US Policy on the Use of Force in Cyberspace

The United States’ ability to defend and protect itself in cyberspace has evolved at an incredible pace. This evolution has been accomplished largely due to various frameworks such as the US National Cybersecurity Strategy (NCS), Joint Publication 3-12 and Presidential Policy Directive 21. The US government has made several moves over the last few years to secure its critical infrastructure against cyberthreats that could disrupt or destroy lives. The goal of this strategy is to promote international cooperation against disruptive cyberoperations in a digital ecosystem built on certainty, transparency and the law. An analysis of the US policy on the use of force in cyberspace reveals numerous challenges faced by policymakers and IT professionals, such as the legality of conducting offensive and defensive cyberoperations under current international law.

The US Cyberdeterrence Policy

The United States established the NCS during the Trump administration, and US Cyber Command has used a policy of forward presence, such as “persistent engagement,” “defending forward” and “hunting forward,” to confront adversaries in cyberspace, disrupt their operations and, as a result, cause them to divert resources to identify vulnerabilities in their own systems. The underlying principle of this policy is that if the United States causes its enemies to spend more time and money on their own systems, they will have fewer resources to devote to targeting US systems. In addition, one of the priorities of the NCS is to create an international cyberdeterrence initiative that relies on collaborative intelligence to counter and impose consequences on malign cyberinfluence and cyberinformation operations. The US Department of State will play a major role in building this international initiative to promote acceptance of and adherence to the US-developed framework of responsible state behavior in cyberspace.

Former US Secretary of State Mike Pompeo approved the creation of the US Bureau of Cyberspace Security and Emerging Technologies (CSET) to lead diplomatic efforts on a wide range of international cybersecurity and emerging technology issues that affect US foreign policy and national security.

Roncs Etame-Ese
Is a graduate student at Marymount University (Arlington, Virginia, USA) and an NSF CyberCorps Scholarship for Service student. He has worked as a cybersecurity analyst for a technical consulting firm for approximately three years.

Daniel Odei
Is a graduate student in the cybersecurity program at Marymount University. He is also a data center technician LV4 (IT support III) at Amazon Web Services (AWS) and has an AWS Certified Developer Associate certificate.

Sean Manning
Is a graduate student in the cybersecurity program at Marymount University.

Eric Mavakala
Is a graduate student in the cybersecurity program at Marymount University. He has worked in IT support and security Chanssee, complying with EU General Data Protection Regulation (GDPR) and working with personally identifiable information.

Andrew Hall, Ph.D.
Is an associate professor of cybersecurity and data science at Marymount University. Previously, he was on the faculty at the United States Military Academy at West Point and was the director of the US Army Cyber Institute, where he directed and oversaw research, leadership development and partnership efforts across the cyber domain.
including securing cyberspace and critical technologies, reducing the likelihood of cyberconflict, and prevailing in strategic cybercompetition. With the establishment of CSET, the US State Department can take the lead in ensuring arms control in cyberspace, establishing frameworks for responsibility and restraint and, most important, incorporating elements of deterrence into cybersecurity diplomacy. In addition, as the NCS states, through an alliance with like-minded nations, the objective is to coordinate and support allies’ responses to significant malicious cyberincidents through intelligence sharing, the buttressing of attribution claims, public statements of support for responsive actions taken and the joint imposition of sanctions against malign actors. For deterrence to be successful, cooperation among like-minded states must be coordinated through a joint task force, which will enable the cyberforces of any partner state to contribute to defensive measures implemented by another partner state.

The Conduct of Offensive Cyberoperations

When conducting offensive cyberoperations, combatants must adhere to the regulations set forth by Joint Publication 3-12. This document defines offensive cyberoperations as planned actions executed by an organized group with a defined purpose in and through hardware and software used to create, process, store, retrieve and disseminate information in different types of interconnected networks that create a large global network built and used by a wide variety of people. It is imperative that as warfare transitions from the traditional battlefield to a digital one, cyberwarriors have defined rules of engagement under which to operate. In response to the downing of the MQ-4 Triton, a US$240 million military drone, US Cyber Command conducted an offensive cyberoperation that targeted a database used by an “Iranian spy group ... to track and target military and civilian ships passing through the economically important strait of Hormuz.” It is important to note that before the attack in June 2019, former US President Trump reverted to a cyberresponse as opposed to a kinetic response once he learned that multiple Iranians would die as a result of the latter. Although offensive cyberoperations are not intended to cause loss of life, they may lead to collateral damage, causing cyberoperators to be targeted both digitally and physically.

Response to a Cyberattack on the United States

What would a cyberattack on the United States look like? To answer this question, the infrastructure services and functions likely to be targeted by cyberthreats need to be defined and examined. Then it must be determined whether the United States is genuinely prepared for such an attack.

“IT IS IMPERATIVE THAT AS WARFARE TRANSITIONS FROM THE TRADITIONAL BATTLEFIELD TO A DIGITAL ONE, CYBERWARRIORS HAVE DEFINED RULES OF ENGAGEMENT UNDER WHICH TO OPERATE.”

Cybersecurity and Infrastructure Security Agency

In the event of a cyberattack on critical US infrastructure, the primary agency leading the response would be the US Cybersecurity and Infrastructure Security Agency (CISA). CISA is tasked with protecting 16 critical infrastructure sectors in collaboration with other sector-specific agencies such as the US departments of Agriculture, Energy, Defense and Treasury. The assets, systems and networks of these 16 sectors, whether physical or virtual, are considered so vital
to the United States that their incapacitation or destruction would have a debilitating effect on the nation’s security, economy, public health and safety. The 16 sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; IT; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.\(^8\)

For example, the election infrastructure, which falls under the government facilities sector, includes a wide range of physical and electronic assets such as storage facilities, polling places and centralized vote tabulation locations, in addition to information and communications technology (ICT) such as voter registration databases, voting machines and other systems required to manage the election process and report and display results on behalf of state and local governments.\(^9\) One of the most important tasks in defending US national security is preventing meddling in the democratic process and, although federal elections receive more attention in this regard, safeguarding state and local elections is just as important.

**Presidential Policy Directive 21**

The Obama administration in the US issued Presidential Policy Directive 21: Critical Infrastructure Security and Resilience on 12 February 2013. The goal of this directive was to establish a national policy on critical infrastructure security and resilience; refine the critical infrastructure–related functions, roles and responsibilities across the federal government; and enhance overall coordination and collaboration.\(^10\) To accomplish this, the federal government partnered with state, local, tribal and territorial entities, and public- and private-sector partners. This partnership sought to enhance existing critical infrastructure by reducing vulnerabilities, minimizing consequences, identifying and disrupting threats, and hastening response and recovery efforts.\(^11\) Because a majority of critical infrastructure is owned by the private sector, establishing this public-private partnership was essential to securing the computer networks that control Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS).

The US Secretary of Homeland Security is responsible for providing strategic guidance, promoting a unified national effort and coordinating the overall goal of promoting the security and resilience of the nation’s critical infrastructure. The secretary’s specific roles and responsibilities include several important functions, such as:

- Identifying and prioritizing critical infrastructure, considering both physical and cybersecurity threats, vulnerabilities and consequences, in coordination with sector-specific agencies and other federal departments and agencies.
- Maintaining national critical infrastructure centers to provide situational awareness, which includes integrated, actionable information about emerging trends, imminent threats and the status of incidents that may impact critical infrastructure.
- Conducting comprehensive assessments of the vulnerabilities of the nation’s critical infrastructure in coordination with sector-specific agencies and in collaboration with state, local, tribal and territorial entities and critical infrastructure owners and operators.
- Reporting annually on the status of national critical infrastructure efforts, as required by statute.\(^12\)

**The Impact of Collateral Damage**

Once US critical infrastructure has been identified, the question becomes what collateral damage might be imposed on it because of a cyberattack targeting another nation. An example is the Russian military intelligence-backed NotPetya attack on Ukraine. Although it was originally meant to target only the Ukrainian government and industry, the attack spread throughout global enterprises.

---

\(^8\) ONE OF THE MOST IMPORTANT TASKS IN DEFENDING US NATIONAL SECURITY IS PREVENTING MEDDLING IN THE DEMOCRATIC PROCESS
operating inside and outside Ukraine, following their infrastructure back to corporate headquarters in Denmark, England, the United States and elsewhere. The problem with advanced malware of this nature is that once it is on the Internet, it can spread like wildfire, meaning that anyone with the technical capability to reverse-engineer the code can propagate the malware for their own malicious purposes. Although NotPetya was designed to look like a ransomware attack, it wiped data off any device connected to the infected network. The method of infiltration was a QuickBooks program called M.E.Doc, which was used throughout the government and private sector in Ukraine. Russian attackers hacked into the distributor and planted an attack package that exploited a known vulnerability in Microsoft server software, combined with a password-hacking tool and instructions to spread to any connected device on the network, wiping them of all software. If there is any lesson to be learned from NotPetya, it is that the most important aspects of security from an organizational standpoint are a continuous vulnerability management program, malware defenses, and incident response and management.

Consider a hypothetical scenario: During the COVID-19 pandemic, courts have continued to operate via Zoom. Some malicious actors discover a known but unpublicized vulnerability in the Zoom videoconferencing program, and they decide to exploit it by adding a NotPetya-like capability to the next Zoom update. A court in Miami, Florida, USA, updates the program, and NotPetya infects the network. Appearing in court via Zoom that day are a power company employee, an emergency room nurse and a nuclear waste disposal expert. The malware infects these three people’s devices, including their cell phones, which they take to work the next day. Suddenly a hospital is shut down during a global pandemic, and a nuclear waste disposal facility is unable to operate its machinery. The power company is completely crippled, leading to blackouts all over Miami. The court’s devices are wiped as well, shutting down not only the courthouse, but also other government facilities whose employees have been to the courthouse. Within 24 hours, all these major institutions are affected.

In another hypothetical example, consider the power grid under the energy sector. Lloyd’s of London, an insurance underwriter, creates a plausible scenario of an attack on the Eastern Interconnection, one of two major electrical grids in the United States that services approximately half the country. The hypothetical attack targets power generators and causes a blackout affecting 15 states and the District of Columbia, leaving 93 million people without power. This would be a devastating attack on critical infrastructure, as all 16 sectors rely on electricity. The security of the grid’s control systems is very poor because those systems were built on general computing systems from a generation ago. They were not designed with security in mind and cannot be updated. This problem has not been corrected with the latest generation of smart-grid technologies; the US Government Accountability Office (GAO) found that these devices lack the ability to authenticate administrators and cannot maintain the activity logs necessary for forensic analysis, among other deficiencies. In the end, simply asking the power companies to invest in these technologies will not be enough incentive for them to do so. They must be convinced that implementing good cyberhygiene will be a good investment for them.

Addressing the International Cybersecurity Problem

The problem of cybersecurity can be solved with a financial investment or incentives for enterprises to invest in the necessary technologies. As the 2015 incident in Ukraine illustrates, the wake-up call has been received. Because critical infrastructure is threatened in many countries, an international treaty to protect critical infrastructure from cyberattacks, such as the Budapest Convention on Cybercrime, should be enacted to address these global threats.

The United States must strive to establish an international set of norms that defines peacetime behavior and contingency expectations for state
behavior in cyberspace, communicate clear foreign policy related to cyberspace, pursue cyberdefense capacity-building measures with developing nations and establish an international understanding of the nature of critical infrastructure. Building an internationally accepted framework of behavioral norms and confidence-building measures in cyberspace is foremost among these efforts. This framework will provide a new level of strategic stability in cyberspace and afford the US government freedom of action in cyberspace consistent with the nation’s principles and interests. The hallmark of the US effort is prevention in the preconflict phase, where the government can capitalize on the momentum already underway across various sectors and institutions.

Responding to and Recovering From a Cyberattack

Cyberattacks are becoming more frequent and highly sophisticated, and they can have devastating consequences. Determined hackers have proved that with enough commitment, planning and persistence, they will inevitably find a way to access the information they want. The United States needs to enhance its cyberincident response plan and update existing disaster recovery plans to quickly mitigate the effects of a cyberattack, prevent a data breach and recover from such an attack. For example, IT environments should include intrusion detection systems to alert administrators; incident response teams to react to threats; mitigation techniques, such as disabling a network during an incident; reporting to management through official channels; preparing for recovery by rebuilding systems from data backups; applying remediation after performing a root cause analysis; and examining incidents and responses to identify lessons learned.19 There are a variety of security information and event management (SIEM) tools, such as ArcSight and Splunk, that provide real-time analysis of events occurring on systems throughout an enterprise.

Recovering from a cybersecurity incident can be a daunting undertaking, especially if the information lost is critical to the running of an enterprise, such as at a manufacturing facility. However, governments can limit the damage to their data and reputations by developing a solid recovery plan. A good recovery system requires backups: If a computer breaks, an employee makes a mistake or a malicious program infects the system, backups will be able to restore the data. Without backups, information must be manually recreated from paper records and employees’ memories. In the end, it is important for countries to collaborate and cooperate to effectively protect themselves from malicious servers and the tools used by nation-states’ intelligence services.

"IT IS IMPORTANT FOR COUNTRIES TO COLLABORATE AND COOPERATE TO EFFECTIVELY PROTECT THEMSELVES FROM MALICIOUS SERVERS AND THE TOOLS USED BY NATION-STATES’ INTELLIGENCE SERVICES."

Conclusion

The US government has launched a series of initiatives, directives and policies to ensure a safer cyberspace. These efforts are based on the four pillars of the NCS:

1. Protecting US citizens, the homeland and the US way of life
2. Promoting US prosperity
3. Preserving peace through strength
4. Advancing US influence

As a major global power, the United States has established itself as a giant capable of deterring criminal actors, hostile organizations and any country seeking to harm the nation. Although the United States has been proactive in taking precautionary actions, problems still arise because most critical infrastructure is extremely vulnerable to cyberexploitation. Globalization facilitates a domino effect when a cyber ally or a US enterprise located abroad is affected by malware. Therefore,
international collaboration is needed to create a safer cyberenvironment and to protect US economic, political and critical infrastructure interests.

Endnotes


8 Ibid.


11 Ibid.

12 Ibid.

13 Clarke, R.; Fifth Domain, Penguin Books, USA, 2020

14 Ibid.


17 Ibid.
