Introduction

Cyberthreats have become a top-tier challenge to international security. Three trends made it so: the vulnerability of the networks and data of cyberspace; the digital transformation of global society; and a lack of investment by organizations and governments in the people, processes, and technologies required to deter and defend against cyberattacks. Governments, corporations, and organizations have taken steps in improve their cybersecurity posture by building cybersecurity teams, developing response policies and mechanisms, and implementing security technologies – but progress has been insufficient to meet the threat.

The threat environment

Nation-state and non-state attackers steal, destroy, and manipulate data in and through cyberspace. While hostilities have yet to be declared through a cyberattack, adversaries flourish in the "gray space"[i] below the level of outright conflict and appear undeterred in pursuing their goals. Significant recent attacks on U.S. national interests include China's campaign to steal U.S. intellectual property, including the data for the Joint Strike Fighter (F-35);[ii] North Korea's 2015 theft of $81 million from the Bangladesh Central Bank and U.S. Federal Reserve;[iii] China's theft of 21.5 million federal personnel records from the U.S. Office of Personnel Management (OPM);[iv] and Russia's attacks on the Ukrainian electric grid in 2015-2016.[v] These are just a few examples.

Nation-state actors present the greatest threat in cyberspace because they have the resources to put hackers on salary and can work diligently over time to penetrate a target. In recent years they have shifted their focus from data theft and destruction to data manipulation of political and media targets, altering how populations perceive political events and the nature of society at large. The Russian hack of the 2016 U.S. presidential election is the most notable example. On the direction of Russian President Vladimir Putin, Russian military intelligence hacked into the networks of U.S. political organizations and political leaders and exploited vulnerabilities in social media business practices to spread propaganda and foment mistrust within the American population.[vi] The Russian operation hit three parts of the American "center of gravity" during a period of political transition: the American population, the political leadership, and key technology companies. Other states have since taken similar actions; China reportedly penetrated Cambodia's electoral networks in 2018, affording it the potential opportunity for election manipulation.[vii]

Why is the problem so acute? The problem stems in part from global socio-economic trends. Increased urbanization, the proliferation of affordable dual-use technologies, and the interconnected nature of the world economy mean that smaller groups of individuals can have an impact disproportionate to their size. The British sociologist Anthony Giddens terms this phenomenon the "high-consequence risk" nature of modernity. Historic examples include the terrorist attacks of al-Qaeda, the actions of sub-prime lenders and their impact on the mortgage market, and, most recently, the Russian government's cyberspace operation against the U.S. presidential election. Just like al-Qaeda's attack on September 11, 2001, when 19 men slipped past the security establishment and turned airplanes into missiles, a small group of Russian operatives found a seam in American security and conducted a high-risk asymmetric attack.

The Internet grew from zero to 3.8 billion in less than 35 years [viii] and access to data increased without a commensurate or popular understanding of risk, whether from the vulnerabilities of computer code or the impact of social media enclaves on socio-political identity formation.[ix] Networks, data centers, and cloud environments are vulnerable to breach – and society is vulnerable to manipulation.

Deterrence and Defense

As a priority, countries should focus on deterring nation-state cyberattacks. Deterrence is a function of perception and it works by convincing a potential adversary that the costs of conducting an attack will outweigh the benefit. Effective deterrence requires the ability to impose costs on an attacker (i.e., through sanctions or military means); defensive tools to repel an incoming attack, like firewalls; and, in the event that a hacker gets through the perimeter, resiliency capabilities to limit the impact, to include micro-segmentation. Investments in each can help shift the cost-benefit balance to deter attack. This testimony treats each in turn.

For a country focused on deterring, defending against, and withstanding a cyberattack, the first step is to formulate a strategy for the public and private sectors.[x] Put simply, a strategy should identify a country or organization's interests; assess strengths, weaknesses, opportunities, and risks; set goals and objectives; and identify required investments in people, processes, and technology. To implement a cybersecurity strategy, governments need to align their roles and missions also – a process that took years to mature in the United States and which continues to evolve. [xi] Canada has made progress in this regard and the 2018 National Cyber Security Strategy provides a platform on which to build.

In the United States, the private sector developed its cybersecurity capabilities on its own and with help from the U.S. government. A number of high-profile breaches led the financial sector to invest significantly and today it and the information technology sector are the most mature in their capabilities and regulatory approach. Other sectors have invested but are further behind.

Positive global developments between the public and private sector include the rise of information sharing and analysis centers (ISACs) and organizations (ISAOs); the development of the National Institute of Standards and Technology (NIST) cybersecurity framework; the evolution of the regulatory environment, to include Europe's General Data Protection Regulation, Colorado and California's state laws, Canada's Personal Information Protection and Electronic Documents Act;[xii] and New York's Department of Financial Services (DFS) cybersecurity regulation.[xiii] Governments now need to enforce organizational compliance.

"Defend forward"

Two propositions arise from recent history to inform this committee's inquiry. First, adversaries have escalated in cyberspace despite the U.S. government's efforts at deterrence; the United States and other countries must therefore take a more aggressive stance to deter aggression. In 2018 the U.S. government embraced this position – notably through the Defense Department's doctrine to "defend forward" in cyberspace.[xiv]

As adversaries escalated in recent years the United States often chose to indict or sanction them. These response actions, while reasonable, do not seem to have set a precedent or effectively deterred escalation. For example, even after sanctioning Russia for the 2016 presidential election hack, Russia reportedly continued to implant malware on the U.S. electric grid through the end of 2018.[xv] Each new hack indicates that deterrence is not working in the gray space below the level of outright conflict.

So what does it mean to "defend forward" in cyberspace? For years U.S. Cyber Command has worked with the National Security Agency and the intelligence community to monitor adversaries and their infrastructure to prepare to blunt and disrupt incoming cyberattacks. If U.S. Cyber Command has ever conducted a counter-offense operation to blunt an cyberattack, however, it was done outside the public eye. The closest the military appears to have come was in October 2018 when it sent direct messages to Russian operatives warning them that if they conducted an attack, the United States would take action.[xvi] This operation did

not disrupt adversary cyberinfrastructure – but it proactively warned adversaries that they were being watched.

If it has indications and warning of an impending cyberattack, the United States must push back against an adversary if there is any hope of achieving deterrence; a more aggressive policy is therefore the right approach. Other countries may reach similar conclusions as to those of the United States; nation-states have the right to defend themselves against hostility, including hostility conducted through cyberspace. To maintain peace and stability any operation must be conducted within the Law of Armed Conflict and with allied and partner nation support. To this end the United Nations should continue to foster norms of behavior for cyberspace operations to control escalation and manage unintended consequences.[xvii]

Assume Breach

The need for a more forceful deterrence posture is one of the first take-aways from the last decade of cybersecurity policy. The second is the need to "assume breach" and plan for adversaries to penetrate perimeter defenses and gain access to crown jewel applications.

What does this mean? While organizations are aware of some of their most critical applications (i.e., a database), most lack a map of how those applications interact and have yet to secure their data centers and cloud environments internally. The lack of internal security leaves organizations vulnerable to the spread of breaches. Once a hacker has penetrated a network, the average time for an intruder to dwell insider a data center is six months; in that time they can move unencumbered and implant malware for whatever purpose they choose. An organization's crown jewel applications, like its key databases, are readily available for a hacker to steal, destroy, or manipulate.

Consider the Chinese hack of the U.S. Office of Personnel Management. One of the smallest agencies of the U.S. government, OPM serves as the "chief human resources" agency for governmental personnel. In 2015, OPM repelled over 10 million attacks per month. When an intruder inevitably broke past OPM's perimeter defenses, they moved easily throughout the environment. Over a period of months the intruder jumped from server to server until they found the crown jewels: the personally identifiable information for 21.5 million federal employees.[xviii] No rules existed to govern how applications and servers would interact internally. The doors were left wide open.

Building Resilience: Micro-segmentation

Micro-segmentation assumes that at some point you will be breached so it establishes an internal defense to prevent breaches from spreading. At its most basic level, it puts walls around vital applications to segment them away from the rest of the cloud environment, data center, and open Internet. An intruder may be able to claim three servers but not 3,000. Since micro-segmentation works with existing infrastructure, it also mitigates risks in legacy architectures, like unpatched servers or applications.

Today in Canada and across the globe most organizations are investing in perimeter defenses. But securing the outside isn't enough. Micro-segmentation provides a deep foundation for cyberresilience – the last line of defense within an organization's suite of security investments. For critical infrastructure like the financial sector, such cybersecurity improves the health of the nations it serves.

Conclusion

It is not a question of *if* but *when* a breach will occur. Countries need to proactively defend against aggressors to achieve deterrence, but they also need to assume breach and implement defense-in-depth strategies to withstand cyberattacks.

Leadership enables success across all parts of the cybersecurity project. In his seminal essay "The Challenge of Change," the historian Arthur M. Schlesinger said, "Science and technology revolutionize our lives, but memory, myth and tradition frame our response." That is true – and our ability to manage technological change depends ultimately on the success of the leader and his or her ability to tell a story to drive results, manage teams, and make strategic decisions for society.

After a decade of focused effort, today we have a crop of strong cybersecurity leaders across the United States. Technology's momentum and evolution may never end – but good leaders have always helped society adapt and manage change, from the rise of aviation to the dawn of the nuclear age. Cybersecurity is just the latest chapter in our story. Ultimately, leadership is underpinned by sound analysis – and that makes this committee's work all the more important. Thank you, and I welcome your questions.

---

[i] https://www.csis.org/analysis/five-risks-watch-2019
[ii] https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/
[iii] https://news.abs-cbn.com/business/09/07/18/us-charges-north-korean-in-bangladesh-central-bank-sony-hacks
[iv] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
[v] https://www.wired.com/story/russian-hackers-attack-ukraine/
[vi] https://www.dni.gov/files/documents/ICA_2017_01.pdf
[vii] https://www.apnews.com/0b52e20517a74b678cf5eae5d0e177ab
[viii] https://cltc.berkeley.edu/wp-content/uploads/2017/12/asianfutures.pdf
[ix] On this issue, which is not our central point of inquiry, please see *inter alia* Nathaniel Persily, https://www.journalofdemocracy.org/article/can-democracy-survive-the-internet, and Cass Sunstein, *Republic.com 2.0*, https://www.jstor.org/stable/j.ctt7tbsw

[xi] This is harder than it sounds to achieve. In the United States, the principal agencies responsible for cybersecurity are the Department of Homeland Security, the Federal Bureau of Investigation, and the Department of Defense and each has specific missions. The Department of Homeland Security engages the private sector in the United States and in some instances abroad to prepare for, mitigate, and recover from attacks; it is the agency responsible for securing the nation's critical infrastructure writ large, including in cybersecurity. The Federal Bureau of Investigation conducts law enforcement operations at home to stop criminals and nation-states from conducting cyberattacks; it is the only agency with authority to conduct counter-offense operations on U.S.-based networks, an important authority for blunting and blocking a foreign-based attacker that is using a U.S. based server to attack American interests. The Defense Department works to defend military networks, prepares to defend the United States against significant attacks from abroad, and conducts cyberspace operations to terminate a conflict on terms favorable to the United States, as in the case of cyberspace operations against Daesh. Within the military, the principal organization responsible for cyberspace operations, U.S. Cyber Command, is run by a four-star general or flag officer in the chain of command from Secretary of Defense and the President. It was initiated in 2010 and is supported by the Cyber Mission Force of 6,200 servicemembers and achieved full operational capacity in 2018. Working with the FBI, DHS, and the CIA, the Department of Defense works to deter attacks against U.S. national interests. The Central Intelligence Agency also has an operational role to play in analysis and in covert operations if granted under presidential authority. Given their unique authorities, all of these agencies work in close planning and operational partnership through the National Security Council and other coordination mechanisms.
[xii] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/
[xiii] https://www.dfs.ny.gov/about/cybersecurity.htm
[xiv]https://cdn.defenseone.com/b/defenseone/interstitial.html?v=8.24.1&rf=https%3A%2F%2Fwww.defenseone.com%2Fideas%2F2018%2F11%2Fwhat-happens-when-us-starts-defend-forward-cyberspace%2F152580%2F
[xv] https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html
[xvi] https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html
[xvii] https://www.un.org/disarmament/topics/informationsecurity/
[xviii] https://www.opm.gov/cybersecurity/cybersecurity-incidents/