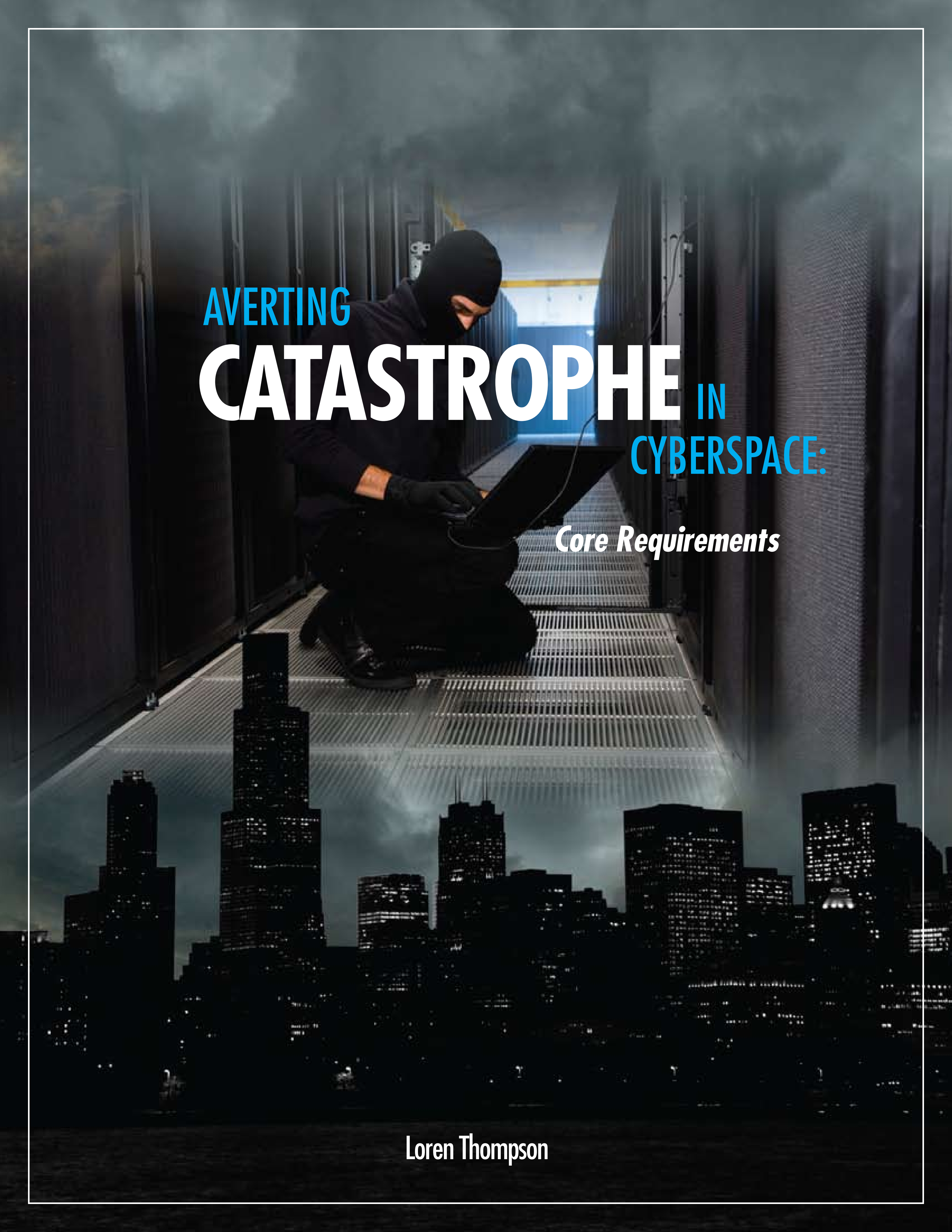

AVERTING CATASTROPHE IN CYBERSPACE:

Core Requirements

Loren Thompson

FINDINGS IN BRIEF

The information revolution has transformed every facet of commerce and culture, including the military enterprise. Unfortunately, it has also empowered extremists, criminals and agents of enemy nations who can use cyberspace to subvert or destroy information resources vital to U.S. security. The federal government has launched a comprehensive cybersecurity initiative to counter such threats. The most advanced, persistent threats are posed by state-sponsored perpetrators, especially those operating in China and Russia.

The federal government has made major strides in developing defenses against cyber espionage and aggression. However, its efforts are impeded by the changing character of threats and the infancy of techniques for addressing them. The absence of agreed standards and metrics for assessing performance sometimes leads federal agencies to select cybersecurity providers who lack the breadth and depth to cope with all potential threats. The government cannot sustain a truly comprehensive cybersecurity posture unless its top providers satisfy five core requirements:

1. *Situational awareness*. Capable providers must be able to precisely monitor the performance of information systems and networks they are protecting, predicting and/or detecting threats based on extensive understanding of adversary behavior. Awareness of dangers must be shared with potential victims in time for them to minimize harm, and providers must then be able to assess the success of remedial actions.

2. *Full-spectrum skills*. A comprehensive cybersecurity posture requires providers with expertise and experience in the full array of relevant skills. That includes all the major disciplines associated with computer-network defense, computer-network attack, and computer-network exploitation. Without an integrated understanding of all the necessary skills, federal providers cannot deploy the full panoply of tools needed to counter advanced threats.

3. *Operational agility*. The pace of activity in cyberspace requires providers that are extremely agile in responding to new threats. Ideally, those providers should be able to apply their situational awareness and full-spectrum skills to anticipate danger before it actually occurs, but at the very least they must have the capacity to detect, analyze, isolate and defeat enemy moves quickly, even when the threat is a "zero-day" attack with no previous history.

4. *Organizational maturity*. Maturity models are used in many fields to assess organizational effectiveness in applying best practices. In the cybersecurity arena, such models can be used to assess both government preparedness and the practices of outside providers. Mature solutions to cyber challenges typically stress values such as affordability, scalability and technical readiness. Companies capable of providing those solutions tend in turn to have mature cultures stressing retention of talent, continuous training, and diverse expertise.

5. *Enterprise commitment*. Cybersecurity is an infant industry with many recent entrants. The commitment of some providers to the business is hard to gauge. However, it is not feasible to fashion comprehensive responses to cybersecurity challenges unless customers and providers alike are committed to the mission. The commitment of providers can be determined by assessing how long they have been in the business, how deeply they have invested in talent, and how extensive their collaborative ties are with other centers of expertise.

This report was written by Dr. Loren Thompson of the Lexington Institute staff as part of the institute's continuing inquiry into the changing requirements of national security.

INTRODUCTION: Averting Catastrophe in Cyberspace

During the closing decades of the last century, global civilization entered a new era driven by the emergence of digital information technologies. The centerpiece of this new age was the Internet, a system that enabled thousands of previously isolated computer networks to be integrated into one seamless web. For the first time in history, people with inexpensive hardware and communications links could gain access to vast amounts of information scattered in millions of locations around the world. They could also share diverse content with other Internet users, collaborate to fashion new forms of expression, and conduct virtually any facet of their daily affairs online. The digital environment in which these complex interactions occur has come to be known as "cyberspace."

Digital technology has spawned a surge of innovation revolutionizing every aspect of commerce and culture, creating new sources of wealth while wiping out old ones. Novel devices such as smart phones and I-Pads are continuously appearing, hosting diverse applications leveraged off the limitless connectivity afforded by the Internet. Even the military enterprise has been transformed as forces previously isolated in the fog of war have been linked together to achieve awareness and agility that would have been impossible only a generation ago. The organizational and cultural barriers that once limited options are rapidly disappearing for military commanders -- just as they are for educators, entrepreneurs and everyone else.

Unfortunately, everyone else in this case includes criminals, fanatics, and the agents of enemy nations. They too have access to the Internet, smart phones, flash drives and other tools of the digital age, and they have proven increasingly adept at using those tools to advance their interests. While few perpetrators of online aggression can match the resources or expertise of the U.S. government, the amorphous nature of cyberspace and the imagination of its most ruthless inhabitants have become a continuous threat to America's information-based economy and society. Foreign governments have discovered they can exploit U.S. dependence on information networks to weaken military forces and undermine markets. Analysts have coined the term "cybersecurity" to refer to the challenge of protecting networks and operating successfully in an environment where essential information resources are under continuous assault.

This report is about the requirements that must be satisfied to provide effective cybersecurity for government networks and vital infrastructure in the information age. It focuses on the most fundamental goals that must be met in countering cyber threats, and the kinds of providers best equipped to meet them. The report begins by describing the nature of cyber threats and the steps taken thus far by the government to combat them, and then sets forth five overarching imperatives for successful defense: awareness, skill, agility, maturity and commitment. Each of these terms has a specific meaning in the cybersecurity realm, and thus implies particular attributes in a successful provider. The report concludes by detailing the devastation that could result from seeking protection in suppliers who lack the qualities necessary to combat a constantly changing challenge.

A Danger Without Borders

There is nothing new about the efforts of criminals and foreign agents to exploit or disrupt the electronic transmission of information. When the telegraph was first introduced in the 19th Century, concern about the security of messages led to elaborate safeguards including use of codes. Interference with radio signals began while Marconi was still testing the new technology, and soon became a widespread practice as broadcasting companies and military forces sought to gain an edge in using the electromagnetic spectrum. The advent of the telephone gave rise to wiretapping as business interests, law-enforcement officials and foreign spies sought to eavesdrop on sensitive conversations. Every new information technology seems to stimulate the development of novel methods for stealing secrets and defeating competitors.

However, several features of the modern information environment make today's cybersecurity challenges different from the dangers of the past. First, digital networking technology has enabled an unprecedented degree of connectedness among information systems. Second, the migration of business and government functions to the Internet has increased their vulnerability to subversion by parties with malicious intent. Third, certain design features of the Internet permit perpetrators of online crime to conceal their identities. Fourth, the paths followed by modern communications conduits no longer conform closely to political boundaries, weakening the ability of governments to regulate online behavior. Fifth, the continuous proliferation of new devices and applications for storing, sharing and manipulating data has made digital technology ubiquitous in modern society in a manner that few earlier technologies could have been. And finally, that same pattern of constant innovation has made it difficult for defenders of networks to keep up with all the tools now available to aggressors.

The fact that virtually every electronic device is now networked (or soon will be) and contains computer code creates unprecedented opportunities for criminals, spies and others to exploit or degrade their operation by penetrating information systems and using their own software programs against them. The danger to society is especially great when the penetrated computers and networks control vital infrastructure such as electrical grids and financial networks. This danger is exacerbated by the fact that much of today's information technology was designed and installed before planners realized how dependent society would become on it, or how vulnerable that would make people to interference by outsiders. Thus, the "borderless" character of the new global economy has become both a blessing and a curse as foreign interests acquire the means of gaining access to the most sensitive sources of national strength.

The threat of information warfare is particularly pronounced for America's military, which now relies on digital networks, sensors and computers for every facet of its operations. In 1995, outsiders sought to break into military computer systems 250,000 times; fifteen years later, the volume of attacks had increased to 250,000 every hour. In addition, many of today's attacks are what cyber specialists call "advanced persistent threats," meaning sophisticated intrusion attempts mounted by agents of foreign governments. Such attacks, when successful, may exploit penetrated networks and computers for weeks or months before being detected, stealing huge amounts of information or infecting equipment with malicious software that can disable operations. To understand how such tactics might upset the balance of global power and undercut U.S. success in future conflicts, it is useful to consider the country currently mounting the most sophisticated cyber threats, China.

The Chinese Cyber Threat

It is often difficult to determine the source of attacks on U.S. networks because the Internet was not designed to facilitate tracking and “anonymization” software is available to further obscure the identities of perpetrators. However, many experts agree that the People’s Republic of China is the biggest source of advanced, persistent threats -- the intrusions that are hardest for U.S. defenders to detect and counter. Because such intrusions require extensive skill and resources to execute, analysts believe those originating in China are carried out either by the People’s Liberation Army or other state-controlled institutions such as universities. China’s state-sponsored cyber aggression differs markedly from that of online criminals and activists, repetitively targeting information systems with critical economic or security functions.

In March, 2012 the U.S.-China Economic and Security Review Commission released a study prepared by analysts at the Northrop Grumman Corporation illuminating the strategy and organizations underpinning Chinese cyberwar efforts. The analysts found that Chinese military leaders view the electromagnetic spectrum as a crucial domain of modern warfare, and are preparing to assure the access of friendly forces to the spectrum in future conflicts while denying access to adversaries. In addition to using traditional “kinetic” methods such as bombing enemy communications nodes in any such campaign, the People’s Liberation Army would also utilize “non-kinetic” methods -- most notably electronic jamming and cyber operations. The study detailed how Chinese forces might employ information warfare in a Taiwan-invasion scenario to hobble U.S. military capabilities in the Pacific while deterring effective responses.

The Chinese military is assigning increased importance to cyber operations in the way it organizes its forces and carries out joint warfighting exercises. Responsibility for computer-network defense and exploitation (espionage) is vested in the same military organization charged with collection of signals intelligence, while responsibility for computer-network attacks is located in the organization charged with overseeing electronic jamming. The latter arrangement is consistent with Chinese doctrinal emphasis on integrating all the elements needed to secure information dominance in wartime. Dozens of subordinate organizations and universities receive funding to develop various facets of the overall cyber posture. For instance, the People’s Liberation Army Information Engineering University in Henan Province employs hundreds of professors and researchers who regularly generate studies on propagating computer viruses, evaluating network-attack characteristics, and detecting malicious software.

Chinese authorities justify such efforts as necessary to defend their own information resources against what they describe as a continuous onslaught by foreigners. However, there is extensive evidence that the Chinese are engaged in a secret campaign to compromise U.S. networks. Chinese operatives were probably behind the theft of sensitive information from a U.S. computer-security firm that later enabled outsiders to breach the defenses of military contractor Lockheed Martin. In another case, analysts were able to trace intrusions aimed at stealing information from Google and 33 other companies to operatives backed by the Chinese government. U.S. intelligence agencies believe that Chinese agents have stolen vast amounts of information from public and private computer systems, and are seeking to penetrate networks supporting military operations, the electric grid, financial transactions and other critical functions.

Federal Cybersecurity Efforts & Organizations

The U.S. government has a longstanding concern with the security of its information resources, and has included exploitation and defeat of enemy information systems in its military plans since the early days of the Cold War. However, the character and intensity of cybersecurity efforts began to change markedly in the 1990s with the spread of the Internet. Previously isolated systems became connected in a way that made them more useful but also more vulnerable, leading the Clinton Administration to begin a $1.5 billion effort in 1999 aimed at protecting government computers by installing intrusion-detection devices. Despite expanded funding for network security, the scale and diversity of cyber threats grew rapidly during the next decade as state-sponsored perpetrators began mounting assaults far more sophisticated than those previously carried out by criminals and online activists.

Following a series of major breaches in computer defenses, the Bush Administration launched a Comprehensive National Cybersecurity Initiative in 2008 aimed at integrating previously fragmented federal efforts. When President Obama took office in 2009, he directed a review of cybersecurity measures that resulted in the Bush initiative being broadened to encompass consolidation of federal access points, interagency exchange of threat information, enhanced detection of intrusions, improved response times and tools, techniques for threat isolation and mitigation, expanded workforce training and better coordination of federal research efforts. A series of new government organizations and positions were also established to take the lead in combating cyber threats, including a dedicated presidential advisor.

Within the military establishment, in what cyber experts call the "dot.mil domain," the lead organizations for protecting computers and networks are the National Security Agency (NSA) and U.S. Cyber Command, a sub-command of U.S. Strategic Command. U.S. Cyber Command became operational in 2010 and is headed by the same general officer who leads NSA, the intelligence community's principal eavesdropping and cryptological agency. The command is supported by component commands in each of the military services that provide units assigned to cybersecurity missions. Cyber Command oversees the day-to-day defense of networks operated by the military and major intelligence agencies; its activities are linked through its commander to the network exploitation and attack programs of NSA, which provide important insights into how threats can most effectively be countered.

The lead agency for securing the information resources of civil agencies and the commercial economy is the Department of Homeland Security (DHS). The National Protection and Programs Directorate within DHS oversees most of the government's efforts in cybersecurity preparedness, risk assessment, and incident response outside the dot.mil domain. The Office of Cybersecurity and Communications housed in the directorate manages a network-intrusion detection system for all civil agencies of the government called Einstein, oversees the U.S. Computer Emergency Readiness Team, and runs a center that coordinates the functions of the six biggest cyber operations centers located in other civil agencies. The DHS approach to centralizing cybersecurity across the federal government emphasizes three features: automation, interoperability and authentication of users. Legislation is pending to clarify the department's authority for assuring the integrity of private-sector information systems that are vital to the management of economic infrastructure.

Infancy of Cybersecurity Missions & Metrics

Although global spending on cybersecurity topped $60 billion in 2011 according to the PwC consultancy, both the mission of securing information resources and the metrics used to assess progress are in their infancy. Legislative and regulatory schemes such as the Federal Information Security Management Act specify minimum levels of preparedness, but compliance with their mandates has provided little assurance of security in a field where threats are constantly evolving and professional standards are still in flux. As in any other infant industry, the way in which cyber terminology, standards and methods are employed varies from user to user, and from supplier to supplier. Experts have little difficulty determining when a major breach of cyber defenses has occurred, but the absence of a universally accepted framework for measuring the adequacy of those defenses impedes the creation of a seamless federal posture.

Modern information systems and the technologies used to protect them typically generate many measures of system status and performance. For example, federal networks are equipped with antivirus software, intrusion-detection systems, vulnerability scanners and firewalls that routinely report data about potential threats. However, individual measures mean little when considered in isolation, and so they must be combined into more general metrics designed to inform decision-makers about the overall security of systems. Even at this higher level of generality, though, the significance of metrics will tend to change over time because standards, threats and expectations are unstable. Seemingly reliable metrics of safety can be quickly overtaken by a shift in adversary tactics or the introduction of new information technologies.

As the enormity of the cybersecurity challenge has become apparent, the federal government has funded research projects aimed at developing reliable standards and metrics for assessing the adequacy of defenses. The most extensive work has occurred in the Department of Defense, the Department of Homeland Security, and the National Institute of Standards and Technology. DHS, for instance, says it is seeking metrics that are "quantitative, validated against known truths, accurately measured, affordable both in time and cost, repeatable independent of the performer, and scalable from single computers to major national systems." Each organization has produced useful insights, but their missions are different and thus the metrics they develop cannot be universally applied. The security standards in a military unit facing diverse tactical threats to its information systems will necessarily be different from those that DHS seeks to apply to private-sector networks supporting critical infrastructure. Even if the mission requirements weren't different, the political obstacles to implementation would be.

Without agreement on standards and metrics, decision-makers will have difficulty discerning which outside providers are best equipped to support the government's cybersecurity efforts. If all suppliers present their capabilities in similar terms and there is no consensus framework for assessing quality, the federal customer will tend to default to the lowest bidder that seems technically qualified. However, that approach could spell disaster for warfighters and civilian workers who have become utterly dependent on computers and networks to accomplish their jobs. Even in the absence of agreed metrics, policymakers must have a clear idea of which requirements matter most in securing the nation's information resources. The next five sections of this report propose five core requirements that must be met by suppliers of cybersecurity services if the federal government is to adequately protect in the current information environment.

The United States continues to lead the world in traditional measures of military power such as the size and capabilities of its naval fleet. However, U.S. military leaders depend on a global grid of information networks to alert and employ forces that is potentially subject to subversion, disruption or destruction. The performance of U.S. forces in future conflicts depends heavily on the integrity and resilience of vital information resources.

REQUIREMENT #1:

Situational Awareness

In military lexicon, situational awareness is knowledge of conditions in a warfighting domain bearing upon current operations, including an understanding of the likely consequences resulting from various courses of action. In other words, situational awareness is the ability to cut through the "fog of war" and understand one's circumstances clearly. The joint force and intelligence community have invested heavily in sensors, datalinks and analytic systems for enhancing situational awareness, with the aim of fashioning a common operating picture that can be shared by all friendly forces deployed in a given region or domain. Without this common operating picture, warfighters might be unable to anticipate aggression or respond appropriately, and might even do harm to their own side -- the problem known as fratricide.

Effective cybersecurity, especially in the defensive realm, requires multifaceted, timely situational awareness. First, defenders must have a detailed understanding of how their own information systems are configured, including how they link to external networks and what protections have been installed such as firewalls and intrusion-detection devices. Second, they must be able to monitor the status and performance of their information systems in "real time" -- as events are unfolding -- using instruments and measures that capture the most significant indicators of danger. Third, they must have sufficient knowledge of potential threats to interpret what security indicators mean, particularly in terms of fashioning a response. Fourth, they must be able to quickly share information about emergent threats with other friendly operators, describing the scope and nature of dangers with sufficient fidelity so those operators can take action to preempt intrusions. And finally, they must be able to assess whether remedial actions have had the desired effect in restoring system integrity and security.

Although the elements of situational awareness are similar across all warfighting communities and domains, they entail unique efforts in cyberspace because of the special characteristics of the operating environment. For example, determining the source of threats is typically much harder in cyberspace than it is in the physical world, a challenge that experts refer to as the problem of attribution. Also, the boundaries of information systems may be harder to define because of the way in which digital networks transcend bureaucratic, political and geographical barriers. Recognizing the amorphous character of the current information environment, the government's Comprehensive National Cybersecurity Initiative places great stress on enhancing situational awareness through steps such as establishing operations centers, creating alert systems for sharing information, installing monitors on traffic flows and training employees to understand the significance of online phenomena.

However, there are many obstacles to situational awareness in cyberspace, with the anonymity of the Internet only being one of them. Federal organizations may lack the capacity to detect or measure certain types of threats, to combine threat intelligence from multiple sources, to correctly interpret the meaning of threat indications, or to share threat information with other operators in a timely fashion. General Keith Alexander, the head of U.S. Cyber Command, warned in 2010 that "we have no situational awareness," describing federal cyber efforts as far too dependent on after-the-fact forensics. Although major progress has been made since Alexander offered his bleak assessment, it is clear the government needs more outside providers with an in-depth understanding of how to build comprehensive situational awareness in cyberspace.

REQUIREMENT #2:

Full Spectrum Skills

As the challenge of achieving adequate situational awareness in cyberspace illustrates, security in the information age is a mission that has few clear boundaries. The whole world is now thoroughly interconnected by digital networks, and thus developments anywhere around the globe might potentially have some bearing on the integrity of vital information resources in the United States. Successful defense of friendly networks necessarily requires an interdisciplinary approach in which many different skills must be brought to bear. The more fragmented those skills are within the government or among its outside suppliers, the harder it will be to establish an integrated cyber posture that can anticipate dangers and respond in a timely fashion.

In the absence of an established framework or standards for identifying the best long-term solutions to cybersecurity needs, there is a natural tendency to favor providers who can address the most pressing problems. However, those problems will tend to change over time, and a preference for "point" solutions -- tightly-focused responses to particular vulnerabilities -- will produce a patchwork defensive posture that lacks resilience or adaptability. The government needs organic organizations and external suppliers with sufficient breadth and depth of expertise to understand the relationship between various parts of the cyber puzzle, people who can transcend point solutions to fashion what it already describes as a comprehensive national cybersecurity posture. Relatively few contractors have the experience to lead such an effort.

U.S. Cyber Command defines full-spectrum cyber operations as employment of the complete range of cyberspace operations to support combatant-command requirements and the defense of military information networks. That includes efforts such as computer-network defense, computer-network attack, and computer-network exploitation. Computer-network defense is defined as actions taken to monitor, detect, analyze and respond to unauthorized activity within Department of Defense information systems and computer networks. Computer-network attack is defined as actions taken to disrupt, deny, degrade or destroy information resident in computers and information networks -- or to impair the computers and networks themselves. Computer-network exploitation is defined as enabling operations and intelligence-collection capabilities conducted through the use of computer networks to gather data from target information systems. All three types of operations are necessary to sustain a comprehensive cybersecurity posture; if pieces are missing, or are not adequately integrated, then the posture will not be able to deliver adequate protection against advanced, persistent threats.

Ideally, contractors that lead federal cybersecurity efforts would possess sufficient experience and expertise to understand the relationship between the components of a full-spectrum posture. For instance, signals intelligence collected by the National Security Agency and various military organizations plays a crucial role in characterizing cyber threats, but finding competent cybersecurity providers who can generate synergies from the use of such arcane and secret skills is not easy. Finding contractors with credentials in both computer-network defense and computer-network attack is similarly difficult, although skill in penetrating adversary networks could be highly useful in developing defenses of friendly ones. While the government always has the option of serving as a system integrator of inputs from suppliers with narrow-gauge skills, it is likely to get better results from selecting companies with full-spectrum skills to manage the integration of efforts by diverse subcontractors. In some cases, those full-spectrum companies will have broader experience than federal organizations, giving them an advantage in identifying the most effective solutions to cyber challenges.

REQUIREMENT #3:

Operational Agility

In cyberspace, attackers tend to have an advantage over defenders. Like bomber pilots in the days before radar, they can spend weeks or months planning an attack, and then strike at the weakest point in the defenses of target nations with little or no warning to their victims. If the vulnerability they seek to exploit has not been previously detected or corrected by defenders -- a "zero-day exploit" in the cybersecurity lexicon -- then defenders may have few options other than to shut down the affected parts of their information grid. Even that may not be a viable response if the compromised networks are supporting essential warfighting or economic functions.

General Keith Alexander, head of U.S. Cyber Command, has likened the circumstances in which cyber defenders find themselves to the Maginot Line constructed by France along its eastern border after World War One. France's static perimeter defense worked reasonably well against traditional threats advancing along expected axes, but when new methods of attack emerged that could circumvent the fixed defenses, the Maginot Line became irrelevant to the outcome of battle. So it is with cyber defenses today. Although well-trained defenders usually have a better grasp of how friendly networks are configured than adversaries do, they seldom can anticipate when and where an attack will occur, and the static nature of their defensive posture allows adversaries to invest considerable time in developing attack plans that have a high likelihood of succeeding. The most advanced, state-sponsored adversaries develop a detailed understanding of target networks, and then scan defenses continuously until they identify a weakness that can be exploited to gain access.

In such circumstances, it is not enough for defenders to have exquisite situational awareness and full-spectrum skills. They must be able to react fast. Ideally, they should be able to act even before an intrusion has occurred, on the basis of signals intelligence and other warnings that aggression is imminent. That kind of agility requires cybersecurity providers with extensive technical depth and experience that can detect danger in advance of damage, generate immediate solutions, and then if necessary reconfigure vulnerable networks without disrupting the activities they support. Given the speed with which cyber attacks are manifested, defensive responses may need to be automated to avert losses, relying on machine intelligence and carefully crafted software algorithms to execute necessary actions. Unfortunately, that kind of agility does not yet exist in many parts of the U.S. government; a senior advisor to the Air Force's cybersecurity command disclosed in early 2012 that it typically takes the service over a month to determine forensically how a breach of its network defenses occurred. That kind of delay in finding answers could be fatal in wartime.

The Department of Defense has reacted to the need for greater agility in cybersecurity efforts by establishing a fast track for development of urgent defensive needs that bypasses traditional acquisition practices. In that regard, cybersecurity is analogous to the challenge that faced U.S. warfighters in Iraq and Afghanistan when the danger of improvised explosive devices arose. With enemy tactics constantly evolving, there was no time to go through the usual channels in crafting solutions. Warfighters needed to adapt quickly to enemy moves. The situation is much the same in the cybersecurity field: providers of cybersecurity solutions must be able to predict and react fast to changing adversary tactics, isolating intruders and dynamically reconfiguring networks before enemies can achieve their goals.

REQUIREMENT #4:

Organizational Maturity

As threats to information networks have proliferated, analysts have developed concepts for assessing how prepared the government and private industry are to cope with them. One commonly used tool is the "maturity model," which has long been used in other fields to rank organizational effectiveness using best practices. The basic idea behind maturity models is to construct a continuum of capability ranging from weak and disorganized to strong and resilient, identifying key attributes in each of the intervening steps that enable an organization to progress from vulnerability to dominance. The cybersecurity field has now evolved to a point where it is feasible to construct such continuums, not just for the organizations needing protection but also for the outside suppliers providing it.

The most widely-cited maturity model in the cybersecurity business identifies five successive stages of preparedness. At the most rudimentary level, where most organizations were five years ago and some still are, cybersecurity practices are ad hoc and manual, typically being triggered only when an external attack threatens operations. A somewhat higher level of preparedness exists in the next stage, where analytic tools are employed to assist organizations in reacting faster to threats, but responses are still piecemeal. At the next stage -- the level of preparedness to which many organizations are currently building -- defenders have an integrated picture of the local cyber environment that supports situational awareness and timely responses. A fourth stage of preparedness is achieved when organizations are sufficiently skilled and aware to be predictive about threats and proactive in their actions; at that higher stage of capability, responses are largely automatic and precisely tailored to whatever challenges arise. The highest level of preparedness, which is more theoretical than real at present, envisions an organization that is resilient in the face of even the most advanced and persistent threats, able to continue functioning regardless of what dangers appear.

It is too early in the evolution of the threat environment to know whether truly resilient enterprises will be feasible, given the way in which new dangers are continuously emerging. However, it is not too early to identify attributes likely to get organizations closer to that desired level of technological maturity. For instance, a truly resilient organization would be able to anticipate threats and adapt rapidly to their emergence, regardless of the velocity and volume with which they are manifested. A truly resilient organization would possess a cybersecurity posture that is integrated both internally and externally, sustaining collaborative links with a broader community of users that enable comprehensive situational awareness and collective defense.

Similar standards of technological maturity can be applied to the companies that provide cybersecurity services to the government. If they are capable providers, then they should be able to deliver the standard of security described at the higher stages in the maturity model. Their solutions should be readily scalable from a local setting to the enterprise level, they should invest sufficiently in products to offer high technical readiness at an affordable price, and they should be able to recruit world-class talent that is continuously trained and retained. Only a few providers at present have the depth and diversity of a Northrop Grumman or Lockheed Martin that enable them to rotate employees internally through all the relevant disciplines to produce superior expertise, but without such expertise it is doubtful that they can deliver a mature cybersecurity posture to customers.

REQUIREMENT #5:

Enterprise Commitment

Federal plans for coping with threats to the nation's information systems and networks envision a fundamental restructuring of the government's internal security posture -- a cultural shift that will take many years to implement and has no logical end point as long as new dangers continue emerging. Some of the tasks associated with the Comprehensive National Cybersecurity Initiative such as maintaining situational awareness, monitoring network traffic for malware, and managing supply-chain risks will persist indefinitely, because they are inherent features of security in the information age. The long duration of federal plans points to one more requirement that is essential to success in the cyber realm: commitment.

Commitment in this context is the recognition by federal agencies and private companies that they must permanently change the way in which they operate if they are to secure information resources essential to their missions. For companies providing cybersecurity services, commitment is the recognition that they must organize and invest with the intention of sustaining long-term ties to customers who will be relying on them for vital support over extended periods of time. However, commitment and dedication are not always the values that prevail in infant industries, which is what the cybersecurity field is today. Players with a wide range of motives gravitate toward newly emerging markets, and customers often have no reliable way of sorting out which ones are truly committed to the business for the long term.

That element of uncertainty as to motives and reliability is definitely present in the federal cybersecurity market today. Government outlays for network defense, exploitation and attack are expected to grow in the years ahead even as other facets of national-security funding shrink, and so many companies with only modest cybersecurity experience are trying to bolster their credentials through acquisitions or internal development. In addition, the fragmented and unpredictable nature of cyber threats has spawned scores of narrow-gauge enterprises aimed at addressing specific aspects of the challenge, and the staying power of these startups is highly questionable. Thus, while the commitment of federal organizations such as the National Security Agency and the Department of Homeland Security to their cybersecurity responsibilities can hardly be doubted, the long-term reliability of outside suppliers proposing to support them is sometimes not so clear. Late entrants to emerging markets often are the first to exit.

There are a few simple questions federal customers can pose that will help in determining how committed private-sector providers are to the cybersecurity field. First, how long have they actually been in the business? Second what is the level of effort that companies are dedicating to cybersecurity in terms investment, facilities, research and workforce training? Third, how closely do the competencies and business strategies of companies align with the demands of long-term relationships in the cybersecurity field? Fourth, what kinds of collaborative relationships have companies established with credible academic institutions and enterprises in the cyber field? And finally, what internal structural and cultural features do companies exhibit that are conducive to offering comprehensive, affordable security solutions? In general, companies that have been working in cybersecurity for a long time, that invest heavily in relevant research and skills, that have appropriate competencies and collaborative relationships, and that are organized to think in a holistic and cost-effective fashion about cybersecurity can be said to have made a strong commitment to the field. Companies lacking these features may not have the staying power or dedication to be long-term players.

CONCLUSION: The Danger of Picking the Wrong Providers

Cyber assaults against the vital networks of the federal government and private industry are expanding rapidly in their scale and intensity. In 2011, the number of attempted intrusions into the computerized control systems of domestic electric grids, oil refineries, transportation networks and other critical infrastructure rose fivefold from the previous year. Criminals stole the algorithms for controlling the International Space Station, which were stored on an unencrypted NASA laptop computer. And Chinese agents executed a sophisticated intrusion into the sensitive information systems of Lockheed Martin, the nation's biggest defense contractor. In response to these and other instances of cyber aggression, the Director of National Intelligence has elevated the priority assigned to cyber threats; the only threats now ranked as posing a greater danger to national security are weapons of mass destruction and global terrorism.

Despite official recognition of the need for improved cybersecurity, efforts to address the danger have been uneven. For instance, a 2012 report by the defense department's Director of Operational Testing and Evaluation found that, "in general, information technology and personnel were not fully prepared to operate in realistic and contested cyberspace conditions." The report catalogued several key aspects of cybersecurity in which the joint force's vulnerability to threats seems to be growing because of failure to consistently implement best practices such as updating virus signatures and installing software patches. Even if best practices were rigorously applied, vulnerability might still be growing due to the proliferation of sophisticated threats and the difficulty of predicting where attacks will occur.

In such circumstances, government agencies clearly need trusted and competent private-sector partners to help them carry out the mandates of the Comprehensive National Cybersecurity Initiative. At the very least, those partners should be able to satisfy the five overarching requirements cited earlier in this report: situational awareness, full-spectrum skills, agility, maturity and commitment. Contractors who are unable to deliver one or more of these essential items are not equipped to assume leadership roles in the war against cyber aggression; they may have useful contributions to make, but they are too limited in their capabilities to fill the role of long-term integrator and partner for the government. Simply awarding cyber work to the lowest-cost, technically acceptable provider is unlikely to secure the kind of relationships the government needs to protect vital information resources in a constantly changing threat environment. Cybersecurity is a field where the gap between best price and best value can be very great -- great enough to make the difference between victory and defeat in a national crisis.

Experts in the field have been warning for many years that a crisis is coming. The head of U.S. Cyber Command stated bluntly in November of 2011, "What we see is a disturbing trend -- from exploitation to disruption to destruction." In practical terms, this means that U.S. utilities might cease functioning without warning. Military command networks might collapse in the midst of a conflict. Financial, transportation and healthcare systems might be paralyzed. Such possibilities are the dark side of the great advances the information revolution has delivered. The only way of averting these dangers is to fashion a partnership between government and the private sector that provides seamless protection against all known threats. But that partnership won't work unless agencies and companies select providers who can deliver comprehensive, state-of-the-art cybersecurity in an agile, mature and dependable form.

The foundations of U.S. power and prosperity reside largely in the private sector. Cybersecurity solutions that work well in the government are harder to apply to the private economy because officials lack the information and authority required to establish consistent standards. The success of federal efforts to protect vital economic infrastructure can be enhanced by picking cybersecurity providers with a broad array of competencies and experience.

Printed in The United States of America, July 2012

Lexington Institute

1600 Wilson Boulevard • Suite 900 • Arlington, VA 22209
Tel: 703.522.5828 • Fax: 703.522.5837
www.lexingtoninstitute.org • mail@lexingtoninstitute.org