelling and Catherine Coles, *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities,* (New York: Free Press, 1996).

[19] Professor Jack Goldsmith has made the often-quoted remark that "there is no international law of espionage and never will be." See also David Talbot, "Cyber-Espionage Nightmare," *MIT Technology Review,* (July/August 2015).

[20] See Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies,* (2015). It required significant investment to ensure all nuclear explosions worldwide and in space would be detected and that, after multiple countries developed nuclear weapons, whose bomb might have exploded. With the advent of fears of "loose nukes" or deliberate proliferation by North Korea or Pakistan, the situation is a little more muddled. Nevertheless, there is still a dramatic difference between ease of identification and attribution between nuclear and cyber. There is some nuclear parallel to covertly emplaced logic bombs in the possibility of nuclear weapons covertly emplaced in American cities to surmount defenses and even preemption or preventive attacks. Again, the model scenarios are very different even if one can identify some similarities at the edge.

difficult problem for cyberattacks. An attacker may be able to obfuscate ultimate responsibility by using various proxies or loosely aligned groups.[21]

Even if attribution is definite based on classified sources, the need to protect intelligence sources and methods can too easily result in a lack of overt action or in highly visible diplomatic or economic reprisals in the absence of visible justification. Improving technical capabilities for timely, publicly usable and convincing attribution is one key to an effective response and thus to many kinds of deterrence. The possibility of clear attribution that can't be used publicly raises the need to consider the possibility of such covert responses and whether the prospect of covert responses can be communicated effectively in advance as needed for deterrent effect.

## 1.5 Variable and Uncertain Cyber Targeting.

For some sorts of cyber actions, both attackers and responders are affected by the possibility that cyber actions will escape beyond the original targets and cause more widespread damage than expected. Diplomatic and economic actions currently dominate U.S. responses to undesirable behavior by state actors in the cyber domain. This condition reflects the difficulty of crafting a coherent doctrine of proportionality and variably selective targeting in cyber operations executed, sponsored, or tolerated by state actors.[22]

Both the degree of state or organizational support and the qualities of the attack itself are relevant to the appropriateness of a response. Compared to nuclear use, which is always toward the upper end of an escalatory ladder, cyber actions can occur far below the threshold of conventional warfare but also may be able to cause damage much greater than attacks with limited

[21] In many cases it may simply be a case of "outsourcing" a complex technical task. While some U.S. agencies rely heavily on external contractors, this ecosystem is highly dissimilar to the compelled labor economies used by, e.g., Russia, to meet their operational needs. Criminality among those groups is tacitly encouraged to make operations self-sustaining, provide cover for espionage, and to create a dependency by participants in on the protection of the Russian state against extradition and prosecution.

[22] A state actor may employ an extensive environment checking framework in using a tool possessing a replicant capability (i.e. a 'wormable' component). The use of such a framework may result in granular targeting, with the tool taking no action on most susceptible hosts. That same replicant capability, employed by a less advanced actor, may be used without such constraints to achieve maximum penetration among the same population of susceptible hosts. See Stamatis Karnouskos: "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," in *37th Annual Conference of the IEEE Industrial Electronics Society*, (IECON 2011),

conventional military forces, at least if defenses are lax, and certainly in comparison to the marginal cost of the attack.

## 1.6 Asymmetries in Digital Vulnerability

Developed societies such as the United States are assumed to have a larger cyber "attack surface" which translates to an increased vulnerability, as compared to less advanced states, resulting in relative "cyber dependence."[23] The possibility of attacks by non-state actors and non-state actors serving the interests of nation state adversaries is also problematic, for these groups may contrive to have very small digital attack surfaces. Cyber dependence assumes that a high rate of penetration of advanced information and communications technologies within civilian critical infrastructure directly results in susceptibility to catastrophic attack.

In less-advanced states their economies and militaries may have prioritized adoption of digital technologies and not emphasized protection or resilience, resulting in extreme vulnerability or fragility.[24] Advanced militaries may have developed effective cyber defenses resulting in increased resilience, stability, and incident response capacity after generations of technology development.[25] So, while asymmetry in the cyber domain is a strategic problem, it is far more complex than the notion of "cyber dependence" suggests, and requires detailed analysis of particular opponents and scenarios.

## 1.7 Cybersecurity as a Mission Area

Cyber deterrence is more complicated than nuclear deterrence because there are far fewer bright lines and a great deal more ambiguity between acceptable and unacceptable behavior. On the other hand, unlike nuclear or

[23] http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-83/jfq-83_19-26_Hughes-Colarik.pdf?ver=2016-10-19-102201-033.

[24] For example, an alleged attack by the Venezuelan hacktivist group Binary Guardians resulted in much of the .ve domain going offline, including all government and Supreme Court web properties. The relatively unskilled attack further crippled several public telecommunications companies resulting in the suspension of mobile communications services to 70% of Venezuelan subscribers. https://www.rapidtvnews.com/2017081648430/venezuela-s-public-telcos-collapse-under-cyber-attack.html#axzz4rGmqBZGN.

[25] Organizations that have had a longer digital history may have a patchwork of legacy systems with their own vulnerabilities and newly digitizing organizations may have opportunities to install systems with state of the art uniform protections.

conventional warfare, because of the continuity with criminal activity and espionage, cyber defenses are tested daily and so potentially may be more reliable than nuclear ones. Cyber operations, unlike nuclear ones, are often clandestine operations as authorized under Title 50 (intelligence authorities) as well as military activities under Title 10 (military authorities) of the U.S. Code.[26]

The policy and institutional matrix affecting the cybersecurity of the U.S. – even the part of cybersecurity of direct concern to DoD – is unusually complex and should be considered in investment plans and broader policy discussions. While technological solutions are uniquely important in this operational domain they must be included in this complex policy and institutional context. It is essential to liberate cyber deterrence thinking from inappropriate hangovers from Cold War nuclear deterrence to enable a more active and effective approach that is continuous across artificial distinctions between "costly intrusions" and "attacks."

Clarity is needed about *whom* is to be deterred from doing *what* through what sorts of threats that are communicated through specific channels with characteristics tailored for credibility and persuasiveness in the mind of the target audience. Deterrence not only depends on the credibility of the threat but also on the alternatives available to and perceived by the adversary.

It is important to grapple with this complexity because cyberattacks either on the IT systems supporting military and related national security operations or on those supporting critical infrastructure have at least a

[26] For a review of Title 50 *vs.* Title 10 issues, see Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, & Covert Action," 3 HARVARD NATIONAL SECURITY JOURNAL (2011); Robert Chesney, "Military Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy*, (October 2011); See also, Joseph B. Berger, III, "Covert Action: Title 10, Title 50, and the Chain of Command," *Joint Force Quarterly,* Issue 67 (2012), and Gary D. Brown, "Spying and Fighting in Cyberspace: What is Which?" 8 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 621 (2016). Title 50 has parts that deal with nuclear weapons also, but that is not the focus here. Congress's attempt to limit the Executive's war powers is codified in Title 50. Wall concludes that when it comes to military operations the Title 10-Title 50 distinction is mostly a matter of different modes of Congressional oversight. Current thinking in some quarters is that a unitary executive would militate against a strong distinction. It is also the case that maintaining NSA and CYBERCOM as "co-joined" activities avoids problems that might otherwise arise and a useful umbrella for utilizing the authorities of both Title 50 and Title 10 at the same time. Recent statements with respect to elevating CYBERCOM to a full operational command with a commander that is separate from the Director, NSA is an important step in this direction.

theoretical potential to have a system-wide debilitating effect on military capability at very low direct cost and conceivably with a degree of deniability.

To the extent these vulnerabilities are real or cannot be discounted, adversary actors may attempt to deter U.S. use of force by implied or explicit threats of cyberattack, and U.S. leadership may refrain from using cyberattack or military force based on this deterrence. The U.S. must ensure that its defenses against and deterrence of enemy cyberattack prevail over enemy efforts to use the cyber threat to constrain foreign policies, and to use cyber attacks to hobble military operations and the domestic consensus required to underwrite them.

## 1.8 DARPA's Role in Cybersecurity

Technologies that now comprise cyberspace had their origins as what was the Advanced Research Projects Agency (ARPA) in the 1960s, with the agency latter adding the term "Defense" to its name.[27] ARPA undertook the development of ARPAnet as a technical experiment in network optimization, with no dream that it would ever evolve into cyberspace and the largest media revolution since the invention of moveable type in the 16th Century. The few nodes on the "net" were all hard-wired mainframe computers and terminals connected to them; users were a limited number of scientists and system administrators; and there was scarcely any content to steal or hack. Concerns

[27] There is a considerable literature on the development of the Internet and cyberspace. See Stephen Segaller, *Nerds 2.0.1 – A Brief History of the Internet,* (New York: TV Books, 1998); Vincent G. Cerf, "On the evolution of Internet technologies," *Proceedings of the IEEE* (September 2004); Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, *A Brief History of the Internet,* (Reston, VA: The Internet Society, 2011); National Research Council, *The Internet's Coming of Age*, (Nat'l Acad. Press, 2001); Sharon Weinberger, *The Imagineers of War* (New York: Alfred Knopf, 2017); Katie Hafner, and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of The Internet,* (New York: Simon & Schuster, 1996); Janet Abbate, *Inventing the Internet* (Cambridge: MIT Press, 2000); and Peter Salus, "The Net: A Brief History of Origins," 38 JURIMETRICS 671 (1998).

about cybersecurity at the time were limited, at best. Privacy and legal issues were not serious matters then either.

The transition from the ARPAnet to the public Internet after 1989 created a new world with many unanticipated consequences. Along with the base network technology, lower cost hardware, other technologies and revolutionary software caused cyberspace to evolve in a way and scale never anticipated – at DARPA or anywhere else. Local and wide area nets quickly spread through the government; commercial enterprises; as well as educational institutions.

During these years the field of communications merged with that of information technology into the world now known as cyberspace. New technologies enabled remote access for users while commercial service providers emerged to meet a rapidly expanding user base. Development of the "web" and browser software enabled easy access to a rapidly growing set of net content and applications. More recently these technologies have come to include "social media" along with media of every other type.

Growth of cyberspace during the 1990s was clearly exponential and these were the "Wild West" days of the Internet. During these years DARPA's portfolio of programs in the information sciences and communications areas continued to grow and included an ever-expanding set of areas in both software and hardware. Network security became an increasing concern for DARPA but was one just one of many areas competing for agency resources.[28]

As network access grew exponentially and the set of threats expanded from mischief and early cybercrime to far greater issues of both crime and national security resources were not available to keep pace with the threat environment at the time. Unfortunately, they were not available elsewhere in the government at the time.[29]

---

[28] One early DARPA program was the creation of the CERT Coordination Center (CERT/CC) as the coordination center of the computer emergency response team (CERT) at Carnegie Mellon University in November 1988 at in response to the Morris worm incident. This highly successful program continued under DARPA sponsorship for many years and now resides with the Department of Homeland Security.

[29] In several ways the 1990s were a "lost decade" for cybersecurity, as at least one presidential panel found in 1998 as well as a technical panel working under the auspices of the Director of Central Intelligence at the same time. For most of the 1990s there was also a debate within DARPA as to what role the agency should play as the Internet became increasingly important in the areas of intelligence collection and warfare. For most of this

Recent years have seen a significant expansion in the DARPA portfolio of programs in the broad areas of cybersecurity. In part this has been in response to the reality that the Defense Department; the military services; as well as the Intelligence Community and other national security users have all become highly dependent on Internet resources and infrastructure. Vulnerabilities have rapidly become a major concern for the national security community and priority for solutions has increased for available resources.

Apart from this extensive and unique history, DARPA brings to the area a set of program management resources which are unparalleled either within the U.S. government or private industry. These cannot be easily or quickly replicated. As the government now seeks to scale up cybersecurity efforts it will need to rely on and expand these efforts if success is to be achieved.[30]

period DARPA limited its programs to network security and refrained from projects in network exploitation for intelligence purposes and cyber warfare. See, Director of Central Intelligence, *Report of the DCI Global Information Infrastructure Panel,* (1996).

[30] There are far too many examples of government agencies and offices attempting to execute complex and costly technical projects without the programmatic expertise and support infrastructure accomplish the task. Almost all have resulted in costly disasters.

# 2. Prior Issues in Cybersecurity

## 2.1 A Technology Revolution at Lightning Speed

What is unique in the rapid evolution of cyberspace is that it was the merger of several revolutions concurrently in ways that were not imagined or anticipated, including networking and communications technologies. These technologies also gave rise to a worldwide social and cultural revolution where the use of net-connected devices have become a part of everyday life that was also never imagined.[31]

The initial ARPA experiment which demonstrated that packet switching using TCP/IP protocols was far more efficient than traditional line-switching was a major success. New technologies in the communications area, including wired and wireless systems, increased the available bandwidth by orders-of-magnitude. Developments in the computer and networking areas led to a new world where low-cost computers proliferated throughout offices, institutions, schools, and homes. These quickly became connected to a rapidly evolving Internet.

Technologies for mobile devices and a myriad of software applications helped bring about a cultural revolution as well. Rapidly falling prices for mobile devices such as cell phones and PDAs as well as the explosive rise of social media made this technology base a part of everyday life for a vast number of people of every economic sphere.[32] Social media also became an

[31] See Paul Freiberger and Michael Swaine, *Fire in the Valley: The Making of The Personal Computer,* (New York: McGraw-Hill, 2000), Jon Agar, *Constant Touch: A Global History of the Mobile Phone*, (Cambridge: Icon Books, 2003), and Gerard Goggin, *Global Mobile Media,* (New York: Routledge, 2011). At the outset in the 1960s there was no idea that ARPA's technical experiment in network optimization would ever evolve into cyberspace. One historical note is that e-mail was never part of the original ARPAnet concept or ARPA's contract with BBN. The e-mail protocol (SMTP) was developed by BBN employee Ray Tomlinson on his own time. The web protocol (HTTP) was not DARPA-sponsored and was done by CERN in Switzerland (1990), while the browser technology which enabled convenient web use was the DARPA MOSAIC program (1993).

[32] See, for example, Gerrard Goggin, *Global Mobile Media,* (New York: Routledge, 2011).

integral element in aspects of foreign affairs, military operations and terrorist activity.[33]

At the same time the nature of data itself became transformed. As the era of "Big Data" evolved the world moved from an analog to digital one where physical media rapidly disappeared and files on net-based systems became the norm. Government documents; financial records; medical records; legal and personal papers as well as entertainment media are on connected servers.

This technology also gave rise to "social media" adding an entirely new dimension to modern life and cyberspace.[34] For its part the Government joined in the stampede into the Internet era with a rapid proliferation of internal networks all connected to the Internet.

Major sectors including national security, electric power, finance and others all adopted these technologies, becoming dependent on the commercial infrastructure supporting it. The speed and extent of these concurrent revolutions was unprecedented in American history, while planning process within the government did not keep pace with the requirements for securing cyberspace. Adequate investments in technology to secure this critical infrastructure were not made. Today these problems are more broadly recognized, and the government far more committed to their solution.

## 2.2 Major Threats Were Largely Ignored

Systems supporting national security as well as critical infrastructure sectors and the U.S. economy overall are vulnerable to debilitating cyberattack and near-term prospects for eliminating the recognized threats are not great.[35] To a large extent this is the byproduct of a failure on the part of the nation, including the federal government and the technology sector to fully recognize the rapidly evolving threat environment in these critical areas.

---

[33] See Abraham R. Wagner, *The Unsocial Network: New Media and Changing Paradigms*, Paper Presented to the 11th International Conference – World Summit on Counter-Terrorism, Herzliya, Israel (September 2011) and Abraham R. Wagner, *Cybersecurity, Cryptology, and Privacy in Historical Context: The Challenge of New Technologies and Media,* Paper Presented to National Security Agency Cryptologic Symposium, (October 2013).

[34] It has also led to a large, growing, and not widely appreciated problem of "cognitive security." See, for example, Magee, Tamlin, "US government can't compete in information war, warns RAND Corporation, *TechWorld,* (February 12, 2018).

[35] See Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* (January 2013).

Until recently cyberspace has not been treated as an important national resource. As the Internet and cyberspace grew from a 1960s ARPA program to a vital national resource, security problems were increasingly recognized but effective solutions not implemented.[36] Real solutions require political will as well as technical focus, funding and effective collaboration with the private sector.

The transition from the limited ARPAnet to the public Internet beginning in FY-1990 initiated a technology revolution in both communications and information technology that was largely unanticipated. At the same time, however, the 1990s were a "lost decade" for cybersecurity in terms of actual programs, which were inadequate, and largely ineffective in meeting the evolving challenge. Evolving cybersecurity problems did receive at least some Presidential attention.

A 1998 White House study conducted under Presidential Decision Directive/NSC-63 clearly recognized the nation's reliance upon critical infrastructure and cyber-based information systems, and stated President Clinton's intent:

> ***It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.***[37]

Notwithstanding Presidential intent and lofty goals, this Directive provided no additional funding for any federal agency to accomplish this task, calling for a

---

[36] See, for example, Segaller, *Nerds 2.0.1: A Brief History of the Internet, op. cit.*; Leiner, et. al, *A Brief History of the Internet, op. cit.,* and Weinberger, *The Imagineers of War: The Untold Story of DARPA, The Pentagon Agency that Changed the World, op. cit.*

[37] Presidential Decision Directive/NSC-63, *Critical Infrastructure Protection* (May 22, 1998). This Directive further set for the goal that "No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of: the Federal Government to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services; the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services."

plan to address the problem within 180 days which was never completed. It also called for a "public-private partnership" in this area, and private industry ultimately was non-responsive to this call.

Again in 2013 another White House study conducted under Presidential Policy Directive/PPD-21 made these same arguments in almost the exact same language, stating:

> ***The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being***.[38]

This directive also pays lip service to the growing threat but provided no additional resources to any other federal agency to meet the growing challenge. PPD/21 fails to even mention the Department of Defense, DARPA or any other Defense component with responsibilities for cybersecurity.

## 2.3 The Internet is Inherently Vulnerable

The Internet still operates on protocols developed in the 1960s that are inherently vulnerable and not appropriate for the role the Internet plays in 21st century society, commerce, and national security. Systems supporting national security users are also been vulnerable.[39] A modern Internet architecture is

---

[38] Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (February 12, 2013). PPD/21 assigns the responsibility for achieving this goal to the Department of Homeland Security (DHS), which has its own Science & Technology Directorate, but still lacks a serious capability to implement an effective solution and provides no specific funding to achieve it. It also assigns part of the responsibility to the National Institute of Standards and Technology (NIST) which similarly lacks the programmatic infrastructure and funding needed. Similarly, Presidential Policy Directive/PPD-41 *U.S. Cyber Incident Coordination* (July 27, 2016) assigns responsibility to the DHS and the Director of National Intelligence (DNI) with no mention of the Department of Defense.

[39] Largely missing from this discussion is the issue of physical vulnerability of the Internet architecture in the U.S. DNS is the single source for Internet address information and is inherently a single point of failure. To mitigate the threat of attack the DNS architecture consists of 13 *root servers* which provide addressing information to a distributed network of DNS *nameservers* for ISPs and other network providers. The 13 root servers are located in commercial buildings, that are not secret, and protected by commercial-grade physical

needed to meet the current challenge. At present there is ongoing debate among computer scientists as to whether the objective of a safe or secure Internet architecture is feasible.[40]

Cybersecurity continues to be composed of patches, fixes and "band aids" that fail to provide the type of security needed, and there is no obvious alternative in sight.[41] Nonetheless, it is reasonable to question whether a major overhaul of the operating protocols will provide the needed solution, or whether there is any other realistic alternative to endless patches.

Detection of "hacks," such as zero-day exploits, using manual methods takes on average over 300 days, which is unacceptable. As the 2016 DARPA Cyber Grand Challenge shows the potential exists for greatly improving the process by utilizing supercomputers and advanced software to identify malware, develop "patches" in real time, and avoid system failures.[42] Whether this type of technology can be developed to a point where it could be operationally deployed remains an open question.

## 2.4 Earlier Cyber Policy Came Without Adequate Resources

Actual resources available for cybersecurity have been limited, and high-level policy such as Presidential Directives PDD/NSC63, PPD/20, PPD/21 and PPD/41 do not assign critical cybersecurity missions to government agencies capable executing them or having the resources and capabilities to undertake technical programs of the magnitude required.

Here "resources" does not simply apply to funding, but also the existence of program offices with skilled managers and infrastructure required for programs on the scale needed. These largely reside within the Department of

---

defenses. It is possible to envision a scenario where a terrorist organization or other adversary destroys all of them concurrently.

[40] Most experts agree that the current network protocols (iPV4 and iPV6) are inadequate.

[41] DARPA never had the top-level direction since 1990 to undertake the types of programmatic solutions needed or had adequate resources to provide the types of fixes needed. Within the limits of available funding, DARPA continues various cybersecurity programs, as does DHS, NIST and other federal agencies.

[42] The 2016 DARPA Cyber Grand Challenge demonstrated the ability of supercomputers programmed to detect and "patch" specific malware inserted into the system in real-time. See here: https://cgc.darpa.mil/. This was an initial proof-of-concept demonstration of a major new paradigm that needs to be further developed for a broad class of exploits in the future.

Defense and the Intelligence Community. Clearly earlier decisions to assign these responsibilities to DHS and NIST for reasons that are obviously not technical or programmatic has severely inhibited progress.[43]

Existing statutes also limit DHS, NIST and other agencies to defensive cyber operations, leaving open the issue as to what extent should the nation separate defensive and offensive cyber activities. Active or offensive cyber operations need to be conducted under either Title 10 of the U.S. Code (military operations) or Title 50 of the U.S. Code (intelligence activities), and only the Department of Defense and the Intelligence agencies have such authorities.[44]

## 2.5 Errant Assumptions About Industry Funding

National policy with respect to cybersecurity has largely been made on the incorrect assumption that industry, led by the technology sector, would address major vulnerabilities that were becoming increasingly evident and respond to demand for increased security. The concept of a "Public-Private Partnership to Reduce Vulnerability" articulated in PDD/NSC-63, for example, explicitly stated that "we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector."[45]

In the time since PDD/NSC-63 (1998), and a PPD/21 (2013) industry funding for the levels needed to adequately address the problem posed by rising cyber threats and vulnerabilities has not materialized. The implicit thought that "the market" would respond to consumer demand for increased security and achieve a certain degree of self-correction, never happened. To a

[43] The Defense Science Board, has initiated a study of this issue. See Undersecretary of Defense (Acquisition, Technology and Logistics), Memorandum for the Chairman, Defense Science Board, *Terms of Reference – Defense Science Board Task Force on the Role of the DoD in Homeland Security* (October 20, 2016).

[44] See Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, & Covert Action," *op. cit*.,; Gary D. Brown, "The Cyber Longbow & Other Information Strategies: U.S. National Security in Cyberspace, 5 PENN STATE JOURNAL OF LAW & INTERNATIONAL AFFAIRS 1 (2017); Gary D. Brown, "Spying and Fighting in Cyberspace: What is Which?", *op. cit*. . A more extensive analysis of this issue is contained in the Annex to this study.

[45] PDD/NSC-63 (1998), *op. cit.* At the time then Vice President Gore was the principal spokesman for this view and was firmly of the opinion that industry would recognize the challenge and fund needed solutions.

large extent this is a classic "public goods" problem, and the idea that private funding for a largely public problem would occur was in error.[46]

For decades DARPA has led the path in terms of working with the technology sector in "catalytic" funding to a wide range of industry projects, both in cybersecurity as well as related technology fields. As the threat environment evolved, this was not at a level to meet the challenge or bring about corresponding investments by the technology sector in security.

## 2.6 Failure to Include Industry as a Full Partner

Solving cybersecurity problems requires a strong partnership with a number of key industry sectors, including the technology sector; the financial sector; power and others.[47] This partnership involves not only funded programs, but data sharing, security clearances and other important elements.

Without a full and genuine partnership government efforts are doomed to failure.[48] Corporations have many incentives that inhibit this cooperation, including potential liability for revelations that they are not meeting a higher standard of care, and differences over past government efforts to develop back-door access to information. Strong, informed, and discerning leadership capable of making key and durable policy trade-offs and commitments is a necessary basis for this partnership to succeed.

In building this partnership it is important to recognize that unlike the communications and SIGINT model, it is not enough to simply include the technology sector and "Silicon Valley" but others, such as the financial sector, who not only have major concerns but are the source of much critical data.

---

[46] The classic statement of this theory is found in Mancur Olson, *The Logic of Collective Action: Public Action and the Theory of Groups*, (Cambridge: Harvard University Press, 1965).

[47] One analog is the strong partnership which the government built with the communications providers (largely AT&T) starting in 1921 which enabled effective SIGINT collection for decades. See Wagner, *Cybersecurity, Cryptology, and Privacy in Historical Context, op. cit.* See also Michael Warner *"Privacy and Security, Yesterday and Today," in Cybersecurity and Privacy: Report of the Expert Workshop Held for the Defense Advanced Research Projects Agency (DARPA),* Institute for Defense Analysis (June 25, 2014).

[48] See Adam Segal, *Rebuilding Trust Between Silicon Valley and Washington,* (Council on Foreign Relations, January 2017), and John Reed, "Pentagon expanding public-private cyber information sharing program," *Foreign Policy,* (September 2012).

## 2.7 Existing Statutes are Inadequate

It is increasingly evident that Cold War statutes cannot accommodate the current realities of cybersecurity and cyberwarfare. While this is clearly not a problem that technology developers can "solve" the legal regime does have a significant impact on how specific technologies are developed and employed.[49] New law and policy need to incorporate the unique, borderless qualities of the domain, offensive and defensive cyber operations.[50]

Failure to understand and incorporate into law and policy the unique, borderless qualities of the domain imperil offensive and defensive cyber operations, as well as the integrity of existing legal structures. Concerns about privacy and individual rights as well as fears of an intrusive government must be addressed to move forward with a policy based on a coherent legal regime.

Many of the problems here stem from the fact that evolution in the legal regime takes place at a pace that is glacial in comparison to advances in technology. Government and the courts are being asked to apply laws developed for technologies that are generations old and no longer make sense. New encryption technologies, for example, are widely available and fly in the face of statutes enacted for a much different world.[51] Similarly the Computer Fraud and Abuse Act (1986) is seen by all as in serious need of revision, which has yet to take place despite strong bipartisan interest.[52]

---

[49] See *Cybersecurity and Privacy: Report of the Expert Workshop Held for the Defense Advanced Research Projects Agency (DARPA), op. cit.,* and Abraham R. Wagner and Paul Finkelman, "Security, Privacy and Technology Development: The Impact on National Security," 2 TEXAS A&M LAW REVIEW 4 (2015).

[50] See, for example, Jennifer Daskal, "The Un-Territoriality of Data," *op. cit.*, and Jennifer Daskal, *A Twenty-First Century Framework for Digital Privacy: Balancing Privacy and Security in the Digital Age, op. cit.*; Jim Harper, *Administering the Fourth Amendment in the Digital Age,* (National Constitution Center, 2017); Neil Richards, *Secret Government Searches and Digital Civil Liberties,* (National Constitution Center, 2017); David R. Johnson and David Post, *Law and Borders—the Rise of Law in Cyberspace*, 48 STANFORD LAW REVIEW 1367 (1996); and Lucas Kello, *The Virtual Weapon and International Order,* (New Haven, Yale University Press, 2018).

[51] See, for example, *Going Dark: Implications of an Encrypted World,* (Center for Advanced Studies on Terrorism, April 2017), and Riana Pfefferkorn, *The Risks of "Responsible Encryption,"* (Stanford University, The Center for Internet and Society, February 2018).

[52] The Computer Fraud and Abuse Act (CFAA) was enacted in 1986 as an amendment to existing 1984 Computer Fraud Law (18 U.S.C. § 1030) which prohibits accessing a computer without authorization, or in excess of authorization and was enacted in response to concern that computer-related crimes might go unpunished.

Also joining the family of antiquated statutes is the 1986 Stored Communications Act (SCA) which creates Fourth Amendment-like privacy protection for email and other digital communications stored on the Internet.[53] Further, it limits the government's ability to compel a service provider to turn over content and non-content information such as logs and metadata. In addition, it limits the ability of commercial service providers to reveal content information to non-government entities.

Legal experts and others see major issues with this old law, generally finding that the protections surrounding electronic communications such as email were "weak, ambiguous, or nonexistent."[54] A recent Congressional (OTA) study of the SCA concluded that "[t]he existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging electronic surveillance technologies." Congress acknowledged the fact that traditional Fourth Amendment protections were lacking. Further, at the time the SCA was enacted social media platforms did not even exist so the SCA limits to electronic communications do not cover this domain at all.

A more fundamental problem is posed by fact that the existing legal system is based on the concept of "territoriality" where persons, companies, systems and data are located in a specific nation over which that nation has control. Increasingly this is not the case, and the legal regime has yet to come to grips with the fact that, in the case of the U.S., it cannot legislate for the world, or a world in which borders are no longer a relevant concept.[55]

Another area of increasing concern here lies with the fact that the legal regime in Europe, particularly the United Kingdom and France, with respect to information service providers and data has been evolving in a manner significantly different from that in the U.S.[56]

---

[53] The Stored Communications Act (SCA) (18 U.S.C. 121 §§ 2701–2712) addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA) that was an update to the Federal Wiretap Act of 1968, which provided protection on telephone (land line) privacies.

[54] See Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 GEORGE WASHINGTON LAW REVIEW 1208, 1211–12 (2004).

[55] See, Daskal, *op. cit*., Johnson and Post, *op. cit.,* and Kello, *op. cit.*

[56] See Kathryn E. Witchger, *The Great Data Race: Lessons from EU Cyber Law* (Center for Advanced Studies on Terrorism, February 2, 2017); Kathryn E. Witchger, *EU Law Update*

## 2.8 Problems of Cognitive Security

While much of the attention to cybersecurity problems has focused on denial of service, destruction, impairment of critical sectors and use of malware to steal or exploit data, a major issue remains in the malevolent use of the Internet and social media for operations related to matters ranging from politics to terrorism and information warfare.[57] Current technology enables these information operations to take place at a speed and extent previously unimaginable, and at cost which is free or close to it.

Today the Internet and social media have created entirely new opportunities for such information or influence operations and the mass manipulation of opinion. These technologies enable accurate targeting of those likely to be most susceptible to their message, often "fake news" and utilize platforms such as Facebook and Twitter where users see only news and opinions that confirm their prejudices.[58]

---

(Center for Advanced Studies on Terrorism, January 24, 2017). See also *Microsoft Corp. v. United States*, (formally titled *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, also known as the "*Microsoft v. Ireland*" case to be heard by the Supreme Court in the 2017–2018 term. The case involves the extraterritoriality of law enforcement seeking electronic data under the anachronistic 1986 Stored Communications Act (SCA) written before the creation of several Internet technologies facilitating global communications. Recently a bipartisan group of Senators introduced the *Clarifying Lawful Overseas Use of Data (CLOUD) Act*—a bill that moots the pending *Microsoft v. Ireland* case and authorizes the executive to enter into bilateral and multilateral agreements to facilitate cross-border access to data in the investigation of serious crime. Amazingly, this legislation has the support of both the Department of Justice and Microsoft – the dueling parties in *Microsoft v. Ireland* as well as the support of numerous other tech companies.

[57] See Rand Waltzman*, Cyber Enabled Information Operations,* Statement before the Senate Armed Services Committee Cyber Subcommittee (April 27, 2017) available at https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations. See also, "My truth against yours - Waging war with disinformation - The power of fake news and undue influence," *The Economist*, (January 25, 2018). In February 2017, in the wake of revelations about Russia's interference in the 2016 U.S. presidential election but before the full extent of its activities on Facebook, Twitter and Google had become known, Russian Defense minister, Sergei Shoigu, announced that he had created units within the army to wage an information war: "Essentially the information conflict is a component of general conflict. Deriving from that, Russia has made an effort to form structures that are engaged in this matter."

[58] Facebook now estimates that during and after the 2016 U.S. presidential election a Russian-linked troll farm called the Internet Research Agency was responsible for at least 120 fake pages and 80,000 posts that were directly received by 29 million Americans.

Traditional cyber security is largely about eliminating vulnerabilities in the information infrastructure and preventing cyberattacks. Such solutions do not, however, provide any defense against use of this infrastructure to influence and manipulate entire populations. This problem requires an entirely different approach and a different set of supporting technologies collectively termed "cognitive security." To emphasize the difference, consider a classical denial of service attack. In this kind of attack, the object is to bring down a computer server by overloading it with a lot of content free messages.

Future, "fake news" combined with the aid of artificial intelligence will be so realistic that even the best-resourced and most professional news outlets will be hard pressed to tell the difference between the real and fake news. At the same time official websites and social-media accounts will become increasingly vulnerable to hackers, who may be able not only to provoke adverse political outcomes, but also riots or other disastrous crises between countries. What is required for cognitive security is an active defense against psychological manipulation through new technologies such as social media.

Through sharing and liking, the number multiplied to nearly 150 million, about two-thirds of the potential electorate. The ads aimed to exploit America's cultural differences. Similar operations have been launched in Europe, where Russia is attempting to bolster support for populist movements that oppose liberal social norms.

# 3. National Policy Goals for Cybersecurity

## 3.1 Missions and Responsibilities for Cybersecurity

The challenges of cybersecurity are not only new, they embrace a far larger set of federal actors than traditional national security problems such as kinetic warfare and even intelligence operations. Following World War II, the nation undertook a major reorganization to meet the challenges it faced at the time with the enactment of the National Security Act of 1947.[59] Among other things that act established the Department of Defense as well as the National Security Council (NSC) as the President's key instrument for managing the national security process.

While a major step, the National Security Act left open many organizational details, particularly in the area of intelligence operations. Much of this was clarified under Executive Order 12333 (1981) which, among other things, assigned specific roles to the elements of a rapidly growing Intelligence Community.[60]

Following the 2001 9/11 terrorist attacks major efforts were made to solve apparent national security problems with the Homeland Security Act (HSA) of 2002 which created the Department of Homeland Security (DHS),[61]

[59] The National Security Act of 1947 was a major restructuring of the nation's military and intelligence agencies, merging the Department of War (renamed the Department of the Army) and the Department of the Navy into the Department of Defense headed by the Secretary of Defense and creating the Air Force as a separate service. Further, the Act established the National Security Council and the Central Intelligence Agency as parts of a national security infrastructure.

[60] Executive Order 12333 *United States Intelligence Activities* (December 4, 1981) extended the powers and responsibilities of U.S. intelligence agencies. It was amended by Executive Order 13355 *Strengthened Management of the Intelligence Community* (August 27, 2004) and by Executive Order 13470 (July 30, 2008) which strengthened the role of the DNI.

[61] Pub.L. 107–296, 116 Stat. 2135. Exactly how "homeland security" differs from "national security" which is the responsibility of the Department of Defense remains unclear. In part this stems from the existing limitation on DoD and the military services to operate within the U.S. under the Posse Comitatus Act of 1878 (18 U.S.C. § 1385, 20 Stat. 152) which – in concert with the Insurrection Act of 1807 – limits the powers of the government in using the military to enforce domestic law and policies within the U.S. See, for example, Tom A. Gizzo

and the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA) which created the Director of National Intelligence (DNI).[62]

National policy for cybersecurity remains in need of such an organizational process, either by statute or Executive Order. The specific roles and missions of the relevant departments and agencies need to be further defined, with an appropriate reporting structure to a senior official within the Executive Office of the President. Also essential is a coordination structure for both analytic, research and operational concerns.

Within the Department of Defense it is possible to organize and coordinate the activities of DARPA, NSA, CYBERCOM and other DoD or military components with cybersecurity responsibilities. The Secretary of Defense, cannot, however, manage activities at DHS, NIST and other federal agencies working in this domain.

The government needs an analog to EO 12333 clearly defining the roles and missions of all agencies involved with cybersecurity, establishing a chain of command to effectively implement them. The Executive Office of the President needs to take charge of an ongoing analytic, policy, and programmatic operation capable of meeting real threats with effective solutions. America must face cybersecurity as it did the threat of strategic nuclear warfare with both a legal and programmatic infrastructure capable of meeting the challenge.

## 3.2 Meeting the Challenge of Cyber Conflict

Current policy clearly recognizes the major role cyber operations will play in any future conflict. In discussing the need to modernize key capabilities the Department of Defense notes:

---

and Tama S. Monoson, *A Call to Arms: The Posse Comitatus Act and the Use of the Military in the Struggle Against International Terrorism*, 15 PACE INT'L LAW REV. 149 (2003).

[62] Pub. L. 108-458. This act established both the position of Director of National Intelligence (DNI) as separate from the position of CIA Director, the National Counterterrorism Center (NCTC), and the Privacy and Civil Liberties Oversight Board (PLCOB). It did not, however, address the problem that unlike most all other nations the U.S. does not have a domestic intelligence service. A key finding of the 9/11 Commission was that the lack of such a domestic capability was a serious national problem in an age of terrorism. Under the 1947 *National Security Act* the CIA is prohibited from such domestic intelligence operations, as is the FBI.

> ***Space and Cyberspace as Warfighting Domains: The Department will prioritize investments in resilience, reconstitution and operations to assure our space capabilities. We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations***.[63]

The Department of Defense has already undertaken efforts to incorporate cyber operations and the prospects of cyber warfare into overall planning and operations. U.S. Cyber Command (CYBERCOM) was established as a unified command while each of the military services established corresponding commands as operational activities. Increasingly the "stovepipes" that separated these commands from NSA and other Intelligence Community elements are being eliminated.

National policy now calls for defensive strategies and programs as well as the ability to conduct strong offensive operations where needed or to help deter attacks by potential adversaries. This approach recognizes threats from nation states as well as non-state actors such as terrorist groups. There is also a potential cyber response to warfare at the strategic level.[64]

As with kinetic warfare, a significant element of meeting the challenge of cyberconflict is strategic warning which enables an effective response. In cyberconflict this relates to the complex problem of not only timely warning but accurate attribution of the attack to a specific nefarious actor – be it a nation-state, non-state actor or some criminal element.[65] Unlike strategic nuclear warfare, cyberwarfare may scale from cyberespionage to major attacks on critical infrastructure. Attackers in cyberspace often have little fear of being caught as current technology makes it extremely difficult in many cases and often impossible, to reliably and confidently attribute their actions.

---

[63] Department of Defense, *2018 National Defense Strategy,* (January 2018), p. 6.

[64] Department of Defense, *Nuclear Posture Review,* (February 2018).

[65] See, for example, Lily Hay Newman, "Hacker Lexicon: What it the Attribution Problem, *Wired* (December 24, 2016) available at: https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/. See also Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* (2015). The identities of malicious cyber operators are often effectively obscured through multiple layers of indirection. The characterization of malicious cyber activity is now based on indicators of compromise, such as file hashes and command-and control infrastructure identifiers, which allows attackers to evade the defense and resume operations simply by superficially changing their tools, tactics, techniques, and procedures.

While policy documents in this area do not explicitly outline an investment strategy to support national objectives for "tailored assurance" in cyber conflict the DARPA portfolio of programs is clearly aimed at supporting these critical cyber missions.[66]

Notwithstanding the good intentions reflected in the Homeland Security Act (HSA) of 2002, precisely what role DHS would play in an actual conflict involving serious cyber operations has yet to be fully defined and exercised. The Department of Defense remains the only government department with Title 10 and Title 50 authorities, as well as operational capabilities to respond effectively.[67]

## 3.3 Securing Critical Infrastructure

The capabilities and economies that Internet technology offered has created a situation where all critical sectors are entirely dependent on commercial infrastructure, including national security, electric power, finance and others. Loss or major damage to this infrastructure would have devastating consequences.[68] Here the Internet still operates on protocols developed in the 1960s that are highly vulnerable and never designed for the role the Internet and cyberspace now play in national security, commerce, and society.

---

[66] As in other aspects of warfare, the nation needs an ongoing analytic, policy development and programmatic assessment of cyber threats and all related issues. This should be undertaken by the Department of Defense; the Intelligence Community; the Justice Department; the Department of Homeland Security; as well as the Departments of Commerce and State. Supporting this effort should be experts from within the government as well as relevant research institutions.

[67] Further, cyber conflict differs from kinetic warfare, in that hostile cyber operations are likely to begin as covert or clandestine activities where immediate attribution may not possible and the initial attack is not regarded as cyberwarfare. In the cyber area there are grey boundary lines between what is domestic and what is international, as well what is defense or offense. How America responds to such attacks raises major organizational and technical issues, pitting the legal authorities, mission, and capabilities of the Defense Department, the Intelligence Community, and DHS. At present DHS is undertaking an internal reorganization in the cyber area responding to this requirement.

[68] See, for example, George R. Cotter, *Security in the North American Grid: A Nation at Risk* (April 8, 2015); Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Center for New American Security, 2015); Frank J. Cilluffo, and Sharon L. Cardash, *Overview and Analysis of PPD-41: US Cyber Incident Coordination* (Lawfare, July 27, 2016) and Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (January 2013).

Systems supporting national security are still vulnerable to cyberattack and as are those supporting power and finance. The problem facing the nation is twofold, specifically one of securing the existing critical infrastructure from a range of cyber threats and a second of replacing outdated elements of the infrastructure which cannot be properly secured.

Sufficient resources are not available for a complete replacement of the entire infrastructure in the near term, and there is not even general agreement on what this replacement would look like. The practical solution lies in a set of technical initiatives that enhance the security of the existing critical infrastructure and where possible to replace vulnerable elements that cannot be secured.

A modern Internet architecture is required to meet the current challenge and needs to be developed. Better standards are also needed for critical infrastructure to make vital networks as secure and resilient as possible. Automated systems for the detection of cyber threats and deploying countermeasures on a real-time basis are essential. Significant capital expenditures must be made to for replacement rather than maintenance of vulnerable legacy systems inside the federal, state, and local governments that cannot meet the growing threat environment.

While much of modern cyberspace is "new" in historic terms, a large part of the existing infrastructure is seriously outdated, including the system architecture, hardware as well as software such as operating protocols and system software. Major cyberattacks have been attributed to antiquated legacy systems where needed security upgrades were not possible for various reasons.[69] Some security specialists are urging "best practices" and "cyber hygiene" as a major element of solving the problem. While this makes sense at some level, it does little to address the fundamental issues.

[69] See, for example, Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government." *Wired,* (October 23, 2016). Analyst scans identified over 2,000 individual pieces of malware on OPM hosts, from routine adware to dormant viruses. Among other things hackers were able to access the complete personnel files of 4.2 million employees. OPM Director, Katherine Archuleta, told the House Oversight Committee that she had no clear idea of how many people had been affected by the attack, and repeatedly mentioned how difficult it is to secure OPM's aging "legacy systems." Other recent hacks that have gained extensive press coverage include Sony Pictures, attributed to North Korea, and systems belonging to the Democratic National Committee, attributed to Russia.

Large-scale legacy hardware systems in both government and non-government locations will take many years to replace. Resources to do otherwise simply don't exist. As a practical matter national strategy needs to focus on what upgrades, largely in the software area, can be implemented in the near-term to mitigate vulnerabilities and prevent cyberattack with the understanding that wholesale replacement of vulnerable legacy systems is, at best, a long-term proposition.

An open question remains as to whether or not it is possible to undertake the development of a new and inherently secure Internet architecture, and what the transition to such a new architecture would entail. Admittedly the Internet continued to use protocols developed many years ago, and even some of the modernized versions, such as iPV4 and iPV6, do not provide a level of security that is required.

## 3.4 Building a Cyber Workforce

America requires a workforce capable of understanding and confronting risks and threats arising from the cyber domain. By some estimates there is a national requirement for some 300,000 people with various skills in the cybersecurity area, which will continue to grow. Many young people will not seek education in this area without funding, including undergraduate and graduate education. Just as America responded to the 1960s challenge of "space race" it is essential that nation strongly support education in computer science and related areas to meet the job requirements in the cyber area.[70]

While this is not specifically a DARPA mission area *per se*, DARPA has a long history of supporting programs that involve university research centers. In many cases such funded research and technology programs provide critical support to both faculty and students. Also included here University Affiliated Research Centers (UARCs).

[70] The creation of ARPA (later renamed DARPA) was itself one element of the national response to the "space race" and the technology challenge of the time posed by developments in the Soviet Union. See, for example, Sharon Weinberger, *The Imagineers of War: The Untold Story of DARPA, The Pentagon Agency that Changed the World,* (New York: Alfred Knopf, 2017), and George A. Kistiakowsky, *A Scientist at the White House* (Cambridge: Harvard University Press, 1976). It is essential that America promote education in computer science and related areas to meet the job requirements in the cyber area. An initiative similar to the National Defense Education Act (NDEA) could be useful in meeting this need. Public Law 107-305, *Cyber Security Research and Development Act* (2002) sought to accomplish this in part but has been grossly inadequate.

It is also the case that building the needed cyber workforce will require financial and other environmental incentives beyond the university. Pay rates and other fiscal benefits of the technology sector need to be competitive with other opportunities. Recent experience has also shown that work ambience is also important in attracting the needed workforce.

## 3.5 Building the Partnership with Industry

The technology sector, financial sector and others are essential partners in meeting the challenge of effective cybersecurity. Beginning in the 1960s DARPA created what is now known as cyberspace entirely through contracts with the technology industry and university research institutions. This technology base which developed and greatly expanded over the last four decades is critical to solving the range of cybersecurity problems facing the U.S. now.

While America's technology industry has been responsible for the myriad of development in cyberspace the U.S. failed to include them as a full and effective partner in meeting the cybersecurity challenges as they evolved. If America is to meet these critical challenges this failed policy must change. The most important changes are not difficult and can be accomplished in a reasonably short time. The most important elements of the new partnership with industry include:

- *Increasing Government-Funded Research and Development and Focusing it on Critical Needs:* America cannot depend on industry funding important research and development in cybersecurity.[71]
- *Expanding Clearances for Industry:* Access to timely cyber threat data and related information is essential for the technology sector as well as the financial sector and others. Clearing a far larger number of personnel at the Secret level is far less costly and more rapid than higher levels and would greatly expedite the process. Other key elements such as the financial sector, which may not

[71] The *Federal Cybersecurity Research and Development Plan* (2016) states only broad and vague goals with no path for achieving them. An actual plan with significantly increased federal funding for cybersecurity research is needed.

have government contracts, also require a pool of cleared personnel to access classified data networks.[72]

- *Downgrading Vulnerability and Threat Data:* A large percentage of cyber-related and vulnerability data does not need to be maintained at Top Secret/SCI levels. It can safely be downgraded to Secret and disseminated in a timely manner to industry. It is also far less costly and burdensome to process and maintain this data at the Secret level as well.
- *Establishing a Secure Network for Vulnerability and Threat Data:* The technology industry would greatly benefit from timely access to important data through a secure network at the Secret level, "CYBERnet." The new network must also include a contingency plan for any endpoint compromise.
- *Improving Management of Cyber Initiatives:* Too many technical personnel lack management skills and thus cannot be promoted effectively into management roles. The traditional concept of a promotion path will not work well in this area and a specific management training initiative is needed.
- *Promoting an Industry Consortium:* Encourage technology firms to focus on cybersecurity problems as a cooperative and collaborative effort to the extent possible, and not a totally competitive environment.[73]

## 3.6 Creating a Responsive Security System

A critical and recurring problem is that a far larger number of personnel in the national security area as well as the technology sector, the financial sector, law enforcement and others need timely access to cyber data, much of which remains classified. Unlike the SIGINT analog which is largely a one-way

[72] An earlier effort along these lines was made under the Defense Industrial Base. See Barry D. Watts, *The US Defense Industrial Base: Past, Present and Future,* (Washington: Center for Strategic and Budgetary Assessments, 2008).

[73] The *Cybersecurity Enhancement Act of 2014,* Public Law 113-274, encourages the public and private sectors to "work together" but provides no mechanism or funding to accomplish this.

collection regime, these sectors also see incoming threat data which needs to be shared on a timely basis with the government.[74]

Many more people in these critical sectors need to be cleared at least at the "Secret" level where clearance processing is far less costly and more rapid than higher levels such as access to Top Secret/SCI data. Accomplishing this will require a contractual basis with firms in the various sectors so that appropriate industrial security systems can be implemented. The critical issue here is one of contractual paperwork and not a level of funding for participating firms.

Often critical cyber threat data is currently collected and maintained at the Top Secret/SCI level, which greatly complicates the dissemination and storage problem, as well as the requirement for personnel to be cleared at these levels. As has been the case with other data collected by classified systems, much of the data can safely be downgraded to the Secret level and made available on a timely basis over the proposed classified network (CYBERNet).[75]

A related concern, which is also closely tied to the issue of creating a cyber work force, is the retention of security clearances for skilled personnel leaving positions in the government or industry for jobs not immediately requiring continued access to classified information. One suggestion here has been the creation of a cyber reserve force, where such individuals are maintained in a cleared status for either a surge requirement or reemployment in critical cyber areas where access needs to be reinstated.

## 3.7 Repairing the Vulnerabilities Equities Process

The United States government has established a Vulnerability Equities Process (VEP) to determine whether to withhold or disclose information about

[74] See Wagner, *Cybersecurity, Cryptology, and Privacy in Historical Context: The Challenge of New Technologies and Media, op cit.*

[75] The term "Zero-Day Vulnerability" refers to a previously unknown computer-software security vulnerability that developers have not yet patched. Zero-days are so named because once they are discovered they may be used immediately to gain access to secure data, thus giving the developer "zero days" to issue a patch or otherwise mitigate the damage of the exploit. At present there is a growing and lucrative market for the purchase of zero-day vulnerabilities. See Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits,* (Santa Monica: The RAND Corporation, 2017).

computer software security vulnerabilities.[76] Under the VEP, the government will evaluate whether to disclose a vulnerability it has obtained or discovered—so that the software developer has a chance to fix the problem—or the government can elect to withhold the information for purposes including law enforcement, intelligence gathering, and "offensive" exploitation.

Equities issues are rife in the adjustments the U.S. Government must make to adapt to the challenges of the cyber domain. A robust and secure supply chain consisting of vendors operating in the unclassified space, sometimes with foreign national employees, is critical to developing offensive cyber tools. Vulnerabilities, exploits, implants and other operational tools also face exposure from adversarial detection, unintended leakage, and bug collision, where an adversary finds and exploits a vulnerability allied services are already aware of or using.

Many of the suggested additions to the VEP would drastically curtail the U.S. operational efforts in cyberspace. Some of the concepts that would have highly adverse consequences to American national security interests include:

- Using vulnerabilities for a limited time before informing the software's developer;
- Using only vulnerabilities that have been patched; and
- Running vendor-purchased vulnerabilities through the same system as government-discovered ones

The plan currently in use, adopted by the prior administration, suffers from severe inconsistencies and issues with scalability. The VEP is extremely difficult to discuss as a coherent policy since by definition it is hedging classes of unknown risks, and much of the known data is classified or simply scattered.[77]

---

[76] The government typically obtains zero-days either by discovering them or by purchasing them from malware vendors. The *Washington Post* has reported that the NSA spent $25 million dollars on the purchase of zero-days in 2013 alone. Once the government procures an exploit, the VEP should be triggered to determine what to do with the knowledge of the vulnerability. The government's use of the VEP remains controversial as the policy gives rise to several security and privacy concerns.

[77] If an unpatched exploit remains secret, it leaves data and systems vulnerable to attack. Thus, if the government does not disclose these vulnerabilities that it obtains, then both public and private systems will be put at risk. The VEP also makes clear that the government may use vulnerabilities for law enforcement purposes as well as intelligence

Likely policy wins for the VEP are perhaps in the edge cases such as perception handling for when vulnerabilities leak or are discovered, greater understanding by multiple agencies as to the value and composition of our offensive program, and acceptance or awareness as to the value of various synergistic defensive programs.

Part of better leveraging a more centralized approach to exploits and vulnerabilities is being able to build detections into EINSTEIN and other similar systems across the various networks that the government can monitor and tying national incident response efforts into it.[78] Likewise, the U.S. has a major opportunity to influence the NATO partners' approach to coordinating on offensive information as they build offensive cyber programs.

It is important to note that defensive technology is rapidly advancing. While it currently seems unthinkable for exploits to get caught on a regular basis, this is a likely outcome of modern intrusion detection innovations. Any serious discussion of the VEP must take this into account.

## 3.8 Approaching Internet Governance with Realism

In recent years, lawyers and diplomats have invented a field known as "Internet Governance" which includes several issues, both real and imagined. With the transition from the ARPAnet to the Internet after 1989, and the proliferation of connected networks there was little or no intervention on the part of any federal agency or international organization. It was simply a more efficient communications technology that worked.

---

collection. This raises additional concerns with respect to amendments to Rule 41 of the Federal Rules of Criminal Procedure recently issued by the Supreme Court. These amendments authorize judges to issue "remote access" warrants to search computers, even when the targets are outside the jurisdiction of the court. Thus far there are no clear guidelines for the application of Rule 41 to provide for adequate methods in seeking warrants against anonymized criminal activity while keeping Fourth Amendment constitutional protections against unreasonable search and seizure.

[78] The EINSTEIN Program was originally an intrusion detection system monitoring the network gateways of U.S. Government departments and agencies in the for unauthorized traffic. The software was developed by the US-CERT at the DHS. When it was created, Einstein was an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. Einstein does not protect the network infrastructure of the private sector. Its purpose is to "facilitate identifying and responding to cyber threats and attacks, improve network security, increase the resiliency of critical, electronically delivered government services, and enhance the survivability of the Internet.

As policy issues have emerged, particularly regarding the balance between security, law enforcement, national security, and privacy, the concept of Internet governance has conflated management of the technical resources necessary for network stability with discussion of behaviors emerging from the *use* of the Internet in what is known as the content layer.

Cyberspace and the Internet are American technologies increasingly seen as a global resource. Some nations see the Internet as so important as to require state control or at least greater state control than now exists. Exactly why is unclear. Advocates also see a need for Internet regime construction and seek to define regime rules and procedures as well as underlying principles and norms for which there is no obvious need. In reality nations control Internet-related policies within their own borders, such as laws prohibiting online gambling, protecting intellectual property, or blocking/filtering access to certain content.[79]

As the Internet grew globally the concept broadened considerably. At the 2005 U.N.-sponsored World Summit on the Information Society (WSIS), Internet governance was defined as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."[80]

The U.S. has so far been forced to address these issues on an ongoing basis. While the 2005 WSIS established the Internet Governance Forum (IGF) to open an ongoing, non-binding conversation about the future of Internet governance, it has accomplished nothing of operational significance. Actual Internet governance is conducted by an international set of groups including

[79] Some authoritarian governments censor political and social content much as they do in traditional media. They see the Internet as expanding the possibility of popular communications, thus posing a threat to centralized control and dictatorship. China, Cuba, and Iran, for example, have been the most repressive countries in terms of Internet freedom. It is within their right to do so, even though the U.S. can advocate greater openness and freedom. See, James A. Lewis, *Sustaining Progress in International Negotiations on Cybersecurity,* (Center for Strategic and International Studies, July 2017).

[80] See Catherine Lotrionte, "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence," *Georgetown Journal of International Affairs*, (April 2014); Oona A. Hathaway, *et al*., "The Law of Cyber-Attack," 100 CALIFORNIA LAW REVIEW 4 (August 2012); and Jack Goldsmith, "How Cyber Changes the Law of War," 24 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1 (2013).

governments, the private sector, and research communities that create shared policies and standards that maintain the Internet's global interoperability.

To maintain interoperability, key technical and policy aspects of the core infrastructure are administered by the Internet Corporation for Assigned Names and Numbers (ICANN), which oversees the assignment domain names, Internet protocol addresses, and other key parameters.[81] The notion that whoever controls the ICANN contract somehow "controls" the Internet is a myth. Assignment of domain names and IP addresses is largely a bookkeeping exercise. Actual "control of the Internet" would consist of the ability to prevent use or abuse of this worldwide network and the withholding of any name or block of IPs could not accomplish this purpose.

Many experts emphasize that Internet governance is not the product of an institutional hierarchy, but rather comes from the decentralized, bottom-up coordination of tens of thousands of mostly private-sector entities across the globe, often referred to as "stakeholders" including network and server operators, domain name registrars, standards organizations, and Internet service providers. Governments and civilian organizations participate with the stakeholders in the development of technical policies. Some see a growing need to "police" cyberspace as the world does in other areas and urge creation of a legal regime that encourages certain uses of cyberspace and discourages others.[82]

---

[81] Originally funded under a DARPA contract, ICANN has been the subject of criticism, controversy and litigation. The 2016 decision to terminate the federal contract with ICANN was portrayed as an effort to reduce, not increase, state control over the Internet. In reality it did neither. The claim that this would help make the Internet more resilient in coming decades is nonsensical. Some claim that the most important features of the Internet users care about – openness, diversity, and fundamental resilience—are likely be better protected with less American control than with more. There is also need for security certificate authorities to be independent organizations, and not governments, since governments could effectively falsify websites to censor or collect information on the populace. This is most likely the case now in Iran and China, and quite possibly other nations as well.

[82] See Richard N. Haass, "Why the World Needs to Police the Growing Anarchy of Cyberspace," *Fortune.com*, (February 7, 2017). This article suggests a "single, integrated linked system" that would "limit what governments could do to stop the free flow of information, prohibit commercial espionage and theft of intellectual property, and severely constrain what could be done over cyberspace in peacetime to interfere with or disrupt either civilian or military systems that depend on cyberspace, as virtually all systems do now." Critics see such a concept see it as simply not achievable, and akin to outlawing espionage or war entirely.

America needs to provide guidance to those engaged in the process so that it preserves the values and opportunities the U.S. sees as essential to ongoing Internet operations, recognizing that no one government, company or organization owns, runs or controls the Internet, which has no official governing body. Each connected network establishes its own policies in keeping with a set of agreed upon protocols which have emerged over time and have come from this industry. They were never imposed by government fiat or regulation.

## 3.9 Reforming Export Control to Serve America's Interests

A paradigm shift in defense technology is under way and the export control regime will have a significant impact on how this evolves. Export Control is not only a significant issue, but also demonstrates the cracking of the older levers of power from the new realities. America's post-WWII supremacy in both civil and military technologies is increasingly challenged by the pacing of competitor states, such as China and Russia, and earlier strategic thinking about how to sustain the U.S. advantage is no longer effective. In the past, overmatch depended on the development of proprietary technologies within the U.S. defense industrial base and defending exclusivity of those capabilities through aggressive export control regimes.

The U.S. is not only suffering from prior agreements in the area of international trade, but also from international agreements such as the Wassenaar Arrangement which, if implemented, would not only have been harmful to U.S. industry but also put the nation in a far weaker position to deal with the actual issues of cybersecurity to make America safe.[83]

Experts from industry, the Departments of Commerce, Homeland Security and Defense universally agree that export controls designed for hardware cannot be universally applied to software and software development

[83] In 2013 a meeting of the 41 nations involved in the Wassenaar Arrangement which sought to control the export of encryption technology, as an arrangement on export controls for conventional arms and dual-use Technologies. This raised serious concerns both in the U.S. as well as Europe and elsewhere over the utility of the proposed rules and possible consequences for software development critical to national and related cybersecurity requirements. At the time the Department of Commerce indicated that monitoring and enforcement of these proposed rules would require significant resources and served no useful purpose. At the time DARPA led the DoD effort to oppose adoption of the Wassenaar Arrangement and put forth the position ultimately adopted by the NSC.

tools. Indeed, they may not achieve their stated objective and ultimately have the potential to be harmful to American industry and cybersecurity efforts.

## 3.10 Recognizing that the World is Going Dark

Computer systems and applications are rapidly adopting encryption schemes to meet user demands for privacy and security.[84] Legislation to prevent this development or work around it is doomed to failure, as this is a worldwide phenomenon and a technology path that cannot be stopped, and the U.S. needs to support specialized technical programs that meet this reality.

In the age of "big data" there is an ongoing debate about the use of encryption and what "going dark" really means in technical and legal terms; what impact this will have on their operations; as well as what can be done to mitigate the problem. The use of sophisticated encryption technology stands to impede operations by both intelligence and law enforcement agencies that meet even the most stringent privacy requirement of the Fourth Amendment.

While an earlier legal regime that permitted controls over encryption technology is no longer viable various solutions have been proposed that would force companies to enable access to user data to the government pursuant to a legal process. Proponents press for them under the belief that the Congress can legislate effective solutions in a world market over which they have no control. In the future commercial firms may simply not be able to comply with court orders given the state of the evolving technology.

In an earlier analog world, users were largely in control of their own personal data which often existed as paper files which they could control. With the transition to the digital world, almost all personal data now reside on servers and systems over which users have no control and are subject to hacking, theft and other forms of misuse. It is also the case that they cannot control what is done with their data by various services and vendors.

As awareness of this problem has grown, so has the demand for security and solutions which involve encryption technologies have been responsive to this user demand. Looking into the future it becomes important see the likely

[84] For an extensive analysis of this problem see, *Going Dark: Implications of an Encrypted World, op. cit.* See also, Riana Pfefferkorn, *The Risks of "Responsible Encryption,"* (Stanford University, The Center for Internet and Society, February 2018).

technical solutions that will be implemented and unintended consequences which will impact on government requirements.

User demands for greater privacy and security have impacted suppliers of both devices and software who are meeting this demand with new products employing various encryption schemes and other security features. They do so at a time when the available technology supports increasingly effective encryption and when the legal regime cannot control its application.

In most cases, the new types of protection can be provided to users at zero marginal cost and free from any effective restrictions other than export control. Legislation to prevent this or work around it is doomed to failure, as this is a worldwide phenomenon that cannot be stopped. The U.S. must support specialized technical programs that meet this reality.

## 3.11 Protecting Digital Privacy and Intellectual Property

Increasing hacks and theft of data, as well as legitimate surveillance programs important to national security have raised concerns among many Americans. New programs need to meet critical intelligence and law enforcement requirements that also protect privacy interests.[85] America can no longer allow other nations to steal the intellectual property of U.S. companies and must partner with and empower U.S. firms to increase security against all cyber threats including the theft of intellectual property by electronic means.

Central to the issues of cybersecurity as well as the needs of national security users in an era where terrorism is major concern is the concept of privacy embodied in the Fourth Amendment. Public awareness of privacy issues has been heightened recently, due to publicity over hacks and numerous leaks about government surveillance programs. A related controversy has arisen over whether firms such as Apple should be forced to help the government access the phones used by the terrorists and other criminals.[86]

---

[85] See *Cybersecurity and Privacy: Report of the Expert Workshop Held for the Defense Advanced Research Projects Agency (DARPA), op. cit.*

[86] See Kim Zetter, "How the Feds Could Get Into iPhones Without Apple's Help," *Wired* (March 2, 2016) and Jonathan Zdiarski, "Apple, FBI, and the Burden of Forensic Methodology," (February 18, 2016). https://www.zdziarski.com/blog/?p=5645

Along with the development of the Internet has been the dramatic rise of social media as a major means of communications and information sharing worldwide. This new medium has become central to all aspects of modern life and has brought with it a host of privacy and security issues that are a central part of the cyberlandscape which must be addressed.

It is not possible to implement truly effective cybersecurity programs needed to keep America safe and provide the level of personal privacy users are now demanding while acceding to every demand made by groups across the political spectrum. There has always been a dynamic tension between legitimate needs for data and individual rights, and it is increasingly becoming an issue in the cyber domain.

A wide range of groups have brought increasing attention to the vulnerability of personal data transmitted by all of the devices currently in use as well as data maintained by the commercial suppliers of network services. The world has entered an era where the vast majority of personal data is being maintained on vulnerable servers as well as large-scale data commons over which the users have no control. Major concerns here include:

- *Legitimate access to data:* Intelligence and law enforcement authorities need timely access to data, including metadata, for cybersecurity missions to make America safe.
- *Insertion of false data:* Closely related to manipulation of data, many technical experts believe that the insertion of false data to be potentially the most serious threat to cybersecurity.

National policy needs to revisit the statutes in each of these areas as well as operational programs designed to protect the privacy of users in each category.

## 3.12 Responding to Information Warfare

While most cybersecurity efforts focus on denial of service, destruction, impairment and use of malware for the theft of data for various nefarious purposes, a major issue remains in the use of the Internet and social media for information operations or information warfare related to matters ranging from politics to terrorism to geopolitical warfare. Information warfare is not a new concept; it has been a serious enterprise

for Russia and the Soviet Union for many decades, often referred to as "disinformation" or simply propaganda.[87]

New technologies and modern media provide opportunities for information operations at a scale and cost never even imagined in the days of the Soviet Union. If nothing else, various investigations following the 2016 U.S. presidential election have brought new light on such operations, although documented Russian activities in this sphere are worldwide, and have been particularly intense in eastern Europe, such the Ukraine.

[87] See, for example, Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Innovations in Warfare and Strategy, Parameters,* (2017); Paul M. Joyal, "Cyber Threats and Russian Information Warfare," Jewish Policy Center, (Winter 2016); Timothy L. Thomas, "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," *Journal of Slavic Military Studies,* (1998); and Jolanta Darczewska, *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*, (Warsaw: Centre for Eastern Studies, May 2014). There is an extensive literature on Soviet and Russian "disinformation" operations which reflect the seriousness with which such activities are viewed there.

# 4. Deterring Cyber Attack

## 4.1 Reducing Vulnerability with Defense

Recent events have refocused attention on the vulnerability of critical infrastructure to cyberattack. Credible attack capabilities against not only national security systems but systems such as the electric power grid, the financial sector, health care, voting systems, telecommunications and others that could significantly damage American society and its power projection capabilities for extended periods.

While the government and the commercial sector have undertaken various efforts to improve cybersecurity, the level of protection is obviously imperfect. The Department of Defense and the military services depend heavily on these keys sectors and have a clear interest in ensuring that protection is as strong as possible. DoD must cooperate with other federal agencies including DHS, NIST and others on these matters in terms of both technology development and defense.

Reducing the vulnerability of critical infrastructure can be seen in terms of several distinct types of technology-supported interventions:

- *Generally applicable cyber prophylaxis.* Since critical infrastructure shares the vulnerabilities of the Internet and applications as entry points, programs that enhance cybersecurity will protect critical infrastructure as well.
- *Mapping systemic vulnerabilities.* Important to meeting the challenge is a mapping of systemic vulnerabilities and a strategy for achieving greater resilience of the infrastructure to disruption. An ability to operate through disruption and to reconstitute rapidly is relevant to natural disasters and physical attacks as well as cyber threats.
- *Enhanced monitoring of specific threats to critical infrastructure.* Threat monitoring, combined with active and preferential defenses targeted on current, emerging, and evolving threats is critical to cybersecurity.

- *Strategic, operational, and tactical cyber intelligence.* A range of intelligence as well as potential offensive measures specific to cyber threats on critical infrastructure from adversaries and enemies and in gray zones in needed. Signatures specific to attack preparations on critical infrastructures can guide this approach.

Government activities are under way in most of these areas, although as yet there is no concerted central activity to bring together vulnerability mappings, intelligence information, innovative concepts, and technical judgment with input from the private sector to conduct net assessments and focus resources on the most cost-effective interventions.

DARPA, which has the longest history of programs in this area as well as the deepest technology base, has innovative technology approaches to these critical questions. In the absence of a net assessment activity[88] focusing on systems vulnerability, however, it is difficult to fully understand how valuable these individual technology efforts might be.[89]

The evolving "cyber community" finds itself in a similar situation to that facing the Intelligence Community in the 1970s, beset with a number of problems at a time of major Cold War challenges. One major element of solving the organizational problem at the time was Executive Order 12333 (1981).[90] This historic Executive Order assigned roles and missions to each of the

[88] During the 1970s the Office of the Secretary of Defense (OSD) established the Director of Net Assessment (OSD/NA) with a supporting staff and contractor base to provide net assessments in critical policy areas during the Cold War. For decades DARPA was a collaborator with OSD/NA in accomplishing many of these key net assessments.

[89] DARPA's Rapid Attack Detection, Isolation and Characterization Systems (RADICS) Program, for example, represents a serious technology effort aimed at dealing with the most serious aspects of infrastructure vulnerability. RADICS seeks to develop innovative technologies for detecting and responding to cyberattacks on U.S. critical infrastructure, especially those parts essential to DoD mission effectiveness, and provide early warning of impending attacks, situation awareness, network isolation and threat characterization in response to a cyberattack on the power grid and its dependent systems. Further work in this critical area is not only essential for DoD, but the nation as a whole. Another key DARPA Program is High-Assurance Cyber Military Systems (HACMS) which seeks to create technology for the construction of systems, which are functionally correct and meet appropriate safety and security properties. Such systems inherently reduce vulnerability in a critical area and contribute to the deterrent posture.

[90] Executive Order 12333 of December 4, 1981, 46 FR 59941, 3 CFR 1981. Subsequently amended, this EO remains as the organizational basis of the U.S. Intelligence Community.

Intelligence agencies along with specific guidance about how these missions were to be performed. Such top-level guidance is now essential in the cyber domain.

## 4.2 Asymmetry in Cyber Vulnerability

In light of these challenges "deterrence" is unlikely to be a silver bullet for preventing cyberattack by capable actors, and so reducing cyber vulnerability and improving systemic resilience are also important. Resilience is improved by mitigating vulnerabilities, eliminating unnecessary complexity, and reducing brittleness in IT systems across the U.S. military, federal civilian government, and critical infrastructure.[91] Since deterrence relies on the enemy's cost-benefit calculation, anything that can be done to reduce vulnerability and improve resilience will also increase the effectiveness of deterrence, just as deterring attacks enhances at least the apparent effectiveness of defenses.

Even leading adversaries to believe that the U.S. is less vulnerable than is the case, or raising uncertainty about existing vulnerabilities, can strengthen deterrence. Establishing a robust mix of defense, resilience and deterrence to head off this threat is critical to national security.[92]

The broad focus on deterrence vs. defense, familiar from the nuclear debate, may obscure subsidiary choices that are more familiar from other domains for warfare. The discussion largely equates vulnerability reduction with defense. Strategic defense in other realms of warfare can include a broad spectrum of options, ranging from pure vulnerability reduction, static fortification, local active defenses, and tactical and even operational-level bombardment or maneuver warfare in response to attack, to preemptive attack on enemy forces.[93] These possibilities are also worth pursuing in the cyber domain.

---

[91] One should distinguish between IT resilience and system resilience – it doesn't help to get the IT system up and running if the power sources such as generators have been destroyed.

[92] See Rebecca Slayton, "What is the Cyber Offense-Defense Balance?" *op. cit.* For a comparative review of the Nye and Slayton papers see Brandon Valeriano, "What Is the Cyber-Offense-Defense Balance? Conceptions, Causes and Assessment," *H-Diplo – ISSF Article Review 83,* (July 26, 2017).

[93] The nuclear policy debate tended to obscure the practice of nuclear war planning, which included many of these aspects. The assured second-strike nuclear deterrent depended on protection of nuclear forces from a first strike, and conversely nuclear targeting included a

Between World Wars I and II, and again during the Cold War, the U.S. focused on the capabilities of the military forces of potential enemies and developed systems and plans to deal with them. ARPA was created following the Soviet Union's surprise launch of the Sputnik satellite as one novel approach to preventing future technological surprise.[94] In the cyber realm, the ambiguity about the onset of operations affords opportunities to characterize the attack capabilities and strategies of adversary elements and may offer opportunities for devising strategies to neutralize these capabilities. As with counter-terrorism, there are overlaps between criminal investigation, intelligence operations and military action that need to be resolved in the development of an effective national response.

There is a need for an organized, central capability to characterize adversary capabilities, develop technical and operational capabilities for active defenses and preemption consistent with the legal regime. This would primarily employ cyber means but also kinetic attacks on communication nodes and lines if needed.

While the FBI and other law enforcement agencies might deploy such capabilities against criminal conspiracies, the Defense Department and Intelligence Community would be needed against national security threats. There are several problems with this dichotomy. It is not always easy to distinguish cyber threats as criminal; espionage; or targeting infrastructure posing a national security problem. They may in fact be one in the same.

Where a cyber adversary relies on a network of proxies for actual operations, it is important to consider the possibility of acting against such networks to reduce their capabilities or willingness to act on behalf of enemy states. The law enforcement strategy of dynamic concentration – a form of deterrence resulting from the example of swift and sure consequences to those engaging in particular behaviors – is relevant to controlling such groups so long as detection of the behavior subject to sanction is relatively cheap. There may

major focus on enemy nuclear forces. See Lawrence Freedman, *The Evolution of Nuclear Strategy (3rd Edition),* (London, Palgrave, 2003).

[94] ARPA's creation was one of several initiatives undertaken by the Eisenhower Administration to deal with what was seen as a catastrophic shortfall in the science and technology area relative to the Soviet Union. Other initiatives such as the National Defense Education Act provided critical funding for graduate education in this area. See George Kistiakowsky, *A Scientist at the White House,* (Cambridge: Harvard University Press, 1976).

be a combination of defenses, both passive and active, as well as web surveillance technologies that achieve these conditions.[95]

The U.S. needs to adopt policies that channel opportunities for cybercrime in ways that do not unduly contribute to an adversary's capabilities to engage in either cyberespionage or cyberwarfare. Opportunities for cybercrime should not be permitted to escalate into a severe national security problem. A key objective here would be to limit cybercrime to the level of a financial nuisance rather than having it ultimately contribute to the evolution of more severe hostile capabilities for a nation state or non-state actor.

## 4.3 Cyber Deterrence and Dissuasion Campaigns

The Defense Science Board task force report on *Cyber Deterrence* offered the useful concept of "tailored deterrence campaigns." where it emphasized that deterrence must be "tailored" to the decision makers being deterred, because deterrence operates by affecting their cost-benefit calculations in deciding whether to trigger an attack.[96] Different adversaries will have different interests that can be brought into the deterrence frame; China with its trade and financial interactions with the rest of the world and its aspirations to global leadership is in a very different relation to the U.S. than North Korea or non-state actors such as terrorist organizations.

Different leadership groups process information differently and so how communications are framed matters. This much is familiar from other deterrence domains, although it has special implications for the cyber realm given the low cost of an attack, problems of timely and accurate attribution, deniability of cyberattacks, as well as continuity of cyber operations from

[95] See Kleiman, *When Brute Force Fails op. cit.*

[96] The 2017 DSB Task Force glossed over two key aspects of deterrence of foes such as ISIS, although it did say that prevention/preemption and defense should be the principal U.S. approach for dealing with such adversaries. First, some adversaries may wish to cause maximum damage to the U.S. irrespective of the immediate repercussions to them. Second, to the extent that the U.S. is already committed to using all its power to destroy an enemy, then there is nothing being withheld from the fight and nothing left to threaten as part of a deterrence campaign. One could make the case that the U.S. would be so enraged by a catastrophic attack on critical infrastructure that it might respond in ways that it would have considered immoral or ill-advised for other reasons previously, for example much higher civilian casualties or putting U.S. combat formations on the ground in the course of destroying ISIS leadership. Still, it may be difficult to assure the American people that everything possible is being done to destroy ISIS and at the same time to deter ISIS leadership through the threat of greater force.

nuisance hacking through exploits aimed at network reconnaissance, data exfiltration and other intelligence purposes, through destructive software, to the activation of software causing various degrees of damage.

It is also important to consider how deterrence impacts not only decision makers but also on operators who would implement any cyberattack. Often a cyber attack relies on proxies and affiliates and not just on forces clearly under direct command and control. As in the U.S., foreign entities often "outsource" technical operations to external groups such as contractors.[97] Focusing on the decision-making of these elements may provide another dimension for deterrence to operate.

What is new in the concept of a deterrence *campaign* is the time dimension. For most national security issues a deterrence posture has been thought of as being established prior to a potential crisis, at which point that posture operates to influence an adversary's decisions. Deterrence against use of weapons of mass destruction or other forms of escalation may continue to operate during wartime, but again these were seen primarily as operating as static constraints rather than as dynamic "campaigns."

The DSB Task Force's notion of a deterrence campaign presumably responds both to newness of the cyber threat and the need for declaratory and other actions to establish deterrence, given the limited responses so far to cyber intrusions and attacks, and to the fact that adversaries are carrying out cyber intrusions and even attacks during peacetime, and so current reactions or the lack thereof are setting expectations. The lack of an effective response now to any level of cyber intrusion is likely to make the later establishment of effective cyber deterrence that much harder.

Because cyber operations are already underway, options for response in the covert realm as Title 50 activities exist that can be calculated to enhance deterrence up the threat spectrum, though there may also be the potential for such interactions to get out of hand – which adds to the argument that such

[97] For some unknown reason, U.S. decision-makers are willing to accept the fact that a large percentage of technical work done by the Intelligence Community and the military is really outsourced to the contractor community, with many working within a highly classified environment, but fail to acknowledge that the Russians and others do so as well, and that these outsourced efforts are in fact integral state activities. On the other hand Russia seems to outsource some activities to groups that are allowed to maintain their own criminal activities, something that has no obvious parallel in U.S. policy.

interactions need to be coordinated and supervised at the national level as part of a whole-of-government campaign strategy.

What are the requirements for conducting a tailored cyber deterrence campaign and how can technology help? To the extent possible, the government needs accurate intelligence on enemy cyber capabilities, strategies, as well as past and current activities, including those aimed at targets besides the U.S., including those advanced through proxies. Together with a vulnerability assessment from a set of red teams this data can be used to develop an indications and warning approach to provide timely knowledge of future cyber intrusions and attacks, not just for defending critical networks and systems, but also for understanding adversary activities.

Essential here is a government-wide, and potentially, an international understanding of what sorts of intrusions may be accepted and what would prompt cost-imposing responses, with what the DSB calls "playbooks" for a portfolio of cyber and non-cyber responses worked through in advance.[98] Further, it is important to have a good understanding of what the leadership group and perhaps those implementing the exploits care about. This provides the U.S. with pressure points for signaled and actual retaliation as part of the playbook for that adversary.

Many leadership groups and their associates have foreign and other assets that are not overt and so holding those assets at risk as part of the lower rungs of an escalation playbook may make sense. Moreover, if some of these actions are carried out against those involved in illegal intrusions short of a catastrophic attack, that will bolster the credibility of focused retaliatory threats, tend to dissuade hackers from lending their talents from attack

[98] There has been an ongoing debate among experts about the possibility of "norms" and international law with respect to cyber warfare. The NATO Cooperative Cyber Defence Centre of Excellence has been addressing the subject of 'cyber norms' since its establishment in 2008 and how existing international legal norms apply to cyberspace by hosting and facilitating the *Tallinn Manual* process. See, Michael N. Schmiitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* (Cambridge: Cambridge University Press, 2013). The other side of this argument is that such "norms" are unmitigated nonsense, since terrorists and other adversaries have no interest in international law, and much adversarial cyber activity falls into the category of espionage for which there are no established norms or international law. See also, James A. Lewis, "The Devil Was in the Details: The Failure of UN efforts in Cyberspace," *Cipher Brief*, (August 2017).

capabilities against the U.S. and impede hostile powers from assembling such capabilities.[99]

Another key area for policy improvement is capabilities for actual and credible public source attribution of intrusions and attacks. Lack of timely and accurate attribution makes retaliation problematic owing to the possibility of false flag attacks provoking an unjust attack on an innocent adversary. Further, the lack of an ability to provide credible attribution to international partners hobbles responses such as sanctions that require joint international actions or access to foreign financial institutions that may require bilateral cooperation. Also, the lack of credible public attribution may inhibit the ability of the U.S. to mobilize public support needed to underwrite strong and sustained action.

Currently, public and international attribution often risks compromising forensic signatures or intelligence sources and methods that would impair the ability to provide similar attribution in the future. It can be presumed that this fact sometimes dissuades the government from responding as forcefully as it otherwise might.

Conceivably it might be possible to create an international institution, possibly under United Nations auspices, with enough secrecy and credibility so that it could certify attributions made with such confidential information and secure the benefits of credible public attribution without the compromise of forensic signatures and sensitive intelligence sources and methods.[100]

These policy and institutional requirements for deterrence campaigns suggest some general categories of technologies that would be useful:

- *Characterization of cyber intrusion and attack capabilities:* Technologies and intelligence techniques that support more accurate and timely intelligence and characterization of cyber intrusion and attack capabilities and current activities by

[99] There are several historic precedents for similar classified activities conducted by the U.N. Another problem with the DSB Task Force Report is the suggestion that deterrence campaigns are really only intended to be focused on major adversaries; they assert that regional powers such as North Korea or Iran, as well as ISIS and similar non-state actors, can and must be denied the capability to cause significant cyber damage. Certainly, this is a desirable objective given the uncertainties of deterring a desperate rogue state or group but one would not want to just assume that regional states and non-state actors are incapable of causing major disruption to U.S. critical infrastructure.

[100] Presumably the International Atomic Energy Agency (IAEA) would be one model, but the timeliness and other technical factors may prove too daunting.

adversaries and their proxies. These would include but not be restricted to mechanisms for aggregating network intrusion indications from systems and networks in the private sector.

- *Timely and Accurate Attribution:* Technologies and techniques that would allow more rapid and certain attribution, and even better, credible public attribution without compromise of sensitive forensic signatures and intelligence sources and methods.

- *Signaling to Adversaries:* Mechanisms and tactics for signaling to an adversary that the U.S. has embedded exploits such as hostile code in their systems or that threatens assets important to leadership or those executing cyberattacks without revealing sufficient information to enable removing or neutralizing such code.

- *Targeting Specific Persons:* Methods and tactics for identifying specific persons involved in cyberespionage and potential cyber attacks, including their bank accounts and other personal information, permitting deterrent and dissuasive messages to be focused on them.

Deterrence needs to operate in advance of a larger attack by imposing costs on hostile activities and intrusions short of a major attack, focusing on impeding the development of capabilities, including latent exploits through dissuasion and sub-national targeting as well as on actual attacks through the threat of unacceptable retaliation. Even below the level of cyberattacks that impose substantial costs on the U.S., retaliation should not be restricted to the cyber domain, but might include targeted economic sanctions and international criminal warrants, among other means.

A non-governmental approach to raising the costs on cyber attackers that has received limited attention would be a change in the law that enables victims of computer attacks try to defend their data and their networks through hacking back or counterhacking.[101] At present such a vigilante approach remains illegal under the 1986 Computer Fraud and Abuse Act which is a deterrent to those entering the field. It would clearly raise the costs for potential hackers and several experts have made the case for changes in the legal regime that would permit this.

Historically vigilantes have been an anathema to the legal establishment for the obvious reasons, and they have often been subject to prosecution.[102] At the same time, however, vigilantes have come into place where the legal regime was dysfunctional or non-existent and did bring "justice" of sorts to lawbreakers and deterred others. Frequently the "Wild West" analogy has been used with respect to cybersecurity, and it was one were vigilantes were the most prevalent.

## 4.4 Resilient Cyber Infrastructure

A key component of the current strategy for cybersecurity is a set of programmatic initiatives that aim to dramatically increase the resilience of the cyber infrastructure. These form an essential foundation for shaping the cyber environment. Programs in this area not only aim to detect malicious cyber activity, but also seek automated remediation and response to cyberattack. Other programs are focused on more basic engineering and software tools to make both the network itself and connected devices more secure, including resilient cyber-physical systems and infrastructure.

---

[101] See Nicholas Schmidle, "The Digital Vigilantes Who Hack Back," *The New Yorker*, (May 1, 2018). See also, Wyatt Hoffman, and Ariel E. Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* (Carnegie Endowment for International Peace, 2017), and Jeremy Rabkin and Ariel Rabkin, *Hacking Back Without Cracking Up; Aegis Paper Series No. 1606*, (Stanford University Hoover Institution, 2016). Stewart Baker, who was previously NSA General Counsel, has correctly stated "Hacking is a crime problem and a war problem. You solve those problems by finding hackers and *punishing* them. When they feel their profession isn't safe, they'll do it less."

[102] There are some possible models for the outsourcing or privatization of backhacking in the law enforcement areas, such as commercial bounty hunters. An easier sell would be in the covert operations area under Title 50 where significant outsourcing already exists and there are far fewer legal bars to such operations.

### 4.4.1 Resilient Networks

Users with significant computing requirements depend on access to large, highly shared data centers for data processing and often there is a high cost and latency of this process, especially when network throughput is limited or when the application requires a rapid time response. The ability to leverage computing power that is available "locally" could substantially improve application performance while reducing mission risk.

A major threat continues to be distributed denial of service (DDoS) attacks, orchestrated by sets of networked hosts that collectively act to disrupt or deny access to information, communications or computing capabilities, generally by exhausting critical resources. Such attacks can range from botnet-induced volumetric attacks, to low-volume attacks that can be more problematic from a defensive standpoint as they target specific applications, protocols or state-machine behaviors to evade intrusion-detection techniques.

- *The Dispersed Computing Program* seeks scalable, robust systems that enable secure, collective tasking of computing assets by users with competing demands, and across large numbers of computing platforms where network connectivity is variable and degraded.[103]
- *The Extreme DDoS Defense (XD3)* improves resilience to DDoS attacks by dispersing cyber assets to complicate targeting; disguising the characteristics of assets through networked maneuver to confuse or deceive the adversary; and using adaptive mitigation techniques on endpoints to blunt attacks penetrating other defensive measures.
- *EdgeCT* seeks to bolster the resilience of communication over IP networks by instantiating new capabilities in computing devices within user enclaves at the WAN edge.[104] New systems incorporate real-time

[103] The lack of programmable computing capabilities within data networks has been a problem since the beginning of Internet architecture when the main protocols were first defined, such as TCP in 1981. Since then network transmission capacities have grown by many orders of magnitude, users' application requirements have changed enormously, and programmable, secure high-speed information processing within the network is now technically feasible.

[104] The U.S. military is heavily dependent on networked communications and the wide-area network (WAN) infrastructure that supports communications is vulnerable to a wide range of failures and cyberattacks that can severely impair connectivity. Examples include inadvertent or malicious misconfiguration of network devices, hardware and software

network analytics, holistic decision systems to determine actions that mitigate network events, and dynamically configurable protocol stacks that implement these decisions.

### 4.4.2 Assured Engineering

Embedded and networked systems underlie modern technologies ranging from large supervisory, control and data acquisition (SCADA) systems to medical devices such as pacemakers; computer peripherals; communication devices; as well as vehicles, airplanes and satellites.[105] Networked devices enable convenient access to diagnostic information, perform software updates, lower costs, and improve ease of use. They are also vulnerable to remote attacks that can cause physical damage while hiding the effects from monitors.

- *High-Assurance Cyber Military Systems (HACMS)* creates high-assurance cyber-physical systems with critical safety and security properties, including interactive software synthesis systems, verification tools, and model checkers enabling for military systems ranging from unmanned vehicles to weapons, satellites, and command and control devices.
- *Cyber Assured Systems Engineering (CASE)* develops design, analysis and verification tools for system engineers to design-in cyber resiliency for embedded computing systems making them tolerant to cyberattacks so that they can recover and continue to function.

### 4.4.3 Eliminating Vulnerability in Algorithms

As new defensive technologies make old vulnerabilities difficult to exploit, adversaries move to new vulnerabilities and exploits based on flawed implementations of algorithms. Once new defensive technologies make vulnerabilities based on flawed implementations more difficult to exploit,

failures, and extended delays in IP route convergence, DoS flooding attacks, and other attacks resulting from malicious code embedded within network devices.

**105** Embedded computing systems are ubiquitous in critical infrastructure, vehicles, smart devices, and military systems. Conventional wisdom once held that cyberattacks against embedded systems were not a concern since they seldom had traditional networking connections on which an attack could occur. Now, however, attackers have learned to bridge air gaps that surround the most sensitive embedded systems, and network connectivity is now being extended to remote embedded systems subjecting them to cyberattacks, either as the end goal of the cyber assailant or means to a greater end.

however, adversaries will turn their attention to vulnerabilities inherent in the algorithms themselves.

- *Space/Time Analysis for Cybersecurity (STAC)* develops tools for identifying vulnerabilities related to the space and time resource usage in algorithms such as side channel attacks.[106] This enables the identification of vulnerabilities in software at levels of scale and speed great enough to support search for them in critical software

### 4.4.4 Automated Repair and Adaptation of Software

As computing devices become more pervasive, the software that controls them has become increasingly more complex. Making software more robust and resilient, ensuring that programs are correct—especially at scale—remains a difficult endeavor. Errors triggered during program execution can lead to major problems, runtime failure or other unintended behavior.

Whether or not a program is operating correctly requires an understanding of its intended behavior, and a means to convey this for automated inspection. Software operates within an ecosystem of libraries, models, protocols and devices which change over time in response to new technologies, as well as a consequence of repairing discovered vulnerabilities. Applications may no longer work as expected because their assumptions on how the ecosystem should behave may have been violated.

- *Mining and Understanding Software Enclaves (MUSE)* advances the way software is built, debugged, verified, maintained with an infrastructure built around a large body of software drawn from open source code now available. Key to this is a specification mining engine that leverages deep program analyses and underlying big data analytics.
- *Building Resource Adaptive Software Systems (BRASS)* realizes advances in the design of long-lived, survivable and complex software systems that are robust to changes in their ecosystem.

[106] Side-channels are unintended indirect information flows that cause a software system to reveal secrets to an adversary. While the software may prevent the adversary from directly observing the secret, it permits the adversary to observe outputs whose varying space and time characteristics are controlled by computations involving that secret.

### 4.4.5 Code Obfuscation

Reverse engineering of software today is not difficult, and generally requires no more than a debugger, a compiler and relatively limited effort to de-obfuscate code that has been obfuscated with the best current methods. Relatively easy program obfuscation is based on "security through obscurity" strategies, often by inserting passive junk code into a program's source code. Program obfuscation methods do not have security models that enable assessment of what is gained by a given obfuscation effort.

- *SafeWare* develops obfuscation technology that renders intellectual property algorithms incomprehensible to a reverse engineer but allow the code to otherwise compile and run normally. This new obfuscation technology provides security that does not depend on the appearance of complexity in code structure, but difficult mathematical problems an attacker would have to solve.

### 4.4.6 Sensing and Detecting Malicious Behavior

Government and non-government users all rely upon commercial "off-the-shelf" (COTS) technology devices, including mobile phones, printers, computer workstations and many others. These devices are the product of supply chains involving vendors from many nations providing components that included large amounts of software and firmware. Long supply chains provide adversaries with opportunities to insert malicious functionality into this software and firmware that can be exploited to accomplish harmful objectives, including exfiltration of data and sabotage of critical operations.

While attempts have been made to manage supply chain risk indirectly by investigating manufacturers, there are no accurate and cost-effective means to examine the software and firmware provided with every new device and software update. The problem of enterprise-scale vetting of the software and firmware on COTS devices is almost impossible, and the nation needs the ability to gain confidence in the software and firmware on their devices by directly examining the devices themselves.

- *Vetting Commodity IT Software and Firmware (VET)* addresses the threat of hidden malicious functionality in COTS devices by demonstrating the

technically feasibility of determining that software and firmware on these devices is free of hidden malicious functionality.[107]

### 4.4.7 Automated Vulnerability Remediation

A critical piece of solving the cybersecurity problem lies in an automated, scalable, capability for vulnerability detection and patching, particularly as more systems—from personal devices to major military platforms—become dependent upon the Internet. The manual process of finding and countering bugs, hacks, and other malicious software is still antiquated, and security professionals spend many hours, searching millions of lines of code to find and fix vulnerabilities that come from nefarious actors.

Addressing this need called for a major effort utilizing supercomputers and advanced software systems previously unknown. The resulting program and the competitors in this grand challenge brought about a truly new paradigm in the field of cybersecurity and computer science.

- *Cyber Grand Challenge (CGC)* was a DARPA effort to overcome these challenges by demonstrating automatic defensive systems capable of reasoning about flaws, formulating patches and deploying them on a network in real time.[108] These technologies may someday overturn today's attacker-dominated *status quo*. This vision requires a new approach to computer security, program analysis, and data visualization leading to remediation, at machine speeds and establishment of an ongoing community for automated cyber defense.
- *Computers and Humans Exploring Software Security (CHESS)* aims for capabilities to address zero-day vulnerabilities at a speed and scale for

**107** This approach supports the *Comprehensive National Cybersecurity Initiative*, (2009) which specifically named developing a "multi-pronged approach for global supply chain risk management" as a key national security goal.

[108] The 2016 DARPA Cyber Grand Challenge included some of the top security researchers and hackers in the world where cyber reasoning systems (CRS) automatically identified software flaws, and scanned a purpose-built, air-gapped network to identify affected hosts as teams were scored on how well their systems protected hosts, scanned the network for vulnerabilities, and maintained the correct function of software. CGC was the first head-to-head competition between some of the most sophisticated automated bug-hunting systems ever developed as these machines played the classic cybersecurity exercise of Capture the Flag in a specially created computer testbed laden with an array of bugs hidden inside custom, never-before-analyzed software. The machines were challenged to find and patch within seconds—not the usual months—flawed code that was vulnerable to being hacked and find their opponents' weaknesses before they could defend against them.

the growing, complex software ecosystem by enabling humans and computers collaboratively reason over software artifacts. This will create opportunities for technical experts to assist in the detection and remediation of known and emerging threats.

### 4.4.8 Binary Resilience

The rapid pace of innovation in software and hardware development has produced systems that still remain highly vulnerable to attack. While less vulnerable hardware and software is possible to design from scratch, basic security improvements that gradually diffuse into the installed base is a process that can take years. One alternative is to produce defensive cyber technology that can be deployed to protect existing and planned software systems without requiring major changes.[109]

- *Cyber Fault-tolerant Attack Recovery (CFAR)* is producing defensive cyber techniques that can be deployed to protect both existing and planned software systems for military and civilian environments without requiring changes to the concept of operations of these systems. This exploits technology developments that have caused CPU manufacturers to offer new features, such as multiple cores and fault-tolerant architectures to detect, isolate and mitigate faults.

### 4.4.9 Critical Infrastructure Rapid Recovery

A major national policy goal is the protection of the critical infrastructure from cyberattack. [110] It is evident that the entire national security community is dependent on many elements of nation's critical infrastructure, such as the electric power grid.

---

[109] Recent advances in lifting compiled binaries to intermediate representations suitable for recompilation may enable the application of this approach to systems for which there is no access to source code. This could potentially make legacy computer systems more secure by recompiling them. The resulting systems would operate identically to the originals, so there would be no retraining costs and no change to existing operations.

[110] Presidential Policy Directive/PPD-21 *Critical Infrastructure Security and Resilience, op. cit.* As noted "The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being."

- *Rapid Attack Detection, Isolation and Characterization Systems (RADICS)* is developing technologies for detecting and responding to cyber-attacks on critical infrastructure and will provide early warning of impending attacks, situation awareness, network isolation and threat characterization in response to cyberattack on the power grid and its dependent systems. These technologies include anomaly detection, automated reasoning, mapping of systems networks; and rapid forensic characterization of cyber threats in control system devices.

### 4.4.10 Internet of Things Protection Using the Analog Domain

A major cybersecurity concern for national security users, as well as others is posed by the Internet of Things (IoT), the network of physical devices embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data.[111] Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

The IoT is due to a convergence of technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems. The technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IoT devices.

- *Leveraging the Analog Domain for Security (LADS)* is developing a protection paradigm separating security-monitoring from the protected system, focusing on low-resource, embedded and Internet of Things (IoT) devices. These technologies associate the running state of a device with its analog emissions to permit decoupled monitoring that confirms the current state of software running on the device and instruction is executing, or which part of memory is being accessed.

[111] See Friedemann Mattern and Christian Floerkemeier*, From the Internet of Computers to the Internet of Things,* (Institute for Pervasive Computing, ETH Zurich, 2016). The traditional fields of embedded systems, wireless sensor networks, control systems, automation and others all contribute to enabling the Internet of Things. See also, James A. Lewis, *Managing Risk for the Internet of Things*, (Center for Strategic and International Studies, February 2016).

### 4.4.11 Data Integrity

A matter of increasing national security concern in is the integrity of data collected by a wide range of information systems. In the imagery area the government has historically operated collection systems that provided imagery with assured integrity, while consumer imaging technology such as digital cameras and mobile phones has become widespread, enabling people worldwide to take and share images and video instantaneously.

Individuals, including relatively unskilled users, now have the ability to manipulate and distort visual media. While some manipulations are benign, some are for adversarial purposes, such as propaganda, misinformation campaigns, and information warfare. This is enabled by the wide-scale availability of image and video editing applications that permit editing that is difficult to with current image analysis and visual media forensics tools. At present automated forensic analysis for imagery does not exist.

- *Media Forensics (MediFor)* provides technologies for the automated assessment of the integrity of an image or video and integrating these in an end-to-end media forensics platform. It detects manipulations and provides information about how manipulations were performed and about the overall integrity of the media.

### 4.4.12 Data Privacy

The movement from an analog world to a digital one is a fact of modern life; people have much less control over their personal data or what is done with it. Paper files and other antiquated media have been replaced by digital files, servers and devices while the data in these systems is vulnerable to "hacks," surveillance programs and commercial exploitation.[112]

As a result of both increased awareness and actual damage, users are demanding greater privacy and security. Commercial suppliers of devices and software are meeting this demand with new products employing encryption schemes and other security features. They are doing so at a time when technology supports effective encryption, and when the legal regime can no longer control its application. The new types of protection are being provided

[112] Unauthorized access to data has gone beyond benign or embarrassing breaches to serious criminal behavior producing substantial economic loss. Non-state actors and hostile countries are endangering the nation's security and its political process. See *Going Dark: Implications of an Encrypted World, op. cit.*

to users at no marginal cost and free from any effective restrictions other than possible export control.

At the same time collection and analysis of information on massive scales has clear benefits for society: it can help businesses optimize online commerce, medical workers address public health issues and governments interrupt terrorist activities.[113] Yet respect for privacy is a cornerstone principle of American democracy. There is a growing desire to understand, control and manage the "digital contrail" of personal information continually being produced – data that other people or organizations could exploit.

- *BRANDEIS* is developing the technical means to protect private information by breaking the tension between maintaining privacy and being able utilize the value of data.[114] The program provides an option enabling safe and predictable sharing of data in which privacy is preserved with tools that enable private data to be used only for its intended purpose and no other by providing the data owner with mechanisms for protecting their data before sharing it with a data user.

### 4.4.13 Configuration Security

The growth of the Internet-of-Things (IoT) and network-connected devices has led to technical diversity in deployed systems. Most consumer devices have minimal security and remain vulnerable to malware. It is then possible to launch distributed denial of service (DDoS) attacks on Internet infrastructure utilizing connected devices and systems that provide a vast attack surface. While the diversity of what can now be connected, monitored,

[113] For an analysis of this area see *Cybersecurity and Privacy: Report of the Expert Workshop Held for the Defense Advanced Research Projects Agency (DARPA), op. cit*. Numerous recent incidents involving the disclosure of data have heightened society's awareness of the extreme vulnerability of private information within cyberspace and of the relationship of private data with personal and national security.

[114] The BRANDEIS program also addresses the cognitive challenge of data volume and complexity in that individuals or enterprises need a meaningful way to make choices about how to share data, including understanding the implications of the use of any stored data about them. The potential impact of the BRANDEIS program is dramatic. Assured data privacy can open the doors to personal medicine, effective smart cities, detailed global data and fine-grained Internet awareness.

and controlled over the Internet has increased dramatically, economies of scale have also decreased platform diversity.

- *Configuration Security (ConSec)* is developing a system to automatically generate, deploy, and enforce configurations of components that address system vulnerabilities and minimize attack surfaces by treating component configuration as an element of the system's behavior and security. More secure systems can be deployed to enhance security without requiring new software development or hardware changes.

## 4.5 Broad Cyber Situational Awareness

Another key component of the strategy for cybersecurity are initiatives that provide more rapid and accurate warning of cyberattack and related threats. Essential here is the timely ability to detect malicious cyber activity. Also critical in dealing with a cyberattack is accurate attribution to the perpetrator of the attack, as well as an ability to then track a perpetrator of a cyberattack to activity within specific systems and hosts.

### 4.5.1 Behavior and Threat Detection

Networks within the U.S. and abroad face cyber threats from a range of adversaries and attack vectors. Malicious activity also crosscuts organizational boundaries, as nefarious actors use networks with less protection to pivot into networks containing critical data. Detection of these threats requires adjustments to network and host sensors at machine speed, and data needed to detect these threats may be distributed across devices and networks while the perpetrators hide their activities and movement, both physical and virtual, inside DoD, commercial, and other networks.

Available commercial tools do not address the scale and speed needed to provide the defense for multiple networks which lack robust mechanisms to collect, share, and respond to threat intelligence. Such data may be diffused and located across many networks and endpoint devices. Traditionally, cyber defense technologies focus on either host or network data. Malicious activity, however, crosscuts networks and hosts, so detection of threats within or across very large enterprise networks is not simply an issue of scale, but also a challenge due to the nature of malicious activities.

A particular problem is posed by wireless networks where most prior work has focused on efficiency and stability in benign conditions.[115] Insufficient attention has been paid to vulnerabilities arising from the new features being added to make wireless networks more efficient. The focus on efficiency has resulted in protocols that implicitly trust all information shared about the state of the nodes and the larger network. Consequently, when the shared information among these nodes is bad, the network becomes unusable.

As the use of wireless systems expands, the likelihood of network compromise, whether maliciously or by unwitting misconfiguration, also increases. Beyond the conventional node-by-node security in use today, network-based checks are needed to ensure that misinformation inserted into the control protocols does not disable the network functionality.

- *Wireless Network Defense* is developing technology for controlling wireless networks by enabling improvement in the robustness of the class of wireless networks that are being fielded in the near future, and also to provide a reliable foundation on which to build the subsequent generation of wireless systems.
- *Cyber-Hunting at Scale (CHASE)* is developing tools to detect and characterize novel attack vectors and disseminate protective measures both within and across enterprises. This will enable networks to reconfigure sensors and disseminate protective measures at machine speed and explore real-time investigations of potential cyber threats through adaptive data collection. These technologies also enable detection, characterization, and strategic data management that can cue automated network protective measures.

### 4.5.2 Enhanced Attribution

Any response to cyberattack depends on the timely and accurate attribution of the attack to a specific actor – be it a nation-state, non-state actor or a criminal element.[116] Malicious actors in cyberspace operate with little fear

[115] See Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, (2005).

[116] See, for example, Lily Hay Newman, "Hacker Lexicon: What it the Attribution Problem, *Wired,* (December 24, 2016) available at: https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/. See also Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies,* (2015).

of being caught as it is extremely difficult, in some cases perhaps even impossible, to reliably and confidently attribute their actions. This is at least in part a result of a lack of end-to-end accountability in the current Internet infrastructure. Cyber campaigns spanning jurisdictions, networks, and devices are only partially observable from the point of view of a defender operating entirely in friendly cyber territory such as an enterprise network.

The identities of malicious cyber operators are often obscured through multiple layers of indirection. Currently the characterization of malicious cyber campaigns based on indicators of compromise, such as file hashes and command-and control infrastructure identifiers, allows these operators to evade detection and resume operations simply by superficially changing their tools, as well as aspects of their tactics, techniques, and procedures. The lack of detailed information about the actions and identities of adversaries inhibits the options for both cyber and non-cyber responses.

- *Enhanced Attribution (EA)* makes currently opaque malicious cyber adversary actions and individual cyber operator attribution transparent by providing visibility into aspects of malicious cyber actions and increases the ability to reveal actions of malicious cyber operators without damaging sources and methods. This is done with techniques and tools for generating operationally relevant information about multiple malicious cyber campaigns involving several operators.

### 4.5.3 Tracking Adversary Actions Within Hosts

Modern computers act as black boxes in that they accept inputs and generate outputs with little or no visibility into their internal workings. This limits the potential to understand cyber behaviors at the level of detail necessary to detect and counter some of the most important types of cyber threats, particularly advanced persistent threats (APTs) which act slowly and deliberately to expand network presence and achieve goals such as information exfiltration, interference, and denial of capability.

APTs can remain undetected for years and their activities can blend with the inherent background "noise." Further, a lack of understanding of complex system interactions interferes with and often inhibits the ability to diagnose less sophisticated attacks or non-malicious faulty behavior.

- *Transparent Computing (TC)* makes opaque computing systems transparent by providing visibility into component interactions during system operation across all layers of software abstraction. It provides

technologies to record, preserve and track the interactions and causal dependencies among system components and assemble dependencies into behaviors that enable reasoning in real-time, thus "connecting the dots" across legitimate but collectively indicate malice.

## 4.6 Accurate and Robust Cyber Response

### 4.6.1 Collaborative Planning and Execution

National policy explicitly recognizes cyberspace as a critical domain of operations by the U.S. military and its protection is a national security issue. This policy clearly defines cyber operations as critical elements in any future conflict scenario. As is the case with other technology areas this includes both defensive and offensive cyber operations.

Since its inception DARPA's mission has been the development of technologies that support Defense Department and related national security requirements. Given the agency's history in the development of cyberspace technologies DARPA can support growing needs for new technologies for cyber operations in the conflict domain. This technology base can be utilized by other defense agencies and the military services with operational responsibilities.

- *Plan X* is a foundational cyberwarfare program to develop platforms for the Department of Defense to plan for, conduct, and assess cyberwarfare in a manner similar to kinetic warfare.[117] The program bridges cyber communities of interest including academia; the defense industrial base; and, the commercial technology industry.

### 4.6.2 Social Engineering Defense

The development of cyberspace over the past 40 years has resulted in a connected world that has also enabled major advances in national security from pervasive real-time intelligence and communications to optimal logistics. With this connectivity has come the threat of cyber attacks on both military systems and critical infrastructure. While a large fraction of current cyber security efforts focusses on computers and networks, more than 80% of cyberattacks and over 70% of those from nation states seek to exploit humans

[117] DARPA has stated that Plan X will not develop cyber offensive technologies or effects, and that national policymakers will determine how the cyber capabilities developed under Plan X will be employed to serve U.S. national security interests.

rather than computer or network security flaws. Cybersecurity therefore requires efforts to not only protect computers and networks but their human users as well.

Attacks on humans are "social engineering" because they manipulate or "engineer" users into performing desired actions or divulging information. Most such attacks simply attempt to get unsuspecting Internet users to click on malicious links. More focused attacks attempt to elicit sensitive information, such as passwords and private information or steal things of value from individuals by earning unwarranted trust where such trust is typically earned through interaction or co-opted via a spoofed or stolen identity. Depending on the level of sophistication, these attacks will go after individuals, organizations, or a large part of the population.

Social engineering attacks work because it is difficult for users to verify every communication they receive, and verification requires a level of technical expertise that most users lack. Compounding the problem, many users have access to privileged information creating a large attack surface.

- *Active Social Engineering Defense (ASED)* develops technology to automatically elicit information from an adversary to identify, disrupt, and investigate social engineering attacks. It does this by mediating communications between users and attackers, actively detecting attacks and coordinating investigations to discover the identity of the attacker.

### 4.6.3 Gray Space Operations

Improving network security alone is not enough to counter major cyber threats as the majority of botnet nodes reside in neutral networks often referred to as "gray space."[118] Malicious actors are able to use collections of compromised and conscripted devices owned and operated by third parties, commonly referred to as botnets with impunity for criminal, cyber espionage, and network attacks. Current incident response methods are too resource and time consuming to address the problem at scale. Active defense methods are

[118] Recent examples of botnets and similar malicious code include Mirai, Hidden Cobra, WannaCry, and Petya/NotPetya. The potential scale of their effects makes such malware a serious national security threat. The May 2017 Executive Order *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* specifically identifies botnets as a high priority national security issue.

insufficiently precise and predictable in their behavior, posing a risk that they may cause processing issues or unintended consequences

The U.S. needs the ability to identify and neutralize botnets and other large-scale malware from compromised devices and networks in a scalable, timely, safe, and reliable manner, in accordance with appropriate privacy and other legal constraints. Such a capability must be effective even if the owners of botnet conscripted networks are unaware of the infection and are not actively participating in the neutralization process.

- *Harnessing Autonomy for Countering Cyberadversary Systems (HACCS)* is investigating the creation safe and reliable autonomous software agents to counter malicious botnet implants and large-scale malware with a quantitative framework and established parameters for their safe, reliable, and effective use. Key to this development are algorithms that measure the accuracy of botnet-infected networks; identifying the type of devices residing in a network; and the stability of access vectors without affecting the systems and networks on which they reside.

## 4.7 Transition to an Inherently Secure Internet

The Internet was not initially designed for security. At the outset there were few ways to access the early ARPAnet and virtually nothing worth stealing. While many of the current cyber vulnerabilities of critical infrastructure stem from this fact and the related issue that antiquated protocols and other key technologies are still in use, many Internet users have strong interests in privacy and anonymity that are at odds with an inherently secure Internet that would provide strong authentication/identification of parties to Internet connections.

An inherently secure Internet would directly prevent common attacks based on phishing, stealing of log-on credentials, and similar activities. It would also afford easy attribution so that not only serious attacks could be identified but even if access was achieved by criminals it might be able to be traced and prosecuted. To what extent such an inherently secure Internet can be developed remains an ongoing debate within the technical community.

A migration path might start with islands having strong authentication and limited access, particularly for national security and critical infrastructure sectors connected as necessary to similar islands with strong encryption. Terminal computers and other connected devices would need to be protected from infecting the secure enclaves, and the enclaves themselves would have to

be protected against insider threats. User access to both the secure and non-secure networks from the same device could be possible but would require features to prevent deleterious migrations between the two segments.[119]

Given the increasing user interest in both privacy and anonymity some version of today's non-secure Internet is likely to coexist with a new secure net.[120] The technological issues associated with cybersecurity in the context of such a heterogeneous Internet can be conceptualized as follows:

- *Authentication and Identification:* The design of the robust authentication/identification scheme, presumably processor-based, accompanied by robust consideration including red-teaming of abilities of high-end threats to spoof or circumvent it.
- *System Gaps:* Maintaining an effective gap between an anonymous Internet and the new secure portions despite the desire of users to use both and to move their own data from one to the other. This is much the way current systems operate that have access to both unclassified and classified networks.
- *Insider threats:* Dealing with insider and other threats not directly handled by robust authentication for access.

[119] Another possible model might be an analogy to the transition from black and white to color television in the 1950s, when RCA offered the new technology of "compatible color" where the broadcast protocols offered both formats, and user sets presented what was available and within their display capability.

[120] See Abraham R. Wagner, and Paul Finkelman, "Security, Privacy and Technology Development: The Impact on National Security," 2 TEXAS A&M L. REV. 4 (2015).

# 5. Transition from Research to Operations

## 5.1 Integrating Defensive and Offensive Cyber Operations

Current policy guidance recognizes the major role cyber operations will play in any future conflict.[121] In this discussion the need to modernize key cyber capabilities the Department of Defense notes:

> ***Space and Cyberspace as Warfighting Domains: The Department will prioritize investments in resilience, reconstitution and operations to assure our space capabilities. We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.*** [122]

The Department of Defense has already undertaken major efforts to incorporate cyber operations and the prospects of cyber warfare into overall planning and operations. U.S. Cyber Command (CYBERCOM) was established as a unified command while each of the military services established corresponding commands as operational activities. Increasingly the "stovepipes" that separated these commands from NSA and other Intelligence Community elements are being eliminated.

National policy continues to be based on the deterrence model, which calls for a portfolio of defensive strategies and programs as well as the ability to conduct strong offensive operations where needed – or to have such capabilities available to help deter attacks by potential adversaries.[123] This

[121] Department of Defense, *Nuclear Posture Review, op. cit.* For the first time this type of review explicitly recognizes the need for cybersecurity, particularly in the command and control (C3) infrastructure utilized for nuclear weapons.

[122] Department of Defense, *2018 National Defense Strategy, op. cit.*, p. 6.

[123] The 2018 *Nuclear Posture Review* also introduces the concept of "tailored deterrence" as well as "tailored assurance" as the basis for strategy and policy decisions, noting that "[T]here is no 'one size fits all' for deterrence. The requirements for effective deterrence vary given the need to address the unique perceptions, goals, interests, strengths, strategies and vulnerabilities of different potential adversaries. The deterrence strategy effective against one potential adversary may not deter another. Adjusting our deterrence strategies accordingly is what it means to tailor deterrence," pp. 26, 34.

policy also recognizes threats from traditional nation states as well as non-state actors such as terrorist groups, and here the *Nuclear Posture Review* outlines a potential cyber response to warfare at the strategic level.[124] While the current *Defense Strategy* does not explicitly outline an investment strategy to support national objectives regarding cyber conflict, the portfolio of programs discussed above is clearly aimed at supporting these critical cyber missions.[125]

Notwithstanding the intentions reflected in the Homeland Security Act (HSA) of 2002, precisely what role DHS would play in an actual conflict involving serious cyber operations has yet to be fully defined and exercised. The Department of Defense remains the only government department with Title 10 and Title 50 authorities, as well as operational capabilities to respond effectively to these cyber challenges.[126]

## 5.2 Supporting National Security Users

Since the end of World War II and passage of the 1947 *National Security Act,* both the nature of warfare and the concept of national security have changed dramatically. The set of national security users has expanded greatly, while the set of potential adversaries has also changed dramatically, from an almost myopic focus during the Cold War on the Soviet Union and allied Warsaw Pact states to a broad number of both nation states and non-state actors such as terrorist groups.[127]

---

[124] *Nuclear Posture Review, op. cit.*

[125] As in other aspects of warfare, the nation needs an ongoing analytic, policy development and programmatic assessment of cyber threats and all related issues. This must be undertaken by the Department of Defense; the Intelligence Community, the Justice Department, the Department of Homeland Security and the Departments of Commerce and State. Supporting this effort should be experts from within the government as well as relevant research institutions.

[126] Further, cyber conflict differs from kinetic warfare, in that hostile cyber operations are likely to begin as covert or clandestine activities where immediate attribution may not possible and the initial attack is not regarded as cyberwarfare. In the cyber area there are grey boundary lines between what is domestic and what is international, as well what is defense or offense. How America responds to such attacks raises major organizational and technical issues, pitting the legal authorities, missions, and capabilities of the Defense Department, the Intelligence Community, and DHS.

[127] See, for example, Lucas Kello, *The Virtual Weapon and International Order,* (New Haven, Yale University Press, 2018) and Henry A. Kissinger, *World Orde,r* (New York: Penguin Books, 2015).

National policy now explicitly recognizes cyberspace as a critical domain of operations by the U.S. military and its protection is a national security issue, and clearly define cyber operations as critical elements in any future conflict scenario. As is the case with other technology areas this includes the full range of potential cyber operations, both defensive and offensive.

Since its inception DARPA's mission has been the development of technologies that support Defense Department and related national security requirements. Given the agency's history in the development of cyberspace technologies, DARPA is in a unique position to respond to growing needs for new technologies supporting cyber operations in the conflict domain. This technology base can be utilized by other defense agencies and the military services with specific operational responsibilities.

## 5.3 Proactive Cyber Defense

It is essential for the Department of Defense, through the various Defense agencies and military commands, to be primarily responsible for defending the U.S. from strategic cyberattack. While many cybersecurity issues are new and emerging, many others evoke familiar painful, lessons from the not too distant past.

A key element of cybersecurity policy and posture is to accurately assess the threats against the nation and to engage in ongoing tests of critical cyber systems by putting them under closely managed stress. Proactive cyber defense goes by various terms including "stress testing," "white hat hacking," "red teaming" and "cyber threat hunting" among others.[128] But these are limited compared to the imaginative approach that is needed to deal with strategic cyberattack.

Tests of the important warning systems are performed on a regular basis; we need to have a similarly pro-active approach to understanding cyber

[128] See Emilio Iasiello, "Cyber Hunt Teams: A Necessary Augmentation to Traditional Security Practices," *Looking Glass Threat Intelligence Blog,* (December 14, 2017), and Robert M. Lee and Rob Lee, *The Who, What Where, When, Why and How of Effective Threat Hunting: A Sans Whitepaper,* (Sans Institute: February 2016). Operationally this is the process of proactively and iteratively searching through networks to detect threats that evade existing security solutions. This contrasts with traditional threat management measures, such as firewalls and other intrusion detection systems, which typically involve an investigation after there has been a warning of a potential threat or an incident has occurred.

vulnerabilities and fixing them.[129] Operationally that may be the only aspect of cyberwarfare that seen before a cyber adversary with malevolent motives shuts down some critical infrastructure. Such efforts are essential since there is an inherent conflict of interest in reporting cyber penetrations and incursions.

Threat hunting can be a manual process where analysts scan available data, utilizing their own knowledge and familiarity with the network to create hypotheses about potential threats. A more effective and efficient approach, however, would be automated or machine-assisted threat hunting. Analysts can then apply software that leverages machine learning and related technologies to identify potential risks to track suspicious network behavior. In addition, "managed cyber stress testing" could be used to identify cyber weaknesses in our critical infrastructures.[130]

Using red teams to evaluate possible cyber-attack modes as well as intelligence on actual adversary capabilities and plans, DoD elements need to work not only with domestic agencies to reduce vulnerabilities to such attacks but also be capable of blunting attacks as they are executed and responding against the attackers. Defensive measures against cyberattacks underway could include physical as well as responsive cyberattacks. Focused preemption is also possible, again possibly using physical as well as cyberattack methods if the threat is serious enough and the warning clear enough.

This approach should go beyond defensive testing to include actively tracking adversary cyberattack capabilities and activities, developing tailored counter-measures, and taking needed actions in the cyber realm to reduce the threat from nation states, non-state actors or others that are intruding into U.S. and allied networked systems.[131]

Such program might include:

---

[129] See, for example, *NATO wins the world's largest live-fire cyber exercise,* (23 April 2018), available at https://www.nato.int/cps/en/natohq/news_154263.htm.

[130] See Daniel Gallington, "The Challenge," *Government Executive,* (August 15, 2011).

[131] To what extent this overlaps or conflicts with the responsibility of the Department of Homeland Security (DHS) remains a serious and open question. There is scant evidence that it was considered at the time DHS was created in the post-9/11 era. The Homeland Security Act (HSA) of 2002, (Pub.L. 107–296, 116 Stat. 2135, enacted November 25, 2002) was introduced in the aftermath of the 9/11 attacks and subsequent mailings of anthrax spores. It is also the case that DHS lacks both Title 10 and Title 50 authorities, so how it would legally operate in this sphere is also open to question.

- Promulgation of a generic list of facilities, activities and industries determined to be "critical infrastructure." This could include, for example, ports, inland waterways, pipelines, railroads, airspace controls, electric power grids and nuclear power plants.
- Liaison with these key facilities and including their regulatory agencies to establish cooperative cyber security testing relationships with them.
- The government could scan the entire range of U.S. IPs for SQLi and other common vulnerabilities to have critical infrastructure to fix issues and at least know who is behind them and who is not. Reports on the testing and technical follow-ups could be made to the relevant Congressional oversight committees.[132]
- *Mapping Internet Attack Routes and Installing Countermeasures.* For certain sorts of attacks, commanding legions of intermediate processors is an important mechanism of attack. Mapping such attack routes in advance may allow the disconnection of key nodes to protect U.S. systems.
- *Targeting hostile computers in advance.* The U.S. has a strong interest in accessing systems being used to develop and launch hostile code. If these can be accessed in advance there is potential for disabling an attack either by disrupting the launch and deployment of the attack, disabling or weakening the payload, or providing signatures that make it easier to deal with the attack once it is on the doorstep of or even inside U.S. networks.

## 5.4 Competing in the Information War

The Intelligence Community increasingly recognizes the growing threat posed by hostile information operations, and the rapidly growing role that the information environment and hostile operations in that space are now playing in politics, terrorism, geopolitical warfare and other important areas.[133] In the

[132] Daniel Gallington, "A new version of an old spy game: The Chinese Cyberhack the Office of Personnel Management," *The Washington Times* ,(September 21, 2015).

[133] Director of National Intelligence*, Worldwide Threat Assessment of the US Intelligence Community. op. cit.* See also, Ellen Nakashima and Shane Harris, "The nation's top spies said Russia is continuing to target the U.S. political system," *The Washington Post,* (February 13, 2018). Related testimony by FBI Director Wray and DNI Coats reiterated this concern,

modern world people have become increasingly dependent on their connected devices, the content they derive from them, and susceptible to the use of techniques of mass and at times individualized manipulation.

Most cybersecurity efforts under way relate to the defense of the information infrastructure in one way or another, and various malicious activities that can be undertaken to disable or exploit it. While certainly necessary, they do not aid in dealing with malevolent use of the infrastructure to influence and manipulate entire populations. Competing in the information war with Russia or any number of other adversaries requires a different set of supporting technologies which have collectively been termed "cognitive security."[134]

One approach to making cognitive security a reality and countering the growing threat from information operations is a two-part strategy. First is the establishment of a Center of Excellence in Cognitive Security, a non-profit, non-governmental organization devoted to research, development and education in policies, technologies and techniques of information operations. This research center would not be operational, but rather set research and development agendas and provide training and advice to operational users.

Second would be a study conducted by the Department of Defense or the National Academy, for example, that would answer three fundamental questions:

- What U.S. laws and policies, laws and authorities present roadblocks to make operations in the information environment difficult to impossible including problems of authorities?

which has clearly been driven by the analysis of Russian information operations related to the 2016 U.S. presidential election. Neither official had a program in mind to effectively counter such operations.

[134] See, for example, Tamlin Magee, "US government can't compete in information war, warns RAND Corporation, *TechWorld,* (February 12, 2018). One cited example is the State Department's Global Engagement Centre (GEC) started in 2016 to combat terrorist messaging and disinformation, and later extended to include state-sponsored disinformation campaigns. Unfortunately, constraints on the program have rendered it largely a disaster. The GEC is not even allowed to look at the raw social media data – they can only look at a sanitized data, with the handlebar removed and are prohibited from downloading any data directly.

- How can those laws and policies be updated to support the realities of the modern information environment, characteristics of which include a near-immediate timeline, and the viral spread of both trusted and untrusted information?
- What kind of organizational structure is needed to manage national efforts to improve foundations for cognitive security and deal with threats to it?

Based on the answers to critical questions such as these it may then be possible to craft a realistic program of both technologies and operations to meet the growing need to fight the information war effectively. The U.S. is now losing – badly, and this should not be allowed to continue.

# 6. Conclusion

## 6.1 A New Foundation for Cybersecurity

It is increasingly clear that an effective approach to cybersecurity requires a new foundation, both in terms of agency roles and missions as well being aligned with current legal authorities. The present study details a number of specific impediments to achieving cybersecurity as well as several policy and technical approaches to improving the situation. While there are significant challenges, the U.S. also has major technical and societal advantages that can be harnessed if the right steps are taken.

Nevertheless, the trend of the last 30 years is that, despite a constant expert understanding of the seriousness of the threat and the difficulties and opportunities for policy as well as effective government organization and public-private cooperation, real preparedness has lagged well behind the development of sophisticated external threats.[135] Despite repeated high-level studies of the problem, roles and missions were not assigned to agencies capable of accomplishing the task; adequate federal resources were never provided; and too often policy was made on the erroneous assumption that private industry would somehow rise to the occasion and solve the problem.

There are good reasons for this failure to cope adequately. The cybersecurity landscape is uniquely dynamic and complex, owing to the rate of underlying technological change, the unevenness of hardware and software adoption, low barriers to entry, the large number of existing and potential actors. It is also the case that both national security and domestic policy and sectors are affected and can't really be separated.

Here there is the necessity for leadership by both government, at national, state, and local levels, as well as by the private sectors. In the legal regime there remains the interplay of authorities in the national security area under Titles 10, 50, and 22 as well as the increasingly complex entanglement

[135] See Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War,* (New York: Simon and Schuster, 2016). As discussed, an extensive list of organizational and programmatic changes was suggested as part of the Trump-Pence Transition in the transition study, *Fixing America's Cybersecurity: A Plan for Cyber Policy and Organization, op. cit.*

of civil liberties that are at the core of the American political heritage, and, most recently, the strong nexus with democratic political decision-making through social media.

A realistic approach to cyber security must fully encompass this dynamic complexity and create technological, legal, and organizational foundations so that responses can adapt as quickly as the technologies and the threats. It must combine a synoptic view of the changing landscape with top-down dissemination of threat perspectives, bottom-up technological and tactical innovation, civic-minded activism by the corporate stewards of key information utilities and platforms and other critical systems, and far-sighted government action to create options and favorably shape the evolution of the cyber battlespace.

It is not enough to devise organizations, policies, and technologies to counter today's threats. The U.S. must also ensure that the nation's systems will correctly understand tomorrow's potential threats and evolve rapidly enough to get ahead of them.

The first and most important step to changing the trajectory of the last 30 years to one that gets ahead of the threat is to organize the federal government to achieve a continually updated high-level view of the overall problem; to provide legally responsible policy coherence and coordinate programs and activities; and to assign roles and missions to capable federal organizations that cumulatively and in cooperation with state and local governments, allies, and the private sector can accomplish what is needed.[136]

## 6.2 Key Cybersecurity Areas

Institutions given new capacity and energy by such a reform would then be in a position to effectively shape the cyber environment to redress what currently appears to be a situation of unacceptable vulnerability. Already considered above are several detailed ideas for steps that should be taken – too many to completely capture here. But the broad outline of the approach includes:

[136] As previously suggested this could be accomplished by a Presidential Executive Order analogous to EO 12333 (1981) which defined the roles and missions for the Intelligence Community which was in a considerable state of disarray in the 1970s. Part I of EO 12333 lays out the "Goals, Direction, Duties and Responsibilities with Respect to the National Intelligence Effort" for various intelligence agencies, including the Departments of Defense, Energy, State, and Treasury.

- *Reduce Cyber Vulnerabilities*: Reduce the cyber vulnerabilities of the military forces and other national security users, the commercial infrastructure and supply chains they rely on and the critical infrastructure of the economy and society.[137]
- *Active Cyber Defense:* Develop a range of active cyber defense capabilities, including tactical and operational offense, focused on adversary capabilities and forces as well as against cyberattack capabilities generally.
- *Concerted Deterrence:* Establish capabilities to conduct concerted deterrence campaigns by supplementing cyber resilience with retaliatory options that would impose unacceptable costs on a cyber attacker and communicating about these capabilities and the will of the U.S. to use them that effectively deters adversaries and proxy forces from attacking and dissuades them from investing in particular cyber capabilities.
- *Effective Information Operations:* Develop effective approaches to information operations and cognitive security at the strategic as well as operational and tactical levels. Although social media platform companies are aware of the need to reduce manipulation of user attitudes and beliefs by malign sources including foreign governments, they lack full information and incentives to deal with this emerging problem on their own.[138]
- *Cyber Workforce:* Sponsor a range of initiatives in the educational domain as well as industry to significantly expand the needed skilled cyber workforce. A major shortage now exists and will only get worse. Americans need to be educated and cleared to meet this growing need.

[137] If this can be done in a way that increases the daily security of Americans in their use of the Internet, so much the better.

[138] Heavy handed government regulation is also not the answer as it would kill required public private collaboration and would not be responsive to changing technologies and threats. Effective coordination of a variety of government agency expertise and authorities combined with private initiative is required, as is a great deal of research on how people use social media and are affected by these interactions. Technological innovations may indeed offer a variety of solutions without compromising privacy or freedom of speech.

Effective policy and operational innovation in these areas can only be achieved and sustained in the context of a dramatically different relationship between the government and corporations and if the nation takes steps to improve the quality and quantity of skilled cyber technicians available to both.

## 6.3 Technology Development to Support Cybersecurity

The present study contains numerous detailed examples of technology programs supporting the specific cybersecurity objectives. In summary it is possible to highlight a few key areas for emphasis and the need for continual review of the changing technology and threat landscape. Such an ongoing review will help to focus the development and deployment of new technology on a short cycle time to get ahead and keep ahead of this dynamic environment – not only in the laboratory but in the real world.

Clearly technology development is needed to support each of these objectives:

- *Reducing cyber vulnerability:* The foregoing analysis identifies a host of near-term initiatives to improve the operational security of current systems as well as research on and development and deployment of more inherently-secure systems in the context of an increasingly connected world.
- *Improving Active Defenses:* They keys to success include automated tools to support rapid global tracking of evolving penetrations and attacks extending well beyond the boundaries of the systems the U.S. need to defend, including a focus on specific threat organizations, computers, and nodes, and technologies for rapid protective responses.
- *Conducting Concerted Deterrence Campaigns:* Rapid, definite, and publicly clear attribution is the key technological requirement for traditional deterrence, and technological capabilities allowing discriminate and targeted communication of specific threats and the ability to respond precisely at a variety of levels are the keys to concerted deterrence campaigns that have the potential to alter the cyber balance in favor of the U.S.

- *Developing Effective Capabilities for Information Operations and Achieving Cognitive Security:* Supporting democratic values while prosecuting information operations, though not easy, is essential if the U.S. is to avoid "destroying the village in order to save it." Technology can assist in validating the information users of social media receive will be essential along to combat the use of technology that promises to develop ever harder to detect false information. Since a "block chain for ideas" is not likely to be immediately available, in many ways this area requires applied social psychological research in technologically mediated spaces in addition to specific technological developments.

# References

Abbate, Janet, *Inventing the Internet,* (Cambridge: MIT Press, 2000).

Abelson, Harold, et al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, (MIT Computer Science and Artificial Intelligence Laboratory Technical Report, July 6, 2015).

Ablon, Lillian and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and their Exploits,* (Santa Monica: The RAND Corporation, 2017).

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar,* (Santa Monica: The RAND Corporation, 2014).

Agar, Jon, *Constant Touch: A Global History of the Mobile Phone*, (Cambridge: Icon Books, 2003).

Alexander, Keith, Emily Goldman and Michael Warner, "Defending America in Cyberspace," *The National Interest* (November-December 2013).

Allison, Graham and Philip Zelikow, *Essence of Decision*, *2nd ed*., (New York: Pearson, 1999).

Arquilla, John and David Ronfeld, *Networks and Netwars: The Future of Terror, Crime and Militancy*, (Santa Monica: The RAND Corporation, 2001).

Axelrod, Robert and Rumen Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academy of Sciences,* 111(4):1298-1301 (2014).

Barash, David P., "The deterrence myth," *Aeon* (January 2018).

Berger III, Joseph B., "Covert Action: Title 10, Title 50, and the Chain of Command," *Joint Force Quarterly,* Issue 67 (2012).

Berman, Paul Schiff, *The Globalization of Jurisdiction*, 151 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 311 (2002).

Borghard, Erica D. and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies," *Orbis,* (Summer 2016).

Borghard, Erica D. and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, 26:3 (2017).

Brodie, Bernard, *Strategy in the Missile Age,* (Princeton: Princeton University Press, 1959).

Brown, Gary D. "The Cyber Longbow & Other Information Strategies: U.S. National Security in Cyberspace, 5 PENN STATE JOURNAL OF LAW & INTERNATIONAL AFFAIRS 1 (2017).

Brown, Gary D., "Spying and Fighting in Cyberspace: What is Which?" 8 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 621 (2016).

Byman Daniel and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*, (Cambridge: Cambridge University Press, 2002).

Carlin, John P., "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats," 7 HARVARD NATIONAL SECURITY JOURNAL 393 (2016).

Cebul, Daniel, "More universities to offer Hacking for Defense program," *www.fifthdomain.com,* (April 5, 2018).

Cerf, Vincent G., "On the evolution of Internet technologies," *Proceedings of the IEEE* (September 2004).

Chesney, Robert, "Military Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy*, (October 2011).

Charlet, Kate, *Understanding Federal Cybersecurity*, (Harvard Kennedy School, Belfer Center for Science and International Affairs, April 2018).

Cilluffo, Frank J. and Sharon L. Cardash, *Overview and Analysis of PPD-41: US Cyber Incident Coordination* (Lawfare, July 27, 2016).

Clarke, Richard A. and Robert A. Knake, *Cyber War: The Next Threat to National Security and What to Do About It.* (New York: Harper-Collins, 2010).

Cordesman, Anthony H., *Cyber-Threats, Information Warfare, and the Critical Infrastructure Protection: Defending the US Homeland,* (Center for Strategic and International Studies, 2002).

Cotter, George R., *Security in the North American Grid: A Nation at Risk* (April 8, 2015).

Cringley, Alex, *Accidental Empires: How the Boys of Silicon Valley Make Their Millions, Battle Foreign Competition, and Still Can't Get a Date,* (New York: HarperBusiness, 1996).

*Cybersecurity and Privacy: Report of the Expert Workshop Held for the Defense Advanced Research Projects Agency (DARPA),* Institute for Defense Analysis (June 25, 2014).

Czosseck, Christian and Kenneth Geers, *The Virtual Battlefield, Perspectives on Cyber Warfare,* (Ios Press, 2009).

Danzig, Richard J., *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies,* (Center for New American Security, 2015).

*DARPA Perspective on Technology to Empower National Cyber Deterrence,* (October 26, 2017).

Daskal, Jennifer, *A Twenty-First Century Framework for Digital Privacy: Balancing Privacy and Security in the Digital Age* (National Constitution Center, 2017).

Daskal, Jennifer, "The Un-Territoriality of Data," 125 YALE LAW JOURNAL 326 (2015).

Davis, Zachary S. and Michael Nacht (eds.), *Strategic Latency: Red White, and Blue, Managing the National and International Security Consequences of Disruptive Technologies,* (Center for Global Security Research, Lawrence Livermore National Laboratory (February 2018).

Demarest, Geoffrey B., "Espionage in International Law," *Denver Journal of International Law and Policy*, (1995).

Department of Defense, Defense Science Board, *Task Force Report on Cyber Deterrence* (February 2017).

Department of Defense, Defense Science Board, *Task Force Report: Cyber Security and Reliability in a Digital Cloud* (January 2013).

Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* (January 2013).

Department of Defense, *National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge,* (January 2018).

Department of Defense, *Nuclear Posture Review,* (February 2018).

Department of Defense, *Special Report: 21st Century Nuclear Deterrence and Missile Defense,* (February 2018).

Department of Homeland Security, *National Infrastructure Protection Plan: partnering to Enhance Protection and Resiliency,* (2009).

Department of Homeland Security, *Publicly Available Social Media Monitoring and Situational Awareness Initiative Update,* (January 6, 2011).

Director of Central Intelligence, *Report of the DCI Global Information Infrastructure Panel,* (1996).

Director of National Intelligence*, Worldwide Threat Assessment of the US Intelligence Community,* (13 February 2018).

Drezner, Daniel W., "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly*, (Fall 2004).

Dyson, George, *Turing's Cathedral: The Origins of the Digital Universe,* (New York: Pantheon Books, 2012).

Executive Office of the President, *Big Data: Seizing Opportunities and Preserving Values,* (May 2014).

Executive Office of the President, *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (May 11, 2017).

Executive Office of the President, *National Security Strategy of the United States of America,* (December 2017).

Executive Office of the President, *NSPM-2: Presidential Memorandum Organization of the National Security Council and the Homeland Security Council,* (January 28, 2017).

Executive Office of the President, *Presidential Decision Directive/*NSC-63 *Critical Infrastructure Protection,* (May 22, 1998).

Executive Office of the President, *Presidential Policy Directive/PPD-21 Critical Infrastructure Security and Resilience,* (February 12, 2013).

Executive Office of the President, *Presidential Policy Directive/PPD-41 U.S. Cyber Incident Coordination* (July 27, 2016).

Executive Office of the President, National Science and Technology Council, *Federal Cybersecurity Research and Development Plan,* (February 2016).

Executive Order 12333, *United States Intelligence Activities***,** 40 Fed. Reg. 235 (December 8, 1981),

Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,* 80 Fed. Reg, 18,077 (April 1, 2015).

Fearon, James D., "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs," *Journal of Conflict Resolution*, (February 1997).

Fidler, Mailyn, Jennifer Granick, and Martha Crenshaw, *Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities*, (master's thesis, Stanford University, 2014).

*Fixing America's Cybersecurity: A Plan for Cyber Policy and Organization,* (Prepared for the Trump-Pence Transition Team, January 13, 2017).

Freedman, Lawrence, *The Evolution of Nuclear Strategy (3rd Edition),* (London, Palgrave, 2003).

Freiberger, Paul and Michael Swaine, *Fire in the Valley: The Making of The Personal Computer,* (New York: McGraw-Hill, 2000).

Gallington, Daniel, "The Challenge," *Government Executive,* (August 15, 2011).

Gartzke, Erik, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* (2013).

Gizzo, Tom A. and Tama S. Monoson, *A Call to Arms: The Posse Comitatus Act and the Use of the Military in the Struggle Against International Terrorism*, 15 PACE INTERNATIONAL LAW REVIEW 149 (2003).

Goggin, Gerard, *Global Mobile Media,* (New York: Routledge, 2011).

*Going Dark: Implications of an Encrypted World* (Center for Advanced Studies on Terrorism, April 2017).

Goldsmith, Jack, "How Cyber Changes the Law of War," 24 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1 (2013).

Goldsmith, Jack, "The Significance of Panetta's Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks," *Lawfare*, (15 October 2012).

Goldsmith, Jack and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World,* (New York, Oxford University Press, 2008).

Haass, Richard N., "Why the World Needs to Police the Growing Anarchy of Cyberspace," *Fortune.com*, (February 7, 2017).

Hafner, Katie and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of The Internet, (New York: Simon & Schuster, 1996).*

Harper, Jim, *Administering the Fourth Amendment in the Digital Age,* (National Constitution Center, 2017).

Hare, Forrest, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective," in *2012 4th International Conference on Cyber Conflict,* (IEEE, 2012).

Harknett, Richard, "Information Warfare and Deterrence," *Parameters* (Autumn 1996).

Harrison, Richard M. and Trey Herr (eds.), *Cyber Insecurity: Navigating the Perils of the Next Information Age,* (New York: Rowman & Littlefield, 2016).

Hathaway, Oona A., *et al*., "The Law of Cyber-Attack," 100 CALIFORNIA LAW REVIEW 4 (August 2012).

Headquarters, Department of the Army (HQDA), *Cyber Electromagnetic Activities*, FM 3-38 (2014).

Hoffman, Wyatt and Ariel E. Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* (Carnegie Endowment for International Peace, 2017).

Iasiello, Emilio, "Cyber Hunt Teams: A Necessary Augmentation to Traditional Security Practices," *Looking Glass Threat Intelligence Blog,* (December 14, 2017).

*Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats* (Center for Cyber & Homeland Security, The George Washington University, October 2016).

Jervis, Robert, *Perception and Misperception in International Politics,* (Princeton: Princeton University Press, 1976).

Johnson, David R. and David Post, *Law and Borders—the Rise of Law in Cyberspace*, 48 STANFORD LAW REVIEW 1367 (1996).

Kaplan, Fred, Dark Territory: *The Secret History of Cyber War,* (New York, Simon & Schuster, 2016).

Karnouskos, Stamatis, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security" in *37th Annual Conference of the IEEE Industrial Electronics Society*, (IECON 2011),

Kelling, George and Catherine Coles, *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities,* (New York: Free Press, 1996).

Kello, Lucas, *The Virtual Weapon and International Order,* (New Haven: Yale University Press, 2018).

Kennedy, David M., *Deterrence and Crime Prevention,* (Toronto: Routledge, 2009).

Kerr, Orin S. "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 GEORGE WASHINGTON LAW REVIEW 1208 (2004).

Kim, Ye Ra, *Before Dark Seoul Becomes Destroy Seoul,* (Columbia University Cyber Program, February 2014).

Kissinger, Henry A., *World Order,* (New York: Penguin Books, 2015).

Kistiakowsky, George, *A Scientist at the White House,* (Cambridge: Harvard University Press, 1976).

Kleiman, Mark A.R., *When Brute Force Fails*, (Princeton: Princeton University Press, 2009).

Knake, Robert K., *A Cyberattack on the U.S. Power Grid,* (Council on Foreign Relations, April 2017).

Kostyuk, Nadiya and Yuri M. Zukov, *Can Cyber Attacks Shape Battlefield Events?* (University of Michigan, unpublished paper, July 12, 2017).

Kris, David, *Digital Divergence,* (National Constitution Center, 2017).

Lee, Robert M. and Rob Lee, *The Who, What Where, When, Why and How of Effective Threat Hunting: A Sans Whitepaper,* (Sans Institute: February 2016).

Leiner, Barry M, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, *A Brief History of the Internet,* (Reston: The Internet Society, 2011).

Lewis, James A., "The Devil Was in the Details: The Failure of UN efforts in Cyberspace," *Cipher Brief,* (August 2017).

Lewis, James A., *Managing Risk for the Internet of Things*, (Center for Strategic and International Studies, February 2016).

Lewis, James A., *Sustaining Progress in International Negotiations on Cybersecurity,* (Center for Strategic and International Studies, July 2017).

Libicki, Martin C., *Conquest in Cyberspace: National Security and Information Warfare,* (Cambridge University Press, 2007).

Libicki, Martin C., *Cyberdeterrence and Cyberwar,* (Santa Monica: The RAND Corporation, 2009).

Lin, Herbert, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, (2012).

Lindsay, Jon R., "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, (July-September 2013).

Lindsay, Jon R., "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity*, (2015).

Lotrionte, Catherine, "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence," *Georgetown Journal of International Affairs*, (April 2014).

Loundy, David J., *Computer Crime, Information Warfare, and Economic Espionage,* (Durham: Carolina Academic Press, 2003).

Lukasik, Stephen, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains." *In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington: The National Academies Press, 2010).

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (2010).

Magee, Tamlin, "US government can't compete in information war, warns RAND Corporation," *TechWorld* (February 12, 2018).

Mattern, Friedemann and Christian Floerkemeier, *From the Internet of Computers to the Internet of Things,* (Institute for Pervasive Computing, ETH Zurich, 2016).

McGraw, Gary, "Cyberwar is Inevitable (Unless We Build Security In," Journal of Strategic Studies (2013).

Mearsheimer, John, *Conventional Deterrence,* (Ithaca: Cornell University Press, 1983).

National Research Council, *The Internet's Coming of Age*, (Washington: National Academy Press, 2001).

Nye, Joseph S. Jr., *Cyber Power,* (Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010).

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

Nye, Joseph S. Jr, *Normative Restraints on Cyber Conflict*, (Working Paper for Circulation at the 2017 Global Digital Futures Forum, May 5, 2017).

Nye, Joseph S. Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly,* (Winter 2011).

Olson, Mancur, *The Logic of Collective Action: Public Action and the Theory of Groups*, (Cambridge: Harvard University Press, 1965).

Owens, William A., Kenneth W. Dam and Herbert S. Lin, (eds.), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington: National Academies Press, 2009).

Pfefferkorn, Riana, *The Risks of "Responsible Encryption,"* (Stanford University, The Center for Internet and Society, February 2018).

Post, David G., *In Search of Jefferson's Moose: Notes on the State of Cyberspace*, (Oxford Univ. Press, 2009).

Rabkin, Jeremy and Ariel Rabkin, *Hacking Back Without Cracking Up; Aegis Paper Series No. 1606*, (Stanford University Hoover Institution, 2016).

Reveron, Derek S., (ed.), *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*, (Washington: Georgetown University Press, 2012).

Richards, Neil, *Secret Government Searches and Digital Civil Liberties,* (National Constitution Center, 2017).

Rid, Thomas and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* (2015).

Rid, Thomas, "Cyber War Will Not Take Place," *Journal of Strategic Studies* (2012).

Salus, Peter, "The Net: A Brief History of Origins," 38 JURIMETRICS 671 (1998).

Schelling, Thomas C., "The Diplomacy of Violence," in *Arms and Influence,* (New Haven: Yale University Press, 1966).

Schmidle, Nicholas, "The Digital Vigilantes Who Hack Back," *The New Yorker*, (May 1, 2018).

Schmitt, Michael N., *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VIRGINIA JOURNAL OF INTERNATIONAL LAW 697.

Schmitt, Michael N (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* (Cambridge: Cambridge University Press, 2013).

Segal, Adam, *How European Data Protection Law is Upending the Domain Name System,* (Council on Foreign Relations, February 2018).

Segal, Adam, *Rebuilding Trust Between Silicon Valley and Washington,* (Council on Foreign Relations, January 2017).

Segaller, Stephen, *Nerds 2.0.1: A Brief History of the Internet,* (New York: TV Books, 1979).

Sharma, Amit, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis,* (2010).

Sharp, Travis, "Theorizing cyber coercion: The 2014 North Korean operation against Sony," *Journal of Strategic Studies* (2017).

Singer, P. W. and Allan Friedman, *Cybersecurity and Cyber War*, (New York: Oxford University Press, 2014).

Slayton, Rebecca, "What is the Cyber Offense-Defense Balance?" *International Security*, Vol. 41, No. 3 (Winter 2016/2017).

Smith, Douglas K. and Robert C. Alexander, *Fumbling the Future: How Xerox Invented, then Ignored, the First Personal Computer* http://www.amazon.com/Fumbling-Future-Invented-Personal-Computer/dp/1583482660 Lincoln: iUniverse.com, 1999).

Swire, Peter P., *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 UNIVERSITY OF PENNSYLVANIA LAW REVIEW (2005).

Taipale, K. A., "Cyber-deterrence," in *Law, Policy and Technology: Cyberterrorism, Information Warfare, Digital and Internet Mobilization,* (IGC Global 2010).

Taipale, K. A., *Power to the Edge: New Threats, New Responses in America's Security Role in a Changing World: A Global Strategic Assessment*, (National Defense University, 2009).

Talbot, David, "Cyber-Espionage Nightmare," *MIT Technology Review,* (July/August 2015).

Tuchman, Barbara, *The Guns of August,* (New York: MacMillan, 1962).

Tucker, Patrick, "The US is Losing at Influence Warfare. Here's Why, *Defense One,* (December 5, 2016).

Undersecretary of Defense (Acquisition, Technology and Logistics), Memorandum for the Chairman, Defense Science Board, *Terms of Reference – Defense Science Board Task Force on Cyber as a Strategic Capability,* (July 15, 2016).

Undersecretary of Defense (Acquisition, Technology and Logistics), Memorandum for the Chairman, Defense Science Board, *Terms of Reference – Defense Science Board Task Force on the Role of the DoD in Homeland Security,* (October 20, 2016).

United States *Cyber Command, Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, (March 2018).

Valeriano, Brandon, "What Is the Cyber-Offense-Defense Balance? Conceptions, Causes and Assessment," *H-Diplo – ISSF Article Review 83,* (July 26, 2017).

Wagner, Abraham R., *Cybersecurity, Cryptology, and Privacy in Historical Context: The Challenge of New Technologies and Media,* Paper Presented to National Security Agency Cryptologic Symposium, (October 2013).

Wagner, Abraham R. and Nicholas Rostow, *Cybersecurity and Cyberlaw,* (Durham: Carolina Academic Press, 2017).

Wagner, Abraham R., Thomas Garwin and Nicholas Rostow, *Cyber Deterrence and Technology,* (Center for Advanced Studies on Terrorism, November 2017).

Wagner, Abraham R., *Privacy in a Free Society,* (Center for Advanced Studies on Terrorism, May 2015).

Wagner, Abraham R. and Paul Finkelman, "Security, Privacy and Technology Development: The Impact on National Security," 2 TEXAS A&M L. REV. 4 (2015).

Wagner, Abraham R., *The Unsocial Network: New Media and Changing Paradigms*, Paper Presented to the 11th International Conference – World Summit on Counter-Terrorism, Herzliya, Israel (September 2011).

Wagner, Daniel, "The Growing Threat of Cyber-Attacks on Critical Infrastructure," *Huffington Post* (May 25, 2017).

Wall, Andru E., "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, & Covert Action," 3 HARVARD NATIONAL SECURITY JOURNAL 1 (2011).

Watts, Barry D., *The US Defense Industrial Base: Past, Present and Future* Washington: Center for Strategic and Budgetary Assessments, 2008).

Weinberger, Sharon, *The Imagineers of War: The Untold Story of DARPA, The Pentagon Agency that Changed the World,* (New York: Alfred Knopf, 2017).

Xu, Wenyuan, Wade Trappe, Yanyong Zhang and Timothy Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing* (2005).

Zagare, Frank C., "Reconciling Rationality with Deterrence: A Re-examination of the Logical Foundations of Deterrence Theory," *Journal of Theoretical Politics,* 16 (2), (2004).

Zetter, Kim, "How the Feds Could Get Into iPhones Without Apple's Help," *Wired* (March 2, 2016).