Fighting Alone is called Losing: The Unlearned Lessons of Fragmented Systems

Lieutenant General (Ret.) Edward Cardon

Cyberspace is a man-made, contested, and competitive domain that is continuously evolving and adapting at speeds and scales difficult to comprehend or imagine. While hardware is geographically located in a physical layer somewhere on earth or in space, the software and data can move freely in a logical layer unless otherwise constrained. The result is a global surface that requires a globally coordinated defense by a global team. Therefore, within the context of cyberspace, the idea of "defending alone" seems ludicrous. Yet, that is exactly how people, firms, and governments have been left alone to approach cybersecurity. As noted in his comments on the SolarWinds hack in March 2021, General Paul Nakasone, the commander of the United States Cyber Command stated that, "[I]t's not that you can't connect the dots. You can't see all the dots. And when defenders *can't see all the dots*, security gaps and breaches happen."[1] Ultimately, the cyber domain's primary lesson is that leaving everyone to defend alone leaves everyone to lose.

Defending in Cyberspace

What makes cyber defense so hard? If we think of the Internet as a neighborhood with associated crime problems, cyber-crime and attacks are quite varied in their approach, intent, and execution. For example, cyber actors use tools and techniques such as malware attacks to break into systems, devices, and networks to steal sensitive data, information, etc. Similarly, cyber actors use social engineering techniques, often referred to as hacking the human, to hack the network. Other cyber actors cut off access to critical services through denial-of-service attacks. Cyber criminals use tools and techniques such as ransomware to deny critical systems, networks, and data. Finally, some cyber actors attack the very structure of our networks and critical systems through hardware or software supply chain attacks.

1. https://www.cyberscoop.com/nsa-solarwinds-russia-china-nakasone/

Lieutenant General (Retired) Ed Cardon's service to our Nation spans over 36 years including work in Germany, Bosnia-Herzegovina, Iraq, and the Republic of Korea. He both transformed and scaled U.S. Army Cyber Command into a world-class cyber force with new organizations, operational constructs, and talent models. Since retirement he has created a portfolio focused on helping individuals and teams solve hard problems with Touchstone Futures, C3 AI, The Cohen Group, and the Advanced Research Laboratory for Intelligence and Security.

Cyber actors can attack using a combination of the techniques as discussed above, can develop completely new techniques, or can even use some combination thereof. And cyber actors do not have to be malicious or criminals – they can be activists, nation states, or normal citizens. Even when an intrusion is discovered, it often takes a deep, multi-disciplinary analysis to confirm the intent behind an attack, and often leaves unanswered questions for cybersecurity experts and professionals to ponder as defenses are evaluated and updated. Was it an information assurance problem? Was it an insider threat? Is the attacker a criminal? Was it a nation state? Could it have been a hacktivist?

The complexity is not just from the threat, but it also comes from the domain itself. The cyber domain is made up of an ever-changing confluence of people, technologies, and processes. It is characterized by disruptive technologies and applications. Time is an important component. Software changes at the speed of coding. Hardware changes at the speed of chip evolution and is increasingly becoming software based. People can change the cyber domain at the speed of thought and learning. In many ways, cyberspace remains largely unstructured, especially when considered in the context of a political map, detailing the physical and sovereign boundaries between nation states. Without physical delineations to define jurisdictions, the established law, authorities, regulations, processes, structure, and concepts applied to the cyber domain are still in flux for both the public and private sectors.

Therefore, it makes little sense to ask all network users, providers, and suppliers to defend their networks, data, critical systems, and information alone, and expect success. Even with the very best technology and processes, when combined with all the potential human factors, there are vulnerabilities in every network. It has become increasingly clear that all networks, regardless of location, are in daily contact with

a multitude of cyber adversaries and threats. Risk of compromise continues to accelerate past what fragmented defenses can withstand.

Three Components Essential to the Team

The lesson to be learned of cyberspace is that decentralized, uncoordinated, standalone defenses are ineffective, and the solution is to create a team to defend our networks and critical systems. At a minimum, this team should contain at least three components – the *owner* of the network itself and all its suppliers; the *government's or governments'* competent representatives or authorities; and the relevant or affected actors in the *private sector.* These three components include multiple sub-units, making it a *team of teams* with each component playing a critical role to avoid fighting alone.

One challenge is that a network is often mistaken for a single entity vice the sum of various individuals' work hours and hardware vendors e.g., end devices, network devices and peripherals. A network is in reality a complex set of component parts that must be integrated, configured, and administered by the team responsible for building, operating, and sustaining the network, and the owner of a network hires that team. Additional network elements also require management: e.g., an Internet service provider, software vendors for products and services, software applications and services that are available on the network, and all the data generated from network use among all its various components and users. Ultimately, a network is never just a network.

Also, networks are rarely stand alone or operate in isolation. As more operational technology components come to rely on IP-based services (i.e., the Internet), more systems are exposed to global threats. The idea that an in-house network administration team can manage a network – both internally and externally – to protect it from all forms of attack is an unrealistic expectation and has been for some time. For example, a typical network analyst is responsible for evaluating, planning, ordering, and installing any technology required for a network, requiring a knowledge of the network user needs, network data and baseline measures, and other skills that require a deep expertise. Increasingly network data analysis is being transferred to various forms of autonomy, automation, and/or artificial intelligence. In addition, information and intelligence is needed on cyber actors and potential threats e.g., their infrastructures, their exploits, their tactics, techniques, and procedures, etc. The in-house teams (even if they do include third parties) have long needed additional support structures to escape fighting alone.

The government has a role in supporting a collective defense. Unfortunately, a major weakness is the lack of organization in the US (and elsewhere) at all levels (federal, state, and local). As shown by the past decade, the U.S. Government's (USG) approach is often too fixated on physical harm. All lesser forms of harm are consolidated and effectively dismissed as just the cost of doing business. If an ongoing cyber-attack caused obvious and palpable harm in the physical world, the likelihood of government action would increase immensely. This is exactly

what happened with the 2021 Colonial Pipeline ransomware attack.[2] People standing in line because gas stations were closing pumps was a physical manifestation of the cyber-attack and many agencies, most publicly the FBI, sprang into action. That was great for the Colonial Pipeline company, but it is not possible for a private company to legally replicate the cyber capabilities of the USG that can take a more proactive, defend-forward posture in cyberspace. To be fair, government responses to cyber-attacks have improved over time, with the creation and redesign of organizations, commands, information-sharing forums, and the revision of statutes and policies, but much work remains to be able to operate defenses at the speed and scale of the various threats.

Part of the team solution is to bring to bear all the components of the private sector that enable the creation, protection and sustainment of networks and associated data. The growth in private sector cybersecurity capabilities has been significant, but advancements tend to maintain an inward focus on protecting internal data, systems, and assets, like intellectual property. Most cybersecurity decisions are driven by the technological innovation expected of these companies in support of their own clients, products, and profit forecasting – not in a manner that will support a collective defense.

Much of the network space and the data needed to understand a cyber-attack are located with and owned by the private sector. There are several legal and/or regulatory issues that limit or prevent the sharing of information between private companies, cybersecurity companies, or governments, primarily over concerns about liability, privacy and civil rights, and reputational risk. And because most of the data that is needed to conduct a holistic and thorough investigation after a cyber-attack is collected, housed, and stored in the private sector, cost quickly becomes a factor that determines whether data is even available or maintained for analysis. In short, cyber defense is fragmented, creating a disjointed environment in which everyone is fighting alone and losing.

To further clarify why fighting alone causes everyone to lose, a use case compiled from recent attacks is instructive. A private company with a national security portfolio made decisions on its information technology budget, and its acceptance of cyber risk, cost, and its competitiveness. Despite best efforts, due to human error, the company network was compromised. The compromise was only discovered after a third-party cybersecurity company informed the company of the compromise while working with a third company on a similar compromise committed by the same malicious cyber actor.

Given the importance of the company's national security portfolio, the Federal Bureau of Investigation (FBI) was notified and opened an investigation. The Cybersecurity and Infrastructure Security Agency (CISA) was also called because this company supports a portion of the national critical infrastructure, and it too opened a separate investigation. Both agencies'

2. Most of the details in this section are found in the following reference; other notes come from personal discussions with relevant cyber subject matter experts and the author's own analysis. Joe R Reeder and Tommy Hall, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack," *Cyber Defense Review* (2021), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2723341/cybersecuritys-pearl-harbor-moment-lessons-learned-from-the-colonial-pipeline-r/.

investigations suffered due to a lack of data for analysis. The data was contractually not available, and it was not collected and stored for forensic type analysis by the network owner and network providers. The U.S. Securities and Exchange Commission (SEC) was also notified.

After the victim company eventually received permission to share information from the company's network vendors due to contract clauses, analysts quickly determined that the breach was most likely committed by a foreign cyber actor. In the case of national security systems, there are processes with strict oversight that enable the National Security Agency (NSA) to support the FBI and CISA. However, the foreign cyber actor used a US commercial cloud as part of its infrastructure precisely to obscure its foreign origins, which further complicated the sharing of information between all investigative teams. Days and weeks went by as each entity tried to do their part to navigate legal and procedural restrictions and guidelines to determine attribution, and to remediate the malicious cyber activity on the network. The response was fragmented at best, and reactionary at worst. In the end, each entity involved generated their own understanding of the attack, but the lack of a holistic understanding at speed and scale ultimately meant that everyone had lost. During the same period, the cyber actors moved on to their next victim, also most likely defending alone.

A private company is responsible for the creation, operation and sustainment of its own network using best practices. Going back to the neighborhood analogy, when crime becomes a problem, it is not unusual for a neighborhood watch to be formed as it is one part of a coordinated response that is nested within local, state, and federal legal frameworks. In a related way, a team of teams is required to conduct a holistic cyber defense. So, does it still make sense, from a cyber defense perspective, that private companies are solely responsible for defending their networks?

Returning to General Nakasone's remarks about SolarWinds: no single entity – be it the owner of the network itself and all its suppliers; the government or governments; and the private sector – can see all the dots. Therefore, no single entity can defend itself sufficiently against the threat of cyber-attack The network owners can only see the dots they can see, the private companies that make and operate the networks can only see the dots they can, and the government is likely able to see additional dots that the others cannot (normally in the intelligence and law enforcement fields). Essentially, a fragmented cyber defense prevents any one entity from creating a complete picture of an attack or threat, which leaves everyone exposed and everyone at risk. The lesson we desperately need to learn from recent history is that integrated and coordinated defenses can be effective. Until we coalesce around a common defense framework in cyberspace, we are stuck with a fragmented system. The common rule of thumb should be *when everyone is defending alone, everyone is losing.*

NOTES

Joe R. Reeder and Cadet Tommy Hall, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack." *The Cyber Defense Review* (2021): 15-39, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2723341/cybersecuritys-pearl-harbor-moment-lessons-learned-from-the-colonial-pipeline-r/.