Global Cybersecurity Day

BOSTON GLOBAL FORUM
IDEAS THAT MATTER.

MICHAEL DUKAKIS
INSTITUTE FOR LEADERSHIP AND INNOVATION

GLOBAL CYBERSECURITY DAY

CYBER-DEFENSE STRATEGY FOR A NATION

DECEMBER 12, 2107

AIWS
AI WORLD SOCIETY

BOSTON GLOBAL FORUM
IDEAS THAT MATTER.

MICHAEL DUKAKIS
INSTITUTE FOR LEADERSHIP AND INNOVATION

Principles for a Cyber Defense Strategy

Derek S. Reveron, Jacquelyn Schneider, Michael Miner, John Savage, Allan Cytryn, and Tuan Anh Nguyen

December 12, 2017

Threat Landscape

The past two years were a watershed for cyber-attacks. From the Russian-led hacking campaigns in the European and American elections, to the spread of ransomware WannaCry and Petya, to the massive data breaches against credit agency Equifax—never before have cyber-attacks had such a significant effect on national security, economies and cultures. Although attacks in developed countries often occupy the headlines, developing countries are also suffering attacks.

In addition to the political and economic implications of cyber-attacks, major infrastructures — electric grids, dams, wastewater, and critical manufacturing — are vulnerable to physical damage from cyber-attack. The U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team says it has never seen so many successful exploitation attempts on the control system layer of industrial systems. Hackers are increasingly infiltrating the networks of major industrial operations all the way down to the sensors and systems that manage our digitized worlds.

And the actors that conduct these attacks are just as prolific and varied as their targets:

- Transnational organized criminal groups harness the power of the internet to steal identities and conduct financial crimes. They have also been tied to nationalist and state hacker groups.
- Terrorist organizations use cyberspace to recruit fighters and promote physical acts of terror. They are increasingly prolific criminals as well, using financial attacks to buttress their funding.
- Nation states employ cyber tools for espionage to lay the groundwork for significant military operations in cyberspace and launch campaigns to steal intellectual property. North Korea—a major conventional adversary—has used cyberspace operations to steal money from banks, to threaten a private film company, and to disrupt South Korean news organizations.

The pace of cyber-attacks and the increasingly large-scale effects created by them suggest that these cyber actors are getting stronger and bolder and that the entry barriers to perpetrate cyber-attacks continue to lower. Even non-technical adversaries can hire "hacking as a service".

If the trends continue, we can expect significant disruptions to critical infrastructure, severe financial impacts, and potential loss of life. With the proliferation of smart technology and the Internet of Things, the attack surface for cyber operations only expands. At risk from these cyber threats are not just individuals or military units, but the increasingly digitized critical infrastructure that undergird modern states' economies and societies. A recent estimate from the private insurer Lloyd's of London estimates a major cyber-attack could cost over $50 billion.

Perhaps because of the diverse nature of threats and the constant barrage of cyber-attacks, governments have struggled to create the strategies and tools needed to successfully deter and defend against cyber operations. Governments have been taking steps either bilaterally like the 2015 agreement between the PRC and US limiting intellectual property theft or multilaterally through the UN, G20, and G7 that produced the 2001 Budapest Convention on Cyber Crime and the UN Group of Governmental Experts to study information security.

Overall, international law and norms are developing slowly, but have proven to be insufficient to safeguard these necessities that citizens universally require. Developed countries are better positioned than developing countries. Cyber-insecurity cuts across many dimensions and simultaneously crosses from technology into political, economic, and social realms. More than ever, citizens, regardless of nationality, are exposed to risks created by cyber *insecurity*. Both public opinion polling and global intelligence agencies' assessments place cyber security as a leading national security challenge and a pressing concern for citizens and policymakers alike.

Role of National Security Strategy

Cyber infrastructure is at the heart of essentially every aspect of modern life: including telecommunications, financial systems, energy, transportation, defense and other critical sectors. The more open a society, the wider the attack surface with vulnerabilities that require defense. Information sharing centers and organizations have proven an effective means to bring stakeholders together, but national security challenges remain in cyberspace.

No longer just a nightmare scenario, a December 2015 attack against a Ukrainian power plant made clear that code can be weaponized. The attack resulted in 225,000 people being without electricity for a period of time. The Ukraine experience demonstrates cyber-attack is a practical instrument that can wreak havoc on civilian populations. Governments should focus not only on preventing such attacks, but also preparing contingency plans and developing resilient societies. Though currently a low probability of occurrence in peace-time, the future is uncertain. Such high-impact events will likely emerge during war-time and perhaps even before. Frighteningly, such attacks might be the surprise attack that launches a war.

As countries grapple with the challenges of cyber defense, they are guided by several interests. First, governments must work to prevent, deter and reduce the threat of a cyber-attack on critical infrastructure since the impact on its society and civilians would be significant. Second, given the wired nature of the global economic system, governments must ensure stability and resilience of major systems that know no borders and extend around the globe. Finally, governments must protect their citizens from external aggression, which can be preceded by a cyber-attack against civilian infrastructure from state or non-state actors.

How can governments build national cyber strategies that accomplish these objectives? Structural goals can support a viable cyber defense strategy. First and foremost, governments should streamline cyber operations by reducing bureaucratic complexities and duplicative responsibilities to maximize time and efficiency. There are many good examples in developed countries that can be emulated.

Among these are: overcoming the inherent insecurity in legacy systems, updating archaic and territorial bureaucratic mechanisms in order to improve information sharing, and aligning cyber capabilities with emerging threats.

Additionally, it is essential to induce public support for a cohesive national approach to cybersecurity. Most network vulnerabilities are exploited as a result of human error or negligence. Although cutting-edge hardware, smart programming (and grids), and artificial intelligence could mitigate vulnerability gaps in the future, they will never close them all. Strengthening digital literacy and education across national populations as a foundational element of national cyber defense can enhance whole-of-government efforts in combatting cyber-attacks from the individual to the systemic level.

Lastly, collaboration with the private sector is not only a preferable course of action, but a necessary one. Developing policies to harness the talent and cooperation of the private sector will be a decisive factor for a cyber defense aligned with the interests and values of the society they are entrusted to defend.

Principles for a Cyber Defense Strategy

By creating standards and promoting information sharing, governments are assisting industry to improve cybersecurity. Given the scope of critical infrastructure, there is no way that any government can create the capabilities or institutions to defend against all attacks. Additionally, each country has its own laws, cultures, and expectations of government that guide strategic development. Nevertheless, there are basic principles that all governments can follow:

Characterize threshold for action. What do we care about? If states understand when actors view cyber-attacks as national security incidents, then they can create more tailored deterrence strategies. At the same time, understanding adversaries' thresholds for action allow states to combat threats with counter-cyber operations that stay under the threshold for escalation.

Resolve hack back authority. Governments attempt to control subversive cyber behavior within their borders with prohibitions against hacking. But there are strong incentives (both technical and economic) for companies to pursue some level of hack-back against cyber attacks. To avoid escalation and misinterpretation, governments must retain the monopoly on legitimate use of force – both kinetic and cyber - preventing companies from conducting unilateral actions. But to ensure that all of a country's resources are engaged to maximum effect without risk of unintended consequences, the respective roles of government and industry need to be clear and aligned. Israel, for example, has clearly delineated that Cyber-Defense is in in the civil sector and led at a senior governmental level, while cyber-offense is left to the defense organizations.

Connect national and local governance. Local responders are generally the first (and quite often the only) government aid to remediate the effects of critical infrastructure attacks. This requires strong connections between national entities and local governments. Governments should work together to identify and remove barriers for information sharing in order to ensure that national and local responders have full access to the problems that they are defending against and responding to.

Collaborate across borders. International collaboration has proven to be effective in many realms, including regional and national security. Governments should lead efforts based on these many successful precedents should be undertaken to enable nations to collectively work to enhance their cyber security.

Facilitate cooperation across critical sectors. The US government has successfully sponsored information sharing centers and organizations within sectors, such as finance and electricity distribution. These models should be extended to address the complex interdependencies among sectors. Government and industry should continue to work together to determine how best to promote and enable working groups of executives across industry sectors, advisory boards, and routine gatherings between government officials and the private sector to address cyber vulnerabilities and dependencies.

Engage the civilian information technology sector. Given that cyberspace is a civilian space, it is important to engage vendors of cyberspace technology in the discussion of norms for responsible state behavior. Corporations such as Microsoft are promoting norms. States should take these nascent efforts seriously. More broadly, government is encouraged to bring technology experts to the table when formulating cyber defense. Government should also reflect on how to better fund cyber defense research and incubate software technologies that enable defense.

Empower digital literacy and education. The most frequent cyber threats occur at the day-to-day individual level. While larger systemic threats are less frequent, though they hold the potential for greater impact. Governments can harness education to mitigate individual threats and simultaneously harden attack vectors toward greater systemic threats.

Practice comprehensive resilience. A long-term cyber defense strategy requires ongoing short-term resilience planning. Efficient standard operating procedures, redundant systems, and competence building exercises can inject trust in the safety of our systems and enhance the public-private sector partnership. A resilient society can also better deter or respond to cyber-attacks. Governments can lead by encouraging resilience training in the information technology and related sectors.

Build partnerships among developed and developing countries. Developed countries are pursuing important standards and generating norms to improve information security. Developing countries, however, often lack the resources to do so. Nations should extend traditional alliances and partnerships designed to promote international peace and security to ones that promote information security.

Next Steps

The most concrete step a state can take for cyber defense is to articulate a comprehensive cyber defense strategy. This must recognize the unique nature of the cyber realm, where there are no natural barriers – borders, distance, or geography - to attack. Plagued with the constant pace of assaults, states have spent too much time responding to the near-term threats without crafting long-term strategies to change the threat landscape.

Cyber defense strategies that identify vital country assets and policy short-falls and that prioritize resources are vital to successful defense. These strategies must extend into the promotion of the cyber-IQ of the nation's population, from personal awareness of safety through social and corporate responsibility. In turn, a well-crafted cyber defense strategy will lead to the development of appropriate institutions, authorities, and capabilities for the entire nation. This also requires sharing best practices for designing and maintaining computer systems. In turn, governments must invest the time and resources to develop effective regulation for critical data and sectors.

Internationally, cyber defense must be tackled beyond the state level. There are many important efforts by OECD, OSCE, ENISA, NATO, and SCO. Additionally, NGOs such as the Boston Global Forum, East-West Institute, the Bildt Commission, and the Global Commission on Cyberspace Stability should continue to promote the development, identification, sharing and adoption of best practices in the cybersecurity arena with particular focus on developing countries. Developing countries should make investments to secure their infrastructure; this is essential to security and preventing a widening gap in the capabilities of nations. These investments are essential to reducing costs resulting from cybercrime and espionage and to increasing the confidence and trust of businesses to operate in developing countries.

Acknowledgments

The authors would like to thank Michael Dukakis, Thomas Patterson, and all other members of the Boston Global Forum for their support and coordination of this endeavor. These are the views of the authors and do not reflect official policy.