CYBER POWER

The Quest Towards a Common Ground

Key Insights

Project Cyber Power

April 2012-August 2012

Version 1.0

Disclaimer

This unclassified research product is provided to stimulate thought and discussion. It does not reflect the views of Air University, AFRI, the USAF or the US Government.

This publication is the first outcome document produced as a result of a year-long effort studying cyberpower, national security, military operations and collective action. It is the product of a series of workshops held at Maxwell AFB in Montgomery, leading to a conference in October 2012. These initial finding constitute part of a larger report to be published by Air University Press in the first quarter of 2013. The report tackles the complex, important and sensitive issue of cyber conflict, and the balance between the preservation of national security and the enhancement of business practices in the current vulnerability and threat environment. Based on project cyber power, conducted in collaboration with partners from across the interagency, academia, private sector and international partners, the final report will reflect the discussions, findings and recommendations of the groups of experts who participated in the workshops and conference on Cyber Power: The Quest Towards a Common Ground.

Background and Purpose

The quest for common ground cyber power refers to the lack of accepted standards for definitions, data structures, threat assessments, and policies both within and across communities that employ cyber power to achieve national interests. Our current national security system was designed in an era when wars were fought with telegraph, landlines and radios. Today, cyberspace as a whole, and the Internet in particular, are the domains where conflicts are being organized and fought. In 2012, the Air Force Research Institute (AFRI) at Air University conducted a symposium series to contribute to a better understanding of the structural sources of cybersecurity challenges and to identify whole-of-society approaches to serve as framework for identifying solutions and better-informed policies. Our project considers current and potential ways to strengthen and expand the way we are organizing the unified response to cyber incidents of national significance. The project is designed to stimulate and develop experientially informed, interdisciplinary research on how to improve interagency effectiveness, private sector collaboration, and international partnerships. The result of our long-term efforts will be the sharing of experiences and selected best practices as a viable, near-term basis for transforming interagency cybersecurity cooperation. This project will also frame strategic issues and suggest plausible directions for the Air University's Cyber Air Corps Tactical School (C-ACTS).

Phase One: April 2012, Senior Leader Engagement in Classified Workshop

The first phase of this project was a classified workshop on Cyber Power, National Security and Military Operation convening on Maxwell AFB on April 2012. Participants were senior US policy makers invited to discuss topics including: *Is the U.S. Government generally acting in an ad hoc manner or is it developing effective strategies to integrate its national security resources in cyberspace? How well are the agencies/departments working together to implement these ad hoc or integrated strategies? What variables explain the strengths and weaknesses of cyber strategy? To what extent are technical capabilities hampered by policy?* Researchers used a modified Delphi methodology to survey participants on questions related to those posed above.[1] The participants were experienced cyber specialists from across the interagency, and the US Air Force.[2] Interagency participation assured that an Air Force perspective did not dominate the discussion. Participants were asked to complete questionnaires, examining a wide range of variables, trends, and futures, currently or with the potential to affect national security and military operations in cyberspace. Questions were scored on a five point Likert scale with "strongly disagree" and "strongly agree" representing opposite ends of the scale. Results were then computed and displayed in order to determine statistically significant divergences of opinion within the room. The participants then spent the remainder to the 1.5 day workshop openly debating the questions posed aided by survey results. Outcome documents from the April event remain classified.

[1] Norman Dalkey and Olaf Helmer, *An Experimental Application of the Delphi Method to the use of Experts*, (Santa Monica, CA: RAND Publishing, 1962), 1. Originally developed by the RAND Corporation in the early 1950s, "Its object is to obtain the most reliable consensus of opinion of a group of experts. It attempts to achieve this by a series of intensive questionnaires interspersed with controlled opinion feedback."

[2] Represented organizations were: Office of the Director of National Intelligence/Cyber, Office of the Secretary of Defense/Cyber Policy, United States Cyber Command, National Security Agency, 24th Air Force, Central Intelligence Agency, Federal Bureau of Investigation, Air Force Research Labs, USAF/A8, Air Force Institute of Technology, Air Force Research Institute, Air War College, and the LeMay Center for Doctrine Development.

By holding the workshop in April 2012, AFRI framed issues for the remainder of the cyber power series, as well as Air University's cyberpower conference scheduled October 2012. The workshop also served to frame plausible directions for the creation of a Cyber Air Corps Tactical School (ACTS) at Air University.

Phase Two: August 2012, Engaging with Whole-of-Society Cyber Stakeholders

In August 2012 AFRI convened a workshop on *Cyber Power, National Security and Collective Action* to examine whole-of-society roles and responsibilities within the context of organizing national cyber power. The need for a whole-of-society approach to resolving the national security issues facing the United States in the twenty-first century was reaffirmed in the 2011 National Security Strategy: "We are improving the integration of skills and capabilities within our military and civilian institutions, so they complement each other and operate seamlessly. . . . However, work remains to foster coordination across departments and agencies. Key steps include more effectively ensuring alignment of resources with our national security strategy, adapting the education and training of national security professionals to equip them to meet modern challenges, reviewing authorities and mechanisms to implement and coordinate assistance programs, and other policies and programs that strengthen coordination."[3] This workshop was designed to provide inputs for a process that will inform the creation of cultures and mechanisms that enable a whole-of-society approach to coordinate elements of national cyber power and engage our adversaries in cyberspace.

Phase Three: October 2012: 2nd Annual Conference on Cyber Power: The Quest for a Common Ground

The debates from the workshop series were expanded to a group of 160 conference Project cyber power concluded its program of work with a conference in October 2012. Following general sessions, participants then grouped into concurrent breakout sessions, and through guided discussion, provide answers to strategic-level questions concerning cyber power, national security and military operations. The results of the conference will be shared by the end of first quarter 2013. To provide an ongoing exchange for research and policy collaboration amongst its members, AFRI will experiment with Internet based technologies to continue the dialogue amongst all stakeholders throughout the year until the 2013 conference on Cyber Power

[3] The White House, *National Security Strategy* (2011), 14.

Project Participants	
Principle Investigator	
Dr. Panayotis A. Yannakogeorgos	Air Force Research Institute
April Workshop Participants	
Gen. (ret). John Shaud, Ph.D.	Air Force Research Institute
Maj. Gen. Jon Davis	OSD/Cyber Policy
Mr. Robert Joyce	National Security Agency
Dr. Richard Raines	Air Force Institute of Technology
Mr. Sean Kanuck	Office of the Director of National Intelligence
Dr. Kamal Jabbour	Air Force Research Labs
Mr. Robert K.	Central Intelligence Agency
Ms. T.H.	Central Intelligence Agency
Dr. Deborah Schneider	Department of State
Mr. Brian W.	Federal Bureau of Investigation
Mr. Brian M.	National Security Agency
Mr. Frank S.	National Security Agency
Col. Lee Wight	US Air Force/A8
Col. Tim Lunderman	US Cyber Command
Maj. Keira Peollet	US Cyber Command
Dr. Dale Hayden	Air Force Research Institute
Dr. John Geis	Air Force Research Institute
Dr. George Stein	Air War College
August Workshop Participants	
Gen. (ret). John Shaud, Ph.D.	Air Force Research Institute
Dr. Lee Fuell	AFISRA/NASIC
Dr. Rick Raines	Air Force Institute of Technology
Col. Forrest Hare	National Security Agency
CAPT (ret) Scott Jasper	Naval Postgraduate School
Mr. Marcus Sachs	Verizon
Ms. Lisa Gumbs	US Cyber Command
Dr. Roger Hurwitz	Massachusetts Institute of Technology
Mr. Jay M.	Central Intelligence Agency
Mr. Mandip Bhuller	Oracle
Dr. Randall Dipert	SUNY-Buffalo
Dr. Jan Kallberg	University of Texas-Dallas
Col. Lee Wight	USAF/A8
Dr. Dan Campbell	Georgia Tech
Mr. Jim Young	Google
Dr. Chad Dacus	Air Force Research Institute
Mr. Mark Langley	Georgia Tech Research Institute
Mr. Michael Ivanovsky	USAF/ LeMay Center
Lt. Col. Melinda Moreau	USAF/LeMay Center
Mr. Michael Cabusao	USAF/ LeMay Center
Mr. Richard Austin	USAF/ LeMay Center
Mr. Jimmy Hataway	USAF/LeMay Center
Lt. Col. Rocky Favorito	USAF/Air War College

The number of invited experts balanced best between the needs for focused and explorative discussions. The participants were chosen from across the military, government, private sector and academia, on the basis of their expertise and involvement in cyber processes.

August 2012 Key Meeting Insights: Organized by Panel Session

This document provides a high-level summary of the discussions at the 29-30 August Air Force Research Institute (AFRI) workshop *on Cyber Power, National Security and Collective Action*. It documents the key takeaways related to the thematic questions posed to the group. In addition, it summarizes the next steps for AFRI's Project on Norms, Stability, Territoriality and Integrity in Cyberspace.

Panel One: National Security and Cyberspace

What is the private sector's role in national security applications of cyberpower?

What functions or tasks should be fulfilled by the US Government/DOD?

What functions or tasks are better fulfilled by private sector?

All the guiding questions are still essentially unresolved. Three issues that have persisted since the 2006 AF Cyber Task Force:

1) What is cyberspace? USAF lost argument there.
2) Why the USAF? What makes USAF special to handle cyberspace? Answer got lost in rice bowls here.
3) Why the military at all? Do we need to militarize cyberspace at all?

Why the military? It's a tough case to make because so little is 'owned' by the military. Most of the assets are controlled by private entities. Two approaches have been taken: (1) Looking at analogous decisions we've made such as piracy on the high seas (ships are still traversing the world despite threat) and public health (West Nile Virus). Also Pearl Harbor—how does the military protect us from a cyber Pearl Harbor? What can these problems and decisions that were made guide us? (2) Weighing the relative merits of different courses of action (brute force method).

How do you make the business case? Examine interdependencies and always keep those in mind. What if the military clamps down on the logistics network that private industry relies on to stay in business? What is a private sector responsibility vs. a public sector responsibility? Perhaps the distinction between public and private is a western artifact. We can take military action against essentially commercial interests when they threaten national security.

Why must we be hamstrung by the law with respect to cyberspace? Private sector is far more innovative so must retain separation but protect through public sector so that public is not subject to outages of critical systems. Companies run the critical infrastructure but should government protect these systems? Injection of military systems into this would raise many jurisdictional issues. "Shamoon" virus (30,000 machines taken offline at Saudi Aramco). Did Iran do this as retribution for sanctions? This was a public organization with private defenses. Private sector often provides the tools even for public entities' defenses. Perhaps Stuxnet is the model for how nation-state attacks will proceed in the future. "Less sexy may be the norm."

What would private sector be willing to sacrifice to have government protect them? This is a societal education and personal responsibility issue. You must protect your own system. How do we raise the level of responsibility? Response was given: You determine who is liable? Do we need minimum certifications for certain jobs required by law?

Auto Industry analogy: Is the evolution of auto insurance/driver licenses the model for how cyberspace environment will evolve? The federal government regulates the highways, and automotive standards. Why not regulate the software industry the same way for cyber safety and hygiene? While there was interest with this analogy, one participant noted that there is no permanence in cyberspace. One second it's a car, and the next it's a pickle.

Judge Green decision breaking up "Ma Bell" ordering AT&T to assist in the creation of seven new regional telephone companies enabled the Internet because public sector got out of the way of private entities. Now we could have third-party services. Previously we had AT&T which was essentially a private firm that was granted a monopoly by the government. We can't regulate the Internet as heavily as we did the telephone companies because the infrastructure cost isn't as burdensome so there is no rationale.

The distinction between public and private is political, so it's artificial to a degree. Who will pay for cybersecurity is the principle guiding public-private partnerships.

Maritime piracy analogy: In the past these were allied with nations while defenses weren't always agents of the government. Today, is it the responsibility of the Russian government to prevent their citizens from attacking other countries? Since the U.S. is the number one origin country, are we responsible for our citizens' actions? Can we just hide behind lack of state sponsorship? One suggestion was for ISP liability, noting the success of the Microsoft-Teliasonera-CERT cooperation. The success of this model resulted in a dramatic reduction of infected computers on the Teliasonera network. One participant suggested this case as a suitable best practice of balancing privacy and civil liberties with national security.

Global perceptions of content versus carriage: Chinese government does not differentiate between content and carriage. Things we wouldn't hold other governments responsible for they would. Perhaps international bodies will arrive at a useful set of international norms. One participant understands there is no hope of getting an agreement on extradition. It seems we don't hold actors responsible because of impermanence of cyber activities. We should if their effects are permanent as we would with terrorism. We're hamstrung by relying on legal paradigm for punishment. Do we need to bring back letters of marquee and reprisals?

What responsibility does the ISP have to keep their systems clean and to keep their users in line? What about aggregation of issues for national security purposes? How could you identify a threshold for responsibility for aggregate behavior? Individual acts may not reach the level of criminality but overall activities make it unacceptable and perhaps even reach the level of national security threat. Maybe we shouldn't look at individual cases but look at the entire pattern of behavior. In other countries it's getting to where you have to show ID to get an account and you are forced to get viruses off your computer or you're taken off the network.

Intent also matters here. Is it Boeing hacking into Lockheed or the Chinese hacking Lockheed? Private sector demands benefit for providing required protection…say some sort of insurance or indemnification against breaches. "If you give us the machine, then protect us when it doesn't work."

Is it analogous to health insurance? Do every Internet connection need minimum levels of protection due to externalities just like health insurance? Historical dialogue is more important than the final decisions. "Piracy was resolved by blowing up the nest." Maritime analogy seems more apt. Insurance was part of the solution there and they are attempting to figure out how to provide it for cyberspace.

Smaller countries maybe a good guide. Estonia, for example, could provide a guide through their public-private partnership.

Harmonizing global laws: Japanese couldn't prosecute cyber criminals until 2 years ago, for example. Swedes passed draconian laws and then reversed them a year later. You'll hold your enemies responsible if there is some doubt as to attribution.

Is public vs. private a zero sum game? Does the private sector have to give something up or can it continue along its path? In addition, how about using a combination of GOTS and COTS? Why does it have to be one or the other?

Attribution and State Responsibility: Another participant noted that it is easy to look at China, for example, through the Google Aurora attacks. And argue "These governments aren't helping us." Now that the Obama Administration has 'taken credit' for Stuxnet, Iran may hold US responsible through international courts. This is the primary issue in offensive cyber. A counterpoint was made that, assuming the media reports are accurate, the Stuxnet example would have been a case where a computer virus was targeting facilities already under UN Security Council sanctions, and thus there would be no case for the Iranian's to take to international courts.

One participant suggested that the federal government should take disproportionate action in response, as the Romans used to do. We don't want to get into a tit-for-tat situation. The government has a strong say because they can require standard before you can do business with them. The technology exists for effective information sharing but the limited degree of anonymity is a hurdle. The government purchasing power is overstated because they can make that up partially through international sales.

For unstable governments, deterrence works much better because consequences (overthrow/execution) are potentially much more dire.

Further questions fielded included issues pertaining about holding the US responsible for private citizens that have been punished through FBI and courts? Once we have attribution, does that really get us closer to doing something about it? Will we really be able to hold people responsible? Several cases, including the transnational Ghost Click investigation were mentioned in response as good indicators of individual responsibility if states cooperate.

Information Sharing and Economic Security If loss of info is so serious that national economy is affected, then it becomes a military issue not a law enforcement issue. Inevitable human behavior that becomes a leadership or discipline issue

A concern regarding focusing on information sharing to prosecute individuals was identified as one problem area. A participant noted that even with prosecution as the end goal, information sharing during international investigations doesn't really have benefit because "it's not going to help us get that money back." Effective norms are part of the solution but don't ensure lock-step cooperation but does induce "social pressure." One participant counter argued with the point that prior to the Law of the Sea Treaty, norms have succeeded on the oceans for hundreds of years prior to the formal treaty.

Difference between 'can' and 'should' is important for DoD vice DHS. DoD can but maybe DHS should.

Cyber IP theft is rising to the level of national security threat, but IP threat has NEVER been considered an act of war. Gen Alexander has no leg to stand on if he wants to pursue these as acts of war and one participant thinks it was irresponsible for him to mention this possibility. Perhaps the sheer magnitude of theft is the difference today. The means for acquiring IP and attacking are so close that maybe that is the distinction for the historical treatment versus in cyber.

Concluding Remarks: What functions or tasks should be led by the government and what activities led by the private sector? What is the threshold for the government taking charge for reasons of national security? Intellectual Property theft? Maybe the appropriate ***action*** determines who should be in charge? For a large scale response, maybe DoD should be in charge because they have the most resources. If it is a case of financial crimes, then Department of Treasury and Secret Service. Cyber espionage then Department of Justice and Federal Bureau of Investigation. Overall, the using the word *lead* makes the interagency people skittish.

Going back to "GOTS": Should we go back to "Government off the shelf" Models? We've finessed this question and it's probably impossible to completely go back to GOTS. The sheer cost of running the cables itself makes it prohibitive. IPv6 allows for government customization. Does the threat getting out of hand force our hand to go to GOTS? It's a cost-risk question. 360 Safe produced by China is an example that is successful in cutting down hacking (not GOTS but indigenously produced). We could learn from that. GOTS means both OS development and software development. What about getting the people and then the timeline that would be involved is quite onerous (10-15 years in total?).

Panel Two: Technology and Policy

How do private-sector applications of technology differ from national security applications of technology?

What role do privacy, anonymity and authentication play in each of these categories of applications?

What is the best way to foster private sector understanding of national security policy?

Private Sector Security Concerns: Main concerns identified were 1) Protecting Identity/Data 2) Buying history, credit cards 3) Securing Personal identifiable information such as social security numbers. All of this is important in order to maintain consumer trust.

Preserving Intellectual Capital: According to FBI reports, corporate Espionage cost US companies $13B since October 2011. Stealing intellectual property (IP) may shave years off research and development time, allowing competitive products to enter the market, and possibly put North American companies out of commission. Nortel is one example.

Abiding By Regulations: Compliance is costly and changes based on local and regional laws. Mostly *tick box and point-in-time* vs. *continual risk based approach*.

Sarbanes-Oxley: The Sarbanes-Oxley Act of 2002, sponsored by US Senator Paul Sarbanes and US Representative Michael Oxley. Effective in 2004, ***all*** publicly-traded companies are required to submit an annual report of the effectiveness of their internal accounting controls to the Securities and Exchange Commission (SEC).

SB 1386 (California Breach Law): California SB 1386 became effective on 1st July 2003, amending civil codes 1798.29, 1798.82 and 1798.84. It requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed). SB stands for (California) Senate Bill.

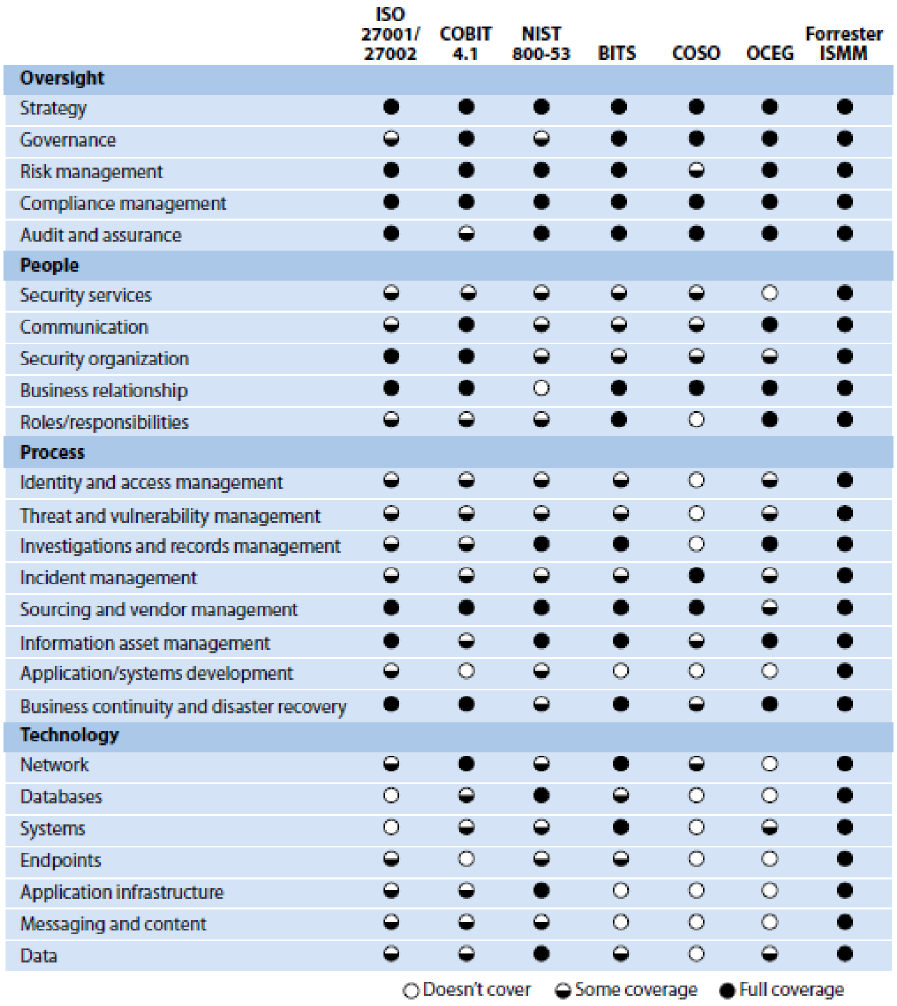
US Health Insurance Portability and Accountability Act (HIPAA): Passed in 1996, HIPAA is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient

Corporate Security Regulations in North America

- US Government Export Regulations - Encryption
- US Sarbanes-Oxley Act of 2002
- SB 1386 California Breach Law
- US Health Insurance Portability and Accountability Act (HIPAA)
- US Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT Act)
- US Electronic Signatures in Global and National Commerce Act (E-Sign)
- US Federal Information Security Management Act (FISMA)
- US E-Government Act
- US Gramm-Leach-Bliley Act (GLBA)
- The Canadian Privacy Act
- The Canadian Personal Information Protection and Electronic Documents Act

information before, during and after electronic transmission. It also identifies compliance guidelines for critical business tasks such as risk analysis, awareness training, audit trail, disaster recovery plans and information access control and encryption.

Figure 1 The Forrester Information Security Maturity Model (ISMM) Versus Other Standards



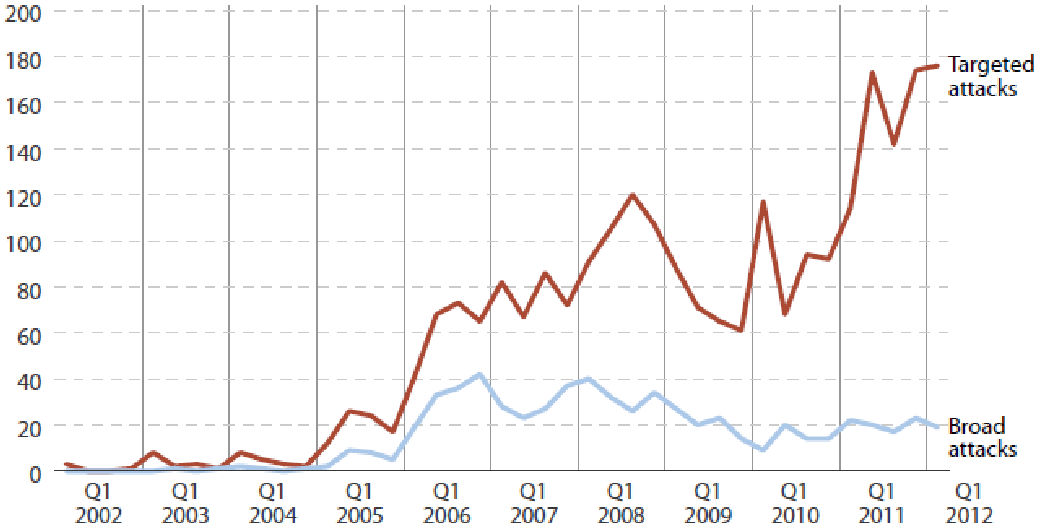
	ISO 27001/ 27002	COBIT 4.1	NIST 800-53	BITS	COSO	OCEG	Forrester ISMM
Oversight							
Strategy	●	●	●	●	●	●	●
Governance	◒	●	◒	●	●	●	●
Risk management	●	●	●	●	◒	●	●
Compliance management	●	●	●	●	●	●	●
Audit and assurance	●	◒	●	●	●	●	●
People							
Security services	◒	◒	◒	◒	◒	○	●
Communication	◒	●	◒	◒	◒	●	●
Security organization	●	●	◒	◒	◒	◒	●
Business relationship	●	●	○	●	●	●	●
Roles/responsibilities	◒	◒	◒	●	○	●	●
Process							
Identity and access management	◒	◒	◒	◒	○	◒	●
Threat and vulnerability management	◒	◒	◒	◒	○	◒	●
Investigations and records management	◒	◒	●	●	○	●	●
Incident management	◒	◒	◒	◒	●	◒	●
Sourcing and vendor management	●	●	●	●	●	◒	●
Information asset management	●	◒	●	●	◒	●	●
Application/systems development	◒	○	◒	○	○	○	●
Business continuity and disaster recovery	●	●	◒	●	◒	●	●
Technology							
Network	◒	●	◒	●	◒	○	●
Databases	○	◒	●	◒	○	○	●
Systems	○	◒	◒	●	○	◒	●
Endpoints	◒	○	◒	◒	○	○	●
Application infrastructure	◒	◒	●	○	○	○	●
Messaging and content	◒	◒	◒	○	○	○	●
Data	◒	◒	●	◒	○	◒	●

○ Doesn't cover ◒ Some coverage ● Full coverage

56671

Source: Forrester Research, Inc.

Figure 8 Targeted Attacks Are On The Rise

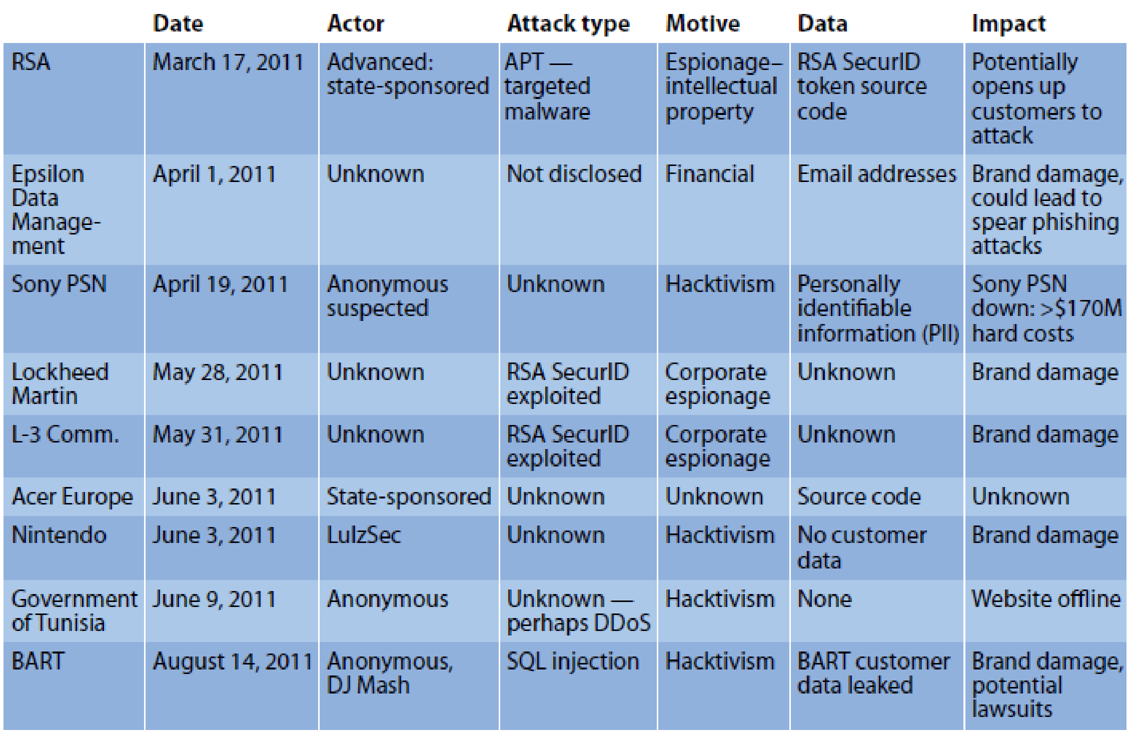


Source: CyberFactors, a wholly owned subsidiary of CyberRisk Partners, and sister company of CloudInsure.com

61544

Source: Forrester Research, Inc.

Figure 1 2011 Notable Hacks



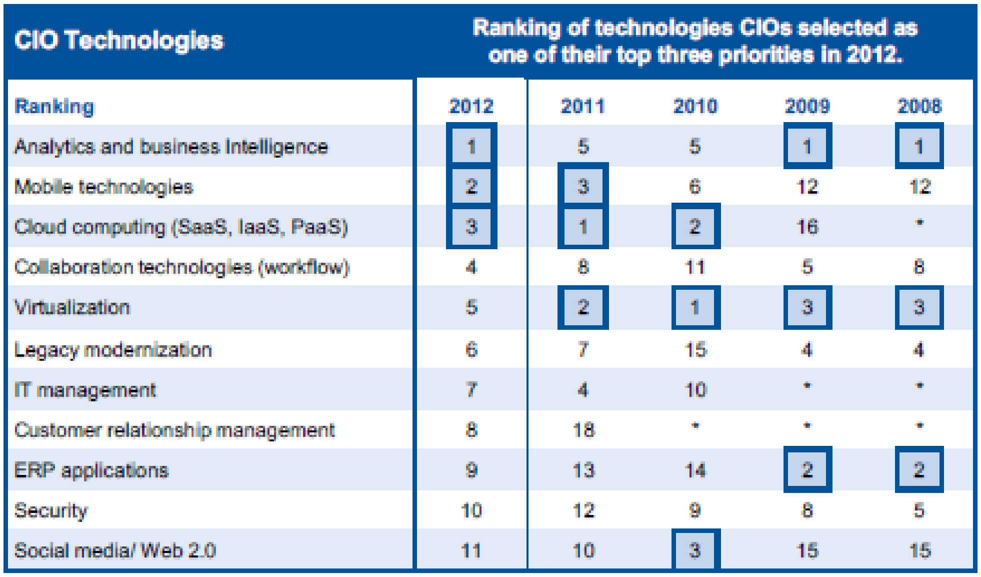
	Date	Actor	Attack type	Motive	Data	Impact
RSA	March 17, 2011	Advanced: state-sponsored	APT — targeted malware	Espionage–intellectual property	RSA SecurID token source code	Potentially opens up customers to attack
Epsilon Data Management	April 1, 2011	Unknown	Not disclosed	Financial	Email addresses	Brand damage, could lead to spear phishing attacks
Sony PSN	April 19, 2011	Anonymous suspected	Unknown	Hacktivism	Personally identifiable information (PII)	Sony PSN down: >$170M hard costs
Lockheed Martin	May 28, 2011	Unknown	RSA SecurID exploited	Corporate espionage	Unknown	Brand damage
L-3 Comm.	May 31, 2011	Unknown	RSA SecurID exploited	Corporate espionage	Unknown	Brand damage
Acer Europe	June 3, 2011	State-sponsored	Unknown	Unknown	Source code	Unknown
Nintendo	June 3, 2011	LulzSec	Unknown	Hacktivism	No customer data	Brand damage
Government of Tunisia	June 9, 2011	Anonymous	Unknown — perhaps DDoS	Hacktivism	None	Website offline
BART	August 14, 2011	Anonymous, DJ Mash	SQL injection	Hacktivism	BART customer data leaked	Brand damage, potential lawsuits

Source: Elinor Mills, "Keeping up with the hackers (chart)," CNET News, August 29, 2011 (http://news.cnet.com/8301-27080_3-20071830-245/keeping-up-with-the-hackers-chart)

60563

Source: Forrester Research, Inc.

Figure 1. Gartner CIO Technology Prioritization Ranking, 2012



CIO Technologies	Ranking of technologies CIOs selected as one of their top three priorities in 2012.				
Ranking	2012	2011	2010	2009	2008
Analytics and business intelligence	1	5	5	1	1
Mobile technologies	2	3	6	12	12
Cloud computing (SaaS, IaaS, PaaS)	3	1	2	16	*
Collaboration technologies (workflow)	4	8	11	5	8
Virtualization	5	2	1	3	3
Legacy modernization	6	7	15	4	4
IT management	7	4	10	*	*
Customer relationship management	8	18	*	*	*
ERP applications	9	13	14	2	2
Security	10	12	9	8	5
Social media/ Web 2.0	11	10	3	15	15

Lack of Corporate Security is Devastating: SONY Playstation network cost over $170M just in clean up costs. Recent analysts estimate that it will cost SONY $1.25 Billion in lost business, compensation and new innovation. Hacker Kevin Mitnick stole Solaris source code, worth $80M at the time. Beijing Motor received 4000 sensitive FORD documents (41 system designs) absconded by Mike Y. The list goes on.

Although persistent attacks are a big worry, Gartner's CIO Technology Prioritization 2012 report indicates that security technology investment is on a downward trend. Companies are reluctant to admit to security breaches. They may not be willing to actively look for intruders inside their networks.

Security is considered an expense. It's worthy of investment with the CFO circles.. This results in most breaches being discovered by outsiders (suppliers, FBI, etc.).

CyberScope: The Department of Homeland Security and the Department of Justice are developing CyberScope. This is an application for handling data for FISMA reporting. Should corporations supply real time CyberScope information?

Are breaches a network problem, law enforcement, or military problem? NSA briefs CEOs at the classified level but they don't get actionable information on breaches they can hand to the CIO to use to improve security.

We have "old" cyber policy; how do we keep up? How do we ever gain traction? One suggestion was to change legal information to make corporations more liable; get rid of extensive user agreements that sign your rights away? Is industry self-governance an option? Question of which level of governance should set policy; easier for private sector to manage if policies are federal; but local/state governments feel they are losing control. It was also noted that if you encrypt your data, no need for regulation. Many countries look to the US to solve the cyber problems we created. Congress is developing domestic policy that doesn't match what the State Department is proposing on the international level.

Policy driving certifications for individuals: No national standards exist; no legal framework for cyber security workers; they are not professionals because they are not licensed and can't be held legally liable. Some certified individuals can't "do" the job they are certified for. Significant problem in academia; COEs stuck in information security; not integrating knowledge in their own campuses; future workforce very narrow-minded. Some vendors are creating their own certifications but these are at the journeyman level. Thus, cyber is not sufficiently professionalized**.**

Analogy to aviation as new technology: How was aviation professionalized? Who should be driving the certification process?

- Standards must be established; must be able to define negligent acts.
- Must have grounding of principles and practices; don't have bedrock established; identify best practices.
- Cyber experts may not feel the need to be bound by ethical standards and practices; antithesis of those who want to develop industry standards. In current cyber environment, no one is responsible because there are so many self-developed specialties.

The fundamental question is how to balance mission assurance: an excellent security program may keep you from getting the job done.

What should be the curriculum for the cybersecurity professional? Security is not part of the basic design of the system; it is bolted on afterwards; should be part of basic computer science academic program; need course in secure coding. Professional engineers must sign off on design decisions; safety requirement.

What about security controls for companies? The Federal Communication Commission Communications Security, Reliability and Interoperability Council (CSRIC) – develops protocols for enterprise IT; let each sector work its own controls.

- How do you apply traditional methods of bestowing responsibility and liability, such as insurance and professional licensing, in a domain where there is great difficulty for traditional auditors to observe implementation of security measures or to identify security breaches?
- Is it possible to regulate cyberspace? Is there a way to control chaos? Internet was developed to survive physical breaks; also made it easy to resist regulations.
    - Self-regulation and government regulation will occur based upon public safety
- Last decade, consumer devices are driving innovation, not defense technology as in past decades; consumers must demand improved security.
- Younger generation willing to take risks for benefits of collaboration.

Panel Three: The Evolving Internet and U.S. National Security

What technology trends and emerging market conditions will shape the future of the Internet?

How might the evolution of the Internet impact national security and military operations?

How will social and political trends influence the future Internet?

No central authority: Internet is the world's largest "get along." There are tens of thousands of interconnected "autonomous systems." This is what makes the Internet a "network of networks"

- For example, AOL Transit Data Network (AS 1668)
- Verizon operates seventeen Autonomous Systems (AS)
- AS's interconnect at peering or exchange points

Based on US military research in the 1960s, 70s, and 80s Still using experimental protocols

- Never designed to support today's commercial uses
- Assumed that end points were trustworthy

Today's trust model is vastly different from 30 years ago: However the protocols are largely unchanged! The "Unwashed" joined the 'Net in the 1990s. Tim Berners-Lee proposed using hypertext to create a "web" of information at CERN in March 1989. First "web page" was created in November of 1990 http://nxoc01.cern.ch/hypertext/WWW/TheProject.html. Early web browsers were text only – Graphical web browsers appeared in mid-1992. Marc Andreessen and colleagues formed "Mosaic Communications Corp" (later Netscape) in 1994. By 1999, "surfing the web" was a household phrase and the dot-com explosion was in full swing –Everybody wanted to be online.

But in the Garden of Good, There Must also be Evil

- 1970s: virtually no attacks The networks were hard enough to run, why attack them?
- 1980s: academic attacks Brain virus, Morris worm. Concept papers on malware
- 1990s: script kiddies take charge Web site defacements, parlor tricks with Trojan horse remote access tools, email viruses, worms
- 2000s: value-oriented attacks, espionage, and terrorists Bots, root kits and zero-day vulnerabilities
    - Social networks and online gaming sites made excellent targets
- 2012s: SCADA, cloud, mobile devices, supply chain are the new targets
    - Hactivism is on the rise – a retro look at the 1990s!

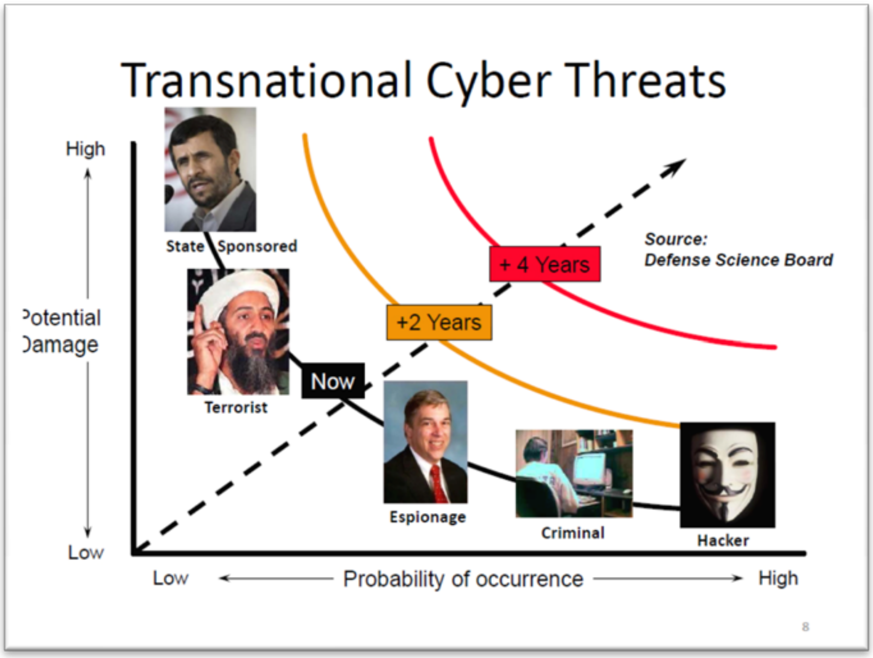
Today's Internet: Same protocols as in the 1970s and 1980s. But a completely different threat model. The Internet is home to hundreds of millions of non-government and non-academic users, and trillions of dollars of financial transactions. It is no longer a research project. It is part of our global society. It is a business. Like the "real world" the Internet is attractive to lots of bad people.

***1993**: 10,000 web sites, 1 million web pages, 3 million Internet users*

***2012** Over 600 million web sites (according to Netcraft) Over 1 trillion web pages (estimated by Google) 2.3 billion Internet users (Internet World Stats)*

Threat Actors in Cyberspace: Threat ranges from script-kiddies to nation state actors. Carrying out a significant successful cyber attack takes skill – or really good luck Sophisticated attack tools are readily available on thousands of web sites
Hiding in cyberspace is trivial for attackers

Noting the evolution of the threat actor landscape, 2012 is very different from 1998 Yesterday's threats were disruptive. Today's threats are quiet, seeking increased access to valuable information and data



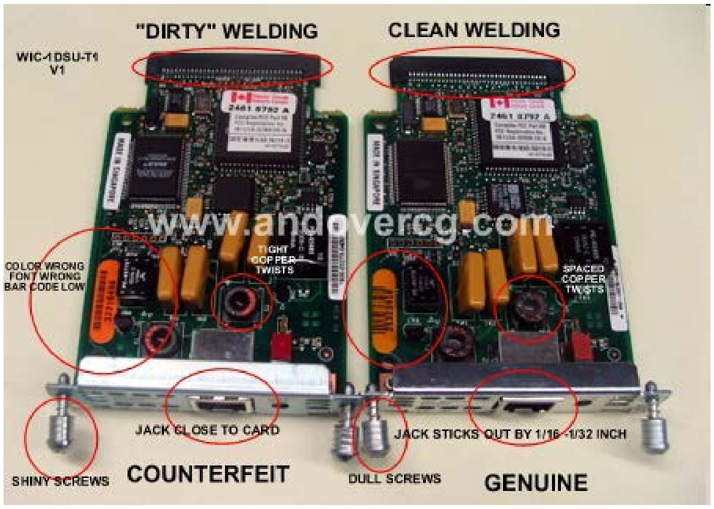
Transnational Cyber Threats

FBI Investigation of Counterfeit Routers and Hardware

Routers Models: 1000 and 2000 Series
Switches Models: WS-C2950-24, WS-X4418-GB (for CAT4000series)

GigaBit Interface Converter (GBIC) Models: WS-G5483, WS-G5487

WAN Interface Card (WIC) Models: VWIC-1MFT-E1, VWIC-2MFT-G703, WIC-1DSU-T1-V2



Counterfeit Versus Genuine
Source: http://www.andovercg.com/services/cisco-counterfeit-wic-1dsu-t1.shtml

The Internet is a “perfect” place for crime: Virtually no taxes, therefore no tax evasion. There is value in everything online. Anonymous access to vast resources Criminal tools look and act like lawful tools No national, political, or religious boundaries . Laws and law enforcement are limited. Numerous opportunities for money laundering (PayPal, BitCoin, WebMoney, etc.). Millions of clueless victims. Many criminals are annoyed that the Internet is “too slow” So much to take, so little capacity to move the stolen goods. Need to stay under the radars, remain undetected.

How Much is That Exploit in the Window?

$50,000: A zero-day exploit for Microsoft operating systems
$20,000 to $30,000 each: Other zero-day exploits
$5,000 and up: Bots that allow users to self-generate botnets
$1,000-$5,000: Customized Trojan program, which could be used to steal online account information
$250: Credit card number with PIN
$80-$300: Change of billing data, including account number, billing address, Social Security number, home address, and birth date
$100: Driver's license
$100: Birth certificate
$50: Social Security card
$4: Credit card number with security code and expiration date
$2: PayPal account log-on and password

Social Customs: We are told as children, “don’t pick something up off the street and put it in your mouth!” “You don’t know where that penny has been!” So why do we pick up a strange USB key and stick it into our computers? “You don’t know where that USB key has been!”

The Future of Network Attacks: DDoS attacks will decrease New mitigation tools are working. “Real Hackers” don’t DoS. Bot Armies will be used for distributed computing rather than DDoS.

Fraud will increase while worms decrease Too many juicy targets, including critical infrastructures and control systems. Too much value on the Internet to ignore. Watch for VOIP and streaming video fraud Online gaming community is a valuable target too

Network components will become targets of opportunity. Voice Over IP, Video Over IP all are potential future targets. Counterfeit products and supply chain attacks are emerging. “Hack and leak” is becoming the new challenge for young minds. In nearly all cases, future attacks will leverage historically insecure protocols, processes, and technologies!

Bringing Good Minds Together: “More information sharing” is a current policy theme. Today, most goes from the private sector to the government Old saying: “Tell me everything you know and we’ll keep it all a secret.” What we should be saying: “Here is what we know. What do you know?” There is lots of room for improvement. Need to start with confidence building Go beyond “trust but verify”

Why is This so Hard? No common taxonomy. Differences in technology And differences in the understanding of technology
Legal barriers Liability, Anti-trust, Privacy (ECPA in particular) all create an environment in which there are low incentives for information sharing. This is a complex problem that needs a different approach for cooperation between organizations

Legal Barriers: Privacy and ECPA: Law allows providers to collect, use, and disclose communications information for certain purposes Need greater clarity for cyber security purposes Sharing with the government is allowed in certain circumstances Need to expand to include situations where the government is the customer. Need to allow providers to collect data from consenting customers in order to provide better cyber security services requested by those customers.

What the Private Sector Tells Lawmakers: Headlines sometimes make it appear that the Internet is so vulnerable that little can be done to safeguard consumers and our country. In reality, public and private sector remediation activities are highly advanced and effective. Private sector operators have aggressively expanded the capabilities needed to identify and address cyber threats.

*Government's role in securing cyberspace centers on leadership – **setting the example** by operating highly secure networks, **building strong partnerships** with the private sector, and **increasing cyber security preparedness** among individuals and communities.*

While Not a "Top Priority" Cyber Security is Important to Congress

Senate: two major bills developed in previous session:

Rockefeller/Snow (Commerce)

Lieberman/Collins (Homeland Security)

Majority Leader Reid wants a consolidated bill passed by the end of this year. In the House several smaller bills have been drafted Cyber Security Task Force led by Rep. Thornberry. Four cyber bills passed the House in April 2012 White House has threatened a veto of the CISPA bill.

Bottom line: Cyber security is not "dead" from a Congressional point of view, but there's little time left this year to pass a bill. The economy, tax cuts, funding the government, healthcare, etc. are the priorities

Panel Four: Cyber International Relations and National Security

What impact do existing/emerging Internet governance institutional structures and norms have on US national security?

How will ongoing Internet governance debates and potential outcomes affect national security strategy?

Can Internet freedom be balanced with concepts of cyber sovereignty and national-responsibility?

Present governing structures of Internet reflects the diversity of interests of key types of players, viz., states, private sector (ICT vendors and carriers) and civil society.

  - A diversity of bodies, some institutionalized, some ad hoc that worry about operations and policies on the Internet, e.g., IETF, IGF, CERTs
  - It all works because there are technical standards that assure interoperability

- Governance and policies also reflect traditional Western distinction between carriage (communication flows) and content.
- The current challenges to the institutions, notably efforts to subordinate ICANN to the ITU (nominally an agency of the UN), would make governance more state-centric and subject content to greater political regulation, e.g., Code of Conduct.
- Any success of such challenges would also facilitate moves towards arms control agreements/ treaties for cyberspace, which would likely ban development & use of offensive weapons of the Stuxnet payload type. The US has traditionally opposed such agreements, believing it hobbles its options, hence weakens national security. One might speculate on an international agency like IAEA empowered to inspect military computer labs. But this is not going to happen and would be less effective than currently IAEA is with relation to nuclear weapons development
- Yet application of LOAC to cyberspace, which US supports, also limits use of cyber weapons vs. critical infrastructures, dependent on digital networks and cyber controls.
- Continuation of multi stakeholder model, which concedes considerable independence to both MNCs and NGOs, also has downsides
  - -openness and respect for privacy increases vulnerability to political, military and economic espionage
  - Incentives rather than commands needed to get improved security from ICT companies
  - NGOs through provocative actions toward other countries raises problem of state responsibility

Key question whether cyber future is toward fragmentation, viz., Internet in one country, per Iran & possibly China.

  - Drivers for that more political = restricting dissent than security
  - Fragmentation would encourage states to develop offensive cyber weaponry rather than focus on defense

- Effective cyber defense at national and alliance level requires quad
  - Resilience & recovery

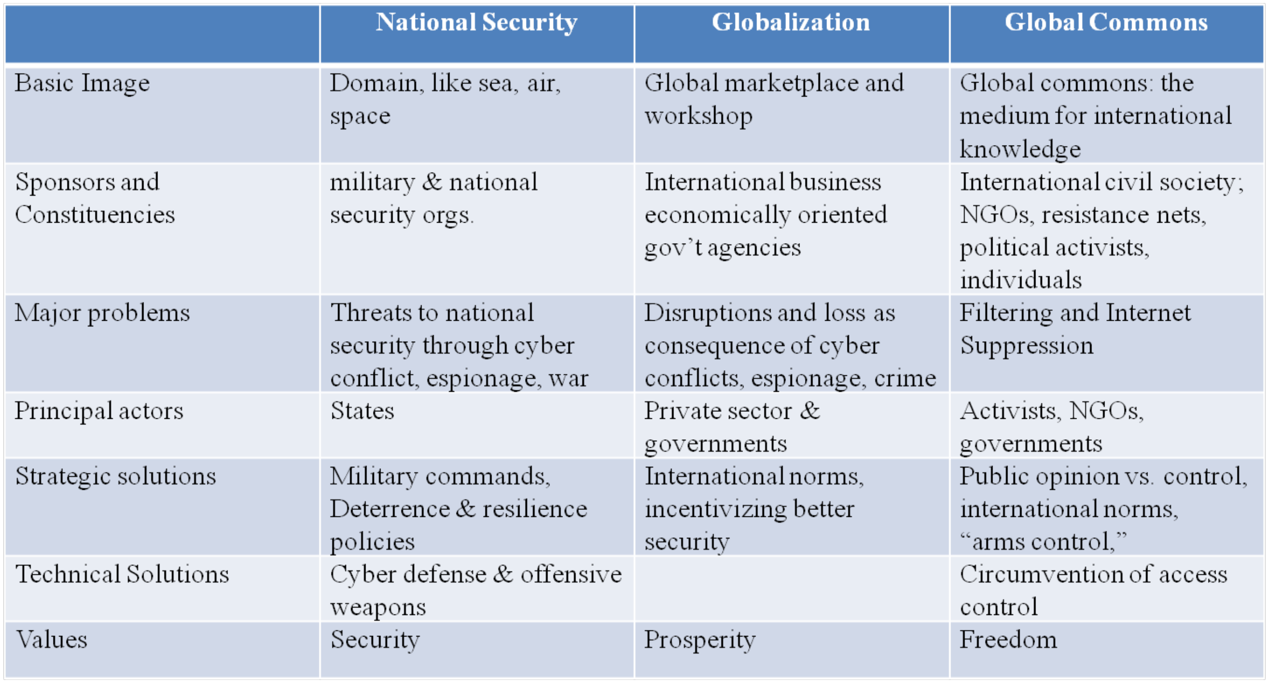
  - Norms
  - Reasonable deterrence (some threshold of confidence in attribution of attack and notions of proportionality)
  - (long term) research and deployment for technological transformation (toward invulnerable operating systems)
- Absent some set of norms (shared expectations) more dependence on deterrence, yet some of the supports of deterrence, e.g., signaling will be deficient – there will be no shared background concerning the meaning of moves and all initially will need be interpreted as instrumental (oriented toward their success/ effects) rather than communicative

US policy

  - Ripped from the headlines
    - Obama: Web freedom will be part of Democratic platform
    - GOP adopts Internet freedom plank
  - Bases
    - Ideological
      - Commitment to free speech
      - Universal declaration of human rights "freedom to information" (to which the US is not a signatory)
    - Political
      - Projection of soft power
      - Part of political campaigns v. certain states, e.g., Iran
  - Articulation & promotion
    - Sec. Clinton after Google (rhetorical)
    - Tor networks and other censorship evasion services & their dual purpose
- Conflict
  - Ideological: starting with national sovereignty or starting with human rights
  - Legal: defining information security/ assurance
  - Political: Defense of weakly legitimated regimented regimes through censorship v. interest in weakening such regimes

- Possibilities of resolution
  - US policy not absolute but selective, e.g., tolerant of Bahrain, Saudi Arabia censorship; more patient towards allies regarding their adoption of online openness
  - Chinese not entirely monolithic, and rely on populations self-censorship rather than solely on filtering and terror
    - Possibility of greater openness to extent leadership appreciates that innovation and national unity may depend on public sphere
    - Note political threats that can organize online are from ultra nationalists as well as social activists; so keeping lid on is not entirely vs. US interests
  - Perhaps sharper, clumsier response to Internet from Russia, where rapid penetration of broadband and use for organizing protests v. Putin took regime by surprise; and shock, when coupled with role of social media in Arab Spring

- Resort to bilateral rather than multilateral with Russia and particularly China on issues of Internet freedom and espionage.
- Agreeing for the present to disagree
    - Is temporizing possible with some important decisions, e.g., the World Conference on International Telecommunications (WCIT-12_, implementation IPv6.



	National Security	Globalization	Global Commons
Basic Image	Domain, like sea, air, space	Global marketplace and workshop	Global commons: the medium for international knowledge
Sponsors and Constituencies	military & national security orgs.	International business economically oriented gov't agencies	International civil society; NGOs, resistance nets, political activists, individuals
Major problems	Threats to national security through cyber conflict, espionage, war	Disruptions and loss as consequence of cyber conflicts, espionage, crime	Filtering and Internet Suppression
Principal actors	States	Private sector & governments	Activists, NGOs, governments
Strategic solutions	Military commands, Deterrence & resilience policies	International norms, incentivizing better security	Public opinion vs. control, international norms, "arms control,"
Technical Solutions	Cyber defense & offensive weapons		Circumvention of access control
Values	Security	Prosperity	Freedom

Participant Commentary

Comment 1: In the 90's people were very idealistic on use of Internet and establish of norms. Things have changed due to increased threats and domain owners and industry owners of address names wanting to influence norms. UN may not be the best place to work norms because each country has one vote. Can you sanction nations by saying no html email and no Skype for you and if you can then can you enforce them? Not sure if you can actually assess results of cyber attack as US joint doctrine states.

Comment 2: Stated it is unhelpful to look at inter as military or nonmilitary. He fears the department of treasury using cyber to conduct actions against a nation's bank vs. CYBERCOM taking action because the military is trained in the use of force. There is a move to make disruptive use of cyber to include psychological disruption is in the military's lane

Comment 3: Surprised that the military is not responsible for defending critical infrastructure**.** Thinks the questions should be when the military is responsible for defending the critical infrastructure. Capability shortfall of collateral damage is an issue but it should not limit the use of the military to defend critical infrastructure.

Comment 4: Content and conduit are two different things so what is the military's role in each category—stated military role should be in conduit not content**.** Broader discussion to the above statement was: How is this different in cyber vs. other domains e.g. military use in physiological ops?

Comment 5: Address the issue of military use of to defend critical infrastructure—difference for being responsible vs. supporting the defense

Comment 6: Mentioned how government funded research is being written and published that describe cyber vulnerabilities. Need a clearing house to ensure the published documents don't give too much away. Also, mentioned he thought that the private sector would be better to defend and even conduct some offensive ops

Comment 7: Private companies that own fiber networks see all data before users do and more data than users get to see because users only get to see data they are authorized to see. Verizon runs government networks for India, Australia etc. Since they run global networks they are actually controlling global data for select customers. Foreign ownership does not mean foreign operations

Panel Five: Project Kick-Off: Norms, Stability, Territoriality and Integrity in Cyberspace (Project NSTIC)

How are cyber-threat actors emerging from nation-states influenced by local economic, cultural, political and social factors?

Is it possible to estimate a nation-state's likelihood of being an origin or transit country for malicious cyber events?

Which metrics are effective in quantifying cyber risk and in evaluating the effectiveness of engagement in cyberspace?

The Air Force Research Institute officially kicked off its project on cyber norms and risk at the 30 August 2012 workshop. Principal investigators, introduced themselves and their methodology, and gave an overview of the key stages in the project.

Purpose: It is the goal of this study to ascertain those states which are -- or are susceptible to becoming-- origin or transit countries for malicious cyber events. Malicious cyber actors exploit gaps in technology and international cyber laws and policies to launch multistage, multijurisdictional attacks. Rather than consider technical attribution the challenge, a more accurate argument holds that “solutions to preventing the attacks of most concern, multi-stage multi-jurisdictional ones, will require not only technical methods, but legal/policy solutions as well.”[4] Deep understanding of the social, cultural, economic and political dynamics of the nation-states in which cyber-threat actors operate in is currently lacking. This project aims to develop a quantitative framework to guide US policy responses to states that are either origin or transit countries of cyber attacks. Some of the research questions to be tackled with this effort include: *How are cyber-threat actors emerging from nation-states influenced by local economic, cultural, political and social factors? Is it possible to estimate a nation-state's likelihood of being an origin or transit country for malicious cyber events? Which metrics are effective in quantifying cyber risk and in evaluating the effectiveness of engagement in cyberspace?*

Methodology and Data: Drilling down into the technological and socioeconomic fabric of societies will allow us to identify and classify countries that may provide an environment hospitable to misusing elements of cyberspace. In the first phase of the study, the research team will employ panel data regression to retain analytical power and then convert the model’s numerical predictions to a color coding to facilitate interpretation. The purpose of the regression will be to answer the research questions posed in the previous section. Panel data regression was chosen because it can incorporate both temporal effects and spatial correlation.[5] Since the motivation for malicious cyber activities may stem from a desire to advance a political agenda or from want of financial gain, potential independent variables will be drawn

[4] David D. Clark and Susan Landau, “The Problem Isn’t Attribution: It’s Multi-Stage Attacks,” in ReArch 2010: Proceedings of the Re-Architecting the Internet Workshop (NY: Association for Computing Machinery, 2010), 1, http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/11-Clark.pdf.

[5] See, for example, Badi Baltagi, Peter Egger, and Michael Pfaffermayr, "A Generalized Spatial Panel Data Model with Random Effects," *Center for Policy Research 53*, 2009.

from both the criminology and counterterrorism literature.[6] A careful review of both the social science and technical literature, coupled with interviews of cyber security experts, will facilitate trimming the number of potential explanatory variables to a manageable number.[7] This project will leverage the extensive quantitative experience of the principal investigators in the area of malicious software discovery and analysis. The principal investigators have developed successful, accurate and performance improving means for detecting and identifying the various types of malicious software through the discovery and analysis of independent and dependent variables.[8]

In the project's second phase, the focus will turn to developing software tools based on shareable data that will accurately predict the cyber risk posed by a country. For this stage of the analysis, the panel data regression results could be used or the study team could choose another approach if it offers better predictive value. For example, the team could employ risk terrain modeling (RTM), which is an empirical approach that uses Geographic Information System (GIS) software to dynamically forecast and visualize the likelihood of enhanced chances of events, and monitor improving conditions. The interdisciplinary RTM approach integrates principles drawn from risk-analysis with virtual representational tools, including GIS software. The utility and originality of RTM is fourfold: (1) The process of dynamic forecasting embedded in RTM could identify likely sources of cyber threats. (2) RTM depicts them visually, utilizing GIS software. (3) Provides an application to a series of insecurities associated with the human security framework, these threats can be identified and visually represented at multiple levels of governance, ranging from the regional to the country and, indeed, the local. (4) Such variance can be identified over time as well as space. For example, given the appropriate data set, the prospective risk of a cyber crime or attack originating or transiting through a country could be isolated both geographically (by state, province, district, or even town or village) and in terms of time.

Potential Implications for National Defense: The long-term goal of this project is to add rigor and precision to the US DoD's global cybersecurity policy and strategy through the creation of a risk model of cybercrime and conflict in each country that is a member state of the United Nations to inform the policy community of global cyber risks by drilling down into the technological and social fabric of societies to examine how vulnerabilities influence the impact of threats and how community, as well as political, responses influence consequences. The software tools produced through this research effort will fill informational gaps within DOD and the US intelligence community. These tools will allow for the evaluation of international cyber policies and help identify those countries that are likely to increasingly serve as origin or transit countries for malicious cyber activities.

[6] Leslie W Kennedy, Joel M. Caplan & Eric Piza. "Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies." *Journal of Quantitative Criminology* Vol. 27, No. 3 (2011) 339-362.

[7] Although the choice of the dependent variable has not been finalized, virus software companies and volunteer groups have collected information on malicious activities for up to eight years. This should provide adequate data for statistically powerful hypothesis testing.

[8] Thomas Dube, Richard Raines, Gilbert Peterson, Kenneth Bauer, Michael Grimaila, and Steven Rogers, "Malware Type Recognition and Cyber Situational Awareness," *Proceedings of the IEEE Second International Conference on Social Computing*, 2010, 938-943; and Thomas Dube, Richard Raines, Gilbert Peterson, Kenneth Bauer, Michael Grimaila, and Steven Rogers, "Malware Target Recognition via Static Heuristics," *Computers and Security*, 31, no. 1, February 2012, 137-147.

Appendix A: Agenda for Workshops and Conferences

Cyber Power, National Security and Collective Action in Cyberspace

An Air Force Research Institute Cyber Power Workshop

28-30 Aug 2012

PROGRAM OF EVENTS

TUESDAY, AUGUST 28

6:00 p.m. **Transportation pickup at lodging**

6:30 **No Host Reception - Dreamland BBQ, 101 Tallapoosa St, Montgomery, AL 36104; (334) 273-7427**

(Dress: Casual)

8:00 **Return to Lodging**

WEDNESDAY, AUGUST 29

7:50 a.m. **Transportation from Lodging to Air Force Research Institute (AFRI)**

8:00 **Morning Refreshments**

8:30 **Welcome, Framing Session and Initial Survey– AFRI**

Gen (ret) John Shaud, Dr. Pano Yannakogeorgos

This session is designed to provide a conceptual framework for the workshop.

All panels will consist of *brief* introductory pitches from "panel leads" followed by participatory discussion.

9:00 **Break/Refreshments**

9:15 Panel 1: National Security and Cyberspace

Panel Lead: Col Forrest Hare

What is the private sector's role in national security applications of cyberpower?

- What functions or tasks should be fulfilled by the US Government/DOD?
- What functions or tasks are better fulfilled by private sector?

11:10 Transportation to Maxwell Club

11:15 Lunch – Maxwell Club Dining Room

12:15 Transportation back to AFRI

12:30 Panel 2: Technology and Policy
Panel Leads: Dr. Rick Raines and Mr. Mans Bhuller

How do private-sector applications of technology differ from national security applications of technology?

- What role do privacy, anonymity and authentication play in each of these categories of applications?
- What is the best way to foster private sector understanding of national security policy?

1:30 Break/Refreshments

1:45 Panel 2: Technology and Policy (cont.)

3:00 Break/Refreshments

3:15 Panel 3: The evolving Internet and U.S. National Security
Panel Lead: Mr. Marcus Sachs

What technology trends and emerging market conditions will shape the future of the internet?

- How might the evolution of the Internet impact national security and military operations?
- How will social and political trends influence the future Internet?

4:30 Adjourn/Transportation to Lodging

6:00 p.m. Transportation pickup from Lodging

6:30 No Host Dinner – Central Restaurant, 129 Coosa Street, Montgomery, AL 36104; (334) 517-1155

(Dress: Coat & Tie)

8:00 Return to Lodging

Thursday, August 30

7:30 a.m. Transportation from Lodging to AFRI

7:40 Morning Refreshments

8:15 Panel 4: Cyber International Relations and National Security

Panel Lead Dr. Roger Hurwitz

What impact do existing/emerging Internet governance institutional structures and norms have on US national security?

- How will ongoing Internet governance debates and potential outcomes affect national security strategy?
- Can Internet freedom be balanced with concepts of cyber sovereignty and national-responsibility?

9:45 Break/Refreshments

10:00 Panel 5: Project Cyber Risk

Panel Leads: Dr. Pano Yannakogeorgos and Dr. Chad Dacus

How are cyber threats emerging from nation-states influenced by local economic, cultural, political and military factors?

- Is it possible to quantify those variables influencing a state's likelihood of being an origin or transit country for malicious cyber events?

11:30 Summary/Way Ahead

12:00 Workshop Adjourns

12:15 Transportation to Lodging/Airport