THE CYBER SECURITY CHALLENGE

BY MICHAEL NACHT

IT IS INCREASINGLY APPARENT THAT CYBER SECURITY IS BECOMING A CENTRAL FEATURE OF THE US NATIONAL SECURITY POLICY DEBATE.

The popular and specialized literature is replete with articles analyzing the problem and advocating responses to this challenge. Congress is mobilizing committees and sub-committees to address the myriad of issues that cyber technology has raised. The National Academies have already conducted several major studies looking at the appropriateness of offensive operations, cyber deterrence, and other issues. This is taking place as the executive branch conducts an intensive effort to sort out areas of authority and responsibility so that there is a coherent governmental approach to the challenge. Simultaneously, however, there is a growing chorus of concern that the threat is being "hyped" because huge budgetary support is at stake. This is especially important at a time of extreme budgetary austerity, where some see cyber security as one of the few growth areas for the national security budget, at least for the next several years.

What are the core elements of the issue and what are the needs that must be satisfied if we are to proceed with a sensible, cost-effective approach?

Core Elements

When the internet was developed, first by the Defense Advanced Research Projects Agency (DARPA) in the 1970s for military purposes but ultimately commercialized for everyone to use by the 1990s, it was heralded as a purely positive technological advance that would transform society. In many respects, this expectation has been realized. Virtually every aspect of modern society — health care, transportation, communication, finance — has been affected if not transformed by this development. Most recently, we have all witnessed the impact of social network technology — especially Facebook and Twitter — in mobilizing communities against authoritarian regimes in the Middle East.

But the introduction of this technology has not altered the fundamental structure of world politics which remains an anarchical system of sovereign states marked by complex patterns of competition and cooperation. Not only are there deep animosities between and among states, but there are powerful terrorist groups and criminal elements that exert their influence across national boundaries. With the ease of use of new technologies, there are individual "hackers" who can cause significant mischief as well as politically motivated "hacksters" who conduct cyber operations in the service of larger political aims.

So the overall challenge is to facilitate the continued use of these technologies for the good of all while protecting against their malevolent application.

The growing significance of cyber technology as a tool of national security policy was illustrated in 2007 when the Russian Federation — allegedly a combination of government organizations and individuals — responded to the removal of a Russian statue in Estonia by disabling the Estonian internet. Then, more significantly, just before Russian forces entered Georgia in August 2008, the Georgian governmental cyber communications system was completely disabled, hampering Georgian abilities to meet the attacking forces.

Some now claim that in modern warfare, the initial action taken will be a cyber, rather than physical, attack against the defenses and command and control systems of the attacked state.

There are three major elements of the US internet system: the ".mil" network; the ".gov" network; and the ".com" network. The first permits the national security community to communicate with itself. It is the job of the Department of Defense (DoD) to protect this network and to ensure its proper functioning. In 2010 a new military organization, Cybercommand ("Cybercom"), was established to shoulder much of this responsibility. The current director is a four-star US Army General, a career intelligence specialist, and the concurrent director of the National Security Agency, the primary signals intelligence arm of the US intelligence community.

The ".gov" network is to be protected by the US Department of Homeland Security (DHS). But this is a vast undertaking. At the moment, Cybercom has far superior capabilities than DHS to conduct effective defenses. It is imperative that Cybercom, DoD and DHS cooperate to insure the .gov network can be effectively defended — a formidable task.

The ".com" network, used by roughly 85-90% of all internet users, has no governmental controlling organization. Voluntary cooperation between the private sector and government — illustrated when Google, after having its network attacked by the Chinese government, allegedly went to the National Security Agency (NSA) for support — is at the heart of the protection of this network. This cooperative activity is hindered by corporations that are reluctant to share proprietary information with their competitors or with the government and by the government's limitations in providing sensitive or classified information to the private sector.

From a national security perspective, there are three main aspects of cyber security: exploitation, defense and offense. The first involves identifying hardware and application vulnerabilities of adversarial networks to obtain critical information, a modern form of espionage. But it is not purely for passive purposes, because huge amounts of information can be "exfiltrated" and can be used to hamper military operations. The second is the building of measures to make it more difficult for attackers to degrade, disable or destroy protected networks. The third is to take initiatives to disable offensive capabilities "preventively" or "preemptively" that are themselves intended for cyber attack. These offensive operations can range from playing a form of defense in peacetime to conducting full spectrum operations in war time. This third area is especially controversial because it runs up against possible violations of national sovereignty in order to conduct "preventive" or "preemptive" attacks.

Major Challenges

The national security community is wrestling with several tough problems which will take considerable time and effort to resolve. These include:

1. DECLARATORY POLICY — The US government has no official policy publicly communicating what it would or would not do in the event of a major cyber attack against US forces, command and control systems, electric power grids, financial networks, or other elements of military power or critical infrastructure. Should there be a declaratory policy and, if so, what should it stipulate? For example, should we define categories of "major cyber attack" that are unacceptable, so-called "red lines," that would likely trigger a major US retaliatory response?

2. DETERRENCE POLICY — Much of the nuclear age has been marked by refinements of deterrence policy crafted to influence adversarial behavior in irregular, conventional and even nuclear war. Are these concepts applicable to the cyber domain where attribution of the attack is often difficult to ascertain and the range of cyber attack damage can be from the trivial (e.g., slowing email receipt) to the profound (e.g., disabling the nation's military early warning systems)?

Professor Michael Nacht holds the Thomas and Alison Schneider Chair in Public Policy. In 2009–10, he participated in the development of cyber security policy as Assistant Secretary of Defense for Global Strategic Affairs.

3. AUTHORITIES AND RESPONSIBILITIES — If cyber attacks against US forces or critical infrastructure originate abroad, a response to them would almost surely involve violation of the sovereignty of the state where the attack originated. What is the legal basis for the US to conduct such operations? This is a very thorny problem. Moreover, there is a huge time lag between obtaining appropriate legal authorities (measured often in weeks or months) and the need for national security forces to respond effectively (measured at times in minutes or hours). How can this time lag be most effectively bridged?

4. GUARANTEES OF CIVIL LIBERTIES — The United States is built on a "government of laws, not men." But cyber security presents a major tension between the policy and legal communities. Given the difficulty in attributing the origins of cyber attacks, and the possibility that some of these attacks could originate in the US or by American citizens, how do we formulate effective policies that still guarantee the civil liberties of our citizens? Under what circumstances would it be justified for

Cont'd. on page 8

Cyber Security Cont'd. from page 5

the US government to monitor the cyber communications of US citizens or, if necessary, to degrade or disable these systems? And who and how should these activities be monitored?

5. OVERSIGHT — What is the role of the US Congress in overseeing US cyber activities by the executive branch? Should new committees be formed — perhaps a Senate Select Committee on Cyber Operations, for example — analogous to how the Congress addresses the oversight of intelligence operations? What type of legislation should the Congress consider that would strengthen, not hinder, US cyber security?

6. INTERNATIONAL CONSULTATIONS, NEGOTIATIONS AND AGREEMENTS — The US is sharing selected information on cyber security with key allies. Should it broaden the dialogue? What types of information should be shared? What should we seek to learn from others, and how can we cooperate? Should the US seek explicit codes of conduct to govern cyber behavior on a bilateral or multilateral basis? Are there advantages to formal treaties, or are they too cumbersome, constraining and difficult to enter into force because of the politicized US Senate ratification process?

7. CROSS-DOMAIN DETERRENCE AND RESPONSES — If the US experienced a major cyber attack, it is not required that the response be in cyber space. What rules should govern the US response that could take a political, economic, diplomatic or military form? Would such actions be seen by potential adversaries as proportional or escalatory?

8. STRENGTHEN PRIVATE SECTOR-GOVERNMENT COOPERATION — How can this best be achieved so that the US financial networks, electric power grids and other essential systems that are in private hands remain well protected? Should, for example, the National Economic Council in the White House play an active role in promoting this cooperative activity or should it be left to specific executive branch agencies?

We are still in the infancy of understanding cyber security — perhaps analogous to the late 1940s in the nuclear age. During the Cold War, it took more than a decade to convince ourselves that we had an understanding of the rules of the road that would protect US national security. Indeed, to this day some critics claim we still don't have it right. We are thus embarking on an extensive period of analysis, debate and implementation to determine how to make our cyber networks — and all that they enable us to do — secure. This is an important, exciting and uncertain road ahead, a major new development for US national security policy. **G**