Information on Current and Future States of Cybersecurity in the Digital Economy

Submission from Chris Williams, co-author of the book, *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats.*

9 Sep 2016

Executive Summary

In the RFI, the Commission on Enhancing National Cybersecurity requests information about current and future states of cybersecurity in the digital economy. This is a topic that we discuss in our book, *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats.* This book, informed by years of battling cyberattacks from advanced adversaries, outlines a framework and strategy for operating a cyberdefense program that is effective against today's cyberattackers. This book is currently being used to teach Cybersecurity management at the University of Southern California in Los Angeles, and at National University in San Diego.

In the book, we lay out a framework for managing a cyberdefense program, and also how to use that framework within a program to coordinate cyberdefense policy, budget, personnel, technology, and assessment. We also discuss techniques for deploying security architectures and capabilities to counter today's most dangerous cyberthreats.

In the book, we introduce a new concept for cybersecurity strategy we call *Generations of Cyberdefense*. Our hypothesis is that part of the current "crisis" is because we are in the process of undergoing a paradigm shift related to the transition from one generation of cyberdefense to a new generation of cyberdefense. In short, new-generation cyberattacks are defeating old-generation cyberdefenses, just as occurs with military techniques and weapons. In our research we identify five generations of cybersecurity:

1. Generation 1: Protection of individual network-connected hosts.
2. Generation 2: Protection using network perimeter
3. Generation 3: Layered defense and active response
4. Generation 4: Automated detection, response, and remediation
5. Generation 5: Data-based protection from insider and stealth attacks

We find this methodology to be useful for considering cybersecurity and cyberdefense, as security capabilities can be characterized in terms of the generation of cyberdefense they represent and enable. Enterprises should proceed through the generations in sequence, and should only add more advanced-generation defenses when they have achieved the preceding generations first.

We encourage the Commission to consider the *Enterprise Cybersecurity* book, and hope that its ideas may be useful to the Commission's effort.

Generations of Cyberdefenses

In the book *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*, we outline a framework for delegating and managing a cyberdefense program that consists of 11 Functional Areas that are then managed across the programmatic areas of Policy, Strategy, Engineering, Deployment, Operation, and Assessment. This allows the cyberdefense program to be well-coordinated, and allows for effective delegation and management of aspects of cyberdefense.

Cybersecurity is in the midst of a Paradigm Shift

In the course of our research, we asked ourselves the question, "Why is cybersecurity in crisis today?" Is it because all of the sudden the attackers have become geniuses? Or is it because all of a sudden the defenders have become fools? Or is it because we are in the midst of a paradigm shift? We believe the answer is the latter, as innovations in cyberattacks over the past several years have rendered the "legacy" cyberdefense consisting of network perimeters and signature-based defenses largely obsolete.

Gen 1:	**Gen 2:**	**Gen 3:**	**Gen 4:**	**Gen 5:**
F-86 Sabre	F-8 Crusader	F-4 Phantom	F-15 Eagle	F-22 Raptor
(1949)	(1957)	(1960)	(1976)	(2005)

Figure: Generations of US Air Force fighter aircraft.

There is precedent for this possibility, as military scientists commonly refer to generations of weapons systems, such as rifles, tanks, ships, or fighter aircraft. In the case of fighter aircraft, each new generation is designed to completely defeat the previous generation of aircraft in combat. Due to this principle, the US Air Force's F-15 fighter has a perfect combat record of 101 victories to zero losses, largely due to the fact that most of its adversaries have been older generation aircraft that did not stand a chance.

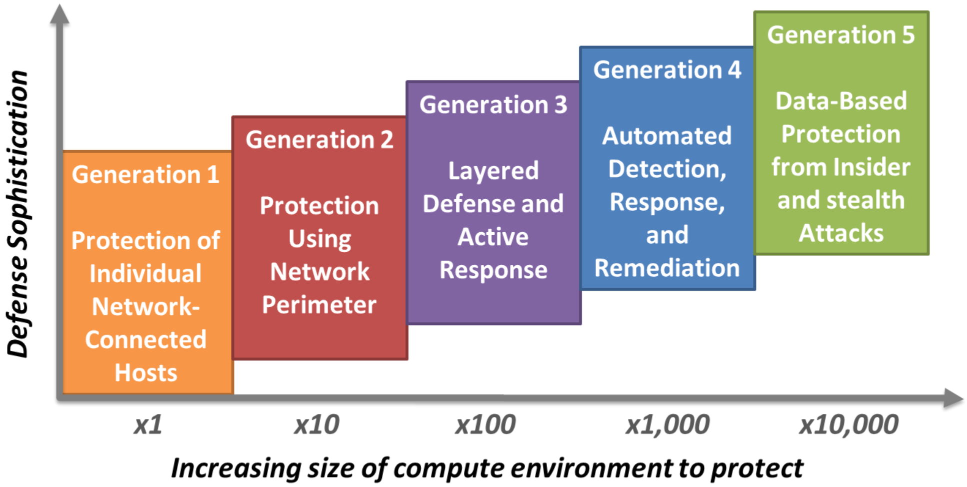
Defense Sophistication
Generation 1
Protection of Individual Network-Connected Hosts
Generation 2
Protection Using Network Perimeter
Generation 3
Layered Defense and Active Response
Generation 4
Automated Detection, Response, and Remediation
Generation 5
Data-Based Protection from Insider and stealth Attacks
x1
x10
x100
x1,000
x10,000
Increasing size of compute environment to protect

Figure: Cyberdefenses can be considered in terms of generations.

In the course of our research, we found evidence of similar paradigm shifts in cybersecurity. We identified five distinct generations of cyberattacks and cyberdefenses, spanning historically from the 1990s through the present and looking to the future over the next decade.

1. **Generation 1:** In the 1990s, most systems were directly connected to the Internet, and security consisted of patching those systems and protecting them from exploitation. Over time, as the number of systems exploded, this approach became less and less practical.
2. **Generation 2:** Starting in the early 2000s, enterprises began establishing network perimeters so their vulnerable hosts could be isolated from the Internet, and host-based security became less critical except for a limited number of Internet-facing DMZ systems.
3. **Generation 3:** Since 2010 or so, advanced attackers have begun exploiting vulnerabilities in the perimeter due to increasing interconnectivity and endpoint complexity and mobility to establish footholds in the enterprise and follow a "kill chain" to achieve their objectives. Defenses against these new threats require segmenting the internal environment, hardening critical infrastructure and security systems, and establishing detection and response against advanced attacks.
4. **Generation 4:** In the future, Generation 3 cyberdefenses will be defeated by swift attacks that accomplish their objectives at machine speed, so even though defenders are alerted, they will not have time to respond. An example of this type of attack is the devastating ransomware attacks that have disabled several hospitals in 2016. Generation 4 cyberdefenses involve automating the attack response process, so that attacks can be detected and contained by the machines as quickly as they are conducted.
5. **Generation 5:** In the future, Generation 4 cyberdefenses can be defeated by stealthy attacks that focus on stealth, not speed, so they are not detected by the defensive framework. Such attacks use the supply chain to embed compromised devices into the network when the network is built, and then use compromised credentials and existing management protocols so attacks look like legitimate activity to defensive systems. Generation 5 cyberdefenses involve data-level protection, and using analytics to detect anomalous activity when it occurs.

We have found this concept to be useful in thinking and strategizing about cyberdefenses. The generations paradigm provides a simple and intuitive explanation for the current challenges in cyberdefense, while also providing a useful vision of what may be coming over the next ten years or so. We hope that this perspective may be useful to the Commission, and that the Commission may consider the *Enterprise Cybersecurity* book as a resource to their efforts.