ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Les Bloom and John E. Savage[1]

AUGUST 2011

CYBER STATECRAFT INITIATIVE

On Cyber Peace

Introduction

The best deterrence to cyber conflict is to aggressively pursue national and international risk mitigation at the same time that we explore a full-spectrum of cyber capabilities. Nations should strive to reduce the emerging cyber arms race by developing a basis for trust. The international community has already taken useful steps in this direction with, for example, the European Convention on Cybercrime and the UN report on cyber security which calls for a set of actions that would make information infrastructures more secure.

As a first step in reducing the risk of conflict, each nation must do an internal assessment of their exposure to attack. This requires a thorough and candid review of their Critical Infrastructure Areas. Second, they must take steps to increase the security of hardware and software. Third, they need to work together with other nations to share information, especially in times of crisis, and to establish norms of behavior.

Finally, a national and international effort to improve the cyber security of computers and networks is in the United States' interest. The development of a new high assurance hardware and software industry has the potential to create technologies, spawn companies, and generate employment.

The Nature of the Cyber Security Problem

Cyberspace has characteristics that are unique among the many domains in which nations compete. As a consequence, experience with other domains, such as the Cold War, does not directly apply. The key tenets of the cyber domain are:

Absolute cyber security is impossible. Today, a determined adversary can penetrate almost any computer or router that is connected to the Internet. Computers and networks were not designed with security as a first priority. While many techniques have been developed to increase security, many have not yet been incorporated into products and others, to be effective, are best run on 64-bit machines. While we now have methods of computing on data that is encrypted and never decrypted except at the destination, these methods, while promising, are currently very inefficient. One indication of the difficulty of securing computers is that it is theoretically impossible to create a program that can tell if another program is virus-free[2], even though in practice it is possible to identify most viruses.

Computer networks are fragile. Small changes, accidental or intentional, can seriously disrupt global communications. The Border Gateway Protocol (BGP) is used to move IP packets across the Internet. Numerous examples exist of unintentional global redirection of packets. When the Pakistan government banned access to YouTube in 2008, a Pakistani ISP announced to a domestic audience that YouTube packets were to be sent to a black hole in Pakistan. This announcement leaked and YouTube packets globally were sent to this black hole. That is, all contact with YouTube disappeared.

Communication networks are globally connected. An individual aggressor can reach around the world in seconds to attack an Internet-based target. In the massive 2007 attack against Estonian organizations it is reported that compromised computers in more than 100 countries generated packets involved in the attack.[3]

---

1 Les Bloom is the lead for Internet Governance for the Chief Information Officer of the Department of Defense. John Savage is the An Wang Professor of Computer Science at Brown University. During the 2009-2010 academic year, John was a Jefferson Science Fellow at the Department of State. The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the Department of Defense, the Department of State or the U.S. Government. This paper is cleared for public release, distribution unlimited.

2 This fact uses Rice's Theorem.

3 BBC News, 17 June 2010.

Critical infrastructures have been connected to the Internet. Resources, such as banking systems and electrical grids, are now readily accessible globally. While the magnitude of the risk of this accessibility has not yet been fully evaluated, an early indication is reflected in the highly sophisticated Stuxnet worm, discovered in 2010 and targeting SCADA systems. One of its targets appears to be the Iranian nuclear industry. If so, this is ominous. Some see it as the first salvo in a new cyber arms race.

A culture of cyber crime has developed. Criminals with minimal computer skills can now acquire technology from experts and deploy it to defraud companies and individuals all over the world.

Commercial espionage jeopardizes national economies. Espionage has grown rapidly. Countries whose economies are heavily dependent on intellectual property (IP), such as the United States, are at serious risk of loss of IP theft.

Hardware and software are at risk of being compromised by foes. This problem is known as the "supply chain problem." It has grown in importance as the computer industry has globalized. Certifying commercial-off-the-shelf (COTS) hardware and software for security is very challenging and time consuming. A new product may take years to certify.

Botnets present a national security threat. The large number of compromised computers on U.S. soil can be used against American interests. It is estimated that at least 1,200 botnets reside in the United States as of January 2010, much more than any other nation.

Attribution on the Internet is notoriously difficult. Proxies, drop points, and peer-to-peer networks, among others, make it very easy to hide the identity and origin of an attacker. Thus, retaliation against an attack becomes problematical.

All cyber actors, be it government, corporate, or private, must consider these key tenets when considering strategies and policies to reduce and manage the risk of conflict in the cyberspace domain.

Domestic Issues

Each nation needs to protect its critical infrastructures from cyber attack, monitor malicious activity on domestic computers and networks, reduce the number of compromised computers, create economic, legal and regulatory frameworks designed to increase cyber security, and increase research and development on cyber security.

Protection of Critical Infrastructures. Protecting critical national infrastructures (CNIs) from attack, whether by criminals, terrorists, or nation states, is vital. In the United States 85% of the CNI is privately owned. The United States needs to heed the call from the 2009 Cyber Security Review and UNGA Second Committee Resolution A/C.2/64/L.8 of 20 November 2009 and provide mechanisms for the U.S. government to collaborate with the private sector to better secure the CNI. Also, the United States must identify the portions of its civilian and military critical infrastructures that are at greatest risk of damage during attack and find ways to both protect and isolate it from civilian infrastructures so that the latter do not suffer collateral damage from attacks on the military CNIs.

Creation of Threat Reduction Centers. Responses to threats and attacks begin with situational awareness. Not only must attacks against computer systems be catalogued and reported, as is done by Cyber Incident Response Teams (CIRTs), assessments must also be made of the global health of the Internet. These assessments need to be shared with governments and network operators who need to be aware of the location of attacks and network disruptions. Although many organizations, including private corporations, monitor the Internet and do have data repositories against which to compare its current status, it does not appear that there is a common set of standards for data collection and presentation. Such standards would make it easier to produce a "dashboard" that can quickly summarize the health of cyberspace.

When good situational awareness is available, an early warning system can be developed that produces reliable reports of emerging problems. Such a system would make it possible to catch and correct problems that arise naturally or are intentional. The Pakistani YouTube incident described earlier would be much more quickly discovered and corrected. Similar incidents have occurred as a result of

BGP announcements. Two occurred within two weeks in March and April 2010 when ISPs in China leaked routes that censored Twitter, Facebook and many other sites.[4]

Threat reduction centers can also provide advice to network operators and large organizations on proven methods of countering computer intrusions and network disruptions. Sharing best practices with other national CIRTs can help to develop this advice. National authorities need to understand the fragility of the global Internet so that steps can be taken to make it more stable.

As part of threat reduction, state and federal police authorities should be trained to identify, pursue, and apprehend cyber criminals in cooperation with police authorities from other nations. Cooperation of this kind is called for in the Council of Europe Convention on Cybercrime.

Reducing the Number of Compromised Computers. When ISPs sign contracts to provide Internet service to customers, they impose certain restrictions on their subscribers. Because botnets represent a national security threat, ISPs should have the authority to quarantine machines known to be part of a botnet or at least flag them as having been compromised. Knowledge of the IP addresses of compromised machines can be used as a defensive mechanism.

Today any vendor is allowed to sell any machine equipped with any software to any customer who then can place the machine on the Internet without meeting any safety requirements. This is akin to the situation when the automobile was first introduced. Because of the hazards of driving vehicles that fail to meet minimal safety requirements, today automobiles must meet U.S. federal requirements before they are sold. To remain on the road, they must be inspected regularly.

Although it is too early to put stringent safety requirements on computers connected to the Internet, it is in our collective interest to start down this path. We could begin by requiring customers to update critical software in which vulnerabilities have been detected and repaired by the vendor. Enforcement could be put in the hands of ISPs who could be subject to penalties for failure to police their networks. This would allow for an arms-length relationship between governments and the private sector in this sensitive area.

Establishing Economic, Legal and Regulatory Frameworks. Hardware and software companies together with the U.S. government should begin to examine economic, legal and regulatory frameworks that might be eventually established to ensure that computers and networks are safe from intrusion. As a first step, vendors should be put on notice that they will eventually be liable for security vulnerabilities in their products. To avoid overburdening the computer industry, liability might be applied in stages to companies based on size and to families of products based on levels of adoption. For example, basic operating systems might be the first products to be incorporated into such a framework followed by hardware and software systems based on use.

Vendors of hardware and software systems must be obligated under penalty of law to promptly repair their systems and make the repairs available to their customers and national CIRTs. If they cannot fix their systems within a reasonable period of time, they should inform national CIRTs of the situation so that other solutions might be found and, if necessary, the public can be warned.

The responsibility of computer owners to maintain their Internet-based computers should also be recognized under law. Penalties for failure to meet this requirement should be sanctioned under law.

Attacks against the U.S. critical infrastructure should be criminalized. The widespread distribution of malware by private citizens for use as offensive weapons should also be criminalized. This rule is not meant to prevent individuals from studying malware or sharing it with limited groups of individuals. The purpose of this rule is to discourage the large-scale distribution of malware.

Legislation should be drafted requiring that each owner of a portion of the U.S. critical infrastructure be responsible to meet minimum cyber security requirements. A Federal agency specializing in cyber security should be assigned responsibility to enforce these requirements.

4 See http://blogs.forbes.com/firewall/2010/04/09/is-china-testing-cybernukes/

Within the USG cabinet officers must be made personally responsible for execution on their cyber security mandates. This requirement should be extended to government contractors. Serious penalties for failure to comply should be set.

Research and Development. Our knowledge today of cyber security is limited. We lack a general theory that explains how to make computation secure and which provides measures for the amount of security that is provided by a given system. In short, we need a science of cyber security.

A new high level of support for research and development is needed now. Proven ideas must be moved into practice and new ideas to protect computers from intrusion and networks from being exploited must be invented.

Researchers are pursuing a great variety of cyber security topics. Below are a few research areas of particular importance:

1) *Techniques to prevent buffer overflow.* It is estimated that buffer overflow is used in 30-40% of malware.

2) *Methods to make computers look like moving targets.*[5] The goal is retain functionality but reconfigure a computer often enough that vulnerabilities move between the times that reconnaissance has been completed and exploitation begins.

3) *Efficient methods to compute securely even after computers have been compromised*. For example, a blacklist of sites suspected of originating or controlling malware could be used to prevent communication with these sites, thereby decapitating the malware.

4) *Methods to improve the security of the Internet*. As mentioned, major instabilities in the Internet have been caused by the intentional or inadvertent misuse of the Border Gateway Protocol (BGP), the procedures for communication between network providers. Research is needed to find methods to secure BGP communication that are practical and acceptable to providers globally.

5) *Improved attribution using technical means*. For example, friendly nations might agree to securely sign packets so that in times of crisis packets that are not signed can be discarded.

6) *Improved attribution using psychological means*. The behavior of cyber criminals, such as their working hours and the holidays they observe, might be used to identify them over an extended period of time.

7) *Economic incentives encouraging compliance with cyber security requirements.*[6] Insurance companies that offer fraud, interruption, and information loss policies might collect actuarial data from customers to better estimate their losses and reduce their prices. Customers would have incentives to seek guidance from insurance companies on best security practices.

8) *Legal and economic disincentives that reduce spam and cyber crime*. Some of these were mentioned above, such as sanctions on ISPs and individuals to keep their networks and computers clean.

Coping with Barriers to Adoption

Organizations and individuals that believe that it is in their interest to preserve the status quo will erect substantial barriers to cyber risk reduction. No one wants a question asked if they can't stand the answer. Overcoming this organizational and individual resistance will require innovative coping mechanisms. These mechanisms need to be organized around the behavioral principles of: amnesty, community, internal transparency, fencing, competition, de-globalization, enforcement, and international norms. The Y2K response is a good model for the change that is needed to make cyberspace secure.

A Role Model. Change is difficult and often thought to be impossible. However, a classic example of change in which the United States played a starring role was Y2K. Much like cyber, Y2K cut across multiple sectors and required far-reaching cooperation. A similar approach is needed to implement cyber risk reduction. Key factors in the Y2K framework were a) broad, inclusive participation across sectors (government, private, and civil), b) a highly

5 Funding for the Moving targets theme has been recommended for inclusion in the FY 2012 budget.

6 This is another theme proposed for FY 2012 funding.

transparent process, and c) timelines and metrics with which to gauge effectiveness of the overall effort. Clear expectations and milestones were set and individuals, particularly in government, were held accountable for meeting these expectations and milestones. However, the cybersecurity problem is much more serious. It is the equivalent of Y2K all the time.

Amnesty. Players around the world could easily spend the next five years pointing fingers and assessing blame for our current cyber vulnerabilities. This approach would only create resistance to risk reduction. Since there is enough blame to tar every cyber stakeholder, we propose that a domestic amnesty be declared and international amnesty encouraged. This amnesty would protect all U.S. commercial/academic stakeholders, individuals and organizations, from any liability due to their part in creating or enabling any cyber vulnerability. The amnesty would take effect on a mutually agreed date and would cover only acts that occurred before that date.

Community. As mentioned above, cyber affects the U.S. critical infrastructure, which means that it affects all citizens, not just a select few. Therefore the best way to allay inclusion concerns is through a national risk reduction effort that involves representatives from non-government and government cyber stakeholders.

Internal Transparency. Any national cyber effort requires that the broadest range of stakeholders be in the room. That includes those that would normally be excluded. For any national cyber risk reduction effort to succeed it must be recognized by the public that it is honestly addressing the problem without flinching, without spin, and without deception.

In Y2K representatives from oversight organizations, namely, those from congressional committees, Government Accountability Office, Inspectors General, Executive Office of the President, State and local Governments, and commercial and non-commercial partners, forged an alliance that produced the desired outcome. The result was an almost incident free Y2K rollover.

Fencing. The quickest way to kill our nation's ability to deal with cyber problems is to politicize the process. Fences need to be erected that ensure that cyber become a politics free zone. What this entails is that no political party or any other cyber stakeholder, individual or organizational, will take credit for any forward progress; instead, the entire stakeholder community will become the sole beneficiary of credit.

Fencing mechanisms help to ensure that the normal competitive and self-aggrandizing political instincts of many stakeholders are held in check. The concept of fencing applies to any systemic issue: if one wants to make progress, have the stakeholders agree that the community will take the credit for achievements and that individuals and specific organizations will not.

Competition. The new demand for high assurance cyber hardware and software will lead to the development of new industries devoted to satisfying that demand. Since cyber vulnerabilities are a worldwide problem, we expect numerous competitor nations to copycat risk reduction efforts instituted by the U.S., resulting in massive worldwide economic benefits.

New industries created to develop, produce, distribute, use, maintain and dispose of high assurance products (the *product life cycle*) do not have to compete with existing product lines. An enormous range of low and medium assurance cyber products are currently produced by a vast number of existing companies. High assurance products, like luxury automobiles that have been grafted on to existing product lines (think Lexus, Acura and Infinity), could be produced in assured facilities by the same companies.

Cyber has an almost unlimited future demand curve and this will not be limited to the high assurance line. We believe that there will be continued strong demand for low and medium assurance products dependent upon their intended use; not everyone wants or needs the highest level of assurance but in critical infrastructure applications there is a blue ocean of potential demand waiting to be satisfied.

De-globalization. High assurance cyber products require that supply-chains be known and managed and that they be as free as possible from contamination and disruption by competitor nations. Manufacturing key hardware components at home and writing critical software domestically can achieve this. This has potential for an enormous positive economic impact on domestic employment rates.

As the high assurance demand space evolves, facilities to support the life cycle of these products will have to be created. This will require a workforce that is trusted and capabilities that are free from competitor disruption. These characteristics call for facilities to be established in the homeland of each competitor nation. Existing overseas facilities for the low and medium assurance product lines will remain where they are; but the high assurance facilities will usher in era of reversing the security issues associated with globalization.

Enforcement. Amnesty for failure to avoid cyber vulnerabilities in the past does not imply that this behavior will be tolerated in the future. To avoid this will require enforcement. It can be done in the United States using a well-publicized national cyber scorecard; by partnering with congressional committees to verify that scorecards are accurate and uncover serious hazards; by highlighting and rewarding those who are doing well; combining audit staffs from the GAO and Inspectors General to do audits; producing white papers and retrospectives that show trend lines; application of penalties for cyber risk reduction non-compliance: revocation of personal security clearances, which affects current and post-government/industry employment; and revocation of Site Certifications, which basically closes down government/commercial organizations.

International Approaches to Cyber Security

Nations need to work collectively to reduce the possibility of cyber conflict. First, they must agree on an expanded list of international norms of behavior. Second, they must share knowledge of threats and the status of the Internet's health with other like-minded nations. They should also establish hot lines for use in times of crisis and collaborate on research to make their networks more robust and computers more secure.

Establish International Norms of Behavior. Nations should cooperate to combat the criminal misuse of the Internet, to help develop a global culture of cyber security, and to take other steps designed to reduce risk including measures such as sharing of incident data, and engaging in best practices. These steps will help to establish a basis of trust that will reduce the risk of conflict during times of tension. Other issues that will help to keep the peace are described below.

Nations should have understandings concerning the use of computer and communications technologies during warfare. That is, they should agree that certain parts of cyberspace are civilian and off limits during both peace and conflict.

Espionage is legal under international law. Because the technical means to conduct espionage and those for exploitation and conflict are almost identical, nations should take steps to distinguish between them, if possible. If such distinctions can be made, exploitations will not be confused with attacks and potential threats eliminated.

Create International Early Warning Systems. As mentioned earlier, it is desirable that nations maintain a mutually agreed upon cyber early warning system. Such a system would alert nations to problems that are emerging, such as errors in BGP announcements, communication outages, and outbreaks of serious attacks. A steady stream of shared information about the status of the cyberspace would help to reassure nations during times of crisis.

Each nation has interest in controlling crime on its territory. Cybercrime is international and requires international collaboration to deal with it. Thus, it is in every nation's interest to participate in controlling it.

As mentioned above, the Internet is currently unstable. It is too easy to redirect traffic, spoof addresses, and launch denial of service attacks. It is in the collective interest of nations to maintain the health of cyberspace. Thus, nations should engage in discussions to address these instabilities.

Nations can also profitably share their national approaches to legislation on computer security and agree on common terminology to improve the communications about computer networks.

Help the Developing World. As the developing world obtains access to the Internet, they will need to learn the importance of keeping their software up to date and employing all the safeguards that are commonly deployed in the developed world. If they come online in large numbers and don't immediately follow established security practices, they will provide a large number of machines that can easily be compromised. This is the situation that is emerging along the western coast of Africa. Undersea cables are being installed that will provide high-speed access to many countries that are very likely to be unprepared for the consequences.

The Role of Diplomacy. Diplomacy will play a role in implementing each of the proposals in this section. As mentioned in the Introduction, important steps have already been taken to develop legal frameworks to cope with international cybercrime, to encourage a culture of cybersecurity, and to initiate discussions of norms, reduce the risk to critical national infrastructures, the use of cyber technologies during warfare, sharing of national approaches to cybersecurity, and helping the developing world, among other things. All nations should be encouraged to increase their commitments to these efforts in these areas. Diplomacy can be very helpful in avoiding cyber conflict and, should it occur, reduce its effect on nations in conflict. It can help to protect critical civilian infrastructures and limit the scope of an attack.

Developing a High Assurance Software and Hardware Industry. As noted earlier, we believe there is a strong latent demand globally for high assurance hardware and software. National interests require that for high security applications the supply chain be secure. This necessarily argues for the de-globalization of key parts of the hardware and software industries. When coupled with the natural competitive instincts of nation states, this should result in the development of new high assurance domestic industries. Such industries have the potential to reduce unemployment, increase tax revenues and be a positive engine for worldwide economic growth.

Establish Security Levels for Cyberspace Products. High assurance software and hardware will be produced by existing and new companies to more stringent practical security standards. For example, no competitor nations will be involved in the development, production, distribution, use, maintenance, and disposal of products. Code will have to be thinned down and have less functionality so that it is easier to assure its reliability. It will have to be hacker-tested and approved with a DEFCON Seal of Approval and required to be used in all national critical infrastructure functions.

Use Government Purchasing Power to Set Standards. The demand within Federal, state, and local critical infrastructure sectors will create a market for high assurance products. Using their purchasing power, they can set standards which other market sectors can exploit. Bipartisan legislation may be necessary to ensure that the domestic critical infrastructure meet high assurance standards.

Conclusions

Cyberspace is highly insecure. It will remain so for the foreseeable future. We will have to contend with cyber threats and vulnerabilities for a long time. Even if diplomacy maintains cyber peace between all competitor nations, there will always exist non-aligned bad actors. Therefore it is in the interest of self-protection that existing and planned offensive and defensive cyber activities be continued by each competitor nation.

In our lifetimes cyber will continue to be the principal enabler of world commerce, social relationships, and security. Offensive and defensive capabilities must continue to evolve much as they have in a nuclear dominated world. We have maintained the nuclear peace not by disarmament but through risk reduction combined with modernization of each competitor nation's offensive and defense capability. What has worked for 65 years for a nuclear world can also work for one that is dominated by cyber.

The Atlantic Council of the United States is a non-partisan organization that promotes constructive U.S. leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.