Cyberspace National Policy Considerations

Kathryn Stephens, NSCI
November 16, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Issues

The United States government is still in the process of developing a cyber national policy. In an article for Government Computer News, former DHS Secretary Michael Chertoff stated the United States has not defined the responsibilities for maintaining situational awareness in cyberspace and that our nation lacks a decision-making framework for coordinating the government's response to a cyber incident. Chertoff also writes that there is no place to allow government defenders to collaborate with the private sector while responding to a cyber attack, and that current policy and legal constraints allow us to respond to cyber attacks in only two ways: the domestic-focused law enforcement approach or an international approach to neutralize attacks. Chertoff, who participated in the Bipartisan Policy Center's Cyber ShockWave simulation earlier this year, says the United States government must develop clear policies that define what the government can do in a cyber emergency, create public/private cybersecurity partnerships, form a national declaratory policy for cyberspace, and define an international regime of what is acceptable and unacceptable behavior in cyberspace.[1]

In an address at the EastWest Institute's seventh annual Worldwide Security Conference in Brussels, Chertoff discussed the main issues that are hindering a U.S. cyber policy. Chertoff says that attribution is a major hindrance, since it is often impossible to "distinguish between active direction by foreign officials and mere tolerance or lax enforcement." Even if attribution were not an issue, we need to define what options for response are available in case of a cyber attack. If a physical attack on the U.S. is always met with retaliation, how does that principle translate to cyberspace? Should cyber responses be limited to cyberspace, or are physical responses also on the table? Chertoff says these decisions need to be discussed and turned into a national declaratory policy that will govern U.S. cyber response actions. Chertoff says, "We must formulate an international strategy and response to cyber attacks that parallels the traditional laws governing the land, sea, and air. As we become increasingly interconnected and interdependent, we cannot postpone the debate until we are in the midst of a catastrophic cyber attack." Chertoff says that an international approach to governing cyberspace will help to foster international collaboration and transparency.[2]

Vice Adm. Bernard McCullough, 3rd commander of the Navy's 10th Fleet, says there are more issues when it comes to defining a framework for launching U.S. cyber attacks and defending military networks. McCullough says the military still does not know how to share cyber among the Army, Navy, Air Force and Marine Corps or how to provide network situational awareness of the battle space which would involve how knowledge is displayed and the interactions of the services' networks and the commercial network grid. "Maintaining situational awareness requires knowing what key systems need protecting, being aware of cyber-attack, and knowing the techniques, tactics and procedures for working through them." Former CIA director James Woolsey, Jr. adds that the

[1] Chertoff, M. (2010, March 10). *Cyber ShockWave exposed missing links in U.S. security.* Retrieved August 29, 2010, from Government Computer News: http://gcn.com/articles/2010/03/15/commentary-chertoff-cyber-shockwave.aspx

[2] *Cyber Attacks: International Responses.* (2010, February 17). Retrieved August 27, 2010, from EastWest Institute: http://www.ewi.info/cyber-attacks-international-responses

infrastructure is privately owned and resistant to government regulation, making it more difficult for the military to protect the power grid.[3]

A panel of government and private-sector experts at a five-day homeland security program hosted by the Heritage Foundation in Washington said the United States cannot defend itself in cyberspace because of the lack of policies and a legal framework for the cyber domain. According to the panel, "The national and international laws of armed conflict that govern conventional warfare don't adequately address issues raised about fighting a war online with digital weapons against enemies who cannot be identified." Herb Lin, chief scientist on the Computer Science and Telecommunications Board at the National Academies' National Research Council, says that although defensive cyber measures have been established, "...offensive action by the military will require policy decisions and legal authorities that have not yet been made."[4]

Ideas

Some experts, including former Carter and Clinton administration senior defense official Frank Kramer, believe that cyber deterrence could follow the nuclear deterrence model, which took years to develop. Harlan Ullman, an Atlantic Council Senior Advisor and chairman of the Killowen Group, says that cyberspace has very unique characteristics since, unlike nuclear, it is available to anyone with access to the Internet. Ullman and Kramer both recommend that a broad structure and framework for cyber policy and strategy be established, which would include input from both public- and private-sector experts with experience in philosophy, politics, strategy, and science.[5]

There are a few studies and guides that could be useful in developing cyber policy.

The Cyberspace Policy Review is the result of the 60-day cybersecurity review requested by President Obama in early 2009. It examined and assessed national cybersecurity strategies, policies and standards.[6] The Cyberspace Policy Review calls on the U.S. government to create a unified framework that would help to ensure a coordinated response from the Federal, State and local governments in case of a cyber incident. Implementation of a national framework would also have to include reporting thresholds, response and recovery plans and information sharing mechanisms.[7]

There is also the Comprehensive National Cybersecurity Initiative from the National Security Council, which was launched by President George W. Bush in January 2008. The CNCI's major initiatives include the establishment of a "front line of defense against today's immediate threats" through improved situational awareness and the ability to quickly reduce current vulnerabilities. The CNCI also calls for the enhancement of U.S. counterintelligence capabilities and strengthening cyber education and research and development.[8]

[3] Fulghum, D. (2010, May 19). *U.S. Completes Cyber-Attack Framework.* Retrieved August 27, 2010, from Aviation Week: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awst/2010/05/17/AW_05_17_2010_p26-225759.xml

[4] Jackson, W. (2010, August 26). *U.S. lacks legal framework to fight in cyberspace.* Retrieved August 31, 2010, from Federal Computer Week: http://fcw.com/articles/2010/08/26/heritage-panel-challenges-cyberwar-readiness.aspx

[5] Ullman, H. (2010, April 7). *Cyber Security Framework and Strategy Needed.* Retrieved August 26, 2010, from Atlantic Council: http://www.acus.org/new_atlanticist/cyber-security-framework-and-strategy-needed

[6] Hathaway, M. (2009, May 29). *Securing Our Digital Future.* Retrieved August 30, 2010, from The White House Blog: http://www.whitehouse.gov/CyberReview/

[7] *Cyberspace Policy Review.* (2009, May). Retrieved August 25, 2010, from WhiteHouse.gov: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[8] *The Comprehensive National Cybersecurity Initiative.* (n.d.). Retrieved August 25, 2010, from WhiteHouse.gov: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Cyberspace National Policy Considerations

Kathryn Stephens, NSCI
November 16, 2010

A paper from the 2010 C3E workshop held by the Office of the Director of National Intelligence and the National Security Agency also provides some valuable ideas for establishing a comprehensive cybersecurity framework. The paper, called “A Framework for Thinking about Cyber Conflict and Cyber Deterrence, with Possible Declaratory Policies for These Domains” discusses how cyber defense relates to traditional military doctrine. Author Stephen J. Lukasik writes that in traditional military doctrine, it is most important to control strategic territory, but that in cyberspace network connectivity is the same as traditional strategic territory. The paper also points out that some aspects of nuclear deterrence can carry over into a cyber deterrence policy. Lukasik says a defense must be feasible, the threat must be credible, and the defending nation must be able to actually carry out the response. The C3E paper also points out that a declaratory cyber policy could be the next step to creating an international treaty on cyber operations. Lukasik writes that we must assign a level of damage to cyber incidents. A simple outage, for example, would not be a significant incident because states would not collapse for a regular communication system problem. However, if communication system failures were widespread and coordinated, a nation could suffer considerably more damage. Physical damage to large, expensive, and difficult-to-replace equipment could also be considered significant.[9]

The Department of Homeland Security is also working with federal, state and industry partners to develop a National Cyber Incident Response Plan. According to Navy Rear Adm. Michael Brown, DHS deputy assistant secretary for cybersecurity and communications, says that DHS released the draft plan to its partners in December 2009, and the final steps of the plan were released and tested at Cyber Storm III, a cybersecurity drill conducted in September 2010. Brown also explained that one version of the DHS plan would be an annex to the National Response Framework and a second version would include more details.[10]

Answers

There are several considerations that must be made when establishing, declaring and executing cyber policy. The following are a few highlights, but by no means are they exhaustive.

It is important to clearly define the roles and responsibilities for the government and private sector in case of a cyber incident. The U.S. government responsibilities might include defending against network attacks, providing warnings of potential incidents and threats, sharing information including best practices, and analyzing new attacks and threats, to include attributing the source of attacks. In case of a cyber emergency, we must also consider how well we will be able to maintain communication and coordinate response and recovery efforts. A national cyber response framework should ensure we have adequate technical expertise to address cyber threats and attacks[11], and it is probable the private sector will have the bulk of cyber experts.

There is also the obvious issue of attribution, since the effectiveness of any framework or response plan would be limited without being able to attribute the source of an attack. Attribution is especially important since a national response would likely be different if the attack came from a terrorist group or individual than the response to a foreign state launching a national cyber attack. A national framework for responding to cyber incidents would also need to define the process for a cyber attack that comes from an individual or independent group. How would we defend against an attack or launch a counterattack against an individual or independent group?

[9] Lukasik, S. J. (2010, July 22). *A framework for thinking about cyber conflict and cyber deterrence, with possible declaratory policies for these domains.* Retrieved August 30, 2010, from C3E: https://www.c3e.info/uploaded_docs/c3e_declaratory_policyv41.pdf

[10] Bain, B. (2009, December 09). *DHS releases cyber incident response draft plan.* Retrieved August 20, 2010, from Federal Computer Week: http://fcw.com/articles/2009/12/09/web-national-cyber-incident-response-plan.aspx

[11] *Cyber Incident Annex National Response Plan.* (2004, December). Retrieved August 28, 2010, from learningservices.us: http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf

Any national cyber framework would also have to address privacy right concerns. To what extent should citizens be willing to surrender their privacy in case of a cyber emergency or attack?

When establishing a cyber policy, it is important to remember that any capabilities used to threaten an adversary must be credible, meaning we must have some way to prove that we can carry out our threats. This is not always possible in cyberspace, especially since any exhibition of cyber force that would deter a potential attacker might entail causing significant, or unpredictable, damage. Cyber deterrence is hindered by the fact that there is no way to prove capabilities or determine the extent of an adversary's capabilities without causing actual damage.

Different declaratory policies regarding cyber attacks have advantages and disadvantages. The C3E paper from Stephen Lukasik discusses the dangers of establishing a line where we would be required to respond to any act that went over that line. Not responding to any situation that crosses the line would then have an impact on American credibility, which could be crippling to a cyber deterrence strategy. An example of a cyber declaratory policy could follow the vision of the International Telecommunication Union, which would say that since information system resources are critical for global discourse, the availability of information resources should not be impeded. There are disadvantages to this policy, of course, such as the controversy that could arise when claiming that access to information resources is basically a human right.[12]

An example of a very extreme cyber declaratory policy could be that any strategic electronic communication attack on the U.S. would be considered a use of force under Articles 41 and 42 of the UN Charter and that the U.S. would then be entitled to employ self defense through air, sea or land forces as necessary to restore peace and security.

There is no doubt a national policy regarding cyberspace is overdue. However, the considerations are admittedly numerous and complex. The government should continue to encourage collaboration among government departments, private industry, and academia to ensure a national cyber policy is robust, yet flexible, and enhances our national security at a reasonable cost. Absent a national cyber policy, we are "making it up as we go" - which is not in our best interests over the long term.

[12] Lukasik, S. J. (2010, July 22). *A framework for thinking about cyber conflict and cyber deterrence, with possible declaratory policies for these domains.* Retrieved August 30, 2010, from C3E: https://www.c3e.info/uploaded_docs/c3e_declaratory_policyv41.pdf