The American
Foreign Policy Council
Defense Technology Program Brief

September 2013 | Washington, D.C. | No. 1

Cybersecurity: New Threats and Challenges

By Dr. Abraham R. Wagner

Briefing Highlights

In 1992 the net became far more user friendly. The U.S. government moved from being the net's chief sponsor to its largest user, but they failed to provide adequate security measures. An early generation of mischievous "hackers" was now replaced by skilled cyber criminals, often operating from foreign locations.

…

Threats to cyberspace come from a variety of sources: "Hackers" of various skill levels; disturbed individuals; criminals whose primary objectives are the theft of money or data; and state and non-state actors (such as terrorist organizations) who are developing cyberwarfare capabilities.

…

Neither the recent Executive Order or the Presidential Policy Directive 21 (PPD-21) come with funds attached and assign responsibilities to the Department of Homeland Security (DHS) and the National Institute of Science and Technology (NIST) – rather than NSA and CYBERCOM.

…

Legislation currently pending before the U.S. Senate and House contain many of the critical elements of a long term solution. Solving the problem first requires increased investment in education for cybersecurity, in much the same way the nation responded to the Cold War challenge of the "space race."

In recent years the vast expansion of cyberspace, not only in terms of user but content and applications, has brought about a set of new threats and challenges never anticipated by the net's designers. At the outset of this technological revolution access to the net was only through a few connected mainframe computers; there was literally nothing to steal or attack; and no infrastructure was connected to the net. Cybersecurity was simply not an issue.

With the transition to the worldwide Internet, and the evolution of e-commerce as well as content of every type imaginable, cyberspace became a lucrative venue for criminals and provided an important set of targets for attack as military and intelligence services became major net users. This new world presents a serious set of challenges which need to be addressed. The present analysis is focused on three key points:

- *Security, privacy and infrastructure protection in cyberspace involve a complex set of legal, technical, economic, and national security issues. All of these are dynamic.*
- *The legal regime for cyberspace is generations behind the technology and threat environment.*
- *Outcomes really matter. The integrity of the national infrastructure and security of the nation are closely tied to solving these problems.*

Stages in Cyberspace Evolution

At the outset in the 1960s the "net" was an experiment in network optimization undertaken by the Advanced Research Projects Agency (ARPA – later DARPA) which looked at the concept of switched packets instead of traditional line switching. The early ARPAnet, as it was known, connected the mainframe computers at a few universities and other contractors, with no way to access the net externally for years, and no content of appeal to criminals or hackers. Cybersecurity in this era consisted of a few ARPA efforts to "break" the net, simply to test the software.

Federal funding in 1989 enabled a rapid transition from the ARPAnet to the Internet along with an explosive growth in e-mail, the web and related applications never anticipated.

Related technologies now allowed a growing base of computers and local

Dr. Abraham R. Wagner *is Professor of International & Public Affairs at Columbia University, and Senior Research Scholar at Columbia's Arnold A. Saltzman Institute of War & Peace Studies. He served for over 30 years in various U.S. Government posts at the National Security Council, the Intelligence Community, and Department of Defense, including the Defense Advanced Research Projects Agency (DARPA) at the time of the transition to the Internet.*

area networks to connect to the net with greater bandwidth and at far lower costs. The proliferation of personal computers as well as commercial Internet service providers (ISPs) made net access easy and affordable. Businesses, educational institutions, the Government and others all installed computers connected to local and later wide area networks which then connected to the Internet, providing global connectivity. For the first time in history, the marginal cost of worldwide communications fell close to zero.

"National security users quickly embraced cyberspace and networked systems as they were highly cost-effective and offered a range of important capabilities, but initially failed to recognize and deal with a host of critical vulnerabilities."

The development of the web protocol and browser after 1992 brought a new era to cyberspace. The net became far more user friendly, with both content and applications being added to the net at a blinding speed. E-commerce, electronic banking, and other applications quickly provided lucrative targets and there was suddenly a great deal to steal. An early generation of mischievous "hackers" was now replaced by skilled cyber criminals, often operating from foreign locations beyond the reach of U.S. law.[1]

This era also saw the U.S. Government move from a net sponsor to its largest user. Virtually all government agencies, offices and the military recognized the utility of the net and rapidly adopted cyberspace as both a communications medium as well as a means for data storage. Here the government quickly became "the pig at the trough" in terms of utilizing the net but failing miserably to provide for its security and safety. Little wonder that potential adversaries began investing in cyber warfare capabilities in light of major security vulnerabilities that were scarcely secret.

One additional stage in cyberspace development has been the increasing connection of what has been termed critical infrastructure to the net. Included here are SCADA systems such as power grids, sewer systems, and a host of others.[2] The vulnerability of critical infrastructure to attack and the need to protect it is not new. Indeed, a review of the problem during the Clinton Administration produced PD/NSC-63 (1998) but little in the way of tangible results. The most recent Executive Order on the subject (2013) as well as the related Presidential Directive PPD-21 are remarkable similar in tone and substance, but also short on a concrete program and essential funding to accomplish this goal.[3]

Cybersecurity – The Lost Decade

It would be hard to fault ARPA for not investing the limited resources available in the early days in cybersecurity, since at the outset the "net" was simply an experiment with no significant content. At the time there were also no commercial or national security applications. Security and privacy were not essential elements of the original net design and much what was done in the aftermath can be characterized as "too little, too late."[4]

With the transition from the ARPAnet to the Internet after 1990, however, and the virtual explosion in terms of the user base as well as net-based content, this situation changed radically as there was now "stuff to steal" as well as a multitude of users to annoy and a rapidly growing potential for real damage. Hackers and others now had access to the net, and in fact organized themselves into shadowy and clandestine groups.[5] Threats to cyberspace come from a variety of sources, ranging from bored high school kids to well-trained military units assigned to cyberwarfare missions. The most important categories of such threats include:

- "Hackers" of various skill levels whose ultimate objectives include annoying people, disabling individual computers, damaging files, insertion of malicious code or "malware." stealing data, and disrupting service;
- Disturbed individuals, such as fired systems administrators who seek retribution against their former employers;
- Criminals whose primary objectives are the theft of money or data (such as credit card numbers, account information, or identity); and
- State and non-state actors (such as terrorist or-

ganizations) who are developing cyberwarfare capabilities.

It is increasingly clear that cyberspace needs to be a secure and safe environment and the essential protections have not kept pace with the explosive growth in the net. While the net's original architects at ARPA never envisioned the current uses, and saw no need for security, they also did not have adequate resources to make security part of the system. They did fund several key initiatives, such as the Computer Emergency Response Team (CERT), but were never able to provide a secure and protected infrastructure.

National security users quickly embraced cyberspace and networked systems, as they were highly cost-effective and offered a range of important capabilities, but initially failed to recognize and deal with a host of critical vulnerabilities. Among these users the Defense Department, the Intelligence Community and State Department did avoid connecting systems containing classified data to the open Internet in any way where they could be "hacked" and sensitive data removed.[6] While these agencies have largely moved to networked computers, they use separate classified networks (such as SIPERNET) to connect authorized systems and users and are protected with high-grade encryption and other security features.[7]

"Threats to cyberspace come from a variety of sources, ranging from bored high school kids to well-trained military units assigned to cyberwarfare missions."

Second, all national security users – including a large contractor base – depend on the commercial Internet for their actual connections and packet transfers. Thus while the data and their networks may be secure, the vulnerability to attack on the overall infrastructure remains.

Cybersecurity has become an essential element of life in the wired world, which is a highly dynamic one. Both the technology base and the threats to it continue to evolve. System architectures are increasingly moving to a cloud concept, while more serious threats from cyber criminals, cyber warriors and cyber terrorists across the globe continue to grow.

For the most part the 1990s can be seen as a lost decade for cybersecurity with far too little being done by either the government or industry to address the rapidly evolving threats. A net that was never designed to be safe and secure was now being used for everything from banking to military operations. Sensitive data and operations were wide open to a host of vulnerabilities with exceedingly little being done to meet them.

This was a time of both bad policies and missed opportunities. In short, cyberspace was not treated as a national resource. Everybody involved thought it was somebody else's job to fix it. Both the government and commercial users largely ignored the vulnerabilities and risks. Underlying this fatal approach was a widespread assumption within the government that industry which had become highly dependent on the net would recognize the need for security and pay to fix the problems. Within industry there was the equally flawed assumption that the government which had been most generous in developing the net, would return to pay for its repair. Clearly both were wrong. The commercial world was quick to adopt the net and offer a vast range of applications, but was largely unwilling and most often uninterested in paying to secure it. Even large banks failed to address the problem until they had been robbed of massive sums of money.[8]

It is not the case that nothing was done. ARPA, which had now become DARPA, funded some limited efforts such as the computer emergency response team (CERT) and some network improvements, but funding was not on the scale that was needed in response to the growing threats. Nor is it at all clear that it was DARPA's job to fix it. By this time the U.S. military and the Intelligence Community, not to mention every other government agency, had become massive net users but invested almost nothing in securing the net.[9]

In large part the drive to make cyberspace secure, safe and private is being driven by user demands. The growth of e-Commerce and business applications brought new demands for security, and the proliferation of networked systems by the Government for national security and re-

lated uses also required secure networks and applications to high standards. Vulnerabilities in almost all hardware and software areas were identified while new threats continue to be identified on a daily basis.

Industry did develop various security products to deal with such problems as malicious code or "malware." These products offered to protect users and remove suspicious code such as viruses, worms and Trojans from infected computers. Other firms offered encryption software, such as PGP, enabling their users to protect sensitive files while a secure version of the web protocol enabled "secure" transactions. Cyberspace was becoming safer and more secure for many users, but the adversarial threat was advancing as well.

Escalating Threats in Cyberspace

While early threats included youthful hackers and disgruntled employees, it was not expected that cyberspace would become a major venue for warfare. Nonetheless both state and non-state actors have developed cyberwarfare capabilities capable of both conventional types of attacks as well as clandestine attacks and espionage.[10] China and other nations continue to develop cyberwarfare capabilities because it makes good sense for them to do so. As the U.S. has become increasingly dependent on net infrastructure it presents a lucrative target set for any adversary. At the same time building a cyberwarfare capability such as the Chinese PLA Unit 61398 requires very little in the way of equipment and facilities compared to other military operations. The only key element is the recruitment of skilled and trainable personnel.

"...all national security users depend on the commercial internet... Thus while the data and their networks may be secure, the vulnerability to attack on the overall infrastructure remains."

While the Chinese case has received increasing media attention this past year, they are not alone and several "axis of evil" states have dramatically increased their hostile cyber activities. North Korea (DPRK) has escalated attacks against the South (ROK) while Iran is building similar capabilities both in response to the STUXNET attacks on that nation's nuclear facilities as well as a general desire to attack potential adversaries such as Israel and the U.S.

Apart from established nation states there is increasing concern that non-state actors and terrorist organizations such as *al Qaeda, Hamas* and *Hezbollah* will acquire the resources to engage in cyber attacks of various kinds. While such organizations may have an eighth century ideology, they are not reluctant to utilize twenty-first century technology. Depending on the quality of the attacks, they may avoid detection for some period of time and in some cases avoid attribution as the attacker entirely. In terms of cyber defense, the issue of timely and accurate attribution is essential. Without the ability to rapidly identify an attacker with a high degree of accuracy an effective response becomes almost impossible.

At present, there is still debate among experts as to the exact nature of future attacks and possible targets. Some authorities foresee the possibility of what they term a "Digital Pearl Harbor" where national and international infrastructures are seriously at risk. Others see an even more serious scenario where an attack on the net not only disrupts some services, but corrupts the data on the network to the extent that it can no longer be relied upon.

Meeting the Challenge

One by-product of the 9/11 terrorist attacks was a new appreciation in the national security community of how critical cyberspace was for both terrorist operations as well as defensive operations. Various programs that have recently received a great deal of media attention at the National Security Agency (NSA) were undertaken as a response to these new threats. Closely related to the NSA programs were the establishment of a unified military command (CYBERCOM) which was co-located with NSA and the NSA Director was also designated as the CYBERCOM Commander.

In addition to this unified command, the individual military services have also established a number of individual service components including the 14th Air Force; the 67th Network Warfare Wing; the Navy 10th Fleet; and the 2nd Army. After a decade of inadequate funding and atten-

tion, these actions demonstrate a significantly increased level of attention and programmatic effort on the part of the military services that are now taking the prospect of a future cyber war far more seriously.

The past decade has also seen significantly increased spending within other elements of the Department of Defense as well as other government agencies including the Department of Homeland Security and others. At

"In terms of cyber defense the issue of timely and accurate attribution is essential. Without the ability to rapidly identify an attacker with a high degree of accuracy an effective response becomes almost impossible."

DARPA, birthplace of the net, a new series of programs with substantial funding are addressing a range of cybersecurity issues that support requirements at NSA, the military services and other users.

Within the past two years the White House has undertaken an overall review of cyber security issues that led to a recent Executive Order and Presidential Policy Directive (PPD-21).[11] To what extent these latter two actions will produce tangible results remains open to question. Neither the recent Executive Order or the PPD come with funds attached and assign responsibilities to the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) – rather than NSA and CYBERCOM. Critics argue that DHS and NIST lack the resources and skills needed for this major assignment and are likely doomed to fail.[12]
The good news is that network technology is largely asymmetrical and favors the defense. It is also the case that the U.S. created this monster and knows the technology well while many of its adversaries are not as technically sophisticated. In theory, at least, protection is easier than penetration and here both the technology and economics are on the side of cyber defense. It is also the case that the world is still in the "Wild West" days of cyberspace and many things are still not well-settled. Topics like Internet Governance are still in the early stages of development and questions about "who is in charge" are not entirely settled.[13]

Over the longer term it is likely that many of the pressing cybersecurity problems can be solved if the nation gets truly serious about meeting the challenge. In part it means taking a system and set of protocols that were never designed to be safe and secure and transforming them into ones that are, and meet the evolving needs of users worldwide.

Legislation currently pending before the U.S. Senate and House of Representatives contain many of the critical elements of a long term solution.[14] Solving the problem first requires increased investment in education for cybersecurity, in much the same way the nation responded to the Cold War challenge of the "space race." Cybersecurity demands the very best minds and here it is essential to provide the incentives for the best minds to enter the field and obtain the skills needed to solve these complex problems. The nation's universities are simply not going to do it on their own, and will require Government support if the country is to succeed here.

The Government also needs to accelerate existing cybersecurity programs with essential management and resources. It must recognize that it can't legislate security – it must fund its development and implementation in the areas of security, resilience and privacy. The nation needs

"Legislation currently pending before the U.S. Senate and House of Representatives contain many of the critical elements of a long term solution. Solving the problem first requires increased investment in education for cybersecurity, in much the same way the nation responded to the Cold War challenge of the space race."

to move from yet another high level Executive Order and Presidential Directive to actual effective programs. At the same time it needs to further refine a strategy for cyberwarfare. The current state of affairs still confuses what are done under Title 10 (Military Operations) and Title 50 (Intelligence Operations) since activities in this area

utilize personnel and techniques from both the military as well as the Intelligence Community.[15] Certainly the establishment of CYBERCOM and related activities are a good start but a great deal more needs to be done.

Finally, meeting the challenge of cybersecurity requires a strong partnership with industry. It is essential to bear in mind that industry built the net and they will fix it. By and large the Government can only write checks – not computer code. Even the military and intelligence agencies are largely dependent on their contractor base in this critical area. The search for a solution is driven by both threats and user demands, both of which are constantly changing. Policies and programs must be responsive to them if the challenge is to be met.

Endnotes

1. It is perhaps a strange coincidence that the birth of the Internet came at the same time as the demise of the Soviet Union, with many of the most serious cyber crimes emanating from the former Soviet Union.

2. SCADA is the acronym for ***s**upervisory **c**ontrol **a**nd **d**ata **a**cquisition*, a computer system for gathering and analyzing real time data, and used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

3. Presidential Decision Directive/NSC-63 *Critical Infrastructure Protection* (The White House, May 22, 1998), *Executive Order – Improving Critical Infrastructure Cybersecurity* (The White House, February 12, 2013), and Presidential Policy Directive/PPD-21 *Critical Infrastructure Security and Resilience* (The White House, February 12, 2013).

4. It may come as a surprise to many that e-mail was not even part of the original design, and the e-mail protocol (SMTP) was an unfunded personal project of BBN employee Ray Tomlinson. This did not, however, stop ARPA from ultimately incorporating SMTP and e-mail into the system.

5. The hacking community has itself evolved into a large and growing subculture, with an annual convention (DefCon) held in Las Vegas. The convention began in 1992 as Dark Tangent and has grown enormously since.

6. In the now famed *Wikileaks* scandal an individual with security clearance used a flash drive to remove classified data from a secure computer, for which he is now facing espionage charges. These are personnel and hardware security issues, rather than a cybersecurity one by most accounts.

7. There is the separate issue of e-mail among national security personnel. Early on many of these users did in fact use commercial services, such as AOL and others, regarding sensitive matters. Violations of security procedures were often gross and flagrant. More recently, the agencies have adopted secure, classified e-mail accounts to support their users. While most users now have several accounts, and keep their commercial ones, hopefully the level of security violations has been reduced.

8. The prime example here is CitiBank which was robbed by Russian cyber criminals of a large and still undisclosed amount of money before taking corrective measures.

9. Both the military and the Intelligence Community constructed classified networks, such as SIPRNET and JWICS which incorporated encryption technologies which they believed made

them invulnerable, only to learn this was not entirely the case.

10. See, for example, Mandiant, *APT1 – Exposing One of China's Cyber Espionage Units* (2013) for an excellent analysis of the development of PLA Unit 61398.

11. See here *Executive Order – Improving Critical Infrastructure Cybersecurity* (The White House, February 12, 2013), and Presidential Policy Directive/PPD-21 *Critical Infrastructure Security and Resilience* (The White House, February 12, 2013)

12. There is also the legal issue that it makes no sense to separate defensive and offensive cyber operations, and that the latter require the legal ability engage in "Title 50" activities (covert intelligence operations) and that DHS and NIST are not authorized to do so.

13. An early analysis of this problem can be found in Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006).

14. This is not a partisan issue, and both the bills before the Senate and House all contain important and useful elements. Included here are the *Cyber Intelligence and Protection Act (CISPA)* (H.R. 3523 – Rogers); the *Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act (PRECISE)*(H.R. 3674 – Lungren & McCaul); the *Cybersecurty Act* (S. 2105 – Lieberman-Collins); and the *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information & Technology Act (SECURE-IT)(*S. 2151 – McCain-Fengold).

15. See, for example, Andru E. Wall, "Demystifying the Title 10-Title50 Debate: Distinguishing Military Operations, Intelligence Activities and & Covert Operations," Harvard Law Review (2011).

Defense Technology Program Brief

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at Harrison@afpc.org.

About AFPC

For over three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

CONTACT

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org