Filling the Gaps in Cybersecurity Awareness: A Whole of Society Approach

Waking up in a cold house you find the power is off. You look out the window and see no signs of electricity. You reach for your phone to check the time and get a news update, but your phone company's network is unavailable. As daylight breaks you check on your neighbors. Like them. you feel a sense of panic. Maybe today the country's financial infrastructure has been compromised? The sanitation system? There's no way to know the extent of the damage or the time required for recovery. How will society react to these conditions? Will you be safe? You think you remember where you stored your transistor radio. That might be your only link to the information that you need.

The effects of cyber warfare can be devastating and deadly against a victim nation. Particularly a technologically advanced ("dependent") nation like the United States of America. Cyberattacks have the potential to paralyze food production and distribution; policing; transportation; make personal wealth disappear; paralyze the financial system; halt industry; turn the lights out on our power grid; cut-off our means to communicate and paralyze our water supply and our sanitation services. These effects are analogous to those created by a nuclear attack- except without the physical effects and stigma associated with the escalation of conflict to the nuclear level.

U.S. adversaries like Russia and China have been forthcoming about the vulnerability that they see in the infrastructure elements of modern societies. In 2021 an article published by the People's Liberation Army (PLA) of the People's Republic of China (PRC) entitled "Analysis of Strategies for Interactions in Cybersecurity" observed, "From a cost-benefit point of view, attacks on key national critical infrastructure [defined as electrical and water, transportation, communications, air, and nuclear power] and military targets can be most effective, and they are the best choice for coercing the target country through cyberattacks." As early as 2006 a Senior PLA colonel Cao Zhengrong, set forth that "network attacks" could paralyze a nation's economy, sow societal disorder and allow one country to impose its will upon another- and that it could be done in times of peace or during war. PRC President and Chairman of the Chinese Communist Party (CCP), Xi Jinping views cyberspace as an arena of fierce strategic competition. He has stated that a country's ability to master the internet determines its rise or fall and that "those who win the internet win the world."

Ever since the Russian attack on Ukraine Ukrainian civil infrastructure has been under constant cyber-attack, and in some cases kinetic attack. In December of 2023 Russia was able to knock Ukraine's largest telecommunications provider offline for several days. About 24 million users were affected. The PRC is not above acts of sabotage against the digital infrastructure of their adversaries. In February, 2023 boats flying Chinese flags severed submarine internet cables connecting the Matsu Islands from greater Taiwan. The attack on the cables had the expected effect of isolating the islands digitally and severely restricting commerce and banking for about a month.

U.S. adversaries are aware that these kinds of effects are likely to cause widespread fear, panic and lawlessness as people struggle to meet the everyday requirements of food, water and shelter.

Cyberattacks could be used as a primary weapon to destabilize the U.S. compromise its leaders and weaken the resolve of its people. Potentially, our adversaries could exert their will over the U.S. without ever having to fire a shot. Perhaps the 2021 MITRE Corporation report entitled "Beyond Solarwinds: Principles for Securing Software Supply Chains" expresses the key point most succinctly when it states "We live in an asymmetric era in which dominance is won through non-kinetic exploitation of open societies."

Will our nation's cyber defense organizations protect us? What role should the American citizen have in cyber defense? In these pages we seek to promote the notion that a "Whole of Government" approach to cyber-defense is not sufficient. The U.S. citizen does have a role in a vital "Whole of Society" approach to cyber-defense and security.

Your Laptop as the Front Line

Data from Statista and the U.S. Census Bureau suggests that an estimated 74% of the 258 million adults (191 million) living in the U.S. in 2020 owned a desktop or laptop computer. Smartphone usage is estimated at 85% of all Americans by Pew Research. The large number of cyber-connected people in the U.S. creates an enormous attack surface and potential vectors for distributed and coordinated cyber-attacks.

Verizon recently reported that 82% of data breaches involved some element of human-induced vulnerability- or that only 18% of the breaches were accomplished through technical means alone. Amazon and the National Cybersecurity Alliance identified the core issue aggravating the cybersecurity posture of the U.S. as "tens of millions of technologically unsavvy Americans". These Americans will continue to pose cybersecurity risks as they continue to fall for phishing scams; click on malware links and fail to keep their anti-virus capabilities and home computers up to date.

Many Americans have had their computers turn "zombie" where their computers have been unwittingly conscripted as nodes of a botnet. Botnets are networks of infected computers or routers that can be commanded to execute malicious functions as an orchestrated group. Cyber-Threats use botnets as anonymization relays to hide their malicious cyber activities. Botnets have been used to execute large-scale distributed denial of service attacks. A federated attack made possible through botnets was able to exploit a vulnerability against Microsoft Exchange server such that tens of thousands of e-mail servers were penetrated in the context of a single attack.

If nothing is to change, Americans will continue to be points of vulnerability that can be leveraged by our adversaries as attack vectors against our own critical infrastructure. Clearly, more must be done to educate the average citizen on matters of cybersecurity. Before that can happen, a policy of open discussion is required. The population needs to be informed about the well-crafted plans to attack their vital infrastructure. Starting during WWII and continuing throughout the height of the cold war, the U.S. engaged in civil defense drills and participated in multimedia tests of civilian-directed emergency response systems. These efforts have since been abandoned as if the U.S. no longer faces any threats. Newer, modern versions of them would be important features in a society-wide effort towards reducing risk and preventing panic and social upheaval in the event of a large-scale cyberattack on civilian infrastructure.

Human beings are the core enabling vulnerability and common denominator for most cyberattacks. They can be tricked, bought-off, lazy, or simply make an honest mistake that can lead to a costly cyberattack. Compromised employees allow attackers to bypass significant portions of an organizations defensive controls. Humans cannot be “patched”. They must be informed.

Lifetime Movie?

The entertainment industry needs to do its part in raising awareness of cybersecurity and cyber warfare risks. After all, the stories write themselves. Take the case of these three massive data breaches that occurred in 2015-2017. The U.S. Government (USG) Office of Personnel Management (OPM), the Equifax credit monitoring agency, and the Ashley Madison online dating service were attacked. All were attributed to cyberthreats associated with the PRC. What makes these hacks their made for tv flavor is that the OPM hack provided the PRC a list of federal government employees. The Equifax and Ashley Madison hacks allowed the PRC to identify government employees that are having financial problems and/or marital problems, respectively. Either is a potential vector for recruitment for espionage purposes or blackmail.

Industry, academia and Government at all levels are fighting daily against cyber intrusions and cyber crime. Their stories should be shared prominently as their front-line efforts are worthy of acclaim and will reinforce the importance of being “cyber-savvy”. A recent report by Crowdstrike indicated that there is a shortage of cyber security talent. Popularizing cyber-relevant games, movies, television shows and graphic novels would likely appeal to a younger demographic and could be particularly effective in educating and in generating interest in an important field and aspect of national security.

Industry, Academia and Government

Government, Industry and Academia should accept the challenge of educating the population on the basics of cybersecurity including risks and best practices. This process could make use of public service announcements and poster campaigns. Academia should emphasize hands on training and internships with government and industry in order to meet the nation’s needs sooner and to make cybersecurity a more inviting career choice.

J.D. Work, a senior fellow with the Atlantic Council’s Cyber Statecraft Initiative points out that in many ways the relationship that the USG and industry has with its domestic hacker community is adversarial. This is in contrast with the approach taken by China and Russia. In these countries the government engages with their hacker community directly and in positive ways. They support competitions and provide education and employment opportunities to the hacker communities. This fosters a perception on behalf of the hackers that they are assets vital to national security and provides a more robust talent pool for the cybersecurity profession. An engaged and sympathetic hacker community would open the door for vulnerability reporting and cybersecurity technology competitions and would provide a pipeline of cybersecurity talent flowing to industry.

Organized cyber-militias within the U.S. could provide enhanced opportunities for fielding systems, monitoring and probing networked assets, practicing cyber techniques, tactics and procedures (TTPs) and executing cyber battle damage assessments among other things. Every citizen could be a cyber sensor and have an active stake in our nation’s cybersecurity.