Jordan Dickson

Jan 18, 2016

65582692

HCP Draft 1: The Rising Need for Cybersecurity in the Modern World

The increasing interconnectedness brought by the internet and the rise of the digital age, has created new vulnerabilities faster than many people, companies, and governments can keep pace with, causing an immediate need for a comprehensive plan for the cyber-defense of personal, commercial, and government data. Current tends regarding the increasing integration of technology in our everyday lives indicate that cyber-physical interactions will increase in both number and significance in the near future. Developing technologies and current research areas in concepts like self-driving cars and the internet of things prove that if nothing is done about creating a cybersecurity plan at the national, commercial, and individual levels, we will become increasingly vulnerable to cyber-attacks.

The need for increased cybersecurity can be found on multiple levels in the modern world. Cybersecurity as an issue of national defense is perhaps the most obvious - and most pressing. In his presentation for General Dynamics "Rethinking Defensive Information Warfare," Geoffrey French begins declaring that "the United States, because of its civilian and military dependency on information technology systems, is vulnerable to attacks on those systems" (1). The logic makes sense and you'd expect that cybersecurity would be a top priority for the national government, but at that time in 2004, little had been done in the way of establishing robust, secure, and adaptive systems to meet the cybersecurity threat. In 2004 French proposed a plan he compared to WWI defense in depth, calling for the development of multilayer, reactive, and diversionary systems that could better protect government and military information. Since

then, many steps had been made towards this goal both for offense and defense. Ten years later, at another cybersecurity presentation in 2014, Mordechai Guri and his colleagues demonstrated AirHopper, a system which allowed a smartphone to literally "listen" to the images on a screen up to 7 feet away by detecting its incidental electromagnetic field. As with any arms race the NSA published countermeasures for it and other government agencies to take that would mitigate the effectiveness of such attacks. The complexity of cyber-attacks and defense has increased exponentially since 2004. While progress has been made towards the goal of total information warfare readiness, without a multilayer defense strategy the United Sates is still only able to react to new threats after they have struck. The nature of cybersecurity changes so quickly as to demand constant reevaluation of threats, adaptation of available resources, and adoption of new countermeasures.

The problem of cybersecurity unpreparedness does not just exist between governments. Commercial enterprises have also experienced the consequences of poor cybersecurity. Many companies have to make accept a tradeoff between security and accessibility. Executives and employees want to have access to their work from anywhere, yet they also want to keep it secure. Such a miracle system has yet to be implemented, and most companies have elected to take convenience and accessibility over security. This has led to a lot of vulnerabilities, especially as companies move more and more of their business online. In "Counterterrorism and Cybersecurity" Newton Lee describes what is called the Sony-pocalypse, the largest and most destructive cyberattack in history against a company operating out of the US. In the 2014 attack "the [Guardians of Peace] had stolen 100 terabytes of data, destroyed 75% of corporate computer servers, and crippled the company's data centers" (13). The idea of cooperate computer servers actually being destroyed remotely though the internet was a disaster for Sony, but could easily

escalate to a catastrophe in the near future as more and more critical systems are connected to the internet. Also worth mentioning, Sony's response was to use its remaining servers to launch denial of service attacks (a basic tactic of cyber-warfare) against websites distributing the stolen data. This incident is one of many that demonstrates corporate vulnerability to cyber attacks. As the frequency and sophistication of cyber attacks increase, companies will either have to develop revolutionary new systems to protect data while ensuring internal accessibility or reevaluate their priorities.

Unfortunately, the cybersecurity problem even effects us people as individuals. Theo Tryfonas points to identity theft becoming more and more common as people move their banking, shopping, and social lives online. Organized crime regularly targets people attempting to steal identity information, bank account information, and even healthcare information. The cyber criminal then sells the information to others to protect his identity. Catching such criminals is very difficult since they can redirect their attacks many times to obscure the source and they almost never use the information they steal for themselves. They can use to internet to target almost anyone from almost anywhere, further increasing the difficulty of their apprehension. While everyone wants to see cybersecurity systems in place to prevent such crimes, the application of cybersecurity on the personal level quickly turns into a debate about privacy vs security. As Sophie Stalla-Bourdillon and her colleagues argue in "Privacy vs. Security" any future cybersecurity system designed to interact with individuals will need to include the right balance of personal privacy and societal security. She argues that we need to rethink our concept of privacy so that we can better integrate it into the cybersecurity systems of tomorrow. For now, the best practices of individuals is to be cautious on the internet, make good passwords, and keep

their antivirus software up to date. None of these are perfect solutions, but without the resources of governments or large companies, the best individuals can do is just follow best practices.

Annotated Bibliography

French, Geoffrey. “Rethinking Defensive Information Warfare.” General Dynamics. White Granite Drive Suite 400, Oakton, VA. Jun 2004. Web. 14 January 2016.

This presentation by General Dynamics at the 2004 Command and Control Research and Technology Symposium outlines the United States’ readiness in the field of information warfare in 2004. It offers a perspective from last decade about perceived threats to and vulnerabilities in our ability to attack and defend in a case of information warfare against a sophisticated enemy. It calls for a change in philosophy from just information assurance, the ability to assure the validity of information, to a system of multiple defensive lines, “honeypot systems” to attract and distract attackers, and reactive systems able to recognize the presence of malicious actors on a network.

Knott, Alexander, David S. Alberts, Cliff Wang. “Will Cybersecurity Dictate the Outcome of Future Wars?.” *IEEE Computer Magazine*. IEEE Computer Society, December 2015. Web. 14 January 2016.

This article from IEEE magazine discusses and summarizes the conclusions of a 2015 conference between academic, industrial, and military scientists and engineers hypothesizing about how the army will function in 2050. After examining current technologies and research areas, most concluded that in the future intelligent systems will be ubiquitous, in our cities and our fighting forces. The ability to collect, process, and interpret data will be a major factor in deciding the outcome of future battles. This article does not focus specifically on cybersecurity, but it offers a look into the importance of cyber defense - and offense - to national security.

Stalla-Bourdillon, Sophie, Joshua Phillips, Mark D. Ryan. “Privacy vs. Security.” *SpringerBriefs in Cybersecurity*. Springer, 2014. Web. 15 January 2016.

This article from the set of SpringerBriefs in Cybersecurity, argues that societal safety is more important than personal privacy in the traditional sense. It advocates the use of large scale data collection to reduce crime and prevent cyber attacks. However, it does not completely forsake privacy, claiming that we need to rethink our ideas of privacy so that they can be integrated into the security systems of the future.

Lee, Newton. “Counterterrorism and Cybersecurity: Total Information Awareness.” Springer. Springer. Second Edition. 2015. Web. 15 January 2016.

This collection of articles features topics from the origins of cyber warfare to why people become hackers, to the impacts of the recent Sony attacks. In its section about why people become hackers, it discusses the different agents acting in different cyber attacks. From high school students to organized criminals to state sponsored attackers, all attacks vary in sophistication, purpose, and the methods employed. Some attack a system quickly looking to gain administrator privileges for just a few hours to steal information. Others take a lower profile in the system quietly listening to whatever they can for months or even years. The variety of cyber attacks and cyber criminals makes it difficult to predict just how one is supposed to best protect their information systems.

Tryfonas, Theo; Askoxylakis, Ioannis. *Human Aspects of Information Security, Privacy, and Trust*. Springer. 2 August 2015.

This collection of articles from the Third International Conference of Human Computer Interaction features articles covering topics including Privacy, User Behavior, Cybersecurity, and Authentication. One of the articles discusses how cyber criminals target individuals for bank information, identity information, and surprisingly healthcare information. These attackers are usually linked with organized crime and they sell stolen information to others to make money. They use various techniques to mask their identity and location from investigators, and int interconnectivity of the internet means they can strike anywhere in the world, certainly outside of the jurisdiction of police local to the person they target. This gives the individual's persecutive on the cybersecurity issue as it is not just a problem between governments.

Burns, Nicholas; Price, Jonathon: Nye, Joseph; Scowcroft, Brent. Aspen Institute. *Securing Cyberspace: A New Domain for National Security*. 2011.

Langston Library: HV6773.2 .S32 2012

I have yet to analyze this source.

Congress. House Committee on Oversight and Government Reform. *Cybersecurity: Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems*. 2010.

Ayala Science Library: Y 4.G 74/7:111-51

I have yet to analyze this source.

Congress. House Committee on Homeland Security. *How Data Mining Threatens Student Privacy*. June 25, 2014.

This Congressional hearing discussed the exact purpose, necessity, and methods by which schools were sending student information to third parties for data mining. It gives an example of the type of data that gets transferred around the internet and is potential at risk. It continues the privacy/security debate stating several positives of data mining. Data mining is one of the methods that information processing systems use to extract data from enormously large input sources. Data mining is in use by many companies trying to determine trends in the population's behavior. It is also used by security agencies to interpret the huge amounts of data steaming in from the many sources available to them.

Moise, Adrian Christian. *Aspects Regarding the Impact of the Internet on the Society*. EBL. 2014.

This article from 2014 discusses the ways in which the internet has effected the average American. New conveniences like online shopping, banking, and communication have also opened the door for potential theft of personal data. It brings up how the cyber world has begun to interact more and more with the physical one and how the government is behind in its regulation of such virtual-physical interactions. It also discusses things like how the internet led to increased globalization and the security privacy debate. This article gives an idea of what the cyber world means to an average american and can be used to predict how we will interact with virtual technologies in the near future.