The American Foreign Policy Council
Defense Technology Program Brief

January 2015 | Washington, D.C. | No. 8

Redefining Cybersecurity

By Trey Herr and Allan Friedman

Cybersecurity Topic Clusters

Information Assurance – Securing computers and networks, including critical infrastructure. This covers the technologies and tactics, as well as education, certification requirements, and design techniques, used to secure applications and networks in private and public sector organizations.

• • •

Internet Security Governance (ISG) – All forms of international collaboration over security issues, including how to maintain a secure and functional Internet and cross-national challenges like export controls for malicious software and arrest of foreign nationals.

• • •

Cybercrime – Law enforcement and regulatory action to either pursue attackers or reform victims. Covers the prosecution of cybercriminal groups, asset seizure, data breach notification, and standards for reporting cyber incidents. Importantly, any attacks or tools that can cause damage are not found here but covered under Military Cyber Operations.

• • •

Military Cyber Operations (MCO) – The organizations, policy, and law related to deploying destructive digital or physical effects on target computer systems or defending against such. Covers both defensive and offensive cyber effects operations.

Cybersecurity is an often abused and much misused term that was once intended to describe and now serves better to confuse. While originally intended to cover security related issues associated with "cyberspace," a phrase coined by author William Gibson in the short story "Burning Chrome," it has become the byword for a staggeringly diverse array of topics[1]. While this is frustrating, the term is popular as shorthand, so we offer this paper to identify and explain four clusters of related topics under the larger umbrella of "cybersecurity."[2] Each is a distinct issue area with unique technical and policy challenges, while retaining some association to the others.

"Cybersecurity" is not special. It encompasses a complicated set of policy issues, most of which are motivated not by fantastic technology challenges but by the uncertain integration of Internet-enabled activities and actors into existing laws and policies. The complexity of "cybersecurity," in other words, comes less from the devices we use than from the people behind them. And many of the problems outlined under each of the clusters (in the box to the left) are simple, but hard to solve.

Topic Clusters

These clusters are defined in opposition of each other. As the graphic below demonstrates, the left-hand column contains two that focus on securing the networks and systems we use, their contents, and the policies that underlie their operation. The right-hand column focuses on offensive action against attackers, whether state or non-state, across a range of circumstances.

Defensive Focus	*Offensive Focus*
Information Assurance	**Cybercrime**
Internet Security Governance (ISG)	**Military Cyber Operations (MCO)**

The key distinctions between Information Assurance and Internet Security Governance is the former's focus on software and network applications, which are both domestic issues, whereas the latter necessarily has an international scope as it deals

Dr. Allan Friedman *is a Research Scientist at the Cyber Security Policy Research Institute (CSPRI) at George Washington University's School of Engineering. He is the co-author of* Cybersecurity and Cyberwar: What Everyone Needs to Know. ***Mr. Trey Herr*** *is a senior research associate with CSPRI and a PhD candidate in political science at George Washington University. He consecutively works as an adjunct researcher at the Institute for Defense Analysis.*

with security of the Internet's underlying architecture, as well as export controls and international legal action. Between Cybercrime and Military Cyber Operations, the key is that within Cybercrime, actors may harass, disrupt, or even steal information but do not cause permanent damage or harm people; under MCO, they do.

Information Assurance

How do you secure the software and hardware that make up a network? This is the principal question for the Information Assurance cluster and a major focus of most "cybersecurity" professionals in the technical community. The work can be tedious and uncertain, for example reverse engineering the latest strain of malware; or it can be simple and repetitive, such as making sure users in a system change their passwords every three months. Information Assurance includes writing secure software, deploying it safely, and managing it to minimize the risk of compromise. The key principles are Confidentiality (that the information on a computer remains secret), Integrity (meaning a system operates the way it is supposed to), and Availability (that the computer system is ready and able to function when needed).[3]

When Target was breached in 2013, malware was able to enter the company's point of sale (POS) systems not because of some "Mission Impossible"-style covert operation but because someone clicked on the wrong attachment. A third party company which supplied heating and ventilation control services to Target inadvertently disclosed login credentials to a billing website that sat on Target's corporate network.[4] Using this server as a launch pad, attackers were able to move their code onto POS systems around the country. Securing the third party vendor's systems, as well as Target's corporate network, against these sorts of attackers were Information Assurance challenges, for which there are a broad array of standards and practices. Add to this the problem of building secure software, of finding vulnerabilities and patching them in existing software, and of managing IT infrastructure, like cloud email services, and you get a tremendous volume of less exciting but highly relevant cyber security topics.

Critical Infrastructure Protection (CIP) falls under Information Assurance as well. For all of the special challenges that emerge with trying to secure industrial control systems and related technology, the basic steps are similar: isolate and protect key applications from the Internet, remove or patch vulnerabilities in software, and make sure users don't break anything. There are differences between the software in your laptop and that used to control industrial systems, but the distinction is only a fraction of what it was a decade ago, and continues to shrink. For some sectors, standards of protection and practice already exist, like for companies involved in electrical power generation and transmission who operate under security standards developed by the North American Electric Reliability Corporation (NERC).[5] For others, like financial services, they are still evolving.

This Information Assurance cluster also covers workforce issues, like how to educate and certify professionals for these jobs. One historically contentious issue is whether to require practical experience and on the job training, like airline pilots who obtain thousands of hours in progressively larger aircraft, or to treat Information Assurance professionals like lawyers, whose professional credibility comes from hundreds of hours of grueling coursework and testing. Information Assurance is a cluster of topics focusing on the design of secure software, defense of information systems and networks against compromise, and the challenge of educating people for these tasks. While not the most headline grabbing, these are bread and butter topics for security professionals and constitute the majority of defensive "cybersecurity" activity in organizations on any given day.

Internet Security Governance

The Internet crosses national and jurisdictional boundaries, so to take legal action outside of our borders or implement new protocols can require the involvement of other state and non-state actors.[6] This topic cluster considers two broad types of issues:

1. Technical agreements and the process of drafting, approving, and promulgating technical security standards and policies across the Internet's architecture

2. Legal agreements, like the use of export controls to restrict the flow of malware components or international collaboration to share threat information

Internet Security Governance (ISG) covers technical and legal security issues that focus on standards or challenges that affect or require the involvement of more than a single country. ISG is similar to Information Assurance in that it covers many technical security topics related to the Internet as a whole rather than individual computer systems and networks. But it differs in its inclusion of legal and diplomatic issues. This topic cluster is different from Internet governance, which deals with free speech issues like content control and the broader administrative challenges of the Internet, which are not security issues per se.

The ability to pass information over the Internet in a secure manner underpins the modern economy, from online retail to personal banking. Transport Layer Security (TLS) is a protocol that allows computers to create encrypted links over the Internet and communicate securely. When a computer connects to an Internet service, such as an online bank using TLS, the bank responds with a certificate containing a cryptographic key, establishing it is indeed the intended bank and not a fraudulent site waiting to steal user's data. These certificates are issued and verified by a small number of large firms which have already proven vulnerable to compromise. In July of 2011, a certificate authority called DigiNotar released a fraudulent certificate for Google that Iranian intelligence services used to intercept information from more than 300,000 Google Mail users. Investigations into the incident revealed that hackers had breached DigiNotar earlier and manipulated the firm's automatic services to issue dozens of certificates for Yahoo, Mozilla, and Tor, among others.[7] As this demonstrates, Internet Security Governance covers a range of technical and legal topics, the underlying theme of which is that they focus on Internet-wide security issues and challenges requiring international collaboration.

Cybercrime

The Target and Home Depot data breaches were spectacular examples of a long-running effort by criminal groups to build a better hammer in order to smash the proverbial storefront and steal customer payment information. This game of cat and mouse between retailers and payment processors, on the one hand, and criminal groups on the other has been ongoing since the birth of the retail industry on the Internet. The defensive efforts of firms to secure their systems fall under the Information Assurance cluster, but the activities of their attackers and the legal requirements for data breach notification and liability are Cybercrime topics.

Actors in this cluster are interested in anything short of destructive attacks; stealing valuable intellectual property as part of industrial espionage, financial fraud and credit card theft, or even disrupting services for ideological goals ("hacktivism"). From a policy perspective, this cluster includes the legal basis for law enforcement's efforts to track and prosecute criminal who operate over the Internet, including the Racketeer Influenced and Corrupt Organizations (RICO) Act[8] and the Computer Fraud and Abuse Act (CFAA).[9] It also covers the agencies involved with these efforts, as well as substantive issues like the markets available to buy and sell malicious software and the standards for data breach notification and insurance for private companies. Cybercrime includes issues like the legal status of private firms collaborating with Federal agencies in incident investigations and the legality of law enforcement use of hacking tools to obtain information for criminal prosecution or private companies taking security into their own hands as part of an effort to "hack back".

Cybercrime is the topic cluster for oft-reported incidents of information theft from individuals and firms like the Stratfor email breach[10] as well as hacking and harassment incidents like the Lizard Squad's distributed denial of service (DDOS) attack against Microsoft and Sony game

console services after Christmas of 2014 .[11] Importantly, this cluster does not cover attacks that cause damage or harm people (a very small fraction of the total). In terms of the total cost of attacks, Cybercrime represents a far greater portion of the total than the last cluster, Military Cyber Operations.

Military Cyber Operations (MCO)

Military Cyber Operations (MCO) covers the acquisition and use of cyber capabilities in both the strategic and operational realms by states or non-state actors. This involves finding and exploiting vulnerabilities in software and establishing long term access to systems in use by potential targets. At the strategic level, this could involve attacks against critical infrastructure like nuclear weapons refining[12] or heavy industrial facilities.[13] At the operational level, military organizations may use cyber capabilities to target enemy air defense systems.[14]

One well recognized set of issues covered by cybersecurity are those surrounding the development and use of cyber capabilities by states and non-state actors to injure or kill individuals and destroy data or equipment. This cluster covers not only the organizational and budgetary issues involved with US military operations in cyberspace but also the legal and normative constraints on all states and non-state actors.

A recent issue that has emerged in the MCO cluster is the question of how the government acquires and uses software vulnerabilities. The same software vulnerability in Internet Explorer that could be used to pull together a cyber weapon for use against a foreign power may also enhance US security, in both Federal and broad commercial applications, if Microsoft is made known and can patch the vulnerability. The Stuxnet attack on Iran's centrifuge facility is the most prominent recent example of a cyber weapon in use, but while a popular reference in discussions on "cybersecurity" the potential for physically destructive attacks is small, largely because of the complexity involved in crafting the tools required.[15]

This cluster also involves the recruitment and training of the military's cyber operations personnel, across all five services, defense against destructive cyber attacks from other states and non-state actors, as well as the legal and diplomatic environment related to the use of cyber weapons.

Destructive Effects vs. Espionage

There is a substantial difference between the effort required and effects generated in information theft and the attempt to harm individuals or destroy data or physical equipment. Likewise, the policy challenges posed by the two issue areas are distinct.

Actions, whether from state or non-state actors, that attempt to destroy digital information or physical hardware fall into the realm of Military Cyber Operations and can be treated as a national security issue. Efforts to steal information, even if organized by states, fall into Information Assurance, where public and private organizations are primarily responsible for defending data and the state may play a role in reinforcing their security operations. Breaking things with code is difficult and requires a great deal of substantive expertise about the target. Writing software to steal keystrokes or credit card information is comparatively easy, and happens far more frequently.

Information Sharing Up vs. Down

Information sharing has been a major policy focus for the Federal government in the past several years, but there are two very different sets of activities that have been part of the discussion. Information sharing "up" encourages private groups and firms to share their network activity and suspected malicious traffic with the government so that the military and intelligence communities can better understand the national security environment. This sort of persistent large scale network observation and awareness is a Military Cyber Operations topic; it is for situational awareness of national networks for national security purposes.

Information sharing "down," on the other hand, is the process of government intelligence and analysis being shared with relevant private sector actors who may be

potential targets, in order to reinforce their security capabilities and awareness. These activities fall under the Information Assurance cluster, examples of which can be seen in monthly DHS efforts to share threat analysis with industrial control system owners and operators.

Each of these two avenues reflect different goals with distinct outcomes. It is important to understand the difference between asking private actors to share information with the Federal government and passing along threat information and security techniques developed within government to private actors.

National Security vs. Law Enforcement

Much of the language surrounding "cybersecurity" attracts military oriented language. Incidents become attacks, tools become weapons, criminals become attackers, and so on. One problem with this approach is it can raise the importance of largely pedestrian events to the level of national security crises, skewing the distribution of resources and attention. The breaches at Target, Home Depot, and (as appears increasingly possible[16] [17]) Sony Pictures, were undertaken by small groups with the intent to steal information and, at least in the case of Sony, wreak havoc on their target by attempting to disable information systems on the way out. These incidents, and hundreds more like them every year, involve non-state actors stealing information from or disrupting the business activities of private actors across the country and around the world. These groups and their tools are pursued by law enforcement agencies, especially the U.S. Secret Service, and when possible, prosecuted. This type of theft and harassment activity vastly outstrips the amount of destructive malicious activity directed at private or public organizations every year.

This paper serves as a basic explanatory tool for these topic clusters. Future pieces in this series will go into more detail on each cluster and highlight proposed and potential legislative avenues to implement policy solutions to the pressing problems.

Endnotes

[1] "Burning Chrome," Wikipedia, January 22,2015, http://en.wikipedia.org/wiki/Burning_Chrome; William Gibson, "Burning Chrome," Omni Magazine, July 1982, https://archive.org/stream/omni-magazine-1982-07/OMNI_1982_07#page/n37/mode/2up.

[2] Mike Masnick, "The Cyberpolitics of Cyberbellicosity Cyberpushing Cybersecurity to Cyberprevent Cyberwar," TechDirt, June 14, 2012, https://www.techdirt.com/articles/20120614/01590919314/cyberpolitics-cyberbellicosity-cyberpushing-cybersecurity-to-cyberprevent-cyberwar.shtml.

[3] "What is Security Analysis?" Imperial College London, January 22, 2015, http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm.

[4] "Email Attack on Vendor Set Up Breach at Target," Krebs on Security, February 14, 2014, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

[5] "CIP Standards," North American Electric Reliability Corporation, January 22, 2015, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[6] Sarah Pillai, "What is IPSEC and how IPSEC does the job of securing data communication," Root.in, July 27, 2013, http://www.slashroot.in/what-ipsec-and-how-ipsec-does-job-securing-data-communication.

[7] Dan Goodlin, "Fraudulent Google Credential Found in the Wild," Register (UK), August 29, 2011, http://www.theregister.co.uk/2011/08/29/fraudulent_google_ssl_certificate/.

[8] "Racketeer Influenced and Corrupt organizations," 18 U.S. Code §96.

[9] "Fraud and related activity in connection with computers," 18 U.S. Code §1030.

[10] Jim Finkle, "Stratfor Hackers Publish Email, Password Data," Reuters, December 30, 2011, http://www.reuters.com/article/2011/12/30/us-usa-cyberattack-stratfor-idUSTRE7BT10Z20111230.

[11] "Xbox and Playstation Resuming Service after Attack," BBC, December 27, 2014, http://www.bbc.com/news/uk-30602609.

[12] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired, July 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[13] "Hack Attack Causes 'Massive Damage' at Steel Works," BBC, December 22, 2014, http://www.bbc.com/news/technology-30575104.

[14] Ward Carroll, "Israel's Cyber Shot at Syria," Defense Tech, November 26, 2007, http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/.

[15] Herr, Trey "PrEP: A Framework for Malware & Cyber Weapons" Journal of Information Warfare 13, no. 1, February 2014, 87-100, http://bit.ly/1hUOReC.

[16] "Sony Breach Linked to Cashier in the Sony Gift Shop," January 22, 2015, http://sony.attributed.to/.

[17] Nicole Perlroth, "New Study May Add to Skepticism Among Security Experts That North Korea was Behind Sony Hack," New York Times, December 24, 2014, http://bits.blogs.nytimes.com/2014/12/24/new-study-adds-to-skepticism-among-security-experts-that-north-korea-was-behind-sony-hack/?_r=0

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