

How to Survive in a "No-win" Cyberwar

John Steensen

Senior Director, Technology Audit, Visa Inc.

Cybersecurity Essentials – E23



Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is set against a background illustration of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers. The word "CyberSizelT" is written in a large, stylized font where the letters are interconnected. The "C" and "S" are significantly larger than the other letters. The text is colored in a gradient from dark red to light red, with a white outline.

INTRODUCTION



Trust in, and value from, information systems

San Francisco Chapter

A stylized illustration of the San Francisco skyline, including the Golden Gate Bridge, the Transamerica Pyramid, and other buildings, set against a warm, yellowish-orange background.

CyberSizeIT

Disclaimer

The opinions expressed in this presentation are those of the author and may not represent those of his employer. This information is provided for educational purposes only and should not be construed as offering legal advice. Please consult your legal representative to discuss your individual situation. The companies, products and service names used in this presentation are for identification purposes only. All trademarks and registered trademarks are the property of their respective owners.

John Steensen, MBA/TM, CISA[®], CRISC[™]

John Steensen is a Sr. Director of Technology Audit at Visa Inc. His primary focus at Visa is on managing technology-centric audits providing assurance and validation of the control environment and ensuring adherence to corporate and industry standards. His computer security background spans more than three decades and has directed the design, engineering and implementation of highly secure 4-9's multinational infrastructure (data centers and networks) spanning North America and Europe. He has also worked as a computer forensics examiner and as a civilian contractor for the Drug Enforcement Agency's El Paso Intelligence Center (EPIC) as well as at the US Army White Sands Missile Range on secure projects. Mr. Steensen is a Certified Information Systems Auditor (CISA[®]) and is Certified in Risk and Information Systems Control (CRISC[™]). He holds a BS degree in Computer Science from North Carolina State University and an MBA from the University of Phoenix with a specialization in Technology Management. He is recognized as an audit profession thought leader and speaks by invitation at national and local audit profession conferences and forums. Mr. Steensen invests in the audit profession by volunteering as a member of the Board of Directors for ISACA San Francisco Chapter and by working as a voting member of ASTM's E11 Committee on Statistics and Quality, which sets the world's standards for sampling and quality control.

What Are You Up Against?



An arms bazaar like in Tomorrow Never Dies?

<http://www.imfdb.org/images/thumb/b/b2/Tnd-ak2.jpg/600px-Tnd-ak2.jpg>

What Are You Up Against?

Experts call it the “cyber arms bazaar” — an Eastern European underground market in hacking tools, viruses and other forms of infiltration and cyber sabotage that has been developing with little Western attention for around 15 years.

“The most sophisticated shadow economy in the world as it relates to the deep Web services and hacking tools is by far in Eastern Europe,” said Tom Kellehermann, chief cybersecurity officer at security research firm Trend Micro.

The overall cybercrime market long ago surpassed the worldwide illicit narcotics trade as a money maker and is now **surpassing a half trillion dollars in annual value**. The majority of that can be traced back to the cyber arms bazaar in Eastern Europe.

<http://thehill.com/policy/cybersecurity/235726-feds-search-for-ways-to-impede-cyber-bazaar>

A Unique Approach

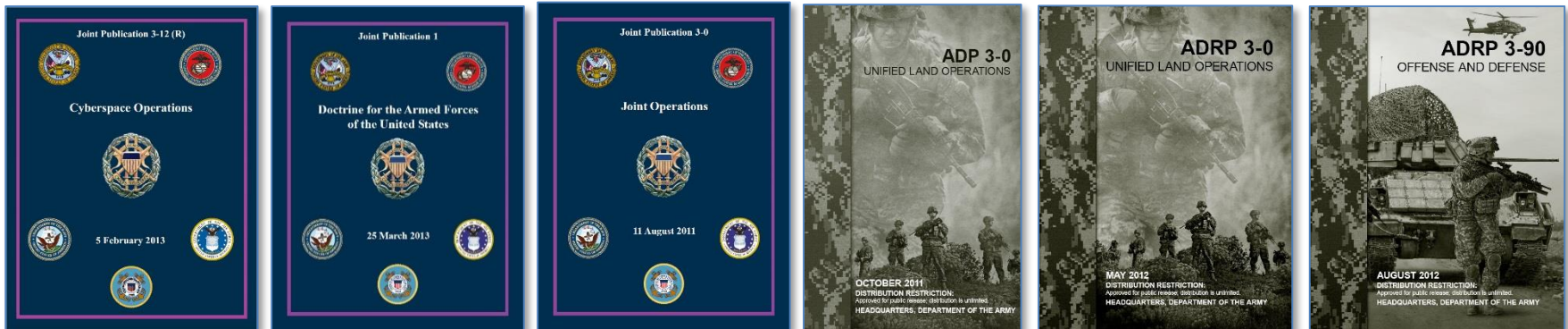
- What if you could get tens of millions of dollars of free consulting to improve your companies cyber security posture?
- What if you could get, for free, cyber security playbooks that went from strategy to planning to tactics that are being used by some of the largest organizations in the world?
- You can!

And A Unique Partnership

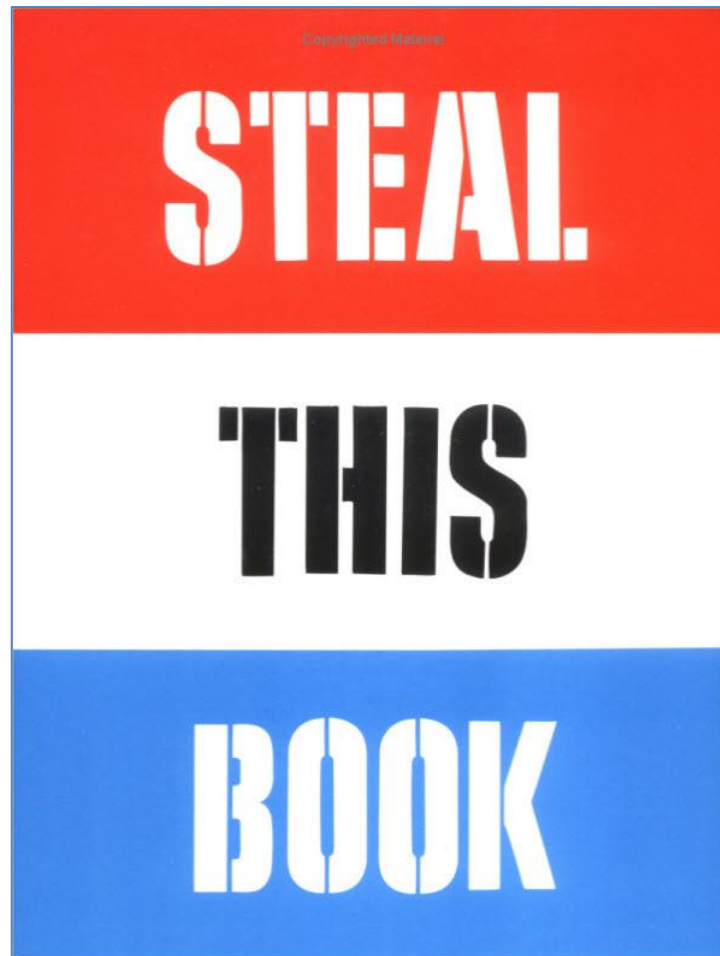
- If you are going to be in a war who do you want on your side?
- Vendor product and marketing managers?
- Vendor salespersons?
- Consultants?
- No, WARRIORS!

Who Are You Going to Call?

- Today we're going to discuss some ways to utilize resources you've already paid for!
- From your friends at the U.S. Department of Defense.



This Says It Best



Session Objectives



CYBER WAR – WHAT IS IT?

Or

How Do You Fight What You Can't Define?



Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is set against a background illustration of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers. The word "CyberSizelT" is written in a large, stylized font where the letters are filled with a red-to-orange gradient and have a white outline. The "T" is significantly larger than the other letters.

CyberSizelT

What is War?

The Merriam-Webster dictionary defines "war" as:

- a state or period of fighting between countries or groups
- a situation in which people or groups compete with or fight against each other
- an organized effort by a government or other large organization to stop or defeat something that is viewed as dangerous or bad

Source: <http://www.merriam-webster.com/dictionary/war>

No, Really - What is War?

War is socially sanctioned violence to achieve a political purpose.

- War can result from the failure of states to resolve their disputes by diplomatic means. War historically involves nine principles, collectively and classically known as the principles of war (objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity).

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

What is Cyber Warfare?

Cambridge Dictionaries Online defines cyber warfare as “the activity of using the internet to attack a country’s computers in order to damage things such as communication and transport systems or water and electricity supplies”

- The use of cyber warfare can destabilize financial systems, the telephone system or the energy grid.
- Cyber warfare has fundamentally changed national security because an attack can come from anywhere.

Source: <http://dictionary.cambridge.org/us/dictionary/english/cyber-warfare>

Why Do We Wage War?

- Because war works
 - at least in the short term!
- Out of necessity – we must engage if we are attacked.
- We put a lot of resources into waging war so war is good for business
 - at least in the short term!

Insight from “The Fifth Element”



Zorg: Life, which you so nobly serve, comes from destruction, disorder and chaos. Now take this empty glass. Here it is: peaceful, serene, boring. But if it is destroyed -

[Pushes the glass off the table. It shatter on the floor, and several small machines come out to clean it up]

Zorg: Look at all these little things! So busy now! Notice how each one is useful. A lovely ballet ensues, so full of form and color. Now, think about all those people that created them. Technicians, engineers, hundreds of people, who will be able to feed their children tonight, so those children can grow up big and strong and have little teeny children of their own, and so on and so forth. Thus, adding to the great chain of life. You see, father, by causing a little destruction, I am in fact encouraging life. In reality, you and I are in the same business.



Priest Vito Cornelius: You're a monster, Zorg.

Zorg: I know.

Source: <http://www.imdb.com/title/tt0119116/quotes>

How Did We Think About War?

The earliest known principles of war were documented by Sun Tzu, circa 500 BCE.

Machiavelli published his "General Rules" in 1521.

Henri, Duke of Rohan established his "Guides" for war in 1644.

Marquis de Silva presented his "Principles" for war in 1778.

Henry Lloyd proffered his version of "Rules" for war in 1781 as well as his "Axioms" for war in 1781.

Then in 1805, Antoine-Henri Jomini published his "Maxims" for War ver. 1, "Didactic Resume" and "Maxims" for War ver. 2.

Carl von Clausewitz wrote his version in 1812 building on the work of earlier writers.

Source: https://en.wikipedia.org/wiki/Principles_of_war#United_States_principles_of_war

How Do We Think About War?

The United States Armed Forces use the following nine principles of war (1-9) and three principles of operations (10-12). Together these are called the Principles of Joint Operations.

1. Objective
2. Offensive
3. Mass
4. Economy of Force
5. Maneuver
6. Unity of Command
7. Security
8. Surprise
9. Simplicity
10. Perseverance
11. Legitimacy
12. Restraint

Source: U.S. Armed Forces Joint Publication 3-0, Joint Operations, August 11, 2011

1. Objective

- Direct every military operation toward a clearly defined, decisive, and attainable objective.
 - The principle of objective drives all military activity. At the operational and tactical levels, objective ensures all actions contribute to the higher commander's end state. When undertaking any mission, commanders should clearly understand the expected outcome and its impact. Combat power is limited; commanders never have enough to address every aspect of the situation. Objectives allow commanders to focus combat power on the most important tasks.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

2. Offensive

- Seize, retain, and exploit the initiative.
 - As a principle of war, offense is synonymous with initiative. The surest way to achieve decisive results is to seize, retain, and exploit the initiative. Seizing the initiative dictates the nature, scope, and tempo of an operation. Seizing the initiative compels an enemy to react.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

3. Mass

- Concentrate the effects of combat power at the decisive place and time.
 - Commanders mass the effects of combat power in time and space to achieve both destructive and constructive results. Massing in time applies the elements of combat power against multiple decisive points simultaneously. Massing in space concentrates the effects of combat power against a single decisive point. Both can overwhelm opponents or dominate a situation. Commanders select the method that best fits the circumstances.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

4. Economy of Force

- Allocate minimum essential combat power to secondary efforts.
 - Economy of force is the reciprocal of mass. Commanders allocate only the minimum combat power necessary to shaping and sustaining operations so they can mass combat power for the decisive operation. This requires accepting prudent risk. Taking calculated risks is inherent in conflict.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

5. Maneuver

- Place the enemy in a disadvantageous position through the flexible application of combat power.
 - Maneuver concentrates and disperses combat power to keep the enemy at a disadvantage. It achieves results that would otherwise be more costly. Effective maneuver keeps enemy forces off balance by making them confront new problems and new dangers faster than they can counter them.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

6. Unity of Command

- For every objective, ensure unity of effort under one responsible commander.
 - Applying a force's full combat power requires unity of command. Unity of command means that a single commander directs and coordinates the actions of all forces toward a common objective. Cooperation may produce coordination, but giving a single commander the required authority is the most effective way to achieve unity of effort.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

7. Security

- Never permit the enemy to acquire an unexpected advantage.
 - Security protects and preserves combat power. Security results from measures a command takes to protect itself from surprise, interference, sabotage, annoyance, and threat surveillance and reconnaissance. Military deception greatly enhances security.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

8. Surprise

- Strike the enemy at a time or place or in a manner for which he is unprepared.
 - Surprise is the reciprocal of security. It is a major contributor to achieving shock. It results from taking actions for which the enemy is unprepared. Surprise is a powerful but temporary combat multiplier.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

9. Simplicity

- Prepare clear, uncomplicated plans and clear, concise orders to ensure thorough understanding.
 - Plans and orders should be simple and direct. Simple plans and clear, concise orders reduce misunderstanding and confusion. The situation determines the degree of simplicity required. Simple plans executed on time are better than detailed plans executed late.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

10. Perseverance

- Ensure the commitment necessary to attain the national strategic end state.
 - Commanders prepare for measured, protracted military operations in pursuit of the desired national strategic end state. Some joint operations may require years to reach the desired end state. Resolving the underlying causes of the crisis may be elusive, making it difficult to achieve conditions supporting the end state. The patient, resolute, and persistent pursuit of national goals and objectives often is a requirement for success.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

11. Legitimacy

- Develop and maintain the will necessary to attain the national strategic end state.
 - For Army forces, legitimacy comes from three important factors. First, the operation or campaign must be conducted under U.S. law. Second, the operation must be conducted according to international laws and treaties recognized by the United States, particularly the law of war. Third, the campaign or operation should develop or reinforce the authority and acceptance for the host-nation government by both the governed and the international community. This last factor is frequently the decisive element.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

12. Restraint

- Limit collateral damage and prevent the unnecessary use of force.
 - Restraint requires careful and disciplined balancing of security, the conduct of military operations, and the desired strategic end state. Excessive force antagonizes those friendly and neutral parties involved.

Source: Joint Publication 1, Doctrine for the Armed Forces of the United States, March 23, 2013, Executive Summary, Commander's Overview

Key Takeaways

- If you are going to war then partner with and learn from professional warriors.
- Understand the principles of warfare and adapt them to your situation.
- You can be sure the hackers are adapting similar principles to their situations.
- Oh, and you are going to war!

WHAT MAKES CYBER WARFARE DIFFERENT?

Or
Why Didn't We See This Coming?

A silhouette of the San Francisco skyline is shown against a background of a bridge and water. The word "CyberSizeIT" is overlaid on the skyline in a large, stylized font with a red-to-white gradient and a white outline.

CyberSizeIT

Long-term Exploits

Hackers Tapped a Bonanza of Data for Traders, U.S. Says

The 2010 marketing effort came in the early days of what U.S. authorities described as a five-year-long global alliance between overseas hackers and traders in the U.S. Together, officials say, they stole nonpublic corporate information and made lucrative bets in the time between when news releases were uploaded by listed companies into newswires' systems and when the services issued public announcements of the news. Traders would sometimes create what prosecutors called "shopping lists" of companies that were expected to make announcements and pass them on to hackers.

It reaped \$30 million in illegal profits, according to prosecutors. The SEC, which uses a different standard for defining unlawful acts, put the figure closer to \$100 million.

Source: <http://www.wsj.com/articles/u-s-charges-nine-in-big-insider-trading-scheme-1439295551?cb=logged0.7991569681413091> (August 11, 2015)

Long-term Non-exploits

Lurking in Cyberspace

“Security experts have discovered foreign malware embedded in supervisory control and data acquisition (SCADA) systems across the critical infrastructure. Its purposeful use could be devastating.

And the potential effects of their operations could be as catastrophic to an industrialized nation as kinetic warfare.”

Source: Ackerman, R. K. (2015, July). Lurking in cyberspace. *Signal*, 6.

Long-term Non-exploits

RAT infestations are just one serious threat

The biggest concern is the critical infrastructure, particularly supervisory control and data acquisition (SCADA) systems, he offers. Experts have found remote access tools, or RATs, in SCADA systems over the years. These RATs would provide outsiders with the ability to control the infrastructure devices. “There are back doors that people don’t know about in many, many systems all the time,” Henry states. “Hundreds or thousands of industrial control systems have been infiltrated by malicious code.”

Source: Ackerman, R. K. (2015, July). Destructive cyber attacks increase in frequency, sophistication. *Signal*, 18.

Definitional Constraints

The Real Dangers of Trojans Are Not What You Think

“Experts fall into a trap if they try to confine adversarial efforts to proverbial boxes that give the illusion of control— a lie that limits defenses by defining the adversary solely by what we know. Adversaries are becoming smarter and more active; their rate of growth itself is disruptive.”

“It is common practice to rely on the likes of Kaspersky Lab, an international software security group, to define malicious items. The lab lists 19 types of Trojans, all “classified according to the type of actions that they can perform on a computer.” As with the Greeks’ Trojan horse, protecting today’s modern day payload-carrying Trojan should not require an altered defensive strategy. If defenders are just looking for a big wooden horse, defeat is inevitable when the wagon filled with poison rolls on by.”

Source: Terrill, F. J., Master Sgt. (USAF), (2015, July). *The real dangers of trojans are not what you think. Signal*, 15.

Difficult to Determine Scope

Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and China have developed advanced cyber capabilities and strategies. Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness.

Note: While technology can detect incidents or patterns of incidents it cannot determine the schemes being supported by the activities which trigger those incidents.

Source: The Department of Defense Cyber Strategy, April, 2015, p. 9

Difficult to Determine Attribution

Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation.

Source: The Department of Defense Cyber Strategy, April, 2015, p. 9

Difficult to Determine Attribution

“Our primary goal is attribution. We want to arrest someone.”

Silicon Valley AFCEA Chapter Meeting, August 5, 2015

Mr. Malcolm K. Palmore

Assistant Special Agent in Charge (Cyber Branch)

San Francisco Division / San Jose RA

U.S. Department of Justice

Federal Bureau of Investigation

Remember: Law enforcement investigates and prosecutes crimes (i.e., after the damage is done).

Treaties Usually Don't Work

Obama: U.S. and China Reach Cyber-Espionage 'Common Understanding'

The United States and China have agreed not to "conduct or knowingly support" cyber-theft of intellectual property or commercial trade secrets, the presidents of both countries announced Friday in an address at the White House Rose Garden.

Overall, Obama said, "we have jointly affirmed the principle that governments don't engage in cyber espionage for financial gain against companies."

Source: <http://www.nbcnews.com/tech/security/obama-u-s-china-reach-cyber-spying-understanding-n433751> (9/25/2015)

Treaties Usually Don't Work

Xi had said during a speech in Seattle on Tuesday that his country and the U.S. could work together to address cyber conflicts, even as the nation continues to deny involvement in those conflicts. Earlier this month, Beijing denounced U.S. claims of cyber-espionage as "groundless accusations."

What the NSA says:



FBI's Cyber Most Wanted



EVGENIY
MIKHAILOVICH
BOGACHEV



NICOLAE
POPESCU



ALEXSEY
BELAN



VIET QUOC
NGUYEN



PETERIS
SAHUROVS



SUN KAILIANG



HUANG ZHENYU



WEN XINYU



WANG DONG



GU CHUNHUI

Treaties Usually Don't Work

Neville Chamberlain (British Prime Minister, 1938) landed at Heston Aerodrome on September 30, 1938, and spoke to the crowds there:

“The settlement of the Czechoslovakian problem, which has now been achieved is, in my view, only the prelude to a larger settlement in which all Europe may find peace. This morning I had another talk with the German Chancellor, Herr Hitler, and here is the paper which bears his name upon it as well as mine. Some of you, perhaps, have already heard what it contains but I would just like to read it to you: ' ... We regard the agreement signed last night and the Anglo-German Naval Agreement as symbolic of the desire of our two peoples never to go to war with one another again.”

Later that day he stood outside 10 Downing Street and again read from the document and concluded:

“My good friends, for the second time in our history, a British Prime Minister has returned from Germany bringing peace with honour. I believe it is peace for our time. We thank you from the bottom of our hearts. Go home and get a nice quiet sleep.”

September 3, 1939 – Britain and France declare war on Germany.

Digital Threats, Kinetic Effects

Behind a Broad Bull's-eye

Money may be the root of almost all evildoing in cyberspace, but malicious attacks are becoming more of a threat to the networked world. These attacks have the potential to wreak havoc on more than just digital assets, however. Every part of a nation's critical infrastructure is at risk, and not just from attacks through cyberspace. Kinetic assaults could be as damaging as digital sabotage—in some cases, even more severe to a nation's social and economic structure.

Source: Ackerman, R. K. (2015, March). Behind a broad bull's-eye. *Signal*, 6.

Cyberterrorism's Next Likely Target

The next big cyber attack likely will strike critical infrastructure assets in the United States, which could bring the world's remaining superpower to its knees, according to cybersecurity experts. This would constitute a crippling assault against national assets such as power facilities, transportation networks, nuclear plants or the drinking water supply, these experts warn.

System administrators and those with privileged access pose a widely exploitable weakness to networks if infiltrated by hackers, who have increased the number of cyber attacks on critical infrastructure and already have targeted power facilities, traffic systems, water treatment plants and factories.

Source: Jontz, S. (2015, March). Critical infrastructure Is cyberterrorism's next likely target. *Signal*, 18.

Key Takeaways

- Cyber warfare has many differences from traditional warfare but also many similarities.
- As the digital connectivity of the world increases (think the “Internet of Things” or IoT) the threats from cyber warfare increase exponentially.
- It’s hard to stop criminals you can’t find, for crimes you haven’t discovered!

HOW IS THE WORLD OF DoD SIMILAR TO YOURS?

Or

Why Do You Need to Understand the DoD Cyberspace Model, Mission and Strategy?

ISACA[®]

Trust in, and value from, information systems

San Francisco Chapter



CyberSizelT

What is Cyberspace?

Cyberspace: A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Source: U.S. Armed Forces Joint Publication 3-12, Cyberspace Operations, February 5, 2013

Why Is Cyberspace Insecure?

“The sheer size of contemporary operating systems (on the order of 100,000+ instructions) and their complexity makes it virtually impossible to validate the static design and implementation of the system. When the dynamic behavior of the system is contemplated as well, there is no practical way to validate that all of the possible control paths of the operating system in execution produce correct, error-free results.

These conditions coupled with flaws or misconceptions in the design, and the fact that the operating systems were not designed to be secure, provide a malicious user with any number of opportunities to subvert the operating system itself.”

Source: Anderson, James P., October, 1972, Computer Security Technology Planning Study (ESD-TR-73-51, Vol. II) for the Deputy for Command and Management Systems HQ Electronic Systems Division (AFSC), L.G. Hanscom Field, Bedford, Massachusetts 01730.

Why Is Cyberspace Insecure?

“In summary, the security threat is the demonstrated inability of most contemporary computer systems to provide a sufficiently strong technical defense against a malicious user who is deliberately attempting to penetrate the system for hostile purposes. The primary technical problem to be solved is that of determining what constitutes an appropriate defense against malicious attack, and then developing hardware and software with the defensive mechanism(s) built in.”

Source: Anderson, James P., October, 1972, Computer Security Technology Planning Study (ESD-TR-73-51, Vol. II) for the Deputy for Command and Management Systems HQ Electronic Systems Division (AFSC), L.G. Hanscom Field, Bedford, Massachusetts 01730.

A House Built Upon Sand...

“...shall be likened unto a foolish man, which built his house upon the sand: And the rain descended, and the floods came, and the winds blew, and beat upon that house; and it fell: and great was the fall of it.”

We have built our computing infrastructure on the sands of insecure protocols, poorly designed and coded software, and inadequately designed and constructed hardware. What did we expect?

Understanding Cyberspace

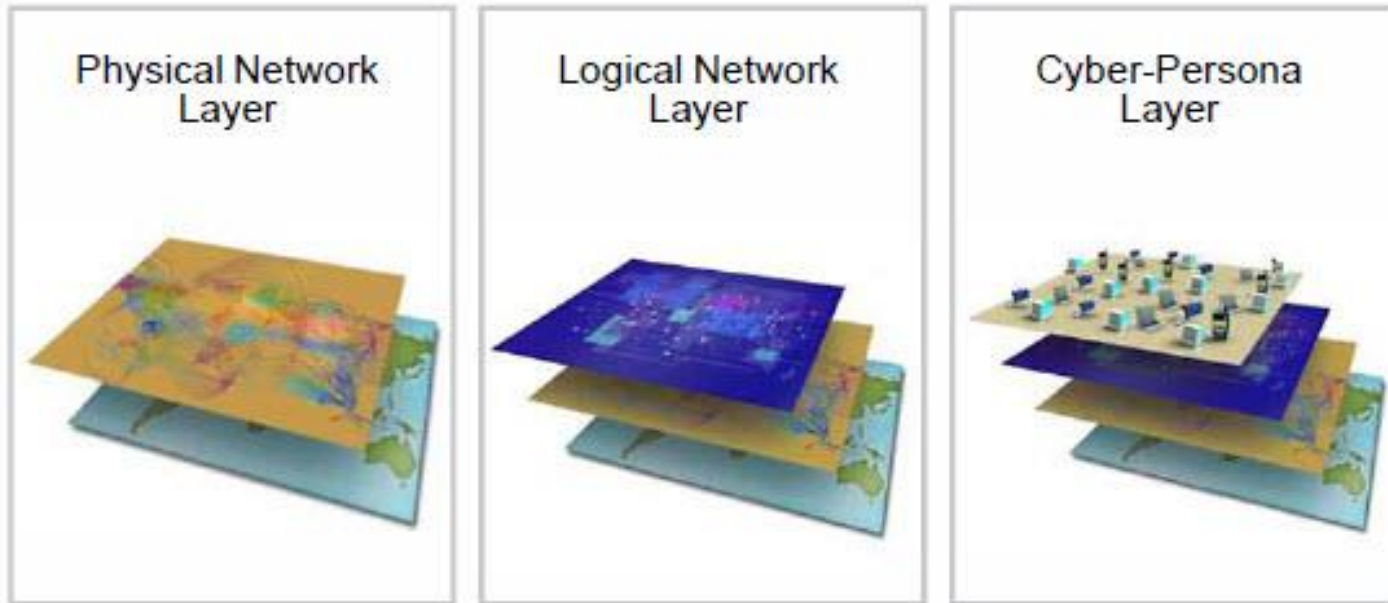
Cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land, maritime, and space. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace.

Even though networks in cyberspace are interdependent, parts of these networks are isolated. Isolation in cyberspace exists via protocols, firewalls, encryption, and physical separation from other networks. For instance, classified networks such as the US Armed Forces Secure Internet Protocol Router network (SIPRnet) are not hardwired to the Internet at all times, but connect to it via secure portals. Additionally, the construction of some hard-wired networks isolates them from most forms of radio frequency (RF) interference. These factors enable these networks to be isolated within cyberspace, yet still allow controlled connectivity to global networks.

Source: Air Force Doctrine Document 3-12, Cyberspace Operations, July 15, 2010
Incorporating Change 1, 30 November 2011

The Three Layers of Cyberspace

The Three Layers of Cyberspace



Source: Joint Publication 3-12(R), Cyberspace Operations, February 5, 2013, p. I-3

The Three Layers of Cyberspace

- The physical network layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel.
- The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node.
- The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network.

Source: Joint Publication 3-12(R), Cyberspace Operations, February 5, 2013, p. I-2,3

Types of Challenges

(1) Threats.

(a) Nation State Threat.

(b) Transnational Actor Threat.

(c) Criminal Organization Threat.

(d) Individual Actors or Small Group Threat.

(2) Anonymity and Difficulties with Attribution.

(3) Additional Challenges.

Source: Joint Publication 3-12(R), Cyberspace Operations, February 5, 2013, p. I-7

Mandated to Partner

- c. Private Industry. Many of DOD's critical functions and operations rely on commercial assets, including Internet service providers and global supply chains, over which DOD has no direct authority to mitigate risk effectively. Therefore, DOD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to improve cybersecurity.¹
- As a matter of first principle, cybersecurity is a team effort within the U.S. Federal government. To succeed in its missions the Defense Department must operate in partnership with other Departments and Agencies, international allies and partners, state and local governments, and, most importantly, the private sector.²

Source ¹: Joint Publication 3-12(R), Cyberspace Operations, February 5, 2013, p. I-8

Source ²: The Department of Defense Cyber Strategy, April, 2015, p. 3

Three Primary Cyber Missions

- The Defense Department has three primary cyber missions.
 - First, DoD must defend its own networks, systems, and information.
 - For its second mission, DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence.
 - Third, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans.

Source: The Department of Defense Cyber Strategy, April, 2015, p. 4-5

Three Primary Cyber Missions Redux

- The Company has three primary cyber missions.
 - First, the Company must defend its own networks, systems, and information.
 - For its second mission, the Company must be prepared to defend the Company and its interests against cyberattacks of significant consequence.
 - Third, if directed by the Company President, the Company must be able to provide integrated cyber capabilities to support business operations and contingency plans.

Source: Adapted from The Department of Defense Cyber Strategy, April, 2015, p. 4-5

Five Strategic Goals

DoD sets five strategic goals for its cyberspace missions:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Source: The Department of Defense Cyber Strategy, April, 2015, p. 7-8

Five Strategic Goals Redux

The Company sets five strategic goals for its cyberspace missions:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the Company's information network, secure the Company's data, and mitigate risks to the Company's missions;
3. Be prepared to defend the Company's facilities and vital interests from disruptive or destructive cyberattacks of significant consequence;
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
5. Build and maintain robust domestic and international alliances and partnerships to deter shared threats and increase security and stability.

Source: Adapted from The Department of Defense Cyber Strategy, April, 2015, p. 7-8

Capabilities Inventory

A cyberspace capability is a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

Q: What are your cyberspace capabilities?

Source: Joint Publication 3-12(R), Cyberspace Operations, February 5, 2013, p. I-6

Key Takeaways

- The DoD has a well-defined model of the cyberspace domain which probably matches your company's model (if you have one).
- The DoD faces both similar threats as your company faces (as well as some unique ones).
- Since the DoD is mandated to partner with the private sector there will be work products available that you have already paid for!

LESSONS FROM THE PUBLIC SECTOR

Or

Don't Make Me Learn That Again!



Trust in, and value from, information systems

San Francisco Chapter

A stylized graphic of the San Francisco skyline, including the Golden Gate Bridge, is positioned behind the text. The text "CyberSizeIT" is written in a large, bold, red font with a white outline, set against a dark background.

CyberSizeIT

Cyber Is a Global Team Sport

U.S. Department of Homeland Security Science and Technology Directorate officials are helping other nations create cyber testbeds that can be linked, forming one large, international virtual laboratory for cyber systems. In addition, they already have in place bilateral agreements with a number of countries and are in discussions with France, Spain, Germany, Mexico and South Korea, which ultimately could expand international cooperation on cybersecurity research and development.

Source: Seffers, G. I. (2015, March). Cyber is a global team sport. *Signal*, 26.

Air Force Cyber Fusion Center

Air Force U.S. Cyber Command is recruiting and training airmen to join one of the Air Force's 39 cyber mission force teams that will be established over the next two years. The command needs about 1,715 airmen for the Air Force teams, as part of a Defense Department-wide effort that will put in place 133 cyber mission force teams with 6,000 personnel by 2017.



Source: <http://www.airforcetimes.com/story/military/careers/air-force/2015/01/03/us-cyber-command-recruiting/21226161/>

Corporate Cyber Fusion Centers

The goal of the CFC space is to bring Target's key information security teams together to work faster and with more agility than ever before. "With no walls between any of the groups, members can connect to share information quickly and make fast and accurate decisions," ...



Source: <https://corporate.target.com/article/2015/07/cyber-fusion-center>

Identity Management

The Next Frontier

The U.S. Department of Homeland Security's Continuous Diagnostics and Mitigation program is beginning a new thrust in which it addresses a growing concern of cybersecurity: identity management.

The Continuous Diagnostics and Mitigation (CDM) program seeks to fortify cybersecurity of government networks and systems against the trillions of cyber events—growing more sophisticated, frequent and dynamic—that attempt to penetrate the systems weekly.

Source: Jontz, S. (2015, March). DHS readies next phase of cybersecurity conformity. *Signal*, 31.

Threat Awareness Starts At Home

Insider threats are a particular concern with government agencies— what Westin calls the “Snowden effect.” The damage caused by Edward Snowden was compounded by his privileged access to highly sensitive information and his ability to access data he was not officially supposed to access.

Source: Kenyon, H.S. (2015, May). Avoiding cyberspace pitfalls with threat intelligence. *Signal*, 50.

Cloud to the Rescue

Applications that leverage reliance on a simplified “platform-as-a-service” will have materially lower development costs. Developers will benefit from an infrastructure that offers bug-free features for the handling of database, security, display, retrieval or communications.

Note: “Bug-free” may be a little optimistic!

Source: Strassmann, P.A. (2015, March). A cloud approach could solve defense infrastructure challenges. *Signal*, 50.

Cyberspace Is Additive

The best way to approach cyberspace at the executive level is to understand that cyberspace adds a new dimension to both economic competition and politically driven conflict, but the existence of cyberspace does not require a fundamental change in our strategic approach to either.

Source: Williams, B., Maj. Gen. (March 13, 2014). Cyberspace: What is it, where is it and who cares?. *Armed Forces Journal*, <http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/>.

Cyberspace Is Multiplicative

The opportunity for cheap, anonymous access to cyberspace creates an inviting environment for a broad spectrum of malicious activity. The threat commonly manifests itself in the form of cybercrime where individuals or specific companies suffer financial loss. More concerning is the opportunity to create a widespread effect that undermines faith and confidence across financial markets. An example of this occurred in April 2013 when a hacked Twitter newsfeed propagated a false report of an explosion at the White House. Within minutes, the U.S. stock market plunged, reflecting a “loss” of over \$130 billion. While the index recovered rapidly, this incident provided a clear warning of our vulnerability to malicious cyberspace activity given the hyper-connected, information-driven nature of the business environment.

Source: Williams, B., Maj. Gen. (March 13, 2014). Cyberspace: What is it, where is it and who cares?. *Armed Forces Journal*, <http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/>.

World War III?

A foreign nation tiptoeing past the firewalls of companies in charge of our critical infrastructure is a real problem that demands a real response. Some have suggested the ongoing digital attacks originating in China are tantamount to war. But let's all take a deep breath before arguing for cyber-counterstrikes that risk escalation with the world's most populous nation.

For one thing, equating espionage to war isn't a standard this nation would want to apply to itself. The United States has clearly spied against foreign nations in the past. It's also widely believed the U.S. government helped create the Stuxnet computer worm that hobbled Iran's nuclear program, a clear act of cyber-sabotage.

Moreover, as UC Berkeley professor Steven Weber points out, if this constitutes war, we're already neck deep in WW III.

Source: <http://www.sfgate.com/technology/dotcommentary/article/Cyber-war-between-U-S-China-4292019.php>

Key Takeaways

- Immense resources are consumed in the production of the services delivered by our public sector agencies and organizations.
- We should learn from them because that learning opportunity is relatively inexpensive compared to other resources.
- There are public sector entities engaged in almost every line or type of business – you just need to look and ask.

RISK MANAGEMENT

Or

Not In My Backyard (NIMBY)!



Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is set against a background illustration of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers. The word "CyberSizelT" is written in a large, stylized font with a red-to-orange gradient and a white outline. The "T" is significantly larger than the other letters.

CyberSizelT

Favorite Risk Management Quote

“The purpose of risk management is to improve the future, not to explain the past.”

Dan Borge, *The Book of Risk*

Source: Borge, D. (2001). *The book of risk*. New York, NY: John Wiley & Sons.

The Risk Management Problem

The causes of vulnerabilities are many. We—the public, industry and government—are not very good at providing the discipline necessary to run our networks. Accountability is lacking and individual and enterprise roles and responsibilities are not properly established; and where they are in place, they often are not enforced. Risk-management strategies tend to be fleeting, bifurcated or ignored.

Source: Shea, R. M., Lt. Gen., USMC (Retired) (2015, July). Confronting cyberthreats. *Signal*, 17.

Beware the Fifth Column

- In warfare a “fifth column” is a serious risk.
- Merriam-Webster Online defines “fifth column” as “a group of secret sympathizers or supporters of an enemy that engage in espionage or sabotage within defense lines or national borders”.
 - Origin of “fifth column”: name applied to rebel sympathizers in Madrid in 1936 when four rebel columns were advancing on the city.

My Dirty Dozen Conjectures

1. There are agents of foreign governments working in every major company in the United States.
2. There are agents of competitive businesses working in every major company in the United States.
3. There are criminals working in every major company in the United States.
4. There are agents of foreign governments working in every major governmental organization in the United States.
5. There are agents of the United States government working in every major company in the United States.
6. Every major company has suffered a loss of intellectual property.

My Dirty Dozen Conjectures, cont.

7. Every major company will continue to suffer losses of intellectual property.

8. Every major company has suffered a loss of customer information.

9. Every major company will continue to suffer losses of customer information.

10. Every commercially available information or communications system is subject to unauthorized access.

11. The vast majority of unauthorized accesses will go undetected.

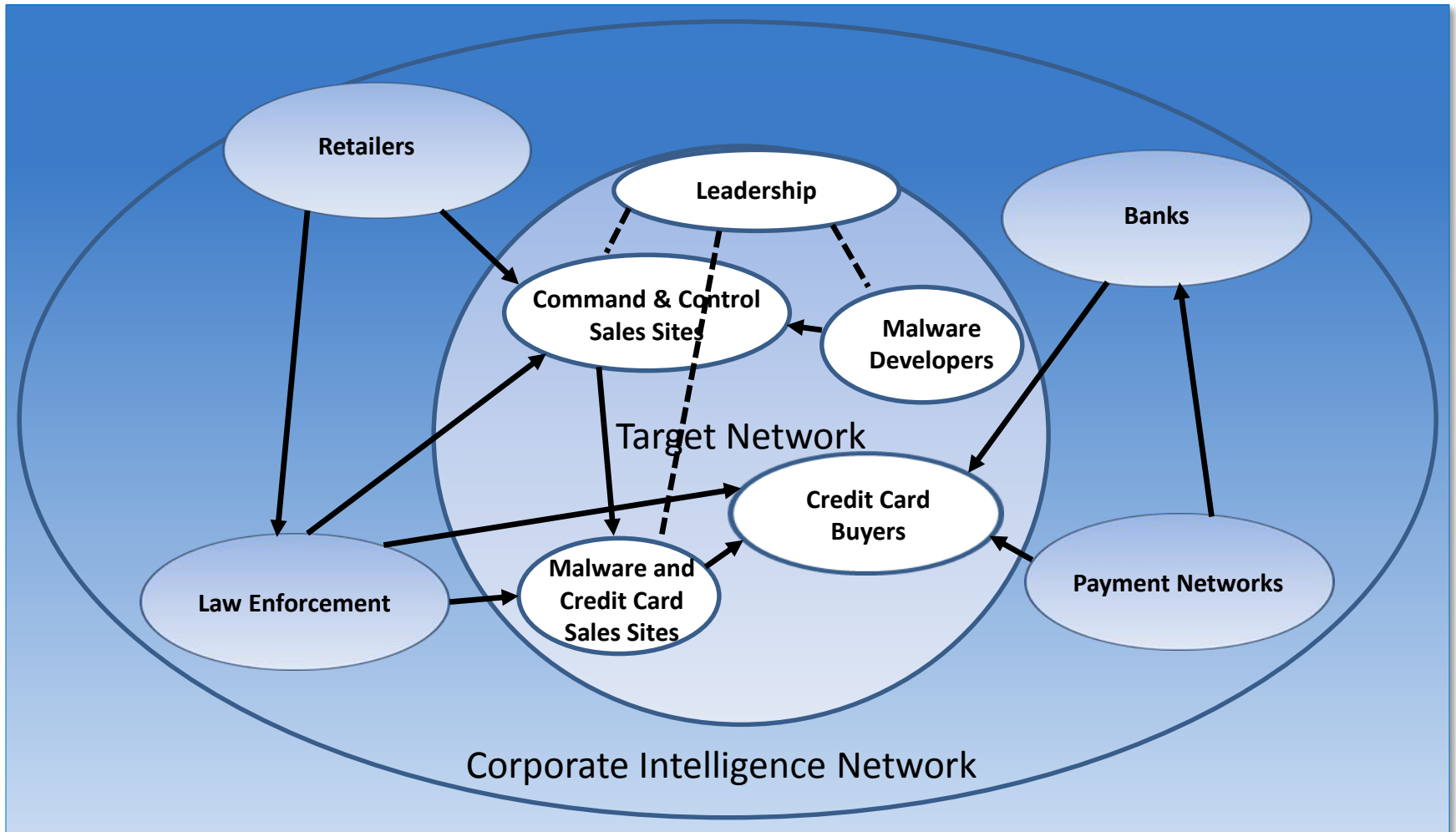
12. The vast majority of unauthorized accesses detected will go unprosecuted.

It's Not Spy vs Spy Anymore



Copyright © E.C. Publications, Inc.

It's Network vs Network



Keep Evolving Your Responses

Insider threats account for about 15% of cybersecurity incidents, and spearphishing [manipulating a user to inadvertently download malware] is still the number-one way that breaches occur. So if a large packet of data is leaving the system, questions should be asked.

Source: Galligan, M. (2015, July). As cyberattacks evolve, so should the corporate response. *Risk & Compliance Journal*, <http://deloitte.wsj.com/riskandcompliance/2014/02/24/as-cyberattacks-evolve-so-should-the-corporate-response/>

Cyber War-Gaming

Q. Cyber war-gaming is one tool used by the financial industry to help improve responses to cyberattacks. Were there lessons learned that can be applied to other industries?

Mary Galligan: Cyber war-gaming is a way to test the effectiveness of an existing incident response plan and identify gaps in areas such as communication and coordination. It's a proactive approach to prepare for a cyber threat. This past July the Wall Street community along with numerous federal government agencies participated in a full-day cyberattack simulation known as Quantum Dawn 2*. Similar to the results of many other war games, participants recognized a need for more effective communication and information-sharing among institutions and federal agencies and companies within the same industry and select third parties, such as law enforcement.

Source: Galligan, M. (2015, July). As cyberattacks evolve, so should the corporate response. *Risk & Compliance Journal*, <http://deloitte.wsj.com/riskandcompliance/2014/02/24/as-cyberattacks-evolve-so-should-the-corporate-response/>

The Weakest Link

A computer system rarely commits an act of aggression without a human participant. Remain aware of the risks associated with “carbon-based units”.



Key Takeaways

- Cybersecurity begins at home!
- You need to use your full network of resources in your fight against the full networks of resources that cyber-attackers are using to attack your company.
- People are your greatest asset AND your greatest source of exposure. Tread lightly but firmly.

CYBER WARFARE ON THE WORLD STAGE

Or
Global Is The New Local!



Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is rendered in a large, stylized font with a red-to-brown gradient and a white outline. The background of the slide features a silhouette of the San Francisco skyline, including the Golden Gate Bridge and the Transamerica Pyramid, set against a warm, yellowish-orange sky.

CyberSizelT

Cyber Warfare Is Everywhere

The cyber attacks that threaten the United States are just as intense and worrisome for NATO, which comes under persistent strikes by nation-states, terrorist groups and criminal organizations all assailing with denial-of-service malware, organized criminal incursions, cyber espionage and website defacements. As the U.S. Defense Department toils at creating a unified and secure network, so too does NATO.

Source: Jontz, S. (2015, May). NATO shapes its enterprise for conflicts of tomorrow. *Signal*, 25.

Cyber Warfare Is Asymmetric

The cyber realm is contested space 24 hours a day, seven days a week, he observes—“and it’s unforgiving.” The enemy needs only to succeed once. With a perfect defense being virtually unattainable, the Army aims for a defense in depth “with a proper articulation of risk,” the general says. “You may not be interested in cyber, but cyber is interested in you.”

Source: Ackerman, R.K. (2015, October). Convergence dominates Army cyber activities. *Signal*, 39.

Kinetic Response

Cybersecurity actions often have been described in war-like terms, but this week Britain and U.S. officials took metaphors to their literal end, instrumenting the killing of an Islamic State hacker in a U.S. drone strike in Syria Tuesday.

The target, Junaid Hussain, a British citizen and convicted hacker, played a leadership role in the organization, officials tell the WSJ, training Islamic State members in cyber warfare and helping encourage the adoption of cutting-edge encryption technology.

Source: <http://blogs.wsj.com/cio/2015/08/28/the-morning-download-drone-strike-offers-reminder-from-a-real-cyberwar/>

No Guarantees

WSJ: Recently you have all these supposedly secure companies — NASDAQ, JP Morgan, Kaspersky, RSA, Ashley Madison — being hacked. Is there such a thing as a company or organization these days that can guarantee data security?

Austin Berglas: I don't believe so. Because of the human factor. You're always going to get someone in that organization who's going to be vulnerable to spear phishing. But there are many ways to be proactive, and to reduce the time between when a network is compromised and the organization recognizes it and fixes it.

WSJ: What would you tell U.S. companies about the implications of this heightened tension with China over cybersecurity? What happens to them if sanctions are imposed?

Austin Berglas: I would say it doesn't change anything. If I'm an organization and my firewall and my network are being scanned and attacked millions of times a day, the best practices are the same. In the short run, it's not initially about attribution — it's not about who's attacking — it's about protecting the crown jewels inside your network. That's first and foremost.

Source: <http://blogs.wsj.com/chinarealtime/2015/09/24/can-the-u-s-stop-chinese-hackers-qa-with-cyber-sleuth-austin-berglas/>

Key Takeaways

- Cyberspace and “real space” coexist and interact on both a virtual and physical level. Both are real.
- World geographies are a legal concept about jurisdictional authorities and which rules of law apply. They do not significantly impede cyber warfare.
- Your company, regardless of physical nexus, exists in a global context.

RESOURCES



Trust in, and value from, information systems

San Francisco Chapter

A stylized graphic of the San Francisco skyline in silhouette against a warm, yellowish-orange background. The Golden Gate Bridge is the central focus, with other bridges and city buildings visible. The word "CyberSizeIT" is overlaid on the bottom of the graphic in a large, red, outlined font.

CyberSizeIT

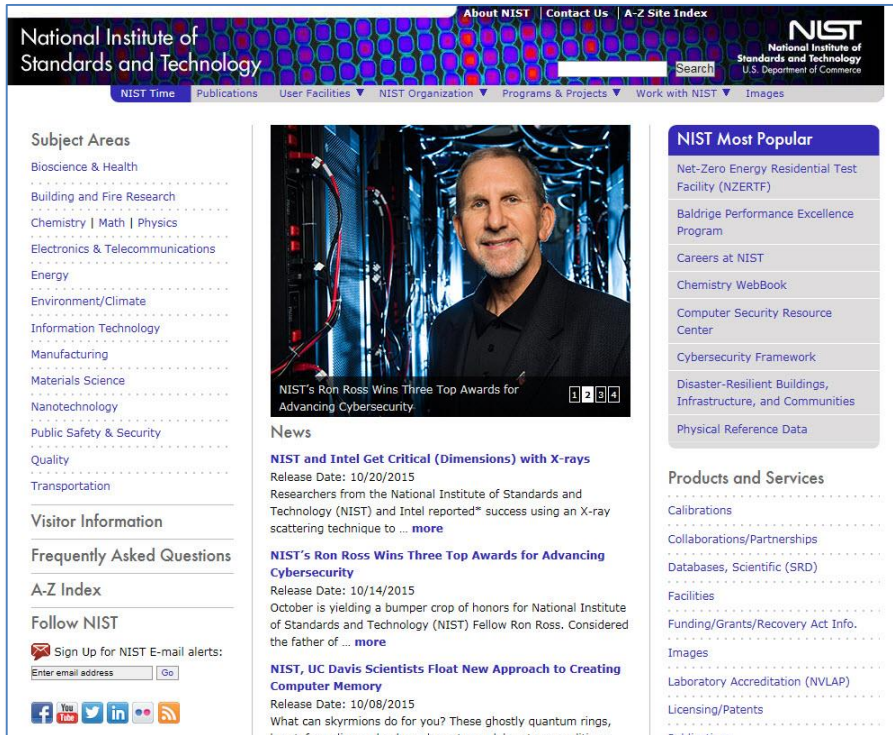
Federal Agencies

Department of Homeland Security (DHS)

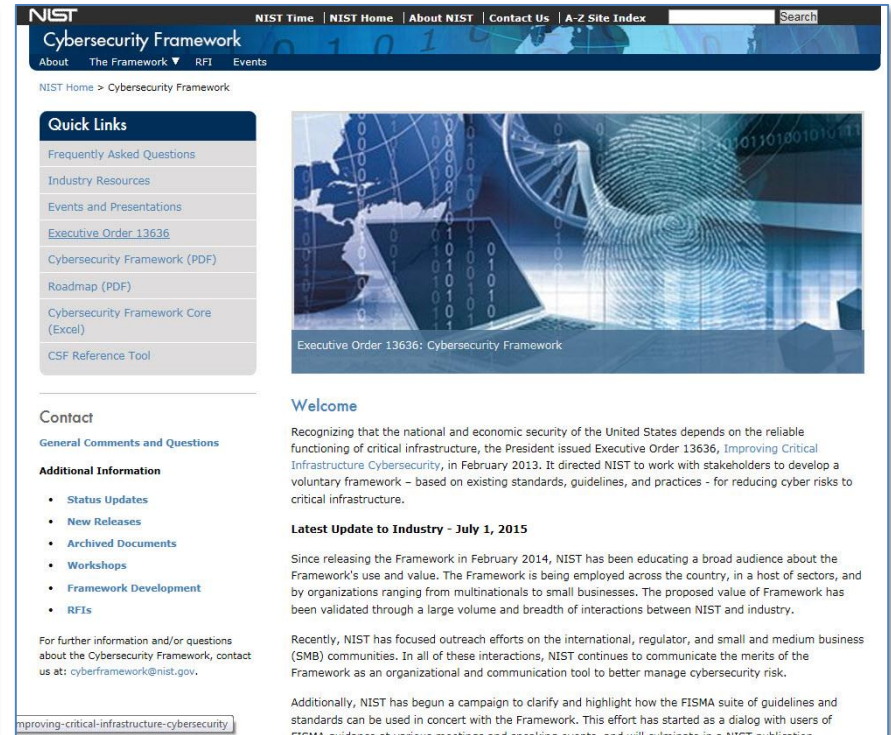
The image shows two overlapping screenshots of the Department of Homeland Security (DHS) website. The top screenshot displays a banner for "October is National Cyber Security Awareness Month" with the text "Cybersecurity is our shared responsibility. Find tips and resources for how to stay safe online with the DHS Stop.Think.Connect. Campaign." and a "Learn More" button. Below the banner is a "Featured Issues & Programs" section with icons for "Frequently Requested Pages", "OPM Cybersecurity FAQ", "Forms", and "Combating Human Trafficking". The bottom screenshot shows the "Cybersecurity" section of the website, featuring a navigation menu on the left and a main content area with articles such as "Cybersecurity Overview", "Combating Cyber Crime", "Securing Federal Networks", "Cyber Incident Response", "Cyber Safety", "Information Sharing", and "Cybersecurity Education & Career Development".

Federal Agencies

National Institute of Standards and Technology (NIST)



The screenshot shows the NIST homepage with a navigation bar at the top containing links for 'About NIST', 'Contact Us', and 'A-Z Site Index'. The main header features the NIST logo and the text 'National Institute of Standards and Technology'. Below the header is a search bar and a secondary navigation bar with links for 'NIST Time', 'Publications', 'User Facilities', 'NIST Organization', 'Programs & Projects', 'Work with NIST', and 'Images'. The left sidebar lists 'Subject Areas' such as Bioscience & Health, Building and Fire Research, Chemistry | Math | Physics, Electronics & Telecommunications, Energy, Environment/Climate, Information Technology, Manufacturing, Materials Science, Nanotechnology, Public Safety & Security, Quality, and Transportation. The main content area features a 'News' section with a photo of Ron Ross and the headline 'NIST's Ron Ross Wins Three Top Awards for Advancing Cybersecurity'. To the right is a 'NIST Most Popular' section listing items like 'Net-Zero Energy Residential Test Facility (NZERTF)' and 'Cybersecurity Framework'. At the bottom left, there is a 'Visitor Information' section and a 'Follow NIST' section with social media icons.



The screenshot shows the NIST Cybersecurity Framework page. The header includes the NIST logo and navigation links for 'NIST Time', 'NIST Home', 'About NIST', 'Contact Us', and 'A-Z Site Index'. The main title is 'Cybersecurity Framework'. Below the title is a 'Quick Links' section with links for 'Frequently Asked Questions', 'Industry Resources', 'Events and Presentations', 'Executive Order 13636', 'Cybersecurity Framework (PDF)', 'Roadmap (PDF)', 'Cybersecurity Framework Core (Excel)', and 'CSF Reference Tool'. To the right is a large image with the text 'Executive Order 13636: Cybersecurity Framework'. Below the image is a 'Welcome' section with a paragraph about the national and economic security of the United States. Further down is a 'Contact' section with a link for 'General Comments and Questions'. At the bottom, there is an 'Additional Information' section with links for 'Status Updates', 'New Releases', 'Archived Documents', 'Workshops', and 'RFIs'. A footer link reads 'improving-critical-infrastructure-cybersecurity'.

Aligned Organizations

Armed Forces Communications and Electronics Association (AFCEA.ORG)

The screenshot shows the AFCEA International website homepage. At the top, there is a navigation bar with links for AFCEA, Defense, Foundation, Europe, Homeland Security, Industry, Intelligence, and SIGNAL Magazine. The main header features the AFCEA logo and the tagline "Bringing Government and Industry Together Since 1946". Below this, there is a "Member Profile" section for a user named John, with options for "Welcome back John" and "Your Account Sign Out". A secondary navigation bar includes links for About AFCEA, Membership, Chapters, Education, Events, News, Publications, and Scholarships. The main content area is divided into several sections: a "Welcome back" sidebar with a "Sign Out" button and "Shortcuts" to various resources; a central "Corporate" banner with a "MEMBERSHIP" sidebar and a "JOIN AFCEA" button; and a "SIGNAL Magazine" section with links to the September issue, online edition, and digital edition. At the bottom, there are social media links for Facebook, Twitter, Google+, and Flickr, along with a "Connect with AFCEA" section.

The screenshot shows the SIGNAL Magazine website homepage. The top navigation bar includes links for NEWS, MAGAZINE, BLOG, NEWSLETTER, WEBINARS, RESOURCE LIBRARY, ADVERTISING, and EBOOKS. Below this, there is a secondary navigation bar with links for All News, Acquisition & Contracting, Cyber, Defense Operations, Homeland Security, Intelligence, and Technology. The main content area features a large banner for "Introducing: THE CYBER EDGE" with a "Read more" link. To the right, there is a "Ultimate Knowledge" button. The page also includes social media icons for Twitter, Facebook, YouTube, and LinkedIn.

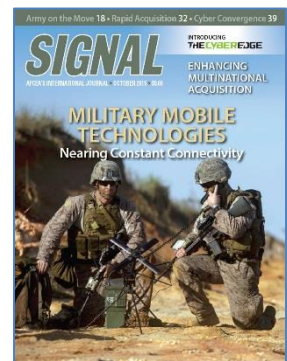
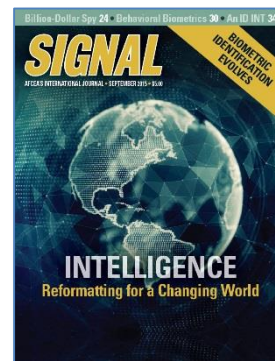
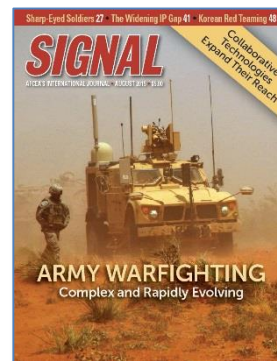
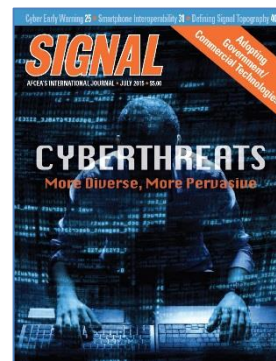
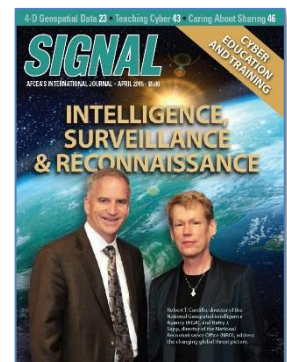
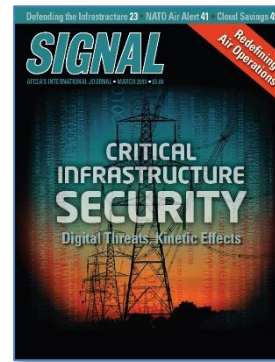
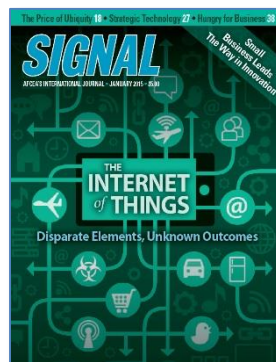
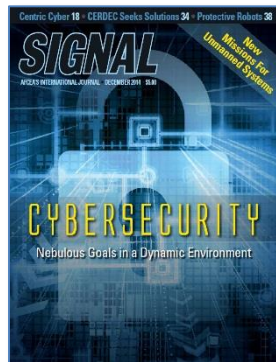
The screenshot shows a news article titled "SMALL DEFENSE CONTRACTORS NEED STRONGER CYBERSECURITY PRACTICES". The article text discusses the challenges small businesses face in the U.S. defense sector regarding cybersecurity. It mentions that the U.S. Defense Department poses serious cybersecurity concerns, in part because of their limited resources to invest in technical and practiced security measures. The U.S. Government Accountability Office (GAO) stated in a recent report that small businesses' cyber practices are often inadequate. GAO investigators recommend providing additional cyber education resources to these small businesses, but they note that there are misconceptions about small business security.

The screenshot shows a news article titled "NIST PILOT PROJECTS SEEK TO IMPROVE CYBERSECURITY, REDUCE ONLINE TAX FRAUD AND IDENTITY THEFT". The article text states that NIST awarded nearly \$3.7 million for three pilot projects that seek to fortify online financial transactions and enhance privacy protections for health care, government services, transportation, and the Internet of Things. The studies address specific cyber-based missions such as reducing tax refund theft, among others.

The screenshot shows a news article titled "ACOUSTIC KITTY AND ZOMBIE HOME APPLI...". The article text discusses the CIA's Project Acoustic Kitty and its connection to zombie-like behavior. It mentions that the CIA's Project Acoustic Kitty have in common with zombie-like behavior is that the answer can be found in three letters: IoT. Left unchecked, the Internet of Things poses notable threats, both commercially and militarily.

Aligned Organizations

AFCEA Signal Magazine



Aligned Organizations

AFCEA Cyber Committee White Papers

- The Security Implications of the Internet of Things
- The Science of Security: A Survey and Analysis
- Cyber Intelligence Sharing
- The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment
- The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework
- Future of Internet Governance
- Critical Infrastructure: Electric Power
- Insider Threat: Protecting U.S. Business Secrets and Sensitive Information
- Secure Mobility
- Cyber Assured Identity
- Looking for the Right Answers in the Clouds
- Security and Cloud Computing
- Security Risks of Not Migrating to IPv6
- Supply Chain Risk Management

Source: <http://url.afcea.org/cyberpapers>

Professional Organizations

ISACA (Information Systems Audit and Control Association)

The image displays two overlapping screenshots of the ISACA website. The left screenshot shows the homepage with a large banner for "ISACA's 2015 IT Risk/Reward Barometer" and navigation menus. The right screenshot shows the "CYBERSECURITY NEXUS" page with an overview, credentialing, and membership sections.

ISACA's 2015 IT Risk/Reward Barometer
Global survey looks at cybersecurity in a world of connected devices
[LEARN MORE](#)

Get Recognized. Register for a December Exam Today
Register online to automatically save US \$75.
[REGISTER NOW](#)

Securing a Connected World
View global member and consumer survey findings on IoT security.
[LEARN MORE](#)

COBIT Conference Europe!
Earn up to 14 CPEs, register today!
[REGISTER TODAY](#)

What's New
ISACA Updates
19 Oct 2015
COBIT Focus: Aligning Universities and Enterprises Using COBIT 5

ISACA Now Blog
19 Oct 2015
APT Study: The Good, the Bad and the Key Takeaways
Today at the CSX North America conference in Washington

CYBERSECURITY NEXUS
Insights and resources for the cybersecurity professional from ISACA

OVERVIEW
In enterprise IT, there is a single point where everything that matters in information, technology and business converges: Cybersecurity Nexus (CSX), a new security knowledge platform and professional program from ISACA. CSX is helping shape the future of cybersecurity through cutting-edge thought leadership, as well as training and certification programs for the professionals who are leading it there. Building on the strength of ISACA's globally-recognized expertise, it gives cybersecurity professionals a smarter way to keep organizations and their information more secure. With CSX, business leaders and cyber professionals can obtain the knowledge, tools, guidance and connections to be at the forefront of a vital and rapidly changing industry. Because Cybersecurity Nexus is at the center of everything that's coming next.

CREDENTIALING
Secure recognition for your expertise. Our globally accepted certifications help advance skills and careers.
[NEW! CYBERSECURITY CERTIFICATIONS AND TRAINING](#)

MEMBERSHIP
Join a global community of more than 115,000 professionals, innovators and thought leaders.
[PROFESSIONAL MEMBERSHIP](#)
[STUDENT MEMBERSHIP](#)

Advertisement
A Cybersecurity Education For Those Who Expect More
[LEARN MORE](#)
American Public APU University

CSX 2015 NORTH AMERICA
AN ISACA CYBER EVENT
Earn up to 32 CPEs!
[REGISTER NOW](#)

Professional Organizations

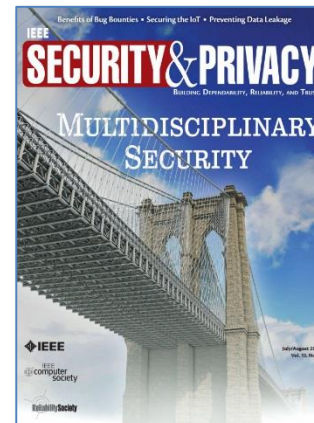
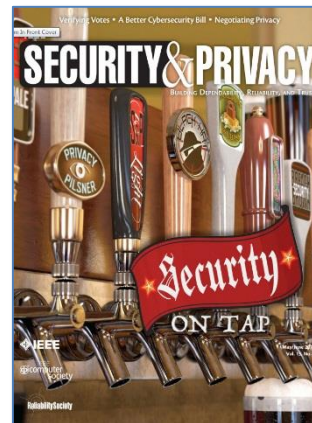
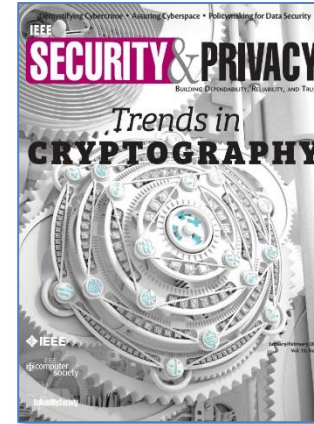
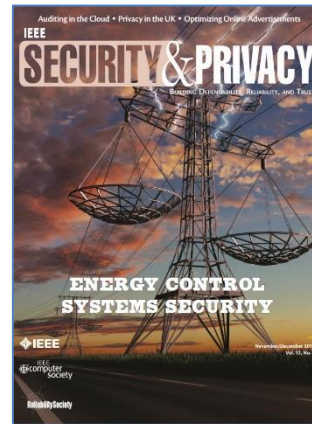
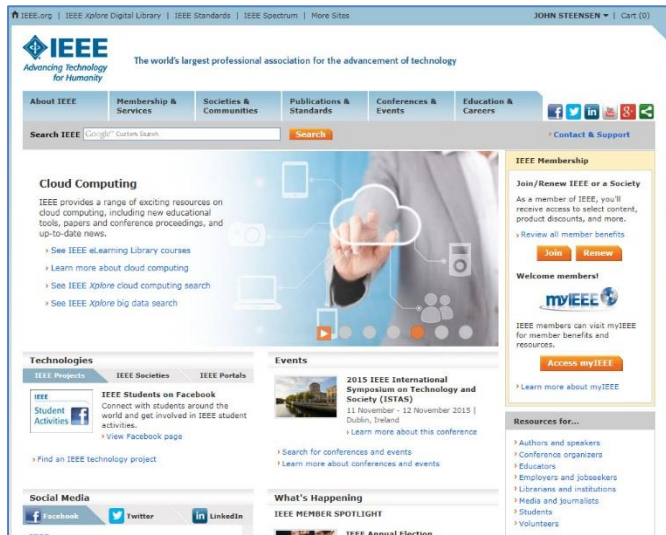
The Institute of Internal Auditors (IIA)

The screenshot shows the IIA website homepage. At the top, there is a navigation bar with links for 'Access Self-Study', 'IA Global', 'Find Your Local IIA', 'Contact Us', 'Join The IIA', and 'Profile'. Below this is the IIA logo and a search bar. A secondary navigation bar includes 'Standards & Guidance', 'Bookstore & Periodicals', 'Certifications & Qualifications', 'Training & Events', 'Membership', 'Services', and 'About Us'. A prominent red button says 'DONATE NOW' and another says 'JOIN THE IIA'. The main content area features a large blue banner for 'Accelerate Your Audit Using Analytic Intelligence' with a speedometer graphic and the text 'Only with IDEA V.10 - Learn More >'. Below this are several smaller boxes for 'Invest in Your Team', 'CGAP Application Fee Waiver', 'Update Your Internal Audit Library', 'Earn and Report CPE', and 'CaseWare Analytics'. On the right side, there is a 'Quick Links' section with arrows pointing to 'Topics and Resources', 'Specialty Audit Centers', 'Bookstore', 'Access CCMS', 'CAE Resources', and 'Audit Career Center'. At the bottom, there are sections for 'Latest News' and 'Upcoming Events'.

The screenshot shows search results for 'cybersecurity' in NA Sites. The search bar at the top indicates 'Results 1-10 of 86 for "cybersecurity" in NA Sites (0.48 seconds)'. Below the search bar, there are two columns of results. The left column has filters for 'Refine by File Types' (PDF, Word, Excel) and 'Refine by Internal Audit Topics' (Technology, Internal Audit Activity/F...). The right column lists search results with document icons, titles, and brief descriptions. The first result is 'Auditing Cybersecurity of Wireless Networks' (138 KB, 10-31-2014). The second is 'Simplifying Audits of Network Cybersecurity' (139 KB, 10-23-2014). The third is 'Cybersecurity Audits for Modern Web Applications' (139 KB, 10-23-2014). The fourth is 'Cybersecurity and Audit of Payment Card Systems' (76 KB, 10-22-2014). Each result includes a 'Show document preview' link.

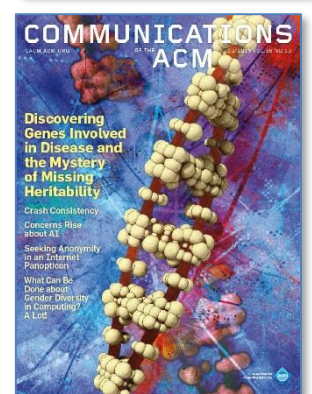
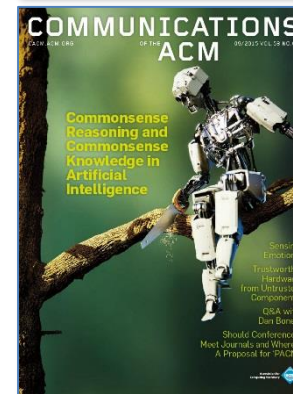
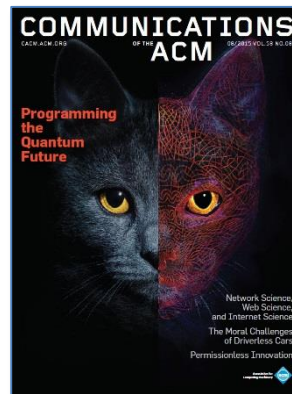
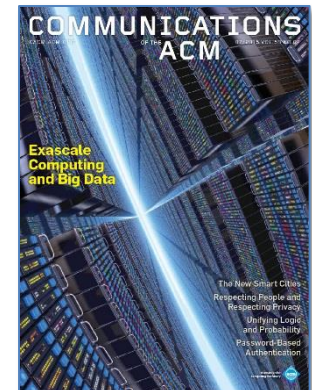
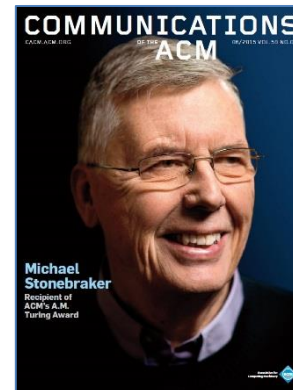
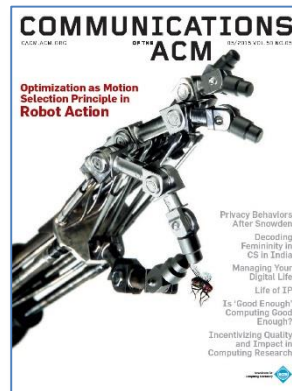
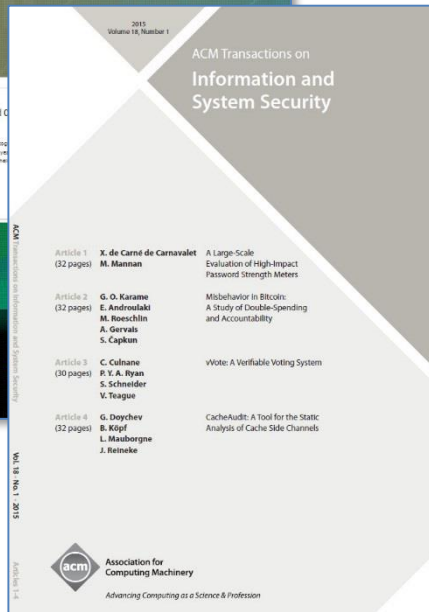
Professional Organizations

Institute of Electrical and Electronics Engineers (IEEE)



Professional Organizations

Association of Computing Machinery (ACM)



Training Organizations

The most trusted source for computer security training, certification and research.

Cyber Defense Initiative (CDI) 2015
 December 12 - 19 | Washington, DC

More than 30 hands-on courses covering all disciplines. Schedule includes:

- Four to Six-day courses: Dec 14 - 19
- NetWars Tournaments including the 4th Annual Tournament of Champions: Dec 17-18
- 15+ Bonus Evening Sessions (check schedule)

[Learn More](#)

1 2 3 4 5

Find Training

Get Certified

Earn a Degree

Free Resources

Upcoming Training Events

South Florida 2015	Fort Lauderdale, FL	Nov 9 - 14
Pen Test Hackfest Summit & Training	Alexandria, VA	Nov 16 - 23
San Francisco 2015	San Francisco, CA	Nov 30 - Dec 5
Security Leadership Summit & Training	Dallas, TX	Dec 3 - 10
Cyber Defense Initiative 2015	Washington, DC	Dec 12 - 19
Las Vegas 2016	Las Vegas, NV	Jan 9 - 14

Consensus Research Projects

- CIS Critical Security Controls
- Top 25 Software Errors
- 20 Coolest Careers in Infosec

Security Resources

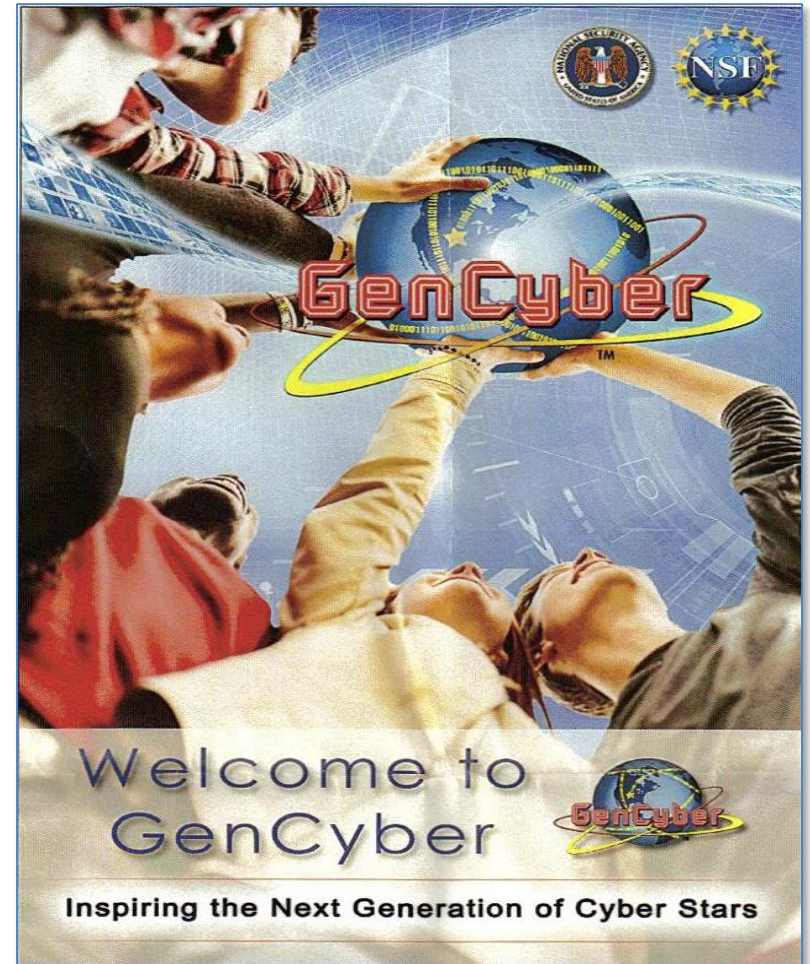
- Infosec Reading Room
- Security Newsletters
- IAD Top 10 Mitigations
- Security Policy Samples
- Intrusion Detection FAQ

SANS CYBER DEFENSE INITIATIVE 2015
 December 12-19 • Washington, DC

SANS SEC501: Advanced Security Essentials - Enterprise Defender

Educational Institutions

Computer Security
History Project at
the University of
California at Davis:
<http://seclab.cs.ucdavis.edu/projects/history/>



Industry Consortia

- Retailers Launch Comprehensive Cyber Intelligence Sharing Center
 - Public/Private collaboration aims to strengthen defenses against cyber attacks and protect customers
- Today (May 14, 2014) the Retail Industry Leaders Association (RILA), along with several of America's most recognized retail brands, launched the Retail Cyber Intelligence Sharing Center (R-CISC). The R-CISC is an independent organization, the centerpiece of which is a Retail Information Sharing and Analysis Center (Retail-ISAC). Among those companies participating with and supportive of the R-CISC are American Eagle Outfitters, Gap Inc., J. C. Penney Company Inc., Lowe's Companies, Inc., Nike, Inc., Safeway, Inc., Target Corporation, VF Corporation and Walgreen Company.

Source:

<http://www.rila.org/news/topnews/Pages/RetailersLaunchComprehensiveCyberIntelligenceSharingCenter.aspx>

Industry Consortia

The banking industry is stepping up pressure on the Senate to pass a cybersecurity bill (Cybersecurity Information Sharing Act - CISA) that would expand information sharing on cyber threats between private companies and the federal government. **(CISA)**

The Cybersecurity Information Sharing Act (CISA) overwhelmingly passed with a vote of 74 to 21.

The financial services industry has largely been supportive of the measure, arguing that greater information sharing across different sectors and the government is necessary to fend off future attacks. But the legislation still faces hurdles, especially due to ongoing concerns by privacy advocates over a lack of consumer protections in the bill.

Source: http://www.americanbanker.com/issues/179_148/banking-groups-push-for-senate-cybersecurity-vote-1069144-1.html

<http://www.insidecounsel.com/2015/08/20/banks-and-cybersecurity-from-a-regulatory-and-a-ri?page=2>

Industry Consortia

FS-ISAC, or the Financial Services Information Sharing and Analysis Center, is the global financial industry's go to resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members and operates as a member-owned non-profit entity.

Source: <https://www.fsisac.com/>

Key Takeaways

- As long as there is financial gain to be realized or political goals to be attained cyber warfare is not going to end.
- There is no “winning” the cyberwar!
- You must design and institute a pervasive counter-measures approach that will allow you to survive over the long haul.
- Constant adaptation must become a mind-set.

QUESTIONS?

John Steensen, MBA/TM, CISA[®], CRISC[™]
JSteense@Visa.com



Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is set against a background of a stylized city skyline with the Golden Gate Bridge. The word "CyberSizelT" is written in a large, bold, red font with a white outline. The "T" is significantly larger than the other letters.

CyberSizelT