FOREIGN AFFAIRS

SEPTEMBER/OCTOBER 2010

Defending a New Domain

The Pentagon's Cyberstrategy

William J. Lynn III

Volume 89 • Number 5

Defending a New Domain

The Pentagon's Cyberstrategy

William J. Lynn III

In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.

This previously classified incident was the most significant breach of U.S. military computers ever, and it served as an important wake-up call. The Pentagon's operation to counter the attack, known as Operation Buckshot Yankee, marked a turning point in U.S. cyber-defense strategy.

Over the past ten years, the frequency and sophistication of intrusions into U.S. military networks have increased exponentially. Every day, U.S. military and civilian networks are probed thousands of times and scanned millions of times. And the 2008 intrusion that led to Operation Buckshot Yankee was not the only successful penetration. Adversaries have acquired thousands of files from U.S. networks and

---

William J. Lynn III is U.S. Deputy Secretary of Defense.

from the networks of U.S. allies and industry partners, including weapons blueprints, operational plans, and surveillance data.

As the scale of cyberwarfare's threat to U.S. national security and the U.S. economy has come into view, the Pentagon has built layered and robust defenses around military networks and inaugurated the new U.S. Cyber Command to integrate cyberdefense operations across the military. The Pentagon is now working with the Department of Homeland Security to protect government networks and critical infrastructure and with the United States' closest allies to expand these defenses internationally. An enormous amount of foundational work remains, but the U.S. government has begun putting in place various initiatives to defend the United States in the digital age.

THE THREAT ENVIRONMENT

Information technology enables almost everything the U.S. military does: logistical support and global command and control of forces, real-time provision of intelligence, and remote operations. Every one of these functions depends heavily on the military's global communications backbone, which consists of 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries. More than 90,000 people work full time to maintain it. In less than a generation, information technology in the military has evolved from an administrative tool for enhancing office productivity into a national strategic asset in its own right. The U.S. government's digital infrastructure now gives the United States critical advantages over any adversary, but its reliance on computer networks also potentially enables adversaries to gain valuable intelligence about U.S. capabilities and operations, to impede the United States' conventional military forces, and to disrupt the U.S. economy. In developing a strategy to counter these dangers, the Pentagon is focusing on a few central attributes of the cyberthreat.

First, cyberwarfare is asymmetric. The low cost of computing devices means that U.S. adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to U.S. military capabilities. A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States'

global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target. Knowing this, many militaries are developing offensive capabilities in cyberspace, and more than 100 foreign intelligence organizations are trying to break into U.S. networks. Some governments already have the capacity to disrupt elements of the U.S. information infrastructure.

In cyberspace, the offense has the upper hand. The Internet was designed to be collaborative and rapidly expandable and to have low barriers to technological innovation; security and identity management were lower priorities. For these structural reasons, the U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses. Adept programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions. In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun. Cyberwarfare is like maneuver warfare, in that speed and agility matter most. To stay ahead of its pursuers, the United States must constantly adjust and improve its defenses.

Cold War deterrence models do not apply to cyberspace, where it is so difficult to identify an attack's perpetrator.

It must also recognize that traditional Cold War deterrence models of assured retaliation do not apply to cyberspace, where it is difficult and time consuming to identify an attack's perpetrator. Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all. And even when the attacker is identified, if it is a nonstate actor, such as a terrorist group, it may have no assets against which the United States can retaliate. Furthermore, what constitutes an attack is not always clear. In fact, many of today's intrusions are closer to espionage than to acts of war. The deterrence equation is further muddled by the fact that cyberattacks often originate from co-opted servers in neutral countries and that responses to them could have unintended consequences.

Given these circumstances, deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through

retaliation. The challenge is to make the defenses effective enough to deny an adversary the benefit of an attack despite the strength of offensive tools in cyberspace. (Traditional arms control regimes would likely fail to deter cyberattacks because of the challenges of attribution, which make verification of compliance almost impossible. If there are to be international norms of behavior in cyberspace, they may have to follow a different model, such as that of public health or law enforcement.)

Cyberthreats to U.S. national security are not limited to military targets. Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks that control critical civilian infrastructure. Computer-induced failures of U.S. power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption. Such infrastructure is also essential to the military, both abroad and at home: coordinating the deployment and resupply of U.S. troops and equipping troops with goods from private vendors necessarily requires using unclassified networks that are linked to the open Internet. Protecting those networks and the networks that undergird critical U.S. infrastructure must be part of Washington's national security and homeland defense missions.

The cyberthreat posed to intellectual property may prove to be the most significant one facing Washington.

Modern information technology also increases the risk of industrial espionage and the theft of commercial information. Earlier this year, Google disclosed that it had lost intellectual property as a result of a sophisticated operation perpetrated against its corporate infrastructure, an operation that also targeted dozens of other companies. Although the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term. Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies. As military strength ultimately depends on economic vitality, sustained intellectual property losses could erode both the United States' military effectiveness and its competitiveness in the global economy.

Computer networks themselves are not the only vulnerability. Software and hardware are at risk of being tampered with even before they are linked together in an operational system. Rogue code, including so-called logic bombs, which cause sudden malfunctions, can be inserted into software as it is being developed. As for hardware, remotely operated "kill switches" and hidden "backdoors" can be written into the computer chips used by the military, allowing outside actors to manipulate the systems from afar. The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat. Tampering is almost impossible to detect and even harder to eradicate. Already, counterfeit hardware has been detected in systems that the Defense Department has procured. The Pentagon's Trusted Foundries Progam, which certifies parts produced by microelectronics manufacturers, is a good start, but it is not a comprehensive solution to the risks to the department's technological base. Microsoft and other computer technology companies have developed sophisticated risk-mitigation strategies to detect malicious code and deter its insertion into their global supply chains; the U.S. government needs to undertake a similar effort for critical civilian and military applications.

The United States rarely predicts accurately when and where military conflicts will occur. Predicting cyberattacks is also proving difficult, especially since both state and nonstate actors pose threats. More important, given that information technology is evolving rapidly, policymakers are left with little historical precedent to inform their expectations. Thus, the U.S. government must be modest about its ability to know where and how this threat might mature; what it needs is a strategy that provides operational flexibility and capabilities that offer maximum adaptability.

NEW STRATEGY

As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such, the military must be able to defend and operate within it. To facilitate operations in cyberspace, the Defense

Department needs an appropriate organizational structure. For the past several years, the military's cyberdefense effort was run by a loose confederation of joint task forces dispersed both geographically and institutionally. In June 2009, recognizing that the scale of the effort to protect cyberspace had outgrown the military's existing structures, Defense Secretary Robert Gates ordered the consolidation of the task forces into a single four-star command, the U.S. Cyber Command, which began operations in May 2010 as part of the U.S. Strategic Command. Cyber Command is slated to become fully operational by October.

Cyber Command has three missions. First, it leads the day-to-day protection of all defense networks and supports military and counterterrorism missions with operations in cyberspace. Second, it provides a clear and accountable way to marshal cyberwarfare resources from across the military. A single chain of command runs from the U.S. president to the secretary of defense to the commander of Strategic Command to the commander of Cyber Command and on to individual military units around the world. To ensure that considerations of cybersecurity are a regular part of training and equipping soldiers, Cyber Command oversees commands within each branch of the military, including the Army Forces Cyber Command, the U.S. Navy's Tenth Fleet, the 24th Air Force, and the Marine Corps Forces Cyberspace Command. Because military networks are not impervious to attack, a critical part of the training mission is to ensure that all operational forces are able to function in a degraded information environment.

The new U.S. Cyber Command will be fully operational by October.

Cyber Command's third mission is to work with a variety of partners inside and outside the U.S. government. Representatives from the FBI, the Department of Homeland Security, the Justice Department, and the Defense Information Systems Agency work on-site at Cyber Command's Fort Meade headquarters, as do liaison officers from the intelligence community and from allied governments. In partnership with the Department of Homeland Security, Cyber Command also works closely with private industry to share information about threats and to address shared vulnerabilities. Information networks connect a variety of institutions, so the effort to defend the United States will

only succeed if it is coordinated across the government, with allies, and with partners in the commercial sector.

Given the dominance of offense in cyberspace, U.S. defenses need to be dynamic. Milliseconds can make a difference, so the U.S. military must respond to attacks as they happen or even before they arrive. To grapple with this, the Pentagon has deployed a system that includes three overlapping lines of defense. Two are based on commercial best practices—ordinary computer hygiene, which keeps security software and firewalls up to date, and sensors, which detect and map intrusions. The third line of protection leverages government intelligence capabilities to provide highly specialized active defenses. And the government is deploying all these defenses in a way that meets its obligation to protect the civil liberties of U.S. citizens.

The National Security Agency has pioneered systems that, using warnings provided by U.S. intelligence capabilities, automatically deploy defenses to counter intrusions in real time. Part sensor, part sentry, part sharpshooter, these active defense systems represent a fundamental shift in the U.S. approach to network defense. They work by placing scanning technology at the interface of military networks and the open Internet to detect and stop malicious code before it passes into military networks. Active defenses now protect all defense and intelligence networks in the ".mil" domain.

Because some intrusions will inevitably evade detection and not be caught at the boundary, U.S. cyberdefenses must be able to find intruders once they are inside. This requires being able to hunt within the military's own networks—a task that is also part of the Pentagon's active defense capability.

Active defense has been made possible by consolidating the Defense Department's collective cyberdefense capabilities under a single roof and by linking them with the signals intelligence needed to anticipate intrusions and attacks. Establishing this linkage was one of the most important reasons for the creation of Cyber Command.

The speed at which active defense systems must act means that the rules of engagement governing network defense must be set largely in advance. Devising these protocols is not easy. Indeed, the effort to define clear rules of engagement for responding to cyberattacks has been exceedingly difficult, and for good reason. These rules of

engagement will first have to assist in distinguishing between the exploits of a mere hacker, criminal activity (such as fraud or theft), espionage, and an attack on the United States. They will then have to determine what action is necessary, appropriate, proportional, and justified in each particular case based on the laws that govern action in times of war and peace.

The best-laid plans for defending military networks will matter little if civilian infrastructure—which could be directly targeted in a military conflict or held hostage and used as a bargaining chip against the U.S. government—is not secure. The Defense Department depends on the overall information technology infrastructure of the United States. For example, it relies on many outside networks in the ".gov" and ".com" domains, including those run by defense contractors that are not protected as effectively as the military's own network. The Department of Homeland Security has the lead in protecting the ".gov" and ".com" domains, but the Pentagon must leverage its ten years of concerted investment in cyberdefense to support broader efforts to protect critical infrastructure.

Critical infrastructure could be targeted directly in a conflict or be held hostage as a bargaining chip against the U.S. government.

The U.S. government has only just begun to broach the larger question of whether it is necessary and appropriate to use national resources, such as the defenses that now guard military networks, to protect civilian infrastructure. Policymakers need to consider, among other things, applying the National Security Agency's defense capabilities beyond the ".gov" domain, such as to domains that undergird the commercial defense industry. U.S. defense contractors have already been targeted for intrusion, and sensitive weapons systems have been compromised. The Pentagon is therefore working with the Department of Homeland Security and the private sector to look for innovative ways to use the military's cyberdefense capabilities to protect the defense industry.

Given the global nature of the Internet, U.S. allies also play a critical role in cyberdefense. The more signatures of an attack one can see, and the more intrusions one can trace, the better one's defenses will be. In this way, the construct of shared warning—a core Cold War doctrine—applies to cyberspace. Just as the United States' air and space defenses

are linked with those of allies to provide warning of an attack from the sky, so, too, can the United States and its allies cooperatively monitor computer networks for intrusions.

Some of the United States' computer defenses are already linked with those of U.S. allies, especially through existing signals intelligence partnerships, but greater levels of cooperation are needed to stay ahead of the cyberthreat. Stronger agreements to facilitate the sharing of information, technology, and intelligence must be made with a greater number of allies. The report *NATO 2020*, a NATO-commissioned study chaired by former U.S. Secretary of State Madeleine Albright, rightly identified the need for the alliance's new "strategic concept" to further incorporate cyberdefense. The U.S. government must ensure that NATO moves more resources to cyberdefense so the member states can defend networks integral to the alliance's operations.

LEVERAGING DOMINANCE

The United States enjoys unparalleled technological resources, and it can marshal its advantages to create superior military capabilities in cyberspace. The Pentagon has already begun to explore how major companies can help the public sector address the cyberthreat. Through a public-private partnership called the Enduring Security Framework, the chief executive officers and chief technology officers of major information technology and defense companies now meet regularly with top officials from the Department of Homeland Security, the Office of the Director of National Intelligence, and the Department of Defense.

The U.S. government's research and development institutions have also turned their attention to cybersecurity. One of the more important innovations to emerge is the National Cyber Range program, developed by the Defense Advanced Research Projects Agency (DARPA). Although the U.S. military routinely exercises units on target ranges and in a variety of simulations, the Pentagon has had no such capability when it comes to cyberwarfare. This is why DARPA, which helped invent the Internet decades ago, is developing the National Cyber Range—in effect, a model of the Internet—which will allow the military to test its cyberdefense

capabilities before fielding them. Simulations are also relevant to understanding malicious software designed to infiltrate computer systems. The Department of Energy's national laboratories have developed computer farms that function as digital petri dishes, capturing live viruses from the Internet and observing how they spread. These training and diagnostic capabilities can help the United States stay ahead of its adversaries' innovative cyberweapons.

DARPA is pursuing even more fundamental research that may improve the government's ability to attribute attacks and blunt intruders' capabilities, thereby making cyberspace a less offense-dominant environment. The agency is also challenging the scientific community to rethink the basic design of the Pentagon's network architecture so that the military could redesign or retrofit hardware, operating systems, and computer languages with cybersecurity in mind. Complex information technology infrastructure will not change overnight, but over the course of a generation, the United States has a real opportunity to engineer its way out of some of the most problematic vulnerabilities of today's technology.

The government must also strengthen its human capital. The Pentagon has increased the number of its trained cybersecurity professionals and deepened their training. This includes a formal certification program that is graduating three times as many cybersecurity professionals annually as a few years ago. Following industry practices, the Pentagon's network administrators are now trained in "ethical hacking," which involves employing adversarial techniques against the United States' own systems in order to identify weaknesses before they are exploited by an enemy.

Even as the U.S. government strengthens its cadre of cybersecurity professionals, it must recognize that long-term trends in human capital do not bode well. The United States has only 4.5 percent of the world's population, and over the next 20 years, many countries, including China and India, will train more highly proficient computer scientists than will the United States. The United States will lose its advantage in cyberspace if that advantage is predicated on simply amassing trained cybersecurity professionals. The U.S. government, therefore, must confront the cyberdefense challenge as it confronts other military challenges: with a focus not on numbers but

on superior technology and productivity. High-speed sensors, advanced analytics, and automated systems will be needed to buttress the trained cybersecurity professionals in the U.S. military. And such tools will be available only if the U.S. commercial information technology sector remains the world's leader—something that will require continuing investments in science, technology, and education at all levels.

Making use of the private sector's innovative capacity will also require dramatic improvements in the government's procedures for acquiring information technology. On average, it takes the Pentagon 81 months to make a new computer system operational after it is first funded. Taking into the account the growth of computing power suggested by Moore's law, this means that by the time systems are delivered, they are already at least four generations behind the state of the art. By comparison, the iPhone was developed in 24 months. That is less time than it would take the Pentagon to prepare a budget and receive congressional approval for it.

It takes the Pentagon 81 months to make a new computer system operational once it is first funded. The iPhone was developed in just 24 months.

To replicate the dynamism of private industry, the Pentagon is developing a specific acquisition track for information technology. It is based on four principles. First, speed must be a critical priority. The Pentagon's acquisition process must match the technology development cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years. Second, the Pentagon must employ incremental development and testing rather than try to deploy large complex systems in one "big bang." Third, the U.S. military must be willing to sacrifice or defer some customization in order to achieve speedy incremental improvements. Fourth, the Defense Department's information technology needs—which range from modernizing nuclear command-and-control systems to updating word-processing software—demand different levels of oversight. An approach to information technology acquisition that embodies these principles is essential to the U.S. military's effectiveness when it comes to cyberdefense.

ENTERING A NEW ERA

THE DAUNTING challenges of cybersecurity represent the beginning of a new technological age. In this early hour, the United States' greatest strength is its awareness of the transformation. Today's predicament calls to mind an urgent letter written to President Franklin Roosevelt on the eve of another new technological era. Dated August 2, 1939, it read in part, "Certain aspects of the situation which has arisen seem to call for watchfulness and, if necessary, quick action on the part of the Administration. I believe therefore that it is my duty to bring to your attention the following facts and recommendations." The letter was signed, "Yours very truly, Albert Einstein." Einstein's warning that breakthroughs in nuclear fission might make possible an atomic bomb led Roosevelt to launch the Manhattan Project, which helped prepare the United States for the atomic era.

The cyberthreat does not involve the existential implications ushered in by the nuclear age, but there are important similarities. Cyberattacks offer a means for potential adversaries to overcome overwhelming U.S. advantages in conventional military power and to do so in ways that are instantaneous and exceedingly hard to trace. Such attacks may not cause the mass casualties of a nuclear strike, but they could paralyze U.S. society all the same. In the long run, hackers' systematic penetration of U.S. universities and businesses could rob the United States of its intellectual property and competitive edge in the global economy.

These risks are what is driving the Pentagon to forge a new strategy for cybersecurity. The principal elements of that strategy are to develop an organizational construct for training, equipping, and commanding cyberdefense forces; to employ layered protections with a strong core of active defenses; to use military capabilities to support other departments' efforts to secure the networks that run the United States' critical infrastructure; to build collective defenses with U.S. allies; and to invest in the rapid development of additional cyberdefense capabilities. The goal of this strategy is to make cyberspace safe so that its revolutionary innovations can enhance both the United States' national security and its economic security.