No. 20
October 2018

The Mitchell Forum

Organizing for Cyber Resilience:
Rethinking the Balance Between Prevention and Response

By Col W. Mark Valentine, USAF (Ret.)

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact on current and emerging policy debates. The views expressed in this series are those of the author, and not necessarily those of the Mitchell Institute.

Abstract

Current policy debate over the best solutions to cybersecurity vulnerabilities and the appropriate organizations to implement them presents the American public with false choices. Who should lead the discovery effort—the Department of Defense or the Department of Homeland Security? What is the US government's proper role in cybersecurity, legislating standards or providing solutions? In most of the debates, additionally, the advertised options address the wrong choices. This is a consequence of incorrectly identifying the nature of the cyber environment. More holistic, effective, and enduring solutions are only feasible when policymakers recognize the complex nature of the cyber system and appropriately consider lessons from the fields of complexity theory and natural security. The most applicable lessons comprise shifting the current weight of effort from security to response and decentralizing responsibilities throughout the system to foster more adaptable organizations.

Introduction

The danger of cyber-attacks will equal or surpass the danger of terrorism in the foreseeable future.

Former FBI Director Robert S. Mueller III
Testimony before the Congress, January 31, 2012[1]

Sometime in the very near future...

Suddenly there is nothing. What began as a typical Friday night in New York City—widely planned revelry and ubiquitous celebration—turns to darkness in an instant. Regional power administrators discover similar outages throughout the US northeast and mid-Atlantic regions. Emergency generators at strategic operations centers kick in, conference calls ensue, and media inquiries pour in. Soon, private operators and government officials isolate the source of the widespread outage: a cyber attack. Investigators uncover the cause, malicious code from an unknown source.

Currently, the policy debate tends to focus on proactive cybersecurity. Most organs of the US government care nearly exclusively about who should lead its cybersecurity efforts, with leading voices split between assigning that responsibility to either the Department of Defense (DOD) or the Department of Homeland Security (DHS).

Physical consequences cascade. Officials continue to investigate the cyber stimulus. As hours turn into days, the lack of electricity paralyzes the region and, for some, threatens the very base of Abraham Maslow's Hierarchy of Needs—the physiological needs and safety concerns of all human beings. Water purification facilities shut down, hot summer days threaten lives, and fleeing residents and tourists jam dark intersections on evacuation routes, further complicating delivery of much needed water and fuel. Communications are severely degraded, hospitals scramble to keep emergency generators operational, and gas stations are unable to fuel stranded evacuators.

Governors of affected states request, and quickly receive, major disaster declarations from the President. The traditional disaster response system kicks in and local, state, and federal officials collaborate to manage surging repercussions. In the midst of this process, citizens and policy-makers alike ask: With all of our focus on cybersecurity how did this happen? Who should manage our cyber response efforts? What cybersecurity lessons can we apply to future incidents to mitigate consequences? And, finally, who should manage these future security efforts?

Currently, the policy debate tends to focus on proactive cybersecurity. Most organs of the US government care nearly exclusively about who should lead its cybersecurity efforts, with leading voices split between assigning that responsibility to either the Department of Defense (DOD) or the Department of Homeland Security (DHS).[2] This is a healthy debate with positive points on both sides, but it overshadows an ultimate solution for two reasons.

First, many involved in the debate incorrectly assume cybersecurity is a specific destination or some static condition the nation can reach through an initial push of regulations and resources, and that it can be maintained with little additional effort. This logic fails to acknowledge the dynamic nature of the cyber environment and its classification as a complex system. Therefore, decision-makers continue to expend scarce resources attempting to secure a fundamentally insecure system.[3] Heavy focus on static security risks missing the arguably more important issue: creating a resilient system able to absorb a shock and quickly return to its original state. This erroneous logic could lead to prioritizing security over response.

Second, such misprioritization creates incentives for leaders to centralize authorities and responsibilities in federal departments and agencies. This trend negates an important lesson observable in nature, which suggests employing decentralized agents increases adaptability and resilience.

This paper presents an argument for classifying the cyber environment as a complex system—one government ultimately cannot secure regardless of the amount of resources it applies toward the enterprise. For support of this conclusion, scholarship by David Snowden on complexity theory and the Cynefin Framework (a decision-making conceptual framework developed in 1999) explores this concept. Following a discussion on the impossibility of achieving cyber invulnerability, a case is made for refocusing much of the current cybersecurity effort into adaptable organizations better equipped to respond to cyber events. Support for this recommendation leans on concepts emerging from the field of natural security, as best articulated by Rafe Sagarin. Finally, this paper will provide some concrete organizational recommendations for cyber response operations. Specifically, that the US government should expand its efforts to integrate private sector capabilities into the cyber operational environment. Additional recommendations include expanding the pool of non-governmental organizations (NGOs), and partnering with cyber volunteers and volunteer organizations, with which the government cooperates as a means to increase the effectiveness of interagency cyber operations.

Cyber as a Complex System

Before introducing the cyber environment as a complex, adaptable system, it is necessary to define some appropriate terms used in this paper. First, a system describes "a group or combination of interrelated, interdependent, or interacting elements forming a collective entity." [4]

Snowden's work in the area of complexity theory helps the reader derive the definition of a complex system. His framework categorizes systems under four umbrellas: simple, complicated, complex, or chaotic. The umbrellas are based on several traits. One of these is the relationship between the agents acting within a system and its overall behavior. Snowden also categorizes systems based on the relationship between cause and effect within them.[5] These definitions are fundamental to understanding his "Cynefin Framework," which attempts to help leaders determine the best problem-solving approach based on the context of a problem and the nature of the system it is impacting (cynefin is a Welsh word loosely translating to "place"). Figure 1 provides a graphical overview of the Cynefin Framework.

The framework is partially founded on ordered systems, wherein a system constrains the agents acting within it. Snowden breaks ordered systems into the "simple" and "complicated" categories, based on different relationships between cause and effect. For example, when this relationship is direct, measurable, and predictable, the Cynefin Framework describes it as simple.[6] In a complicated system, though it still constrains its agents, the relationship between cause and effect is not as direct. The number of variables might preclude an observer from directly measuring, or predicting with any precision, the connection between cause and effect.[7]

In the simple category, where the bond between cause and effect is direct and predictable, the Cynefin Framework recommends a three-phased problem solving approach: Sense the situation, categorize the facts, and respond appropriately.[8] This approach is not unlike the observe, orient, decide, and act (OODA) loop created by Air Force Col John Boyd to describe the importance of speed in military decision-making.[9] Snowden calls this category the "domain of best practices" since the predictable relationship between cause and effect allows leaders to develop a toolkit of best practices and apply them under appropriate conditions.[10]

In complicated systems, the association between cause and effect is still strong, but the logical distance between the two often prevents

Cynefin Category	Simple	Complicated	Complex	Chaotic
Characteristic	Best Practice	Good Practice	Emergent	Novel
Direct cause and effect?	Yes	No	No	No
Measurable?	Yes	Maybe	No	No
Predictable?	Yes	Maybe	No	No
Problem Solving Step 1	Sense	Sense	Probe	Act
Problem Solving Step 2	Categorize	Analyze	Sense	Sense
Problem Solving Step 3	Respond	Respond	Respond	Respond

Figure 1: Overview of David Snowden's "Cynefin Framework."

observers from seeing it. In this category, multiple correct answers might exist, but none may emerge as the clear best choice. The Cynefin Framework, therefore, replaces the "categorize" step with "analyze." This implies the need for expertise in the subject area, which leads Snowden to dub the complicated category as the "domain of experts."[11]

Snowden also highlights logical errors common in each of the Cynefin categories. One of the dangers particularly common in this domain is what he terms "analysis paralysis," where experts essentially deadlock their recommendations due to overly conditioned responses (borrowed from the simple category), bureaucratic interests, and egos.[12]

The opposite of an ordered system (whether simple or complicated) is a "chaotic" one, wherein elements act independently and are unconstrained by the system. In this Cynefin category, cause and effect relationships are so dependent on initial conditions that, for all intents and purposes, they do not exist.[13] Deemed the "novel" domain, the framework response for handling a chaotic system is action first, followed by sensing and then deliberately responding.

At first glance, it seems reasonable, using the Cynefin Framework, to view the cyber environment as an ordered system—complicated yet ordered. After all, what is the cyber environment but a networked group of machines?

Snowden also describes a fourth category where the system lightly constrains the agents, yet the agents also modify the constraining system. This give-and-take occurs in what he terms a "complex" system.[14] In this category, the relationship between cause and effect becomes even more difficult to identify than in a complicated system. Indeed, Snowden contends the co-evolution of agents in a complex system essentially prevents one from identifying cause and effect relationships, even though they exist.

In the complex category, the ultimate link between cause and effect is elusive. In fact, Snowden contends that the evolving nature of the system might prevent the determination of solutions without experimenting on them. Therefore, he recommends changing the problem-solving steps to probe, sense, and respond. In this prescription, to probe means to conduct "safe-to-fail" experiments and using results to inform next steps. In short, this framework advises leaders to avoid forcing a solution based on hindsight, and allowing data to reveal an acceptable course of action. Snowden, therefore, labels this category the "domain of emergence."[15]

At first glance, it seems reasonable, using the Cynefin Framework, to view the cyber environment as an ordered system—complicated yet ordered. After all, what is the cyber environment but a networked group of machines? Indeed, the environment consists of machines that are highly ordered pieces of electronic gear constrained by the laws of physics and governed by strict instructions prescribed by operating systems and resident programs.

Looking deeper, however, it becomes evident that while one might consider individual code as simple and individual machines as complicated, when considered as a whole, the aggregated cyber environment must be considered complex. Ultimately, this is because machines, code, and networking infrastructure share their agency in a system with humans.

Introducing human agents to the system presents multiple issues, but there are two primary factors which turn it into a complex system. The first is humans write the instructions governing computer behavior. At the same time, humans do not communicate with computers in their native tongue. Even the most experienced human programmers manipulate code that is several layers of abstraction above that which directs a machine's behavior.[16] Until humans learn to communicate with machines in their native tongue and eliminate the need for translations, there will always be a variance between what human programmers think they are telling a machine to do and what they are actually telling a machine to do.

This variance creates unintended behaviors that by definition cannot be determined beforehand. Many of these unintended behaviors are expressed as vulnerabilities, leading to the second problem with human agents in the cyber system—vulnerabilities enable unwitting, curious, and sometimes nefarious humans to take advantage of them. As an example, disreputable actors, generally called hackers, routinely install malicious code on the machines of unsuspecting users by exploiting vulnerabilities in document readers, media players, and operating systems.[17]

The cyber environment, therefore, is a system with multiple agents (humans, human organizations, machines, and networking infrastructure) operating in a loosely constrained environment. Each of these agents acts in ways that alter the system and its constraints. Not only do humans introduce unintended behaviors into the machines, but they also attempt to take advantage of resulting vulnerabilities. Furthermore, malicious acts spark humans to develop physical and electronic security measures that themselves further change the system—including organizationally. These organizational changes are evident in the questions posed at the beginning of this article. Specifically, who should lead US government cybersecurity efforts? Before attempting to answer that, it should be noted that Snowden posits leaders must understand the context of the problem.

Based on the introductory scenario and the discussion of the Cynefin Framework, it should be clear that current efforts treat the cyber environment as a complicated system. Almost all governmental efforts in the arena follow the sense, analyze, and respond paradigm. Additionally, disagreement among cyber experts has effectively prevented movement along any cohesive course of action. Disputes over which government agency should lead the effort or debates on the utility of trusted computing modules, cloud computing, or risk management act as evidence to this end. If the cyber environment is in fact a complex system, however, many of these prescriptions are likely wrong. They focus on building more security versus developing systems and organizations that can conduct rapid experiments and quickly adopt emerging solutions.

Based on the introductory scenario and the discussion of the Cynefin Framework, it should be clear that current efforts treat the cyber environment as a complicated system. Almost all governmental efforts in the arena follow the sense, analyze, and respond paradigm.

In essence, understanding the current cyber environment as a complex system should lead decision-makers to conclude that attempting a static, Maginot Line-style defense is futile. Based on the constantly evolving nature of the environment and insights from complexity theory, authorities should attempt instead to create systems and organizations capable of maneuver warfare.[18] The natural follow-up question then becomes: How should authorities build adaptable capabilities and organizations? Ideas emerging from the field of natural security may provide some guidance.

Adaptability in Nature

An internet search on the term "Darwinism" returns approximately 9.6 million results. Performing a similar search using the phrase "survival of the fittest" yields many overlapping results. This seems to suggest many associate Darwin's theory of natural selection with the concept that only the strongest or best organisms survive. This association, though, is wrong. When applied to a complex system like the cyber environment, this logic can waste scarce resources at best, and generate a false sense of security that invites catastrophe at worst.

A closer look at Darwin's theory of natural selection expands upon the shorthand many took away from high school biology. Contrary to popular myth, Darwin never argued only the "fittest" organisms survive. He reasoned an organism did not have to be the best; it only had to be good enough. By good enough, he meant the greatest chance of survival and species propagation is conferred on those organisms most able to adapt to changing environments.[19] The faster the environment changes, the faster successful organisms would have to adapt.

These two ideas—praising "good enough" and "adaptability"—form the foundation of what Dr. Rafe Sagarin has termed "natural security."[20] In his 2012 inquiry on the topic, *Learning from the Octopus*, Sagarin begins with the two concepts and continues by describing those adaptation strategies observable in nature. In general, he finds organisms employing multiple, independently controlled processes for both sensing and responding are more successful than organisms whose similar functions are centralized.[21]

As evidence, he proffers several examples. The two most appropriate for this discussion include camouflage techniques used by the octopus, and the human immune system. The octopus has been around for millennia and is, therefore, a model of adaptation. One of the reasons it has prospered is an impressive ability to change colors and blend in with its environment. The most instructive aspect of this ability is that it occurs automatically, not as a higher-order response specifically controlled by the octopus. The octopus's amazing camouflage skills are an autonomous function through which millions of skin cells independently sense the surrounding environment and react appropriately.[22]

The human immune system provides a more anthropomorphic example where, subconsciously, the system detects foreign invaders and dispatches white blood cells to respond. Additionally, human immune systems evolve over time as they develop antibodies to previously encountered pathogens.[23] In short, the complex system we call nature favors adaptability and adaptability favors decentralized systems.

Sagarin also highlights the benefits redundancy and symbiosis provide organisms in their quest for adaptability. Centipedes, for example, exhibit a relatively simple form of redundancy with their multiple legs.[24] Regardless of cause, should any legs cease to function, the centipede is not left wanting for locomotion to escape a predator or find its next meal or mate. A more creative form of redundancy exists in beetles, which not only developed multiple legs, but whose legs serve multiple purposes.[25]

When applied to the concept of physical security or cyber security, an enhanced understanding of natural security advises decision makers to abandon efforts to create perfect defenses and concentrate on creating those which are good enough.

In symbiotic relationships, organisms create mutually beneficial partnerships. Often, these partnerships form between species one would expect to compete against one another. Sagarin offers a specific example of small fish that eat parasites out the mouths of larger, normally more aggressive fish.[26] The smaller fish gets a meal, and the larger fish gets rid of parasites. Both species win. Additionally, both parties conserve resources to apply to other challenges. Symbiosis, therefore, provides a natural example of the economic concept of comparative advantage.

When applied to the concept of physical security or cyber security, an enhanced understanding of natural security advises decision makers to abandon efforts to create perfect defenses and concentrate on creating those which are good enough. Furthermore, these defenses must constantly adapt to the changing environment and their measure of merit should be response-time. Natural security also suggests that in general, adaptability (e.g., resilience) increases when agents in a system are decentralized. Finally, Sagarin's concepts inform leaders that redundancy and symbiosis are important adaptability strategies in nature. It is now possible to apply these concepts to building more resilience in the complex cyber environment.

Organizing for Cyber Resilience

Lessons from complexity theory and security-in-nature indicate that attempting to mount a static defense of any complex adaptive system like the cyber environment is destined to fail. This does not mean the government should abandon all cybersecurity efforts. To be sure, some defensive measures are necessary, but their ability to adapt to changing conditions should be the standard by which they're qualified. Additionally, defensive exertions eventually reach a point of diminishing returns—the application of additional resources does not provide a proportional increase in security. Since static defensive measures are ineffective and further investment will never make them effective enough, the alternative is to settle on cybersecurity that is good enough and funnel the remaining resources into an adaptable system capable of responding to the inevitable breach.

Cyber adaptability will not improve by centralizing power, budget, and control in a single or even a handful of organizations. To increase adaptability, it will be necessary to create redundancies. Admittedly, redundancy is a difficult term to sell to resource-deficient governments, but the concept of symbiosis discussed above offers a viable complement. Therefore, instead of building ever stronger and taller cyber walls, for example, it is necessary to build more flexible barriers and supplement them with a response force capable of neutralizing threats and patching defenses. Both the barriers and the response force must be able to probe the environment and preemptively respond to emerging threats.

The first step in this process is to shift focus from defending the indefensible to responding to the inevitable.[27] Specifically, cyber actors must train more like emergency managers than security professionals. While most government efforts still focus on security, recent trends point in the right direction. For instance, DHS, mimicking the Federal Emergency Management Agency's (FEMA) response focus in the physical domain, has created the National Cybersecurity and Communications Integration Center (NCCIC) to coordinate response activities in the cyber domain.[28] Forward-looking concepts such as FEMA's Strategic Foresight Initiative have acknowledged the need for a paradigm shift from static to adaptable defenses and the growing need for emergency management disciplines.[29]

Simply creating a national coordination center for cyber response, however, will not change the problem-solving philosophies of those within it. Cyber professionals need to generate a culture of response. In addition to professional courses such as those available through the Emergency Management Institute, nascent cyber emergency managers should internalize a central FEMA truism: Specifically, that every disaster is local, and every disaster is unique. This relatively simple axiom acknowledges disaster response (regardless of cause) usually occurs in the "complex" category of the Cynefin Framework. Additionally, it breeds an innate understanding that pre-packaged, best practice solutions will often fail. In this case, an agency's culture pre-disposes professional emergency managers to probe their environment, sense emergent solutions and opportunities, and then act. In short, emergency managers' experience with natural disasters (which cannot be prevented) has taught them that effectiveness and speed of response often trump defense.

...the longer the delay between patch creation and patch installation, the greater the likelihood an actor will exploit the vulnerability. Therefore, a broader network operating within a common cloud can decrease response time by allowing almost instant inoculation of the entire ecosystem.

The root cause of American cyber woes—technology—might also offer means to refocus ineffective security efforts towards response. Cloud computing, in particular, promises to increase the speed of response efforts. Indeed, much of the current cyber response is hampered by a hodge-podge of organizations that manage individual sovereign networks.

An excellent example is the organization of computer networks in DOD, most of which are administered at the base or post level. This arrangement offers some advantages to individual commanders. Yet, when malware response requires the installation of a security patch, the uncoordinated manner in which local security managers respond creates delays and additional vulnerabilities. In fact, the very act of announcing a new patch highlights the location of the vulnerability it seeks to correct.

In essence, the longer the delay between patch creation and patch installation, the greater the likelihood an actor will exploit the vulnerability. Therefore, a broader network operating within a common cloud can decrease response time by allowing almost instant inoculation of the entire ecosystem. In addition to supporting more rapid patching, enterprise-level organizations can save approximately 40 percent on their computing costs.[30] These organizations can then recapitalize the savings into other response activities or organizational needs.

The second step to organizing for resilience is to incorporate the natural security precepts of decentralization, redundancy and symbiosis. Implied in this step is the recognition of other actors in the system. In the cyber environment these actors include not only various government departments and agencies, but also the vast private sector (which owns the majority of the United States' critical infrastructure), volunteer organizations, and individual citizens.[31]

One might initially conclude centralizing coordination responsibility in the NCCIC is counter to the decentralization ideal. The makeup of the NCCIC and the contents of the National Cyber Incident Response Plan (NCIRP), however, acknowledge the importance in decentralized execution of a centrally coordinated, if not centrally controlled, plan.[32] More specifically, just as FEMA has incorporated private sector representatives into its response activities at the state, regional, and national levels, the NCCIC has adopted a similar approach. Representatives of private sector corporations participate in the NCCIC's daily watch activities and help coordinate response actions when required. During steady state and crisis periods, this provides an important pathway for the federal government to provide intelligence and warning information to the private sector while conversely encouraging the private sector to communicate technical capabilities and solutions back to the government. Additionally, the NCIRP codifies a tiered cyber response system much like the National Response Framework (NRF) has done for the physical response system. While not as mature as the NRF, the decentralized execution described in the NCIRP attempts to mimic the "whole of community approach" sought in emerging, physical response doctrine.[33]

Regardless, decentralization, redundancy, and symbiosis can and should increase. This will demand more independent agents capable of conducting "safe-to-fail" experiments in the system. Since it is unlikely that a highly centralized, efficient (and accountable) system can effectively conduct rapid experimentation, the cyber community should adopt another tactic from the physical response community. Specifically, the NCCIC should attempt to enhance its relationship and increase its connections with the volunteer community.

Volunteers exist in the cyber environment, also. Indeed, groups comprising white hat hackers, concerned cyber specialists, and even industry consortia have emerged as needs have grown.

As an example, FEMA maintains excellent coordination with a number of volunteer organizations through a group called National Volunteer Organizations Active in Disaster (NVOAD). This umbrella group was founded in 1970 to alleviate coordination problems its seven founding charities experienced in their response to Hurricane Camille in 1969.[34] Today, the organization boasts over 50 member charities at the national level, as well as several corporate, government, and academic partners.[35] The primary government partner is FEMA, which communicates response needs to NVOAD, which in turn communicates these needs to its membership. NVOAD member charities then conduct the response activities in a coordinated manner.

Many readers might initially question the true capabilities, capacity, and endurance of volunteers. This would be a mistake. The overwhelming volunteer response to the 2011 tornadoes in the Midwest are a good counter to that assertion. In Joplin, Missouri alone, a town with approximately 50,000 residents, more than 80 volunteer groups logged 126,000 volunteer days and approximately 750,000 hours supporting response and recovery operations. In fact, there were so many volunteers that volunteer organizations sprang up to manage the volunteers. These individuals did not just show up just to be counted. They provided critical services such as debris removal, feeding, sheltering, and rebuilding.[36]

Volunteers exist in the cyber environment, also. Indeed, groups comprising white hat hackers, concerned cyber specialists, and even industry consortia have emerged as needs have grown. An excellent example is the working group that initially detected and fought the nagging Conficker worm in 2010.[37] Additionally, multiple competing information technology companies formed the Industry Consortium for the Advancement of Security on the Internet to share vulnerability information.[38] To increase resiliency through decentralization, redundancy, and symbiosis, the government must expand their efforts to partner with similar organizations.

The NVOAD example offers a useful model. While NOVAD is currently limited to the physical domain, a similar blanket group could harmonize the activities of cyber-focused volunteer organizations or individuals. Much like the NVOAD arrangement, even though no government agency would control volunteer efforts, the government could influence activities by provisioning a needs or challenge list. Indeed, natural security research suggests organisms respond better to challenges than directives.[39] Communication with these cyber volunteer organizations (CVOs) would allow government officials visibility into their operations, in turn offering interagency leaders the ability to focus limited public resources elsewhere.

A primary barrier to such an arrangement has traditionally been security classification guidelines and false assumptions about the motives of cyber savvy activists.[40] Too often, governments assume all hackers are nefarious actors and therefore attempt to hide vulnerabilities behind classified walls. This practice makes sense in certain security scenarios. When responding to a cyber attack similar to the one described at the beginning of this paper, attempting to hide one's (already exploited) vulnerability seems a bit too late. Therefore, the costs of communicating current response needs are probably less than the likely benefits of gaining access to a more diverse network of probing, sensing, and responding minds.

Summary

US federal government departments and agencies have spent too much time in the cyber domain asking "who," and not enough time defining "what." A majority of the debate bandwidth associated with cyber issues is consumed by arguments over which agencies lead and which agencies follow. These are important questions, but they crowd out a more essential discussion about what these cyber efforts actually are or should be. Starting with: who leads organizations to consider solutions based on their own information frameworks, culture, and bureaucratic imperatives? The answers are generally based on imperfect metaphors and attempt to apply variations of pre-existing capabilities to new problems. For cyber, however, many of these metaphors fall short. This problem-solving technique demonstrates that most organizations have incorrectly identified the cyber environment as a simple or complicated system where best practices rule.

The nature of complex systems makes it clear that the cyber environment is better described as a complex system. Consequently, policymakers should focus more on response than security.

The nature of complex systems makes it clear that the cyber environment is better described as a complex system. Consequently, policymakers should focus more on response than security. This is not to say security is unimportant. Certainly, society's connectedness magnifies associated vulnerabilities, and therefore everyone with access to a computer should engage in practices which increase cybersecurity. Digging deeper, one determines invulnerability is impossible, so everyone at some time will be forced to respond to a cyber event. The only remaining variables are the effectiveness and speed of that response.

Moving resources from security to response will not be easy. Few government officials or CEOs will relish addressing their constituents or shareholders with a "stuff happens" message. On the contrary, pressures will likely push leaders in the opposite direction—especially if basic services such as electricity are absent for extended periods.

Difficulty, however, does not equal impossibility. Leaders can and should engage their stakeholders in a more enlightened debate about cyber issues. This debate should include the accurate portrayal of the complex nature of the cyber environment. These leaders should emphasize that the United States has faced similar complex problems in the past and has developed actionable lessons and responses. These lessons occur naturally all around us.

Citizens understand government cannot prevent hurricanes. Therefore, their ire is raised not by the event, but by delayed or ineffective response efforts. Additionally, they accept the inherent risks of hurricanes and attempt to mitigate this risk with tools like insurance. Correctly addressed, citizens will also understand that, regardless of the manmade nature of the domain, the cyber environment shares many of the same complex characteristics as the natural environment. Once citizens better understand the similarities of cyber and nature, they will be more apt to embrace successful examples from the later.

Nature is replete with examples of resilience gained through the adaptation strategies of decentralization, redundancy, and symbiosis. Governments can implement these strategies by refocusing much of the current cybersecurity emphasis towards rapid response, pursuing greater integration with the private sector, and encouraging the creation of a cyber-focused volunteer co-ordination mechanism modeled after NVOAD.

The alternative, of course, is to continue chasing invulnerability, and starting from scratch after an inevitably large-scale failure. Then again, perhaps such a failure will be necessary. In spite of numerous official and unofficial warnings, many individuals simply do not accurately perceive the magnitude of current cyber risks. In many ways, the government fosters such ignorance through well-meaning, if not entirely effective, rhetoric and actions. Based on these conditions, who can blame citizens for not accurately assessing the possible costs of our cyber risks and taking positive action? Darwin would probably agree that most adaptation in nature required some form of crisis—else why change?

Endnotes

[1] Editorial, "A Cyber Risk to the US," *Washington Post*, February 12, 2012, http://www.washingtonpost.com/opinions/a-cyber-risk-to-the-us/2012/02/07/gIQA4q7M9Q_story.html (all links accessed October 2018).

[2] *What Should the Department of Defense's Role in Cyber Be?: Hearing before the Subcommittee on Emerging Threats and Capabilities,* House Armed Services Committee, February 11, 2011, 112-5; Kim Zetter, "DHS, Not NSA, Should Lead Cybersecurity, Pentagon Official Says," *Wired*, March 1, 2012, http://www.wired.com/threatlevel/2012/03/rsa-security-panel; Sydney J. Freedberg Jr., "Military Debates Who Should Pull the Trigger for a Cyber Attack," *Breaking Defense* May 22, 2012, https://breakingdefense.com/2012/05/military-debates-who-should-pull-the-trigger-for-a-cyber-attack/.

[3] Paul Rosenzweig, "Cybersecurity and Public Goods: The Public/Private "Partnership" (2011)," in Emerging Threats in National Security and Law, Koret-Taube Task Force on National Security and Law, edited by Peter Berkowitz, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf, 3.

[4] *Dictionary.com,* "system," http://dictionary.reference.com/browse/system?s=t.

[5] David J. Snowden and Mary E. Boone, "A Leader's Framework for Decision Making," *Harvard Business Review* 85, no. 11 (November 2007), 70; "The Cynefin Framework," YouTube video, 8:37, posted by roylangmaid, October 4, 2011, http://www.youtube.com/watch?v=JEDpcNnlOJM.

[6] Snowden and Boone, "A Leader's Framework for Decision Making*,"* 70.

[7] Ibid., 72.

[8] Snowden and Boone, "A Leader's Framework for Decision Making," 70.

[9] Daniel Ford, *A Vision So Noble* (Durham, NH: Warbird, 2010), 4.

[10] Snowden and Boone, "A Leader's Framework for Decision Making," 70.

[11] Ibid., 71.

[12] Ibid., 71-72.

[13] Snowden and Boone, "A Leader's Framework for Decision Making," 73.

[14] Snowden, "The Cynefin Framework," video.

[15] Snowden and Boone, "A Leader's Framework for Decision Making," 74.

[16] David Aucsmith, "Rethinking Cyber Defense," *High Frontier* 7, no. 3 (May 2011), 35.

[17] Microsoft, "Security Intelligence Report, Volume 11" (Redmond, WA: Microsoft Corporation, 2011), xvii.

[18] Aucsmith, "Rethinking Cyber Defense," 36.

[19] Rafe Sagarin, *Learning from the Octopus* (New York: Basic Books, 2012), 33.

[20] Ibid., xxv.

[21] Ibid., 65-67.

[22] Ibid., 27-29.

[23] Ibid., 64-65.

[24] Ibid., 90.

[25] Ibid., 92-93.

[26] Ibid., 176.

[27] Noah Shachtman, "Military Networks 'Not Defensible,' Says General Who Defends Them," *Wired*, January 12, 2012, http://www.wired.com/dangerroom/2012/01/nsa-cant-defend/?utm_source=fee.

[28] Office of the Secretary of Defense, "Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center," *Department of Homeland Security*, October 30, 2009, http://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened; "About the National Cybersecurity and Communications Integration Center (NCCIC)," Department of Homeland Security, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center-nccic; "Inside DHS' Classified Cyber Coordination Headquarters," J. Nicholas Hoover, *InformationWeek*, accessed June 11, 2012, https://w2.darkreading.com/risk-management/inside-dhs-classified-cyber-coordination-headquarters/d/d-id/1093107?piddl_msgorder=thrd&page_number=1.

[29] Federal Emergency Management Agency, *Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty* (Washington, DC: Government Printing Office, 2012), 2-3.

[30] Ross Tisnovsky, "Risks Versus Value in Outsourced Cloud Computing," *Financial Executive* 26, no. 9 (2010), 64.

[31] Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington, DC: Government Printing Office, 2009), 24.

[32] Department of Homeland Security, *National Cyber Incident Response Plan: Interim Version* (Washington, DC: Government Printing Office, 2010), 4, 24-25, I-1.

[33] *Testimony of Craig Fugate, Administrator, Federal Emergency Management Agency, Before the U.S. Senate Homeland Security and Governmental Affairs Committee,* Homeland Security (2012), http://www.dhs.gov/news/2011/03/17/testimony-craig-fugate-administrator-federal-emergency-management-agency; Department of Homeland Security, *National Response Framework* (Washington, DC: Government Printing Office, 2008), 8.

[34] "About Us," National Volunteer Organizations Active in Disaster, 2014, http://www.nvoad.org/index.php?option=com_content&view=article&id=53&Itemid=188.

[35] "Our Network," National Volunteer Organizations Active in Disaster, 2014 http://www.nvoad.org/index.php?option=com_content&view=article&id=86&Itemid=75.

[36] "Joplin Voluntary Long-Term Recovery Agencies Recognized," FEMA, accessed July 18, 2012, http://www.fema.gov/fema-weekly-employee-articles/joplin-voluntary-long-term-recovery-agencies-recognized.

[37] Mark Bowden*, Worm: The First Digital World War* (New York: Simon & Schuster, 2011), 35.

[38] Rosenzweig, "Cybersecurity and Public Goods: The Public/Private 'Partnership'," 18.

[39] Sagarin, *Learning from the Octopus*, 218-219.

[40] Bowden, *Worm,* 114; Rosenzweig, "Cyber Security and Public Goods," 12-13.

About The Mitchell Institute

The Mitchell Institute educates the general public about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Col W. Mark Valentine, USAF (Ret.) is a former fighter pilot, commander, and staff officer. During his tour on the Joint Chiefs of Staff he served as the senior military advisor to the Federal Emergency Management Agency (FEMA) where he coordinated operational, strategic, and policy guidance between FEMA, the Joint Staff and the Office of the Secretary of Defense to optimize the Department of Defense's ability to support civil authorities and respond to disasters. He currently lives in the Washington, DC area where he leads Microsoft's efforts to support the US Army.

Valentine holds a Bachelor of Science degree in astronautical engineering from the US Air Force Academy, a Master of Arts in national security policy from Georgetown University, and is a graduate of the executive education program at the University of Virginia's Darden Graduate School of Business. He was also a Secretary of Defense Fellow at the Microsoft Corporation, and is a graduate of the National Emergency Management Executive Academy and the State Department's National Security Executive Leaders Seminar. Valentine is also a graduate of Squadron Officers School, Air Command and Staff College, Air War College, the US Air Force Weapons School, and the NATO Tactical Leadership Program.

The opinions expressed in this paper are the author's alone and do not necessarily reflect the opinions of the Department of Defense, the US Air Force, or the Microsoft Corporation.

An Affiliate of the Air Force Association | www.mitchellaerospacepower.org