

The Washington Post

SUNDAY, FEBRUARY 28, 2010

OUTLOOK

To win the cyber-war, look to the Cold War

By MIKE MCCONNELL

The United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking.

The problem is not one of resources; even in our current fiscal straits, we can afford to upgrade our defenses. The problem is that we lack a cohesive strategy to meet this challenge.

The stakes are enormous. To the extent that the sprawling U.S. economy inhabits a common physical space, it is in our communications networks. If an enemy disrupted our financial and accounting transactions, our equities and bond markets or our retail commerce — or created confusion about the legitimacy of those transactions — chaos would result. Our power grids, air and ground transportation, telecommunications, and water-filtration systems are in jeopardy as well.

These battles are not hypothetical. Google's networks were hacked in an attack that began in December and that the company said emanated from China. And recently the security firm NetWitness reported that more than 2,500 companies worldwide were compromised in a sophisticated attack launched in 2008 and aimed at proprietary corporate data. Indeed, the recent

Mike McConnell was the director of the National Security Agency in the Clinton administration and the director of national intelligence during President George W. Bush's second term. A retired Navy vice admiral, he is executive vice president of Booz Allen Hamilton, which consults on cybersecurity for the private and public sector.

Cyber Shock Wave simulation revealed what those of us involved in national security policy have long feared: For all our war games and strategy documents focused on traditional warfare, we have yet to address the most basic questions about cyber-conflicts.

What is the right strategy for this most modern of wars? Look to history. During the Cold War, when the United States faced an existential threat from the Soviet Union, we relied on deterrence to protect ourselves from nuclear attack. Later, as the East-West stalemate ended and nuclear weapons proliferated, some argued that preemption made more sense in an age of global terrorism.

The cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects. So, should our strategy be deterrence or preemption? The answer: both. Depending on the nature of the threat, we can deploy aspects of either approach to defend America in cyberspace.

During the Cold War, deterrence was based on a few key elements: attribution (understanding who attacked us), location (knowing where a strike came from), response (being able to respond, even if attacked first) and transparency (the enemy's knowledge of our capability and intent to counter with massive force).

Against the Soviets, we dealt with the attribution and location challenges by developing human intelligence behind the Iron Curtain and by fielding early-warning radar systems, reconnaissance satellites and undersea listening posts to monitor threats. We invested heavily in our response capabilities with intercontinental ballistic missiles, submarines and long-range bombers, as well as command-and-control systems and specialized staffs to run them. The resources available were commen-

surate with the challenge at hand — as must be the case in cyberspace.

Just as important was the softer side of our national security strategy: the policies, treaties and diplomatic efforts that underpinned containment and deterrence. Our alliances, such as NATO, made clear that a strike on one would be a strike on all and would be met with massive retaliation. This unambiguous intent, together with our ability to monitor and respond, provided a credible nuclear deterrent that served us well.

How do we apply deterrence in the cyber-age? For one, we must clearly express our intent. Secretary of State Hillary Rodham Clinton offered a succinct statement to that effect last month in Washington, in a speech on Internet freedom. "Countries or individuals that engage in cyber-attacks should face consequences and international condemnation," she said. "In an Internet-connected world, an attack on one nation's networks can be an attack on all."

That was a promising move, but it means little unless we back it up with practical policies and international legal agreements to define norms and identify consequences for destructive behavior in cyberspace. We began examining these issues through the Comprehensive National Cybersecurity Initiative, launched during the George W. Bush administration, but more work is needed on outlining how, when and where we would respond to an attack. For now, we have a response mechanism in name only.

The United States must also translate our intent into capabilities. We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options — and we must be able to do this in milliseconds.

More specifically, we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable. The technologies are already available from public and private sources and can be further developed if we have the will to build them into our systems and to work with our allies and trading partners so they will do the same.

Of course, deterrence can be effective when the enemy is a state with an easily identifiable government and location. It is less successful against criminal groups or extremists who cannot be readily traced, let alone deterred through sanctions or military action.

There are many organizations (including al-Qaeda) that are not motivated by greed, as with criminal organizations, or a desire for geopolitical advantage, as with many states. Rather, their worldview seeks to destroy the systems of global commerce, trade and travel that are undergirded by our cyber-infrastructure. So deterrence is not enough; preemptive strategies might be required before such adversaries launch a devastating cyber-attack.

We preempt such groups by degrading, interdicting and eliminating their leadership and capabilities to mount cyber-attacks, and by creating a more resilient cyberspace that can absorb attacks and quickly recover. To this end, we

must hammer out a consensus on how to best harness the capabilities of the National Security Agency, which I had the privilege to lead from 1992 to 1996. The NSA is the only agency in the United States with the legal authority, oversight and budget dedicated to breaking the codes and understanding the capabilities and intentions of potential enemies. The challenge is to shape an effective partnership with the private sector so information can move quickly back and forth from public to private — and classified to unclassified — to protect the nation's critical infrastructure.

We must give key private-sector leaders (from the transportation, utility and financial arenas) access to information on emerging threats so they can take countermeasures. For this to work, the private sector needs to be able to share network information — on a controlled basis — without inviting lawsuits from shareholders and others.

Obviously, such measures must be contemplated very carefully. But the reality is that while the lion's share of cybersecurity expertise lies in the federal government, more than 90 percent of the physical infrastructure of the Web is owned by private industry. Neither side on its own can mount the cyber-defense we need; some collaboration is inevitable. Recent reports of a possible partnership between Google and the government point to the kind

of joint efforts — and shared challenges — that we are likely to see in the future.

No doubt, such arrangements will muddy the waters between the traditional roles of the government and the private sector. We must define the parameters of such interactions, but we should not dismiss them. Cyberspace knows no borders, and our defensive efforts must be similarly seamless.

Ultimately, to build the right strategy to defend cyberspace, we need the equivalent of President Dwight D. Eisenhower's Project Solarium. That 1953 initiative brought together teams of experts with opposing views to develop alternative strategies on how to wage the Cold War. The teams presented their views to the president, and Eisenhower chose his preferred approach — deterrence. We now need a dialogue among business, civil society and government on the challenges we face in cyberspace — spanning international law, privacy and civil liberties, security, and the architecture of the Internet. The results should shape our cybersecurity strategy.

We prevailed in the Cold War through strong leadership, clear policies, solid alliances and close integration of our diplomatic, economic and military efforts. We backed all this up with robust investments — security never comes cheap. It worked, because we had to make it work.

Let's do the same with cybersecurity. The time to start was yesterday.