JANE HOLL LUTE AND BRUCE MCCONNELL SECURITY 02.14.11 7:00 AM

OP-ED: A CIVIL PERSPECTIVE ON CYBERSECURITY

JANE HOLL LUTE *is the Deputy Secretary of Homeland Security. Bruce McConnell is a Senior Counselor at the Department.*

How important is cyberspace? It is hardly possible to overstate it. The internet is an engine of immense wealth creation, a force for openness, transparency, innovation and freedom. Without it, generators stop turning, phones fall silent, critical goods sit on loading docks. Without confidence in the integrity of financial data or health information, the economy trembles. Without connectivity, tens of thousands of communities disappear from view; a deployed solider cannot see her daughter's swim victory, a multiple sclerosis patient is unable to confer with others about the latest medications, and first responders face an unknown chemical spill untethered.

Cyberspace functions as the very endoskeleton of modern life. So it's no surprise that when bad actors emerge to exploit or threaten it — whether profit-driven criminals, electronic saboteurs or international espionage rings — there's a temptation to define the threat in the strongest and simplest terms. These days, some observers are pounding out a persistent and mounting drumbeat of war, calling for preparing the battlefield, even saying that the United States is already fully into a "cyberwar," that it is, in fact, losing.

We disagree. Cyberspace is not a war zone.

Conflict and exploitation are present there, to be sure, but cyberspace is fundamentally a civilian space – a neighborhood, a library, a marketplace, a school yard, a workshop – and a new, exciting age in human experience, exploration and development. Portions of it are part of America's defense infrastructure, and these are properly protected by soldiers. But the vast majority of cyberspace is civilian space.

We're not just talking about the internet here. Complicated and vast, cyberspace is a rapidly growing, interconnected array of information and communications technologies (ICT), characterized by distributed ownership, dynamic connectivity, and diverse systems; its shape shifts instantaneously and organically. Though it relies on machines – e.g., servers – that are each physically somewhere, connected by communications technology that spans the globe, cyberspace is a place where geography matters differently, the reach of national law is incomplete, and the role of nation-states in its security is an open question.

Cyberspace is a new domain of human activity, and vital to the American way of life. For Americans to be able to act with confidence in cyberspace, it must be made more secure – an urgent outcome that requires a broadly distributed effort. Government must play an appropriate role, the contours of which society is still defining. Given cyberspace's overwhelmingly civilian nature, the Department of Homeland Security has an important role to play, and we explore that here.

CYBERSECURITY NEEDS A DISTRIBUTED APPROACH

No single actor has the capability to secure the largely privately owned virtual world that straddles national boundaries. Nor, for that matter, is such a role desirable. Indeed, considerable cybersecurity expertise exists in every part of the world.

For our part, the United States is fortunate to have tremendous cybersecurity capabilities in private industry as well as across the federal government. By law and policy, the Department of Homeland Security (DHS) has two specific roles in U.S. cybersecurity: to protect the federal executive branch civilian agencies (the "dot-gov"), and to lead the protection of critical cyberspace. And so today, for example, DHS' National Cybersecurity and Communications Integration Center is the hub of daily cyberincident management for the U.S. In addition, the Department of Defense, and in particular, the National Security Agency, is a unique national security resource and an essential participant in national, or global, cybersecurity solutions. Other U.S. government agencies also have significant capabilities. For example, U.S. law enforcement agencies, including the FBI, Immigration and Customs Enforcement, and the Secret Service have considerable experience and expertise in investigating cybercrimes and in identifying, pursuing, capturing and successfully prosecuting cybercriminals. Moreover, U.S. multinational firms operate global computer networks that are equipped to detect and respond to cyberintrusions and attacks. The combined knowledge of what's happening on these networks is a resource that can inform all network defenders of the current operational picture.

If the U.S. is to succeed in securing our identities and our information in cyberspace, it must build a system where the distributed nature of cyberspace is used in its own protection. With this perspective, for example, DHS has launched a national campaign – "Stop|Think|Connect" – to cultivate a collective sense of cyber–civic duty. The message begins with a simple wisdom: to ensure cybersecurity for all of us, each of us must play our part. Beginning with individual users, each of us must take the basic steps necessary to maintain our computers and our cyberlives in safety, just as conscientious drivers maintain their currency with driving laws, keep their tires properly inflated, and pay attention to highway conditions. Nearly everyone practices at least some level of cybersecurity, but these measures must also get easier; they are simply too hard right now.

Organizations and enterprises have similar responsibilities. Senior management in each and every office, company and department, whether private or public, must take responsibility for the protection of its own systems and information, by fielding up-to-date security technology, training employees to avoid common vulnerabilities, and reporting cybercrime when it occurs. For its part, the ICT industry must continue to innovate and improve security. Network, software, hardware and related service providers must accept the responsibilities that go with the considerable power they wield in cyberspace. Security must be built in, not added on; products must be shipped with strong security already activated, not disabled or inert; supply chains should be constructed to reduce the risk of product diversion or corruption; and, beyond the ICT industry, critical infrastructure providers must adopt security measures consistent with the threat. The demand for cybersecurity solutions is hardly decreasing; U.S. companies should lead the global market, creating jobs and making money.

DEFINING THE ROLE FOR GOVERNMENT

While America is deeply reliant on cyberspace, the health of this critical ecosystem is itself a work in progress. Indeed, tomorrow's threats and defensive capabilities have probably not yet been invented. Government must engage: to secure government systems, assist the private sector in securing itself, enforce the law, and lay the policy foundation for future success. Where industry lags, policy change can incentivize key actions. Today's environment does not, for example, adequately incentivize companies to write secure software. This must change.

In addition to taking these kinds of immediate steps, government has a role in the longer-term effort needed to change the structure of the internet and to leverage machines' very capabilities to enable agile, real-time notification, protection, quarantine, and response, subject to human-directed policies and controls.

Not everyone agrees with this approach. At one end of the spectrum, some say cybersecurity should be left to the market; that government should abstain from taking a stronger role vis-à-vis the private sector, so as not to stifle innovation or hurt U.S. competitiveness. We disagree. The market will not solve all problems. Indeed, in no other field does the market carry such a

burden, nor should it be expected to here. At the other end, you have the clarion call to treat cyberspace as a theater in a war. If only it were so simple.

We believe that the integrity, confidentiality and availability of information, systems and identities in such an environment must rest on a framework in which users, industry and government assume shared responsibility. There are no single-point solutions; rather, what is needed is a participatory framework in which the rules are clear, security is practical, and accountability is enforced – nationally as well as globally.

DHS has set out on a path to help build a cyber-environment that supports a secure and resilient infrastructure, enables innovation and prosperity, and protects openness, privacy and civil liberties by design. By bringing together other government agencies – including at the state and local level – private sector and non-governmental organizations, and countless individuals, DHS is enhancing today's cybersecurity and building tomorrow's. Over the longer term, DHS is focused on changing the entire cyber-ecosystem – not just technology, but also policy, procedure, practice, and law – to ensure that everything important in cyberspace is fundamentally more secure.

In close partnership with other agencies and the private sector, we are deploying the National Cybersecurity Protection System – of which the EINSTEIN intrusion detection system is a key component – to block malicious actors from accessing federal executive branch civilian agencies, while working closely with those agencies to bolster their own defensive capabilities. In doing so, we are creating layers of protection that will detect and avoid damage from a broad spectrum of threats. DHS also leads the effort to protect the nation's critical information infrastructure – the systems and networks that support the financial services industry, the electric power industry, and defense industrial base, to name a few. DHS is working with the federal agencies that have primary responsibility for each sector of the economy to ensure that the private sector has access to the technical resources it needs to protect itself, and that the government and industry are collaborating as partners to solve common problems. For example, DHS has spearheaded the development of the first-ever National Cybersecurity Incident Response Plan (NCIRP), for those times when passive defense does not suffice and a more active response is required. This plan, which was recently tested during the CyberStorm III national exercise, enables DHS to coordinate the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents of all levels of severity.

In all that we do, we are working to develop and leverage the position of the federal government to align incentives with the outcomes we want as a nation. Likewise, to address global shifts in technology and expectations, we believe any rules should set outcomes, not means. Such rules would apply regardless of technology, allow ample space for innovation, be clear, fair and broadly supported, and respect and reflect the richness of our diverse society. Having said this, we do not believe in cumbersome rule-making where the market is capable of acting more speedily and effectively – few changes would be more profound, for example, than broad adoption of voluntary, interoperable, privacy-enhancing authentication.

To build consensus for the future, DHS is working to stimulate and promote a broad public conversation about the nature of security and conflict in cyberspace. Such a national dialogue must consider the future of cyberspace and the role of government in shaping, safeguarding, protecting and preserving rights and freedoms there. How far should government's role extend? When, if ever, should government actively defend privately owned infrastructure assets? Do companies even need help from the government and, if yes, what do they need? How should government encourage firms to protect themselves and each other? In other words, is more government needed here, or less? In what areas? Questions like these are central to the future, and DHS is reaching out to partners at all levels to focus on them and translate that focus into solutions.

Our message is simple: cyberspace is vital to the American way of life, and DHS is positioning itself to do everything it can to build a cyber-ecosystem that is secure. Yet, we know that we cannot do all that needs doing. Responsibility for cybersecurity begins with each individual user and extends out to every business, school, and other civic and private enterprise. We believe in the vision – indeed, in the imperative, of an open internet. Yet, it cannot be an internet that is open but not secure, and we most assuredly do not want an internet that is secure but not open. We also believe that we – all of us – must move now, deliberately and thoughtfully, to realize this vision – a vision of confidence, not control.

The stakes are high. Criminals and hostile governments are putting their very best minds to work here. We must do the same so that cyberspace becomes a safe, secure, and resilient place where the American way of life can thrive.

Photo: Aijaz Rahi/Associated Press