CYBERSTRATEGY 2.0

Frank J. Cilluffo and J. Paul Nicholas

Great minds have grappled with the manifestations of the information age for decades. Recently, however, it has been one of the information age's most loved and feared catalysts—the Internet—that has taken center stage in national security planning. Even as the Internet went public in the early 1990s, strategic thinkers were already wrestling with its potential implications for communications, commerce, and even conflict.

The power of the Internet derives from its characteristics. Open protocols and easy access make it "flat"; individuals, groups, and nations are somehow equals in the massive network of networks. As a mechanism for rapidly uniting global communities of interest, the Internet is also "sticky," possessing the ability to transmit ideas, information, and actions—power that can be leveraged and focused to create tremendous asymmetric capabilities that can be exercised without attribution.

Therein lies the threat. Individuals, organizations, or nation states with the capabilities to gather, assimilate, shape, project, deny and deliver information in a controlled way could cause nationally significant disruptions in the United States.

FRANK J. CILLUFFO is an Associate Vice President at the George Washington University, where he also directs the multi-disciplinary Homeland Security Policy Institute. Prior to joining GWU, he served as a Special Assistant to the President for Homeland Security, a post to which he was appointed by President Bush shortly after 9/11.

J. PAUL NICHOLAS is a senior security strategist with Microsoft. Previously, he served in the federal government for eight years, including two years as a White House director for critical infrastructure protection coordinating the Bush administration's National Strategy to Secure Cyberspace.

The controlled delivery of information with the intent to exploit, disrupt, or manipulate an adversary's operations is what we term a *weapon of mass effect* (WME). A WME does not have to be a single damaging attack. Rather it could be composed of several smaller, and sometimes discrete, attacks (also known as "exploits") that culminate in a massive disruption. A WME, furthermore, may be triggered by either a person or a technology.

The potential threat of WMEs to the United States, its allies, and its global interests increasingly has been recognized in presidential directives and national strategies. The resulting policies have sparked important efforts in cybersecurity, homeland security, and national defense. Unfortunately, no matter how polished the prose, policy alone does not provide protection. Currently, the United States still lacks fundamental capabilities for discerning, deterring, and defending against sophisticated WMEs that threaten its national interests. Upgrading national security planning, programming, and operations to meet this challenge requires us to develop a richer understanding of the nature of WME threats, early indicators of them, and the means to deter and defend against potential attackers.

Meet the adversaries

Understanding the motivations and capabilities for the use of WMEs is essential for discerning, deterring, and mitigating attempted attacks.

Simply put, there are three broad categories of threats—those posed by individuals, by organized groups, and by nation states—and 13 identifiable sources of potential attack. These run the gamut from "script kiddies" (generally unsophisticated attackers using point-and-click attacks available on the Internet) to highly sophisticated nation state alliances that may employ subtle forms of WME to alter the balance of regional or global power.

In this matrix, individuals increasingly matter. Operators who learn how to harness the asymmetrical power of the Internet can employ that medium as a launching pad for attacks against systems or even people. This constitutes a major development; just a decade ago, only nation states had the technology, the communications tools, and the skill sets that are now commonly available to individuals. In 1997, the President's Commission on Critical Infrastructure Protection estimated that by 2001 there were likely to be 19 million people with the skills to execute various cyber attacks.[1] These estimates predated the Internet boom and the dramatic communications breakthroughs currently under way, and would likely be much higher if undertaken today.

The impact has been profound. Global computer problems and billions of dollars in damage have been caused to date by relatively unskilled coders. Individuals also increasingly can use the Internet to engage and recruit people to join their cause. Terrorist organizations have demonstrated particular sophistication in this regard, uniting people to act on ideas, no matter how extreme. The 2005 grand jury indictment and conviction of Ahmed Omar Abu Ali for conspiring with al-Qaeda in an assassination attempt on President George W. Bush, for example, found important connections with the Internet. The indictment highlights the important role the cell phone, laptop and portable digital media played in al-Qaeda security practices, video surveillance of American operations in Afghanistan and contacts with other al-Qaeda operatives.[2]

Table 1: Threat Categories, Actors, Motivations, Capabilities and Resources In Connection with the Use of Weapons of Mass Effect (WMEs)				
Threat Categories	**Actors**	**Motivations**	**Capabilities**	**Resources**
Individuals	Pawns/Zombies	N/A	N/A	Minimal
	Script kiddies	Thrill seeking, power demonstration, political	Low	Minimal
	Lone hackers	Personal, professional, financial, power demonstration, political	Variable	Minimal
	Spammers/ Phishers	Financial, power demonstration	Low	Minimal
	Virus/Malware authors	Power/skill demonstration	Variable	Minimal
	Botnet controllers	Power/skill demonstration	Moderate	Minimal to moderate
	Ideological recruiters	Power/skill demonstration	Variable	Minimal
Organized Groups	Criminal organizations	Financial	Moderate	Minimal to substantial
	Terrorist organizations	Power demonstration, influence decisions, intelligence collection	Moderate	Minimal to moderate
	Non-state organizations	Political, intelligence collection, influence decisions, power balancing, economic influence	Moderate	Moderate to substantial
Nation States	Foreign intelligence services	Political, intelligence collection, influence decisions, power balancing, economic influence	High	Substantial
	Military components	Political, intelligence collection, influence decisions, power balancing, economic influence	High	Substantial
	Integrated nation state capability	Political, intelligence collection, influence decisions, power balancing, economic influence	High	Substantial
	Nation state alliances	Political, intelligence collection, influence decisions, power balancing, economic influence	Moderate to high	Substantial

The wide deployment of broadband services and "always on" network connections likewise has created a new threat source: "pawns." These are machines that are controlled by entities other than the actual owner, and can be used to clandestinely attack other computers. They also can be tied together into a robot network, or "bot-net." In its 2005 *Internet Security Threat Report*, the security provider Symantec observed an average of 10,352 active "bot" network computers per day, and noted that "bot" networks and customized "bot" code were available for purchase or rent. The report also opined that financial incentives would likely drive attackers to "develop more sophisticated and stealthier malicious code that will be implemented in bot features and bot networks, some of which could attempt to disable antivirus software, firewalls, and other security measures."[3]

There is a distinct risk that, as individual "bot-net" and malware (malicious software) developers begin to be paid for their services by criminals, terrorists, or nation states, they will rapidly become part of "groups," the second category of threats. The assimilation of "bot" designers into criminal, terrorist, or political entities may foster the development of more precise "bot-nets"—ones that are aimed at accomplishing specific financial or political goals.

Indeed, non-nation state groups are growing in power and influence. The Bush administration's 2003 *National Strategy to Secure Cyberspace* identified the threat of "organized cyber attacks" as a primary national security concern. The strategy acknowledges that high technical sophistication is required to execute nationally significant cyber attacks, and warned that "the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving."[4]

Such organized threat sources fall into three general categories: (1) criminal activities such as organized theft, fraud, and trespassing; (2) terrorist activities which may exploit WMEs to further political goals or enhance physical attacks; and (3) affiliations of non-state actors who may be using more subtle WMEs to influence politics or public opinion, gather information, or engage in espionage. And, while nation states still have the most resources to manage, operate, and fund long-term operations, these unique advantages may be diminishing. The U.S. intelligence community has warned that:

> The rapid pace of change in information technology suggests that the appearance of new and unforeseen computer and network technologies and tools could provide advantages in cyber warfare to either the defender or the attacker. Wildcards for the years beyond 2005 include the possibility of fundamental shifts in the nature of computers and networking, driven, for example, by emerging optical technologies. These changes could improve processing power, information storage, and bandwidth enough to make possible application of advanced software technologies such as artificial intelligence to cyber warfare.[5]

The third category of threats, nation states, generally tends to be viewed as a single homogeneous entity. In truth, however, particular elements within a nation state may have distinct and sometimes competing motivations. Some nations may possess strong capabilities for foreign intelligence but lack an inte-

grated national capability for exercising them. Compounding the threat, nation states can enter into partnerships with other countries to enhance their WME operations.

Under the radar

The precursors to crime, terrorism, and war have a certain rhythm and cadence. In general, well-executed incidents all employ planning, intelligence gathering, surveillance, and exercises. These same rhythms will likely be used in information-based conflicts or WMEs that result in nationally significant incidents.

The reason is that the characteristics of WME attacks argue against detection. Assembling the tools for information-based WMEs does not require a specialized infrastructure or unique footprint that can be monitored from satellites. Further, the raw materials needed to build health care databases or WMEs look very similar as they are shipped around the world. Just as the Soviet Union successfully hid a massive biological weapons program from the world by inserting its production infrastructure in civilian facilities and neighborhoods, countries can easily shield the development of offensive cyber tools and methodologies.

Furthermore, the volume of traffic and the constant demands on people and systems provide ample opportunities to test WMEs (or various elements of a single WME) with minimal risk of discovery. The numbers tell the story; between 1995 and 2005, the unique software vulnerabilities reported to Carnegie Mellon's Computer Emergency Response Team surged from 171 incidents to 5,990.[6] And the time from vulnerability to exploitation can take just a few days, while fixes or patches are liable to take much longer.

Likewise, such attacks are modular in nature. Once one is developed, large numbers of variants can also be created—each of which "represents a new, distinct threat … that is modular and customizable."[7] In some instances there can be hundreds or thousands of variants of an attack, each requiring modified defenses. This constant refinement can be attributed, in part, to the fact that some of these codes have been made public, greatly empowering individuals and criminal organizations to participate in the development of variations.

By watching and learning, aggressors—be they terrorists, nonstate groups, or national intelligence/military elements—can gather tremendous operational insights about the thresholds and responses of countries, infrastructures, and individual enterprises. Carefully observing how people, processes, and technology respond to certain types of attacks can help hostile actors to refine their plans and operations.

Here, terrorist groups warrant a special note. While they routinely exploit cyberspace for communications, planning, and operational coordination, they have not yet been detected planning cyber attacks or assembling elements for a WME. However, they have repeatedly demonstrated tremendous patience in planning for attacks, and the willingness to wait, watch and strike with great surprise. As the Global War on Terror erodes the physical capabilities of these organizations, cyber WMEs may yet become a new tool of assault.

Understanding the playbook

For almost ten years, the concept of an "indications and warning architecture" for cyberspace has received

intermittent attention from federal officials. In 1996, Congress called on the Clinton administration to develop a report on how it would detect and defend against a strategic attack on the nation's information infrastructure.[8] Two years later, the Clinton White House responded by issuing Presidential Decision Directive 63, a blueprint for critical infrastructure protection that included plans for "a public-private partnership to reduce vulnerability" to cyber attack.[9]

Subsequently, in 2001, the General Accounting Office recommended that the National Security Advisor ensure the development of capabilities for strategic analysis of computer-based threats and an overall indications and warning framework and methodology.[10] Later still, the 2003 *National Strategy to Secure Cyberspace* envisioned that the newly formed Department of Homeland Security (DHS) would assume the broad analytical challenges required for tactical and strategic analysis of cyber attacks.[11] DHS was subsequently tasked with developing a national "indications and warnings" architecture for both cyber and physical incidents—one that would facilitate the identification of indicators of an impending attack, and have the capacity for detecting and analyzing patterns of such potential strikes.[12]

Yet, over two years later, such a capability has yet to materialize. The threats, meanwhile, are mounting, as the skill sets, technologies, and tradecraft to project the asymmetrical power of cyberspace in a WME continue to proliferate. American planning, programming and operations need to respond to this fundamental shift by building the capabilities necessary to discern, deter, and defend against the spectrum of threats and WMEs that loom on the national security horizon.

Discernment

Fostering the capabilities necessary to detect subtle, sophisticated information attacks requires more than simply determining that particular systems have been compromised.

First and foremost, the U.S. must establish a program office to develop an "indications and warning" architecture for cyberspace. There is a clear federal role for helping discern and detect the precursors to WMEs. This is distinct from protecting computer systems. The protection of computers is the responsibility of the owner and operator of the system. But when there are sophisticated efforts underway with the ultimate intent of creating a WME, the federal government must support efforts to understand and neutralize such attempts with law enforcement or other appropriate tools.

Such an initiative should also be designed to work closely with industry. The federal government is certainly not the place to turn if you want "early warnings" about viruses or worms; there is a robust cybersecurity industry that responds to such needs. However, as attack tools and methodologies become more precise and controllable, attackers can penetrate deeper into particular systems, exacting more damage and achieving more strategic objectives.

The precursors to such events are often subtle and seemingly insignificant, including an occasional system anomaly or a benign incident with no direct consequences on operations. Studying such events can be costly and may not return any immediate finding of wrongdoing or result in a monetary return for private enterprises. This is a beautiful thing for the adversary,

because he/she is able to pursue their goals and remain undetected or at least insignificant to the operator. Successful WME developers are patient and willing to invest the time to gradually calibrate the complexity and intensity of their methods over an extended period of time.

Cyberspace is responsible for an unexpected convergence of human intelligence (HUMINT) and signals intelligence (SIGINT). The smoke-filled gin joints of Le Carré novels have given way to Internet relay chats (IRCs) where conversations composed of icons, acronyms, and hip lingo recruit supporters and cement agreements. You can't defeat an adversary if you can't speak the language. The federal government needs people who speak cyber. There is a compelling need for a new type of expert: part linguist, part sociologist/behaviorist, and fluent in IRC. Assembling this capability may mean we have to recruit or train people who might not otherwise be able to obtain a traditional security clearance.

The second priority, therefore, should be to foster specific analytical discipline and expertise for addressing the challenges related to information-based attacks. Analysts must not fall into the trap of "mirror imaging"—thinking that organizations contemplating using an information-based WME will follow a direct linear path or an "efficient" means of attack. Rather, discerning the potential targets of information-based WMEs requires public-private partnerships to investigate and analyze protracted and intensive intrusions into information systems where the intruder's motives are often obscure. Working together, government and industry can create an analytical framework for more rapidly discerning and detecting structured attacks or intrusions.

Deterrence

Deterring the use of information-based WMEs requires the development of visible and robust capabilities for two functions: (1) response and coordination capabilities, both domestic and international, and (2) the swift apprehension and prosecution of criminals.

Recognizing these needs, the Bush administration made the establishment of a National Cyberspace Security Response System a central component of its cyberstrategy. That system was intended to be a public-private collaboration between government and non-governmental entities for the express purpose of providing analysis, warning and management of incidents of national significance. Unfortunately, it is often easier for federal documents to call for public-private partnerships than it is to actually execute them. For example archaic legislation such as the Federal Advisory Committee Act, which governs how federal and non-federal entities collaborate, can hinder information sharing efforts that are central to responding to cyber challenges.[13] Even today, the development of an effective and efficient national cyberspace security response system and similar entities remains hamstrung by such bureaucratic red tape.

This represents a dangerous deficiency. Rapidly attributing cyber events is critical to both mitigating the attack and deterring future ones. Currently the forensic capabilities for attributing the creation of viruses and worms are still in their infancy. The complex suites of attacks that constitute a WME are at this point almost impossible to unravel. The situation is further complicated as one begins to chase the source of the attacks through multiple networks around the world. Even if a machine

is located, it can be difficult to prove who was the mastermind behind the keyboard.

Once the responsible party has been identified, swift apprehension and prosecution requires a proper legal regime that criminalizes such behavior. The U.S. maintains such laws, but many countries do not. To help promote a more harmonized legal approach to cyber-based attacks, the Council of Europe, with strong support from the United States, Canada, Japan and other countries, has crafted the first international agreement establishing common criminal policy and procedures for cooperation. Eleven countries, including Albania, Bulgaria, Croatia, Romania, Slovenia, Switzerland, and others have ratified the treaty. The United States signed the Convention in 2001, and forwarded it to the Senate for ratification in 2003. It was approved by the U.S. Senate Foreign Relations Committee in the summer of 2005, but has yet to be ratified. Failing to do so will significantly limit U.S. capabilities for deterring non-state actors from pursuing and using information-based WME.

Defense

Establishing national capabilities for defending against information-based WMEs requires developing flexible organizations and tools that can be calibrated for response to the three general threat sources identified above.

In the case of individuals and groups, the U.S. is well on its way to establishing the right types of mechanisms for "managing incidents." For example, DHS has established the National Cyber Response Coordination Group (NCRCG), a forum of federal agencies that coordinates intra-governmental and public/private preparedness for large-scale cyber incidents. Depending on the nature of the incident, the NCRCG can be chaired by one of three departments: Homeland Security, Defense or Justice. Its role includes developing a common operational understanding of incidents of national significance and coordinating federal resources to support response and recovery. Simply put, the NCRCG is intended to help ensure that DHS analysis of, and warning about, an array of threats—and mitigating actions for them—are coordinated with law enforcement and defense.

Of these, organized groups may be the most challenging to defend against. They are the most difficult entities to identify, penetrate, and deter because they are politically motivated and there are few diplomatic channels for diffusing tensions. As well, surprise is essential to the effectiveness of their first-strike capability. Without a credible "indications and warnings" capability, the NCRCG would likely not be activated until after an information-based WME had already been initiated.

Currently, the relatively poor technical and forensic capabilities for attribution, coupled with the lack (as yet) of a cohesive international cybercrime agreement and a common criminal policy, significantly impede efforts to identify and apprehend responsible entities. These deficiencies fall into three basic categories: a lack of laws criminalizing cyber attacks; absence of common data retention policies; and no protocols for law enforcement and Internet service provider (ISP) collaboration. All of these deficiencies, coupled with slow law enforcement responses, provide organized groups with the opportunity to disappear, to launch additional information-based WMEs,

or to use cyber disruptions to cloak physical attacks.

Significantly, while possessing the most power to employ information-based WMEs, nation states are far more cautious about executing such operations. Nations may not want to demonstrate certain national capabilities, because they would rather use them later and surprise a potential adversary. States likewise may fear that if the information-based WME were traced to them, the target may respond with traditional military means. What is unknown is the extent to which individual elements *within* a state (such as clandestine military units or intelligence services) may be engaging in discreet low intensity efforts to penetrate and map information systems as precursors to an attack. Detecting such operations requires careful coordination among key federal entities in law enforcement, homeland security, and intelligence.

Rebooting national security policy

The price of entry is at an all-time low. The skills and technologies for assembling WMEs are widespread. Gone are the days when one needed to raise an army, build a command structure, train soldiers and purchase weapons to attack an adversary. The very efficiencies enabling governments and global enterprises can also arm a range of potential adversaries to execute unexpected disruptions.

American planners need to respond to this fundamental shift by building the capabilities necessary to discern, deter, and defend against the spectrum of threats and WMEs that loom on the national security horizon. Developing WME defenses and policies requires leveraging a troika of people, processes, and technologies. The flat, sticky powers of cyberspace are ultimately neutral. Imagination and innovation are the only limitations we face in harnessing the power of cyberspace to project and defend our national interests.

1. Robert T. Marsh et al., *Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection, October 1997, 9.
2. See "Grand Jury Indictment," United States of America v. Ahmed Omar Abu Ali (United States District Court for the Eastern District of Virginia, September 2005).
3. *Internet Security Threat Report Vol. VIII*, Symantec Corporation, September 2005 (http://enterprisesecurity.symantec.com/content.cfm?articleid=1539).
4. *National Strategy to Secure Cyberspace*, White House, Office of the Press Secretary, February 2003, 9 (http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).
5. Ibid.
6. "Cert/CC Statistics 1998-2005," Carnegie Mellon Software Engineering Institute, n.d. (http://www.cert.org/stats/cert_stats.html).
7. *Internet Security Threat Report Vol. VIII.*
8. This request was encapsulated in the *National Defense Authorization Act of Fiscal Year 1996*, Public Law 104-106, § 1053 (February 10, 1996).
9. *Presidential Decision Directive/NSC-63: Critical Infrastructure Protection*, White House, May 22, 1998 (http://www.fas.org/irp/offdocs/pdd/pdd-63.htm).
10. *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, U.S. General Accounting Office, April 2001 (http://www.gao.gov/new.items/d01323.pdf).
11. *National Strategy to Secure Cyberspace*, 10-31.
12. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, White House, Office of the Press Secretary, December 17, 2003 (http://www.fas.org/irp/offdocs/nspd-7.html).
13. The Federal Advisory Committee Act (FACA) is intended to create a transparent process for non-federal entities to share policy recommendations with the federal government and is an important ethical protection. However, sometimes concerns about FACA requirements can hinder public-private collaboration to address operational security issues in physical and cyber incidents.