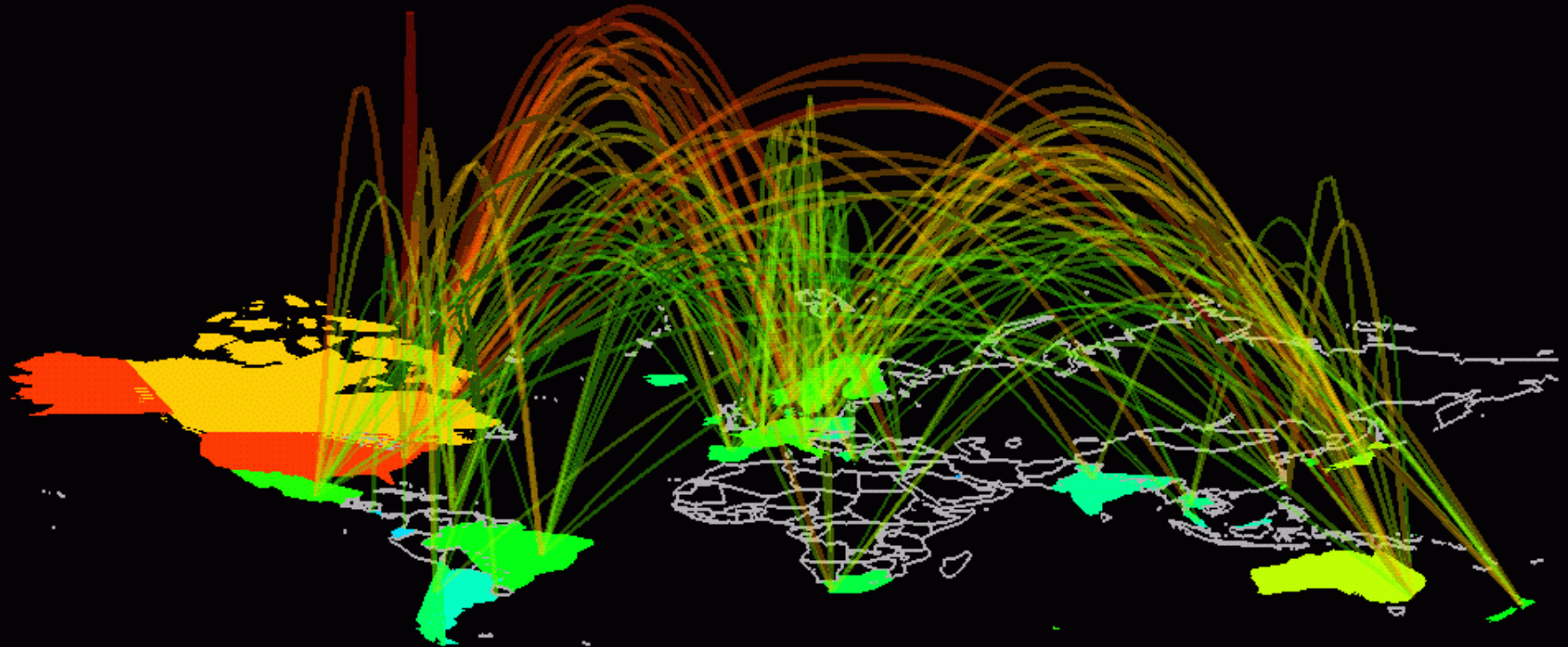




Suppose They Gave a Cyberwar and EVERYBODY Came?



William F. Slater, III, M.S. MBA, PMP, CISSP, CISA
A Presentation for Northshore Chapter of ASIS
August 8, 2013

Agenda

- Introduction
- Cyberwar, Cyberattacks, Cyberdeterrence Defined
- Some Great Writers and Thinkers on Warfare
- Cyberweapons and the Nature of Cyberattacks
- Who Is Doing This and Why?
- The Reality of the Threats
- How Vulnerable Are We in the U.S.?
- Some Worst Case Scenarios
- What Is the U.S. Government Doing to Defend the American Population?
- What Can You and Your Business Do Today?
- The Future of Cyberwar and Cyberattacks
- Conclusion
- Questions

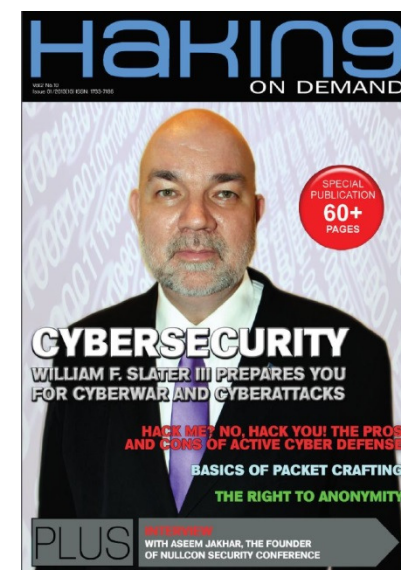
Introduction

- A career Information Technology (IT) professional since July 1977 , starting as a young computer systems staff officer in the United States Air Force supporting the command control information systems that provided real-time war plan asset information to the Strategic Air Command Battle Staff (<http://billslater.com/myusaf>)
- Current a Sr. IT Consultant / Sr. IT Project Manager / Sr. Program Manager in Cybersecurity, Compliance, Auditing, and Data Centers
- Completed Bellevue University's M. S. in Cybersecurity program on March 2, 2013
- Since October 2012, 18 published articles and one ebook
- Since 2009, I chose this topic to research and write about because as an IT professional in cybersecurity, a former U.S. Air Force officer, and a patriotic American, I am deeply concerned about the recent unfolding events of cyberattacks and cyberwarfare in cyberspace.

July 1977



January 2013



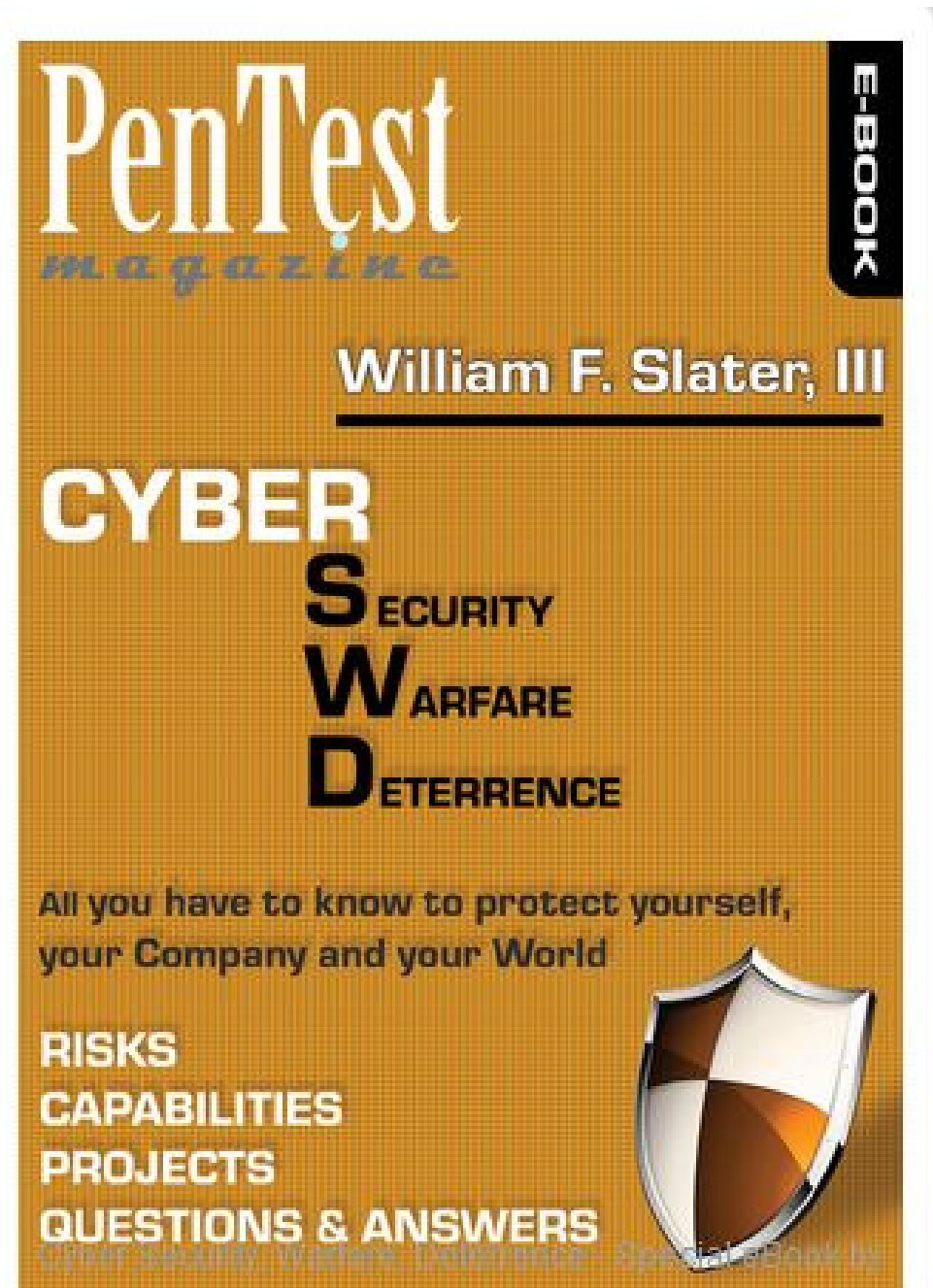
An eBook was published

- William F. Slater III
- June 10, 2013
- Collection of articles and documents related to cybersecurity, risk management and cyberwarfare
- You can read about the book and this link:

<http://billslater.com/ebook1>

August 8, 2013

Suppose They Gave a Cyberwar



WHAT'S REALLY HAPPENING ON THE INTERNET AND WHERE IS IT ALL GOING?

This image was created by Go Globe in January 2011.



Image: nfographic by- Shanghai Web Designers

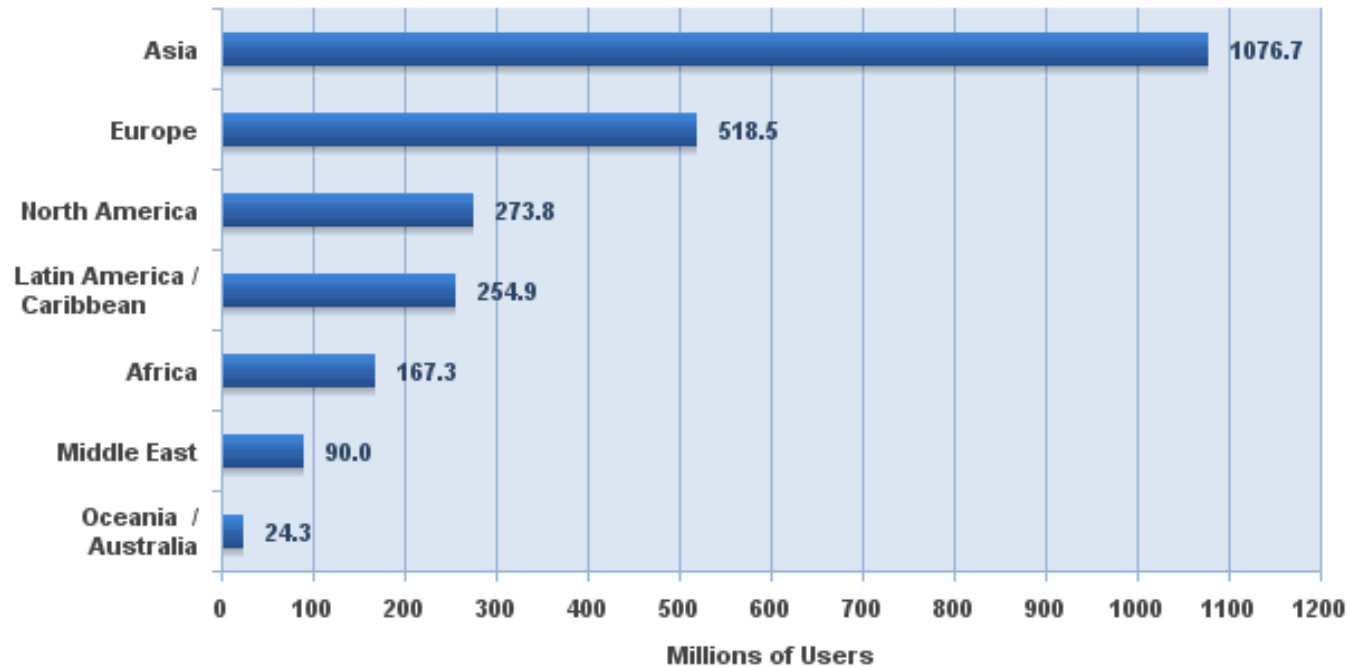
This image was created by Go Globe in January 2011.



Image: Infographic by- GO-Gulf.com Web Design Company

How Many Internet Users?

Internet Users in the World
by Geographic Regions - 2012 Q2



Source: Internet World Stats - www.internetworldstats.com/stats.htm
2,405,518,376 Internet users estimated for June 30, 2012
Copyright © 2012, Miniwatts Marketing Group

Over 2.4 Billion!

Cyberwarfare, Cyberattacks, Cyberdeterrence Defined

- **Cyberwarfare**

Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. (Wikipedia, 2013)

- **Cyberattacks**

Known as **cyberattacks**, this coined term can deal massive amounts of damage to individuals or on a larger scale, companies or government establishments. It does not stop there though, when government establishments or military establishments are attacked through cyber methods, it is a whole new kind of attack known as cyberwarfare or cyberterrorism. (Wikipedia, 2013).

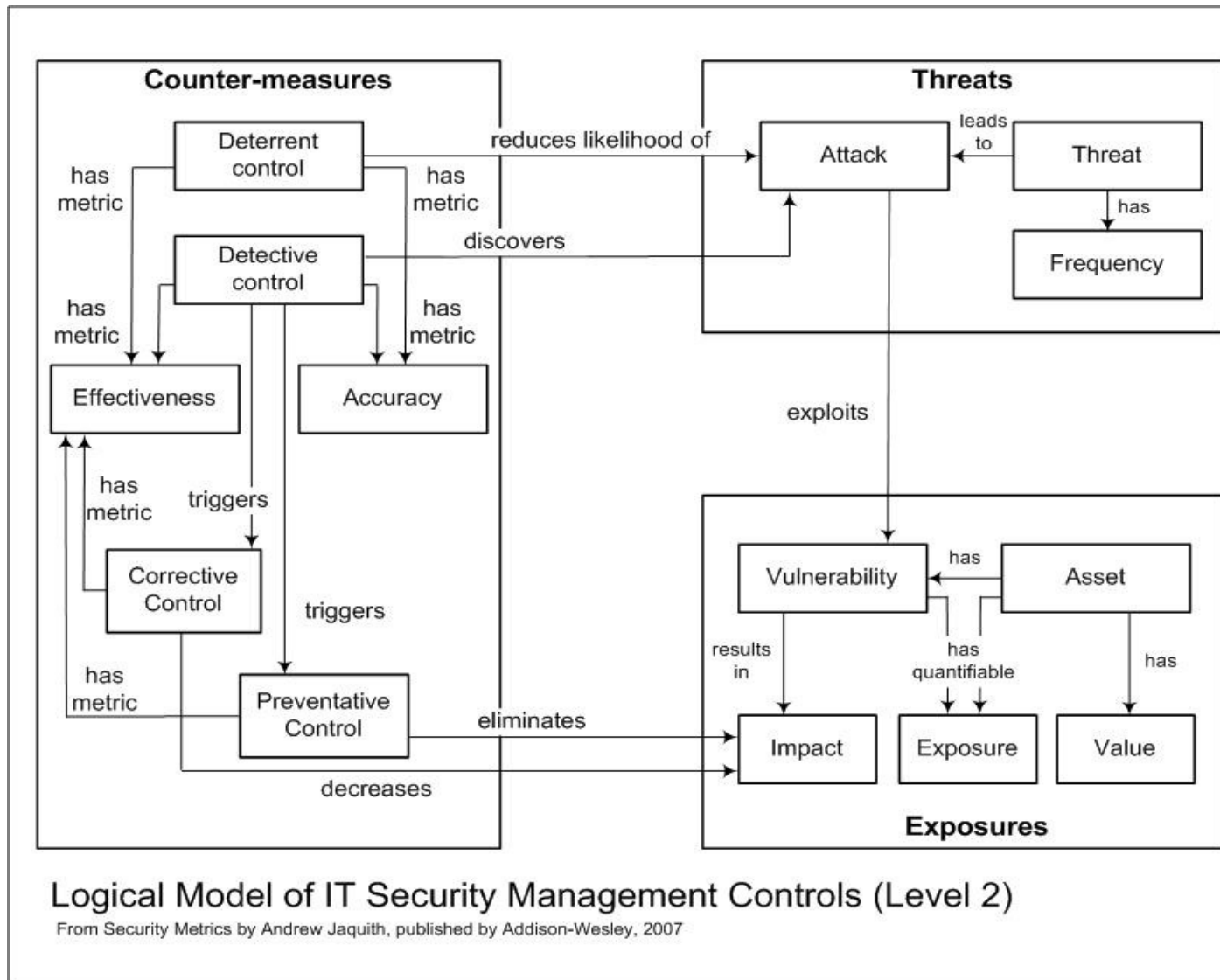
- **Cyberdeterrence**

The efficacy of **cyberdeterrence** relies on the ability to impose or raise costs and to deny or lower benefits related to cyber attack in a state's decision-making calculus. Credible cyber deterrence is also dependent on a state's willingness to use these abilities and a potential aggressor's awareness that these abilities, and the will to use them, exist. (Beidleman, 2009)

Critical Infrastructure?

- NIST takes its definition of “critical infrastructure” from the [42 U.S.C. 5195c\(e\)](#) which states that it is all “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a **debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.**”

Threats, Vulnerabilities, and Controls





Sun Tzu



Napoleon Bonaparte



Carl von Clausewitz



Nathan Bedford Forrest



John Boyd

ESTABLISHED THINKING AND WRITING ON WARFARE

Established Thinking and Writing on Warfare



Sun Tzu



Napoleon Bonaparte



Carl von Clausewitz



Nathan Bedford Forrest



John Boyd

According to Tzu, the proper application of his principles described in the Art of War, will allow the wise commander to win. Wise commanders who seek to keep their enemy guessing, off balance and reacting instead of acting is well on their way to victory. Tzu sees the use of force almost as a last resort in war. The beauty of Tzu's principles is that they focus on victory with the least damage and the swiftest resolution. This approach preserves lives, property, and public support for the government or commanders who apply it wisely. --(Zapotoczny, 2006)

Established Thinking and Writing on Warfare



Sun Tzu



Napoleon Bonaparte



Carl von Clausewitz



Nathan Bedford Forrest



John Boyd

Napoleon is credited with being great tactician and a military genius of his time. He took on all of Europe and gave everyone a pretty good run for the money. His campaigns formed the basic of military education throughout the western world and a lot of the military thinking is still influenced by the great Frenchman. Few, if any, commanders, before or since, fought more wars and battles under more varied conditions of weather, terrain, and climate, and against a greater variety of enemies than the French Emperor. His understanding of mass warfare and his success in raising, organizing, and equipping mass armies revolutionized the conduct of war and marked the origin of modern warfare. From 1796, when he assumed his first independent military command, until 1809, Napoleon displayed an astonishing near-invincibility in battle and an equally astounding ability to use that battlefield success to compel his enemies to grant him his political objectives. A dazzled Clausewitz had good reason to call Napoleon the "god of war."

His genius was essentially practical, and his military concepts evolved from the close study of earlier commanders, particularly Frederick the Great. He made the fullest use of the ideas of his predecessors and breathed life into them." (David Chandler - "Dictionary of the Napoleonic wars" p 18)

August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

15

Established Thinking and Writing on Warfare



Sun Tzu



Napoleon Bonaparte



Carl von Clausewitz



Nathan Bedford Forrest



John Boyd

Clausewitz was largely preoccupied with the massive application of force and attempts to mitigate friction in combat operations. He defined friction as suffering, confusion, exhaustion, and fear. The problem with his line of a single definable center of gravity. Clausewitz stressed the importance of finding the center of gravity, or the critical point at the critical time, upon which the outcome of the conflict depended. In this author's view, Clausewitz makes a mistake in not recognizing that combat often presents multiple smaller centers of gravity. These multiple smaller centers of gravity can be individually exploited and isolated in the pursuit of overall advantage. By exploiting several centers of gravity simultaneously, the enemy can be quickly thrown off balance.

Clausewitz did not see the importance of unconventional operations and how they could decrease the effectiveness of large opposing forces without the need for a decisive clash of massed strength. He also did not pay attention to how friction could be used against the enemy. Instead, he focused on how to limit friction's impact on one's own forces. His concentration on the importance of destroying the enemy in combat using strength against strength goes against Sun Tzu's concept of attacking the enemy's strategy --(Zapotoczny, 2006)

August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

16

Established Thinking and Writing on Warfare



Sun Tzu



Napoleon Bonaparte



Carl von Clausewitz



Nathan Bedford Forrest



John Boyd

Won 31 out of 33 Battles!

Quotes

“War means fighting and fighting means killing”

“Get there first with the most”

“Whenever you see something blue, shoot at it, and do all you can to keep up the scare”

“Charge them both ways” (Forrest caught between two larger Union armies)

Tactics

- Always exaggerated his own strength
- Forrest’s troops, if captured, would also exaggerate
- Surrounded fort in the town, expressed the desire to avoid unnecessary bloodshed
- Invite the enemy commander to see for himself that he is hopelessly outnumbered
- Built campfires for a ghost army
- Knew when it is time to go

August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

17

Established Thinking and Writing on Warfare



Sun Tzu



Napoleon Bonaparte



Carl von Clausewitz

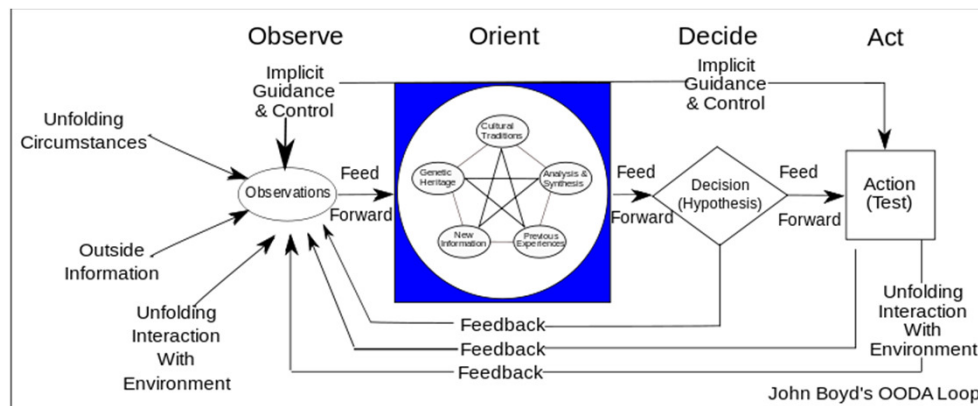


Nathan Bedford Forrest



John Boyd

Revolutionized thinking on Modern Warfare with his Observe – Orient – Decide – Act (OODA) Loop



August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

18

Copyright 2013 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

The OODA Model

(Observe – Orient – Decide – Act)

for Analysis and Conflict Resolution

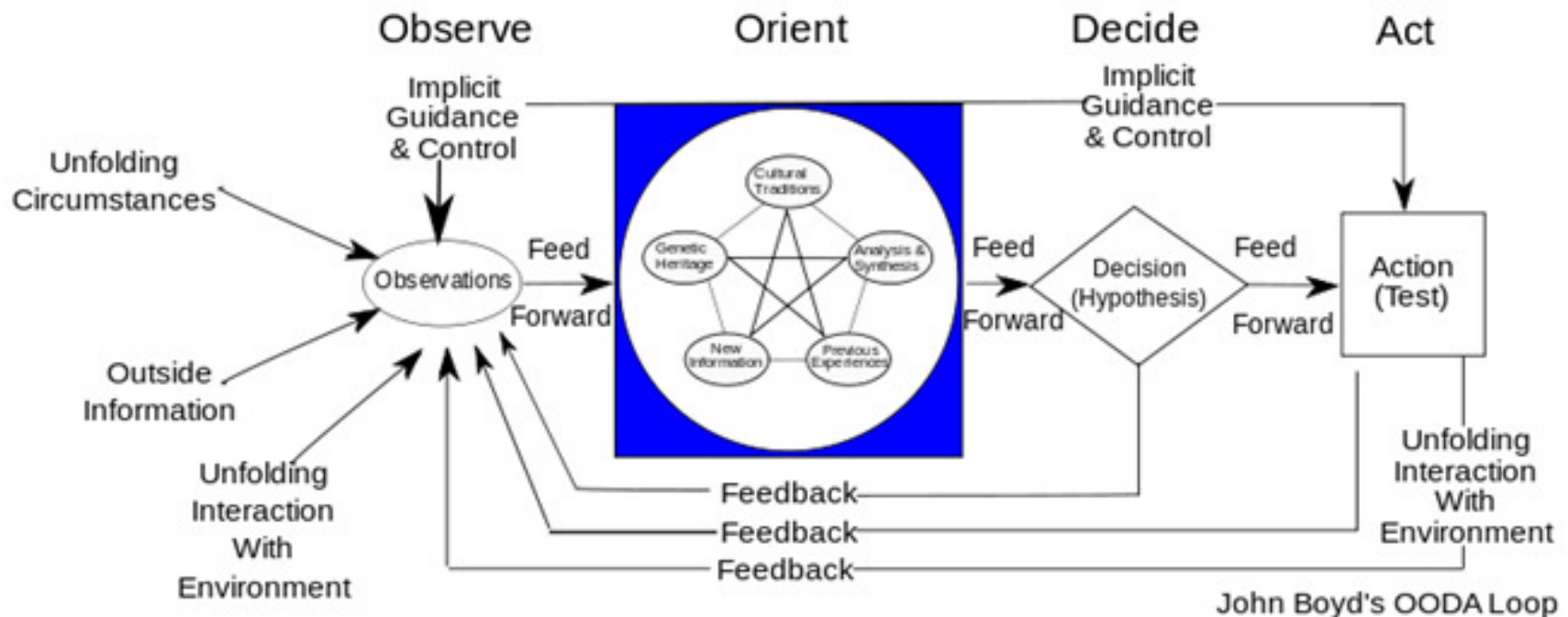
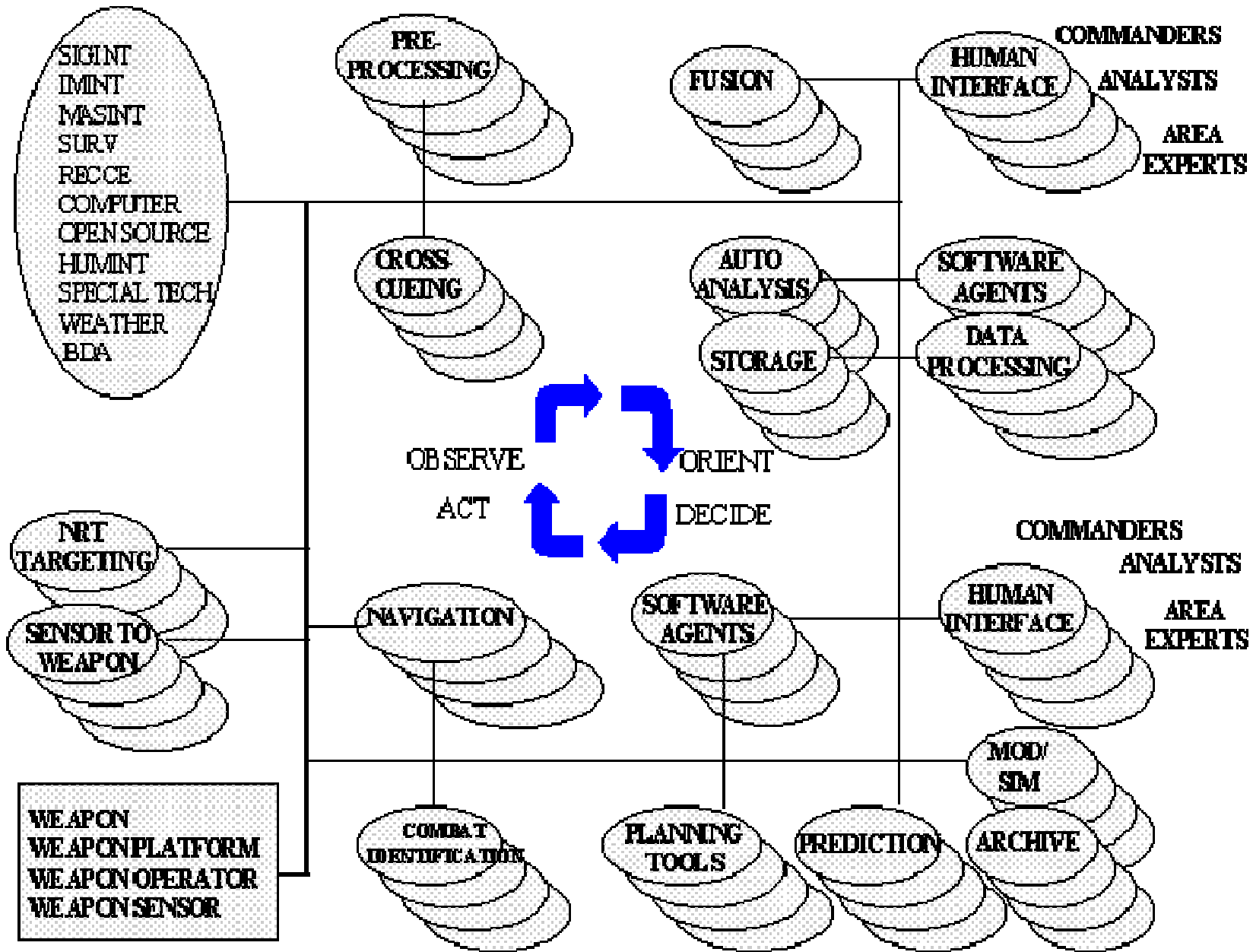


Figure 1 – Boyd's OODA Loop Model (Bousquet, 2009)



CYBERWEAPONS AND THE NATURE OF CYBERATTACKS

Some Characteristics of Cyberwarfare

- It's fast: Cyberattacks happen at Internet speeds
- It happens in "Cyberspace"
- If you are connected to the Internet, you are vulnerable to Cyberattacks
- Targets of opportunity are plentiful (i.e. any IP-device, and also SCADA devices)
- Damage can cripple critical infrastructure, up to entire cities
- Damage from Espionage and DDoS can have far-reaching negative effects
- It's cheap and getting cheaper (thanks to Moore's Law and the "Force Multiplier" advantage)
- It's sophisticated and getting more sophisticated
- It's complex to understand and defend against
- It's extremely complex due to laws, policies, and regulations, in the U.S. and in other countries
- It's not your Father's Battlefield or War.

What Makes Cyberwarfare Difficult to Analyze and Understand?

- Lack of Agreement on Nature and Definitions Among Major International Players
- The Secretive Nature, Lack of Disclosure, and Denials
- Attribution
- Provability
- It's unpredictable
- Who is “the enemy?”
- Who are the “good guys?”
- Constantly changing
- Increasingly sophisticated

Cyberweapon Evolution



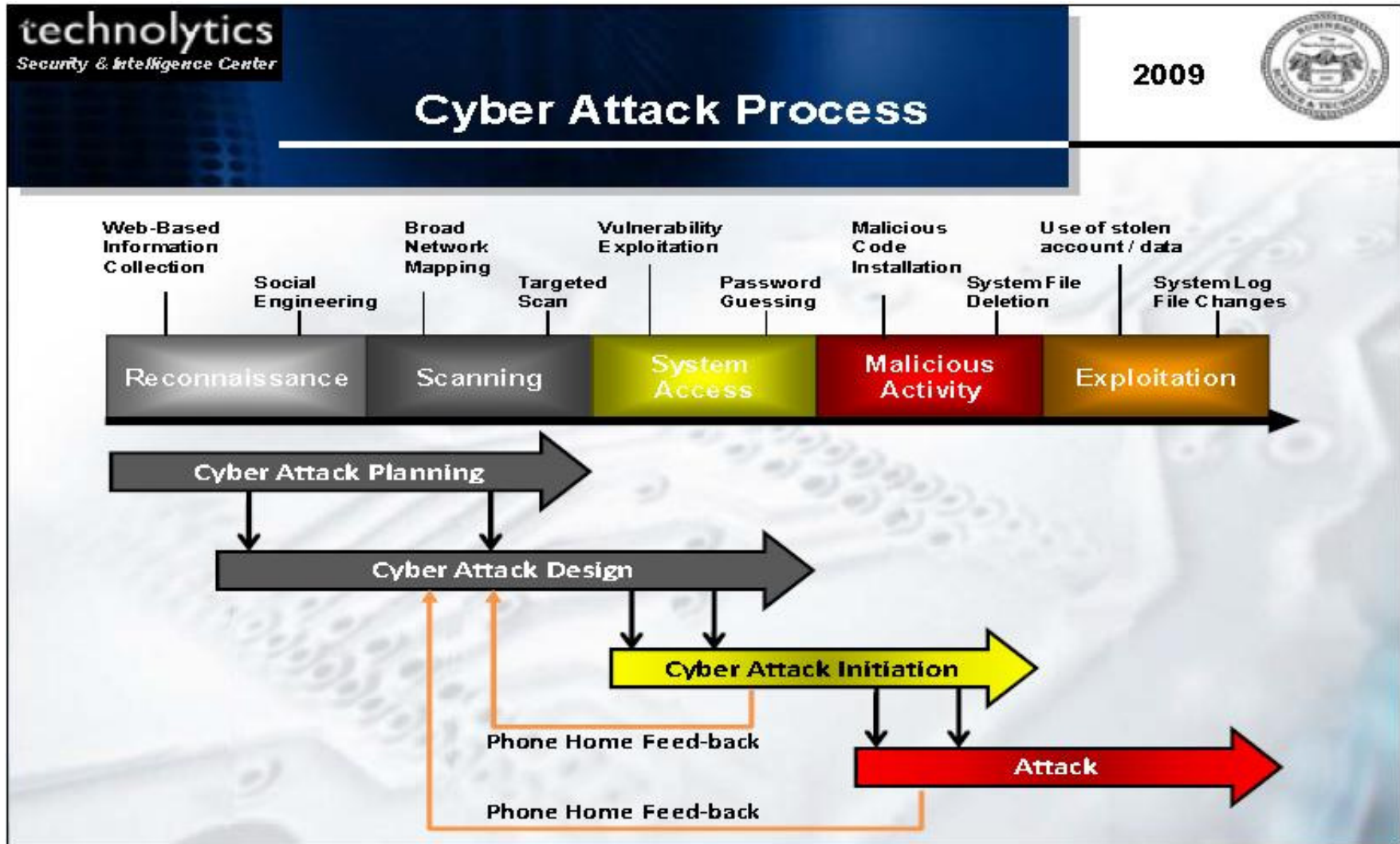
Cyber Weapons Class Capabilities Assessment

Threat Class	Threat Class Rating	Working Definition	2007 Threat Rating	2008 Threat Rating	2009 Threat Rating	Detection Difficulty	Current Availability	Current Usage
Spoofing	3.4	As spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.	3.5	3.8	3.9	3.0	3.0	3.6
Scanning	3.6	A sequential scan, potential attackers target or will randomly select an IP address in an effort to identify system vulnerabilities.	3.5	4.0	4.1	3.2	3.2	3.7
Dictionary Scanning	3.6	This type of attack exploits buffer overflow vulnerabilities in targeted client software through injection of malicious content.	3.4	4.0	4.0	3.2	3.5	3.6
Digital Snooping	4.5	The monitoring of digital networks or connections to uncover passwords or other data.	2.6	3.9	4.5	4.4	4.5	4.4
DoS & DDoS	2.9	The intentional overloading of a system with incoming traffic to cause system crashes.	2.9	3.9	3.9	1.0	3.8	3.0
Tunneling	4.3	Any digital attack that attempts to get "under" a security system by accessing very low level system functions.	3.4	3.9	4.4	4.5	4.2	3.9
Rootkits	5.0	A software tool that allows attackers to have "root level" access to the computer, which means it runs at the lowest level of the machine - below the OS.	NA	4.2	5.0	5.0	3.2	2.1
Counterfeit Hardware	3.4	The seizure of counterfeit IT equipment has raised concerns over cybersecurity. At this time, no practical method of verification exists and supply chain procurement safeguards are very limited at best.	1.5	2.8	4.2	4.8	2.5	2.0
Micro-processor Threats	2.5	The increasing complexity of modern microprocessors or chips is almost certain to lead to undetected errors that can be exploited and the possibility of malicious micro code of circuitry.	1.3	1.6	2.2	4.8	2.1	1.0
Counterfeit Software	3.3	The explosion of counterfeit code has significant security risks. It is very likely that the software is substandard with hidden cybersecurity threats.	1.8	2.0	3.7	4.8	2.5	2.3
Cellular Attacks	2.5	Malware and becoming a node on a BotNet are now threats to cell phone users and services providers around the world. While this activity is relatively new, it is expected to grow rapidly.	NA	2.1	3.0	4.0	1.5	1.6
			1	2	3	4	5	

Cyberweapons Circa 2011

Technolytics, 2012)

Cyberattack Process



Cyberwar and Cyberattacks

- Dangers and incidents related to cyberattacks and cyberwar continue to increase at an alarming rate
- Compliance with security frameworks can help
- But... entire infrastructures, cities, and countries are at risk
- The Solutions will lie in National Policy, Regulation, preparation, and some form of deterrence

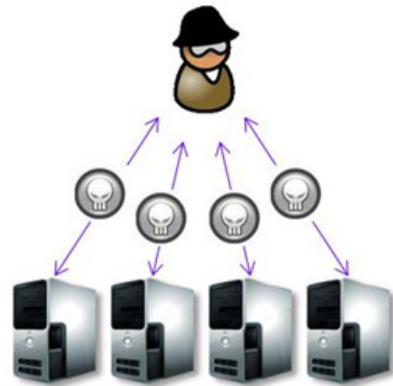


Why Should Data Center Professionals Be Concerned about Cyberwar and Cyberattacks?

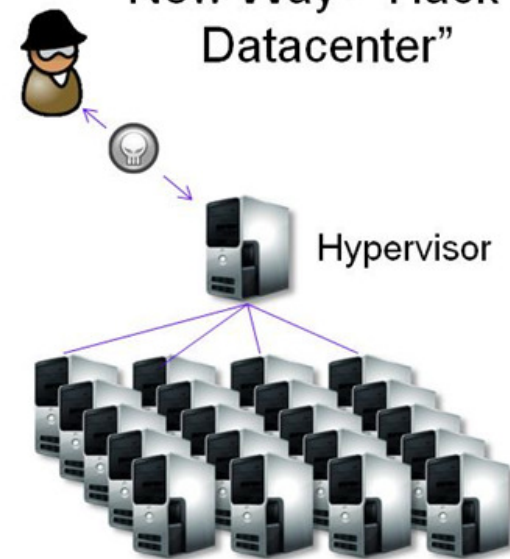
- Data Centers represent huge cyberspace infrastructure targets of opportunity

Virtualization Concentration Risks

“Old Way – Hack a System”



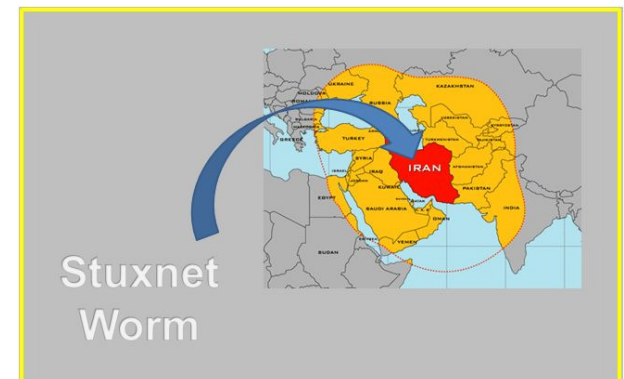
“New Way – Hack a Datacenter”



THE REALITY OF THE THREATS

Some Notable Cyberattacks and Cyberweapons 2007 - 2013

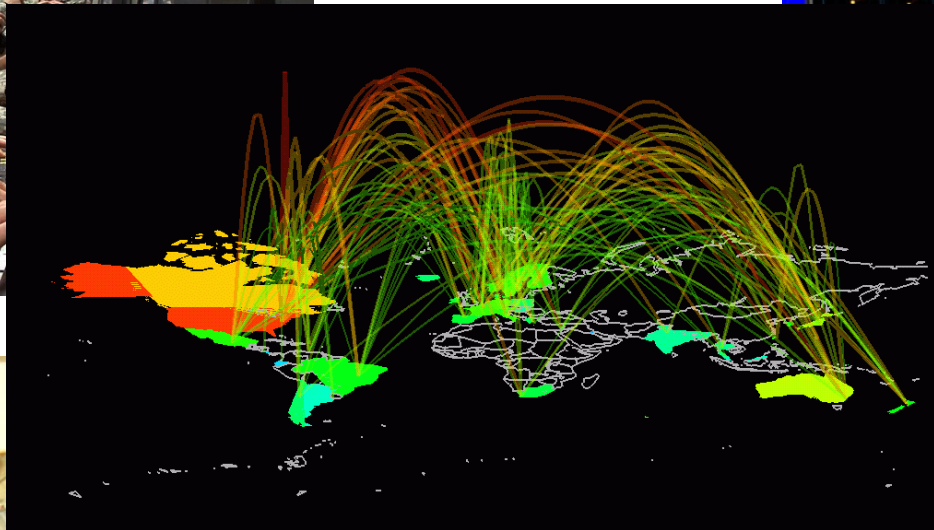
- DDoS – Russia v. Estonia, 2007
- DDoS – Russia v. Georgia, 2008
- DDoS – Russian v. Kyrgyzstan, 2009
- Stuxnet – U.S. and Israel v. Iran, 2009 – 2010
- Flame - U.S. and Israel v. Iran, 2011
- Duqu - U.S. and Israel v. Iran, 2012
- Shamoon – 2012
- DDoS Attacks on U.S. Banks – 2012 and 2013
- Cyberattacks on S. Korean Banks and other businesses on March 20, 2013
- Cyberattacks between Anonymous and Israel – April 2013



Threat Analysis

- The threat of cyberattacks and cyberwar are very real
- The quantity of cyberattacks and cyberwar incidents has increased dramatically since 2007, and it continues to increase daily
- The sophistication of cyberattacks and cyberweapons has grown dramatically since 2009
- There is now a dire need to incorporate strategies to deal with the threats of cyberattacks, cyberwarfare, and cyberdeterrence into the U.S. CONOPS Plan
- The lack of effective national plans and policies to effectively address cyberwarfare and cyberdeterrence constitutes a threat itself

What Most People Think Cyberwarfare Looks Like

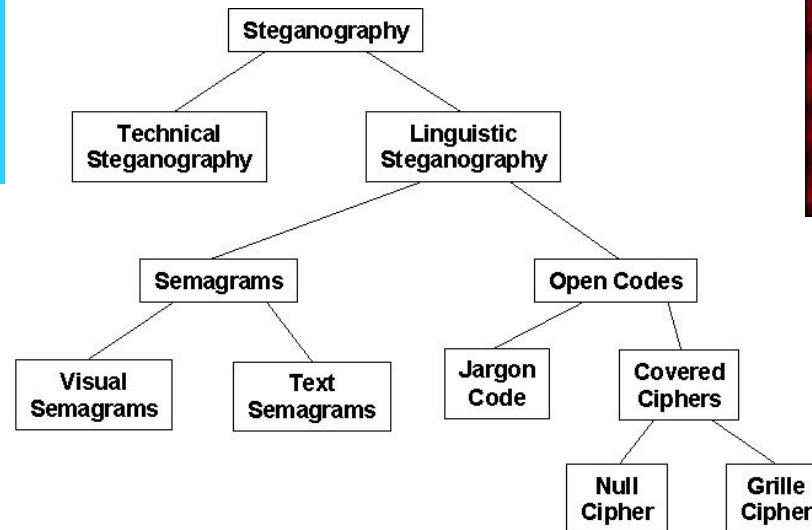
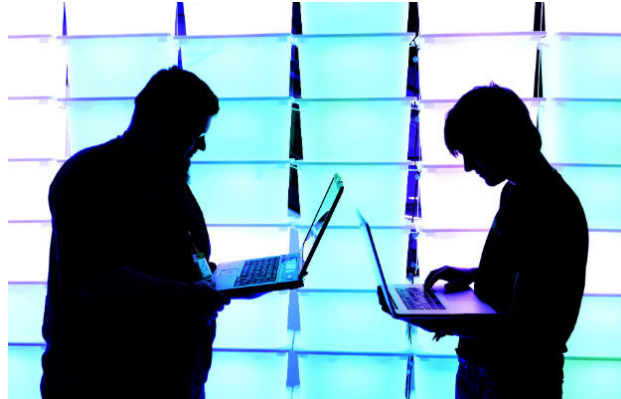


August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

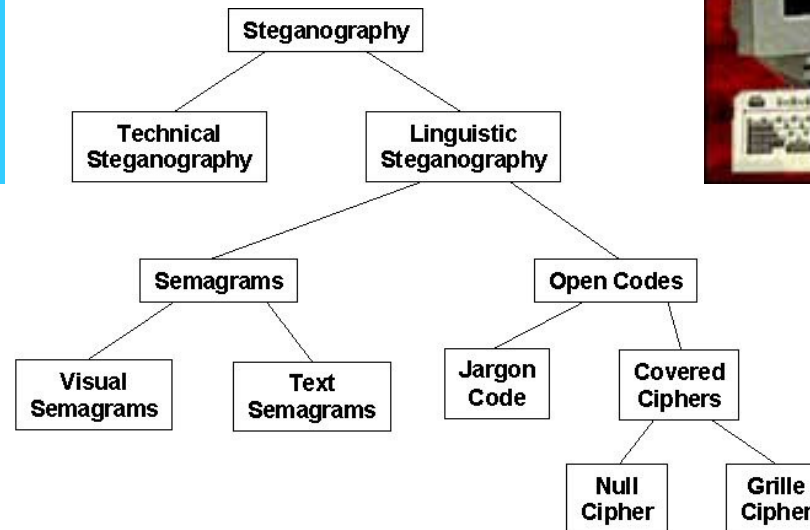
32

But Cyberwarfare May Also Look Like This



Other Cyberwarfare Threats We Should Also Consider

- Information Warfare via
 - Social Media like Twitter, Facebook, Tumblr, etc.
- E-Mail
- Steganography
- Encryption



Other Cyberwarfare Threats We Should Also Consider

- Human aspects (i.e. Edward Snowden)



June 2013 - Former Booz Allen Hamilton contractor at the NSA turns whistle-blower. Leaked highly classified information about NSA data collection, cyberwarfare tactics and activities, etc. Four laptops worth of data! Probably about up to 4 TB of classified data.

U.S. Government Electronic Surveillance in the News

- **NSA**
 - PRISM
 - Boundless Informant
 - Verizon Cell Phone Monitoring
 - Facebook Monitoring
- **Warrantless Wire Tap Act – Renewed on December 30, 2012**
 - No Fourth Amendment protections on the Internet or for phone calls (cell or landline)

U.S. Government Electronic Surveillance in the News

A word to the wise:

Here is the list of words that will get you monitored by a 3-letter security-focused U.S. Government Agency if you mention them in a cell phone call. Probably also works for e-mails, SMS texting, and Facebook postings. A contractor who works for the U.S. Government provided this so I believe it authentic, but may not be comprehensive and complete.

Special note: At one time, I believe cybersecurity was on the list. That was a special concern because I just completed an M.S. in Cybersecurity.

Domestic Security

Assassination
Attack
Domestic security
Drill
Exercise
Cops
Law enforcement
Authorities
Disaster assistance
Disaster management
DNDO (Domestic Nuclear
Detection Office)
National preparedness
Mitigation
Prevention
Response
Recovery
Dirty bomb
Domestic nuclear detection

Emergency management
Emergency response
First responder
Homeland security
Maritime domain awareness
(MDA)
National preparedness
initiative
Militia
Shooting
Shots fired
Evacuation
Deaths
Hostage
Explosion (explosive)
Police
Disaster medical assistance
team (DMAT)
Organized crime

Gangs
National security
State of emergency
Security
Breach
Threat
Standoff
SWAT
Screening
Lockdown
Bomb (squad or threat)
Crash
Looting
Riot
Emergency Landing
Pipe bomb
Incident
Facility

HAZMAT & Nuclear

Hazmat
Nuclear
Chemical spill
Suspicious package/device
Toxic
National laboratory
Nuclear facility
Nuclear threat
Cloud
Plume
Radiation
Radioactive

Leak
Biological infection (or
event)
Chemical
Chemical burn
Biological
Epidemic
Hazardous
Hazardous material incident
Industrial spill
Infection
Powder (white)

Gas
Spillover
Anthrax
Blister agent
Chemical agent
Exposure
Burn
Nerve agent
Ricin
Sarin
North Korea

Health Concern + H1N1

Outbreak
Contamination
Exposure
Virus
Evacuation
Bacteria
Recall
Ebola
Food Poisoning
Foot and Mouth (FMD)
H5N1
Avian
Flu

Salmonella
Small Pox
Plague
Human to human
Human to Animal
Influenza
Center for Disease Control
(CDC)
Drug Administration (FDA)
Public Health
Toxic
Agro Terror
Tuberculosis (TB)

Agriculture
Listeria
Symptoms
Mutation
Resistant
Antiviral
Wave
Pandemic
Infection
Water/air borne
Sick
Swine
Pork

August 8, 2013

Unhappy With U.S. Foreign Policy? Pentagon Says You Might Be A 'High Threat'

Thursday, 08 August 2013 09:01



'A security training test created by a Defense Department agency warns federal workers that they should consider the hypothetical Indian-American woman a "high threat" because she frequently visits family abroad, has money troubles and "speaks openly of unhappiness with U.S. foreign policy."

That slide, from the Defense Information Systems Agency (DISA), is a startling demonstration of the Obama administration's obsession with leakers and other "insider threats." One goal of its broader "Insider Threat" program is to stop the next Bradley Manning or Edward Snowden from spilling classified or sensitive information.'

Source: <http://www.davidicke.com/headlines>

Insider Threat Monitoring: Results



NYT: NSA Searching Americans' E-Mails for Foreign Contacts

Thursday, 08 Aug 2013 11:06 AM

By Sandy Fitzgerald

Share:    More . . .

A A | [Email Us](#) | [Print](#) | [Forward Article](#)

The National Security Agency searches through Americans' e-mails and texts for contacts or information about foreigners who are being monitored for illegal activities, according to intelligence officials who spoke with **The New York Times**.

According to the Times, the searches take place without warrants and are part of the casting of a "wider net" to target suspected terrorists that also includes the gathering of extensive computer data from overseas.

The surveillance is allowed under the FISA Amendments Act passed in 2003, which cleared the way for eavesdropping without a warrant so long as it targets a non-American traveling or living outside the United States.

Judith A. Emmel, a spokeswoman for the NSA, told The Times that the agency's activities are not meant to gather information on Americans, but to target foreign powers, organizations, or terrorists.

According to the Times, hints of the targeting program were contained in secret information leaked recently by Edward Snowden referring to "a set of rules" about how the NSA is legally allowed to carry out its surveillance efforts under the FISA law.

A senior intelligence official, speaking anonymously to the Times, said the NSA copies and then sifts through contents of text-based messages coming into and leaving the U.S. searching for identifying keywords. The keyword hits are then sorted and stored for analysis. All other information related to the texts are deleted.

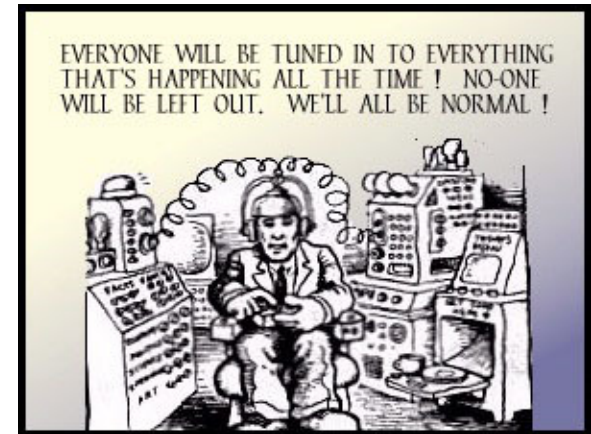
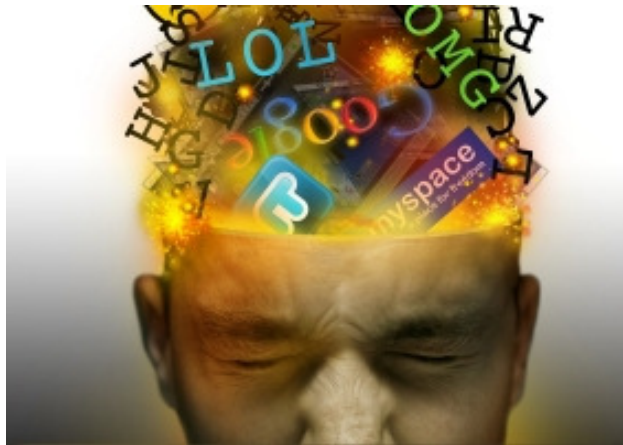
Former intelligence official Timothy Edgar, who worked in both the George W. Bush and Barack Obama administrations, said the data-gathering rule was implemented after a great deal of discussion about how it should be applied.

Source: <http://www.newsmax.com/Newsfront/nsa-searching-emails-times/2013/08/08/id/519396>

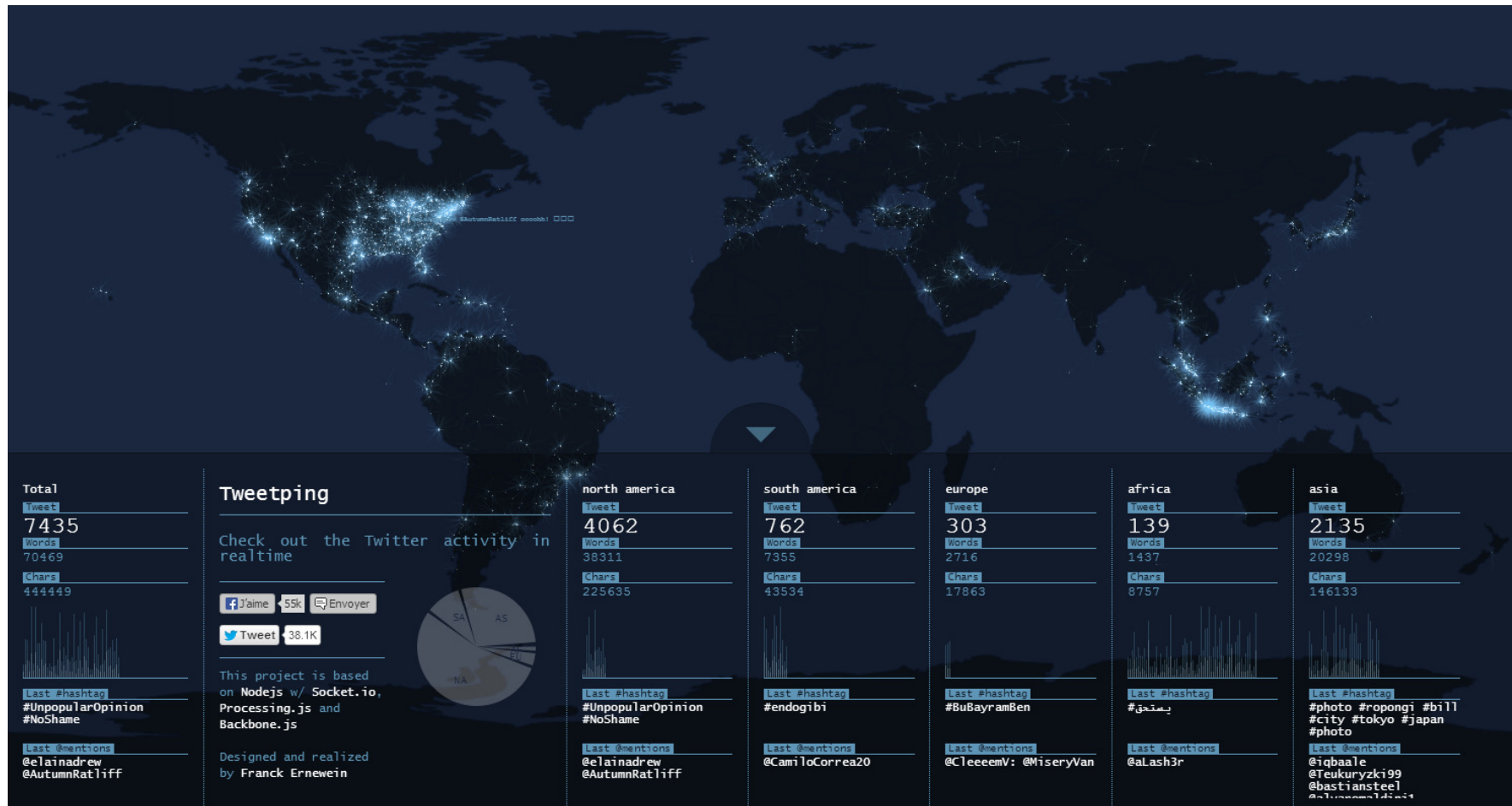
E-Mail Monitoring: If You Have Foreign Contacts



If It's Not Relevant, Why Is The U.S. Government Monitoring All Communications?



The Twitterverse

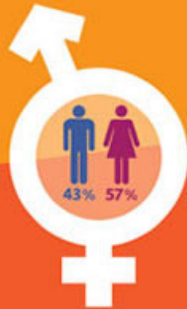


facebook in 2012

1 Billion connections
are shared by users collectively

845 million ACTIVE USERS
Facebook currently has 845 million active users.

Over 50% of the population in North America uses Facebook.



2.7bn Likes Daily

1:5

1 out of 5 web pages viewed by an internet surfer is a Facebook page.



250 million photos are uploaded to Facebook daily.

Facebook Habits

20 min
A Facebook user spends 20min approx each visit

5+
23% of the Facebook population visits the site 5+ times daily

Facebook

The Republic of Facebook

If Facebook were a country....



It would be home to 1 in 7 of the world's entire population

Sources
www.newsroom.facebook.com/Key-Facts
www.en.wikipedia.org/wiki/World-Population

www.blogsession.co.uk

The Republic of Facebook

If Facebook were a country....



It would be the 3rd largest in terms of population

Sources
www.newsroom.facebook.com/Key-Facts
www.en.wikipedia.org/wiki/List-of-countries-by-population

www.blogsession.co.uk

Can You See the New Trend?

TUESDAY, AUG 6, 2013 04:32 PM CDT

Cyberscare: Ex-NSA chief calls transparency groups, hackers next terrorists

Michael Hayden equates potential angry reactions to Snowden indictments to al-Qaida operations

BY NATASHA LENNARD

Follow 1.1k

Recommend 244 Send 83 Twitter 13 LinkedIn Share 0 +1 11

more

TOPICS: TECHNOLOGY NEWS, NEWS, POLITICS NEWS



Michael Hayden(Credit: AP)



Source:

http://www.salon.com/2013/08/06/cyberscare_ex_nsa_chief_calls_transparency_groups_hackers_next_terrorists/

August 6, 2013

General Michael Hayden, ex-Chief of NSA
Calls Transparency Groups and Hackers
the “Next Terrorists”

Strategic Comparative Analysis

Country	Policy	Strategy
China 	China supports cyberwarfare capabilities, especially providing such capabilities in the People's Liberation Army.	The Chinese will wage unrestricted warfare and these are the principles: Omni-directionality Synchrony Limited objectives Unlimited measures Asymmetry Minimal consumption Multi-dimensional coordination Adjustment, control of the entire process (Hagestad, 2012).
Russia 	Russia supports cyberwarfare capabilities, especially providing such capabilities in the Russian Army. The nature of cyberwarfare and information warfare requires that the development of a response to these challenges must be organized on an interdisciplinary basis and include researchers from different branches – political analysts, sociologists, psychologists, military specialists, and media representatives (Fayutkin, 2012).	The ability to achieve cyber superiority is essential to victory in cyberspace. (Fayutkin, 2012).
India 	India supports cyberwarfare capabilities, especially providing such capabilities in the Indian Army. "It is essential for efficient and effective conduct of war including cyber-war. The war book therefore needs to specify as how to maintain no-contact cyber war and when the government decide to go for full-contact or partial-contact war then how cyber war will be integrated to meet overall war objectives. (Sami, 2012)."	Strategies are still under development, but will follow the guidance of policies related to the conduct of war. (Sami, 2012)

The Top Four Countries in Cyberwarfare Capability (as of 2009)

Cyber Military Capabilities <i>2009</i>	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
China:	4.2	3.8	4.0	4.0
United States:	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.8	3.9
India:	4.0	3.5	3.5	3.7

Table 1 – Country Cyber Capabilities Ratings (Technolytics, 2012)

WHO IS DOING THIS AND WHY?

February 2013

Top 15 of Source Countries (Last month)

	Source of Attack	Number of Attacks
	Russian Federation	2,402,722
	Taiwan, Province of China	907,102
	Germany	780,425
	Ukraine	566,531
	Hungary	367,966
	United States	355,341
	Romania	350,948
	Brazil	337,977
	Italy	288,607
	Australia	255,777
	Argentina	185,720
	China	168,146
	Poland	162,235
	Israel	143,943
	Japan	133,908

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	27,327,356
Attack on Netbios protocol	937,476
Attack on Port 33434	687,446
Attack on SSH protocol	669,589
Attack on Port 5353	522,671

March 2013

Top 15 of Source Countries (Last month)

	Source of Attack	Number of Attacks
	Russian Federation	2,446,164
	Germany	1,308,615
	Taiwan, Province of China	536,031
	United States	449,853
	Australia	378,790
	India	358,110
	Ukraine	250,206
	Hungary	237,605
	Brazil	218,265
	China	197,152
	Italy	194,102
	France	184,073
	Argentina	182,166
	Japan	151,861
	Venezuela, Bolivarian Republic of	127,862

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	31,077,005
Attack on Netbios protocol	1,108,033
Attack on Port 5353	921,115
Attack on SSH protocol	919,145
Attack on Port 33434	687,446

<http://sicherheitstacho.eu/>

March 2013

Top 15 of Source Countries (Last month)

	Source of Attack	Number of Attacks
	Russian Federation	2,446,164
	Germany	1,308,615
	Taiwan, Province of China	536,031
	United States	449,853
	Australia	378,790
	India	358,110
	Ukraine	250,206
	Hungary	237,605
	Brazil	218,265
	China	197,152
	Italy	194,102
	France	184,073
	Argentina	182,166
	Japan	151,861
	Venezuela, Bolivarian Republic of	127,862

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	31,077,005
Attack on Netbios protocol	1,108,033
Attack on Port 5353	921,115
Attack on SSH protocol	919,145
Attack on Port 33434	687,446

<http://sicherheitstacho.eu/>

July 2013

Top 15 of Source Countries

Last month ▾

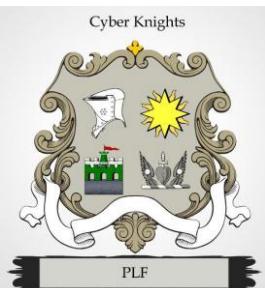
	Source of Attack	Number of Attacks
	Bulgaria	4,117,363
	Russian Federation	1,547,722
	Taiwan	1,334,695
	Romania	657,542
	United States	479,972
	Hungary	468,287
	Germany	450,277
	Venezuela, Bolivarian Republic of	408,620
	China	203,085
	Brazil	171,388
	Poland	167,370
	Italy	165,204
	Ukraine	132,827
	Argentina	122,361
	Sweden	122,057

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	5,793,778
Honeytrap Attacker on Port 19	4,084,812
Attack on Netbios protocol	310,992
Attack on SSH protocol	239,908
Honeytrap Attacker on Port 161	100,765

Cyberadversaries:

Organized, Capable, Equipped,
Talented, and Determined – From Nation
States and Non-State Actors



August 8, 2013

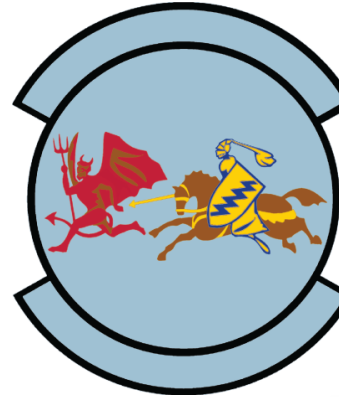
Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)



Cyber Good Guys:
 Also Organized, Capable, Equipped,
 Talented, and Determined – From
 Nation States



יחידה 8200



KÜBERKAITSELIIT
 ESTONIAN CYBER DEFENCE LEAGUE

Nationales
 Cyber-Abwehrzentrum

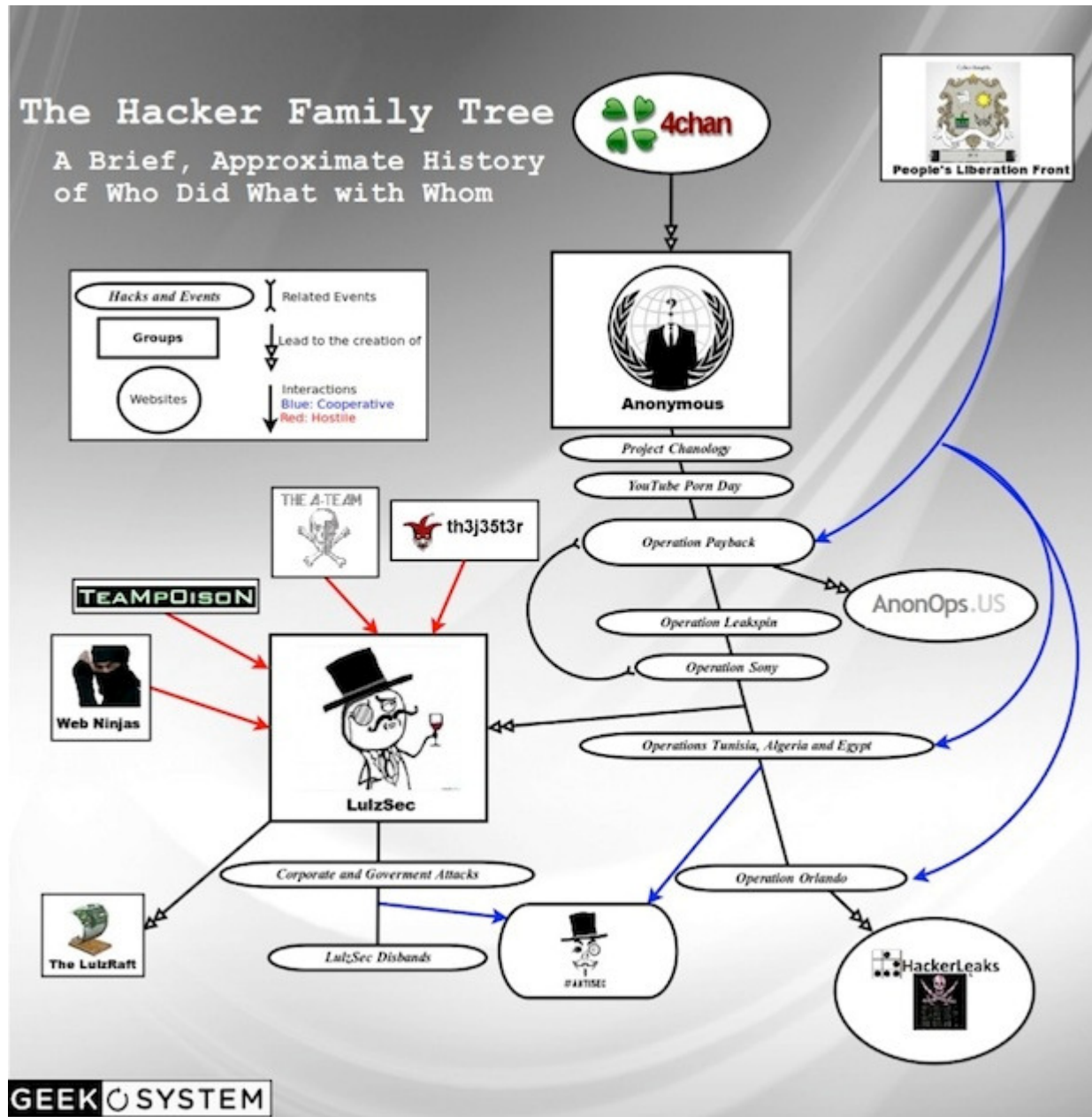
August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

Copyright 2013 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

The Hacker Family Tree

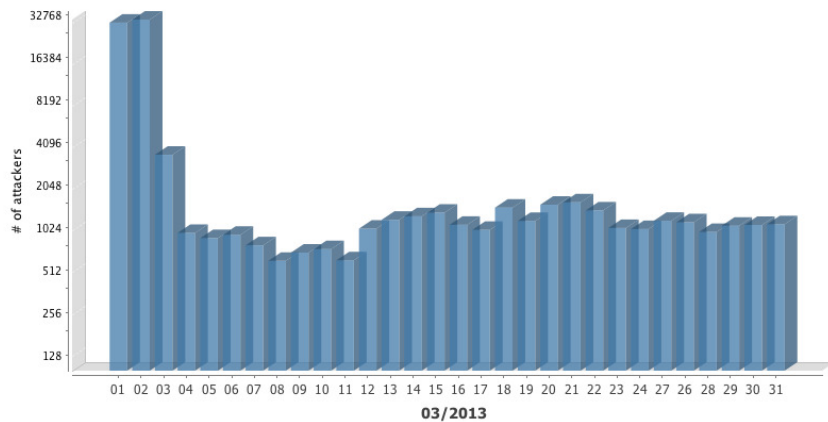
A Brief, Approximate History of Who Did What with Whom



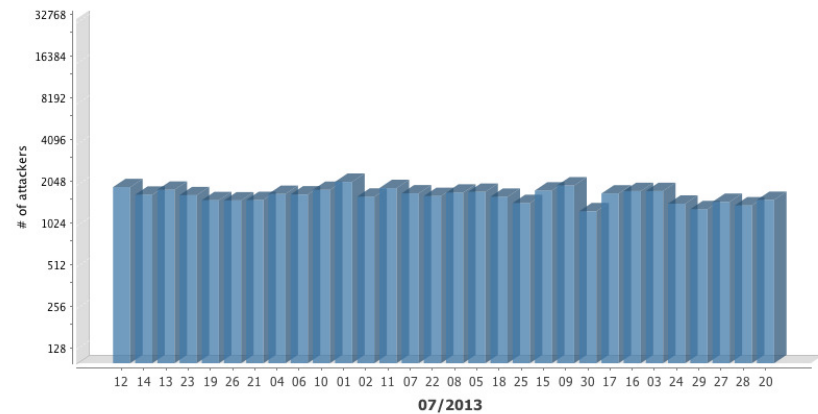
HOW VULNERABLE ARE WE IN THE U.S.?

Recorded Cyberattacks

March 2013



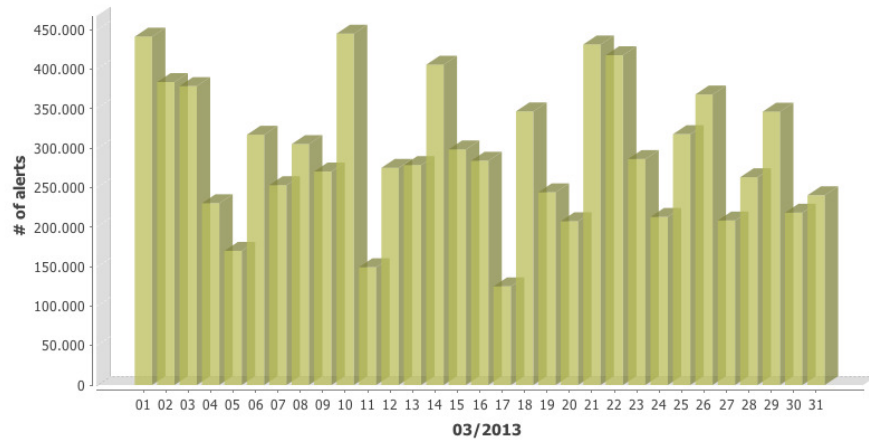
July 2013



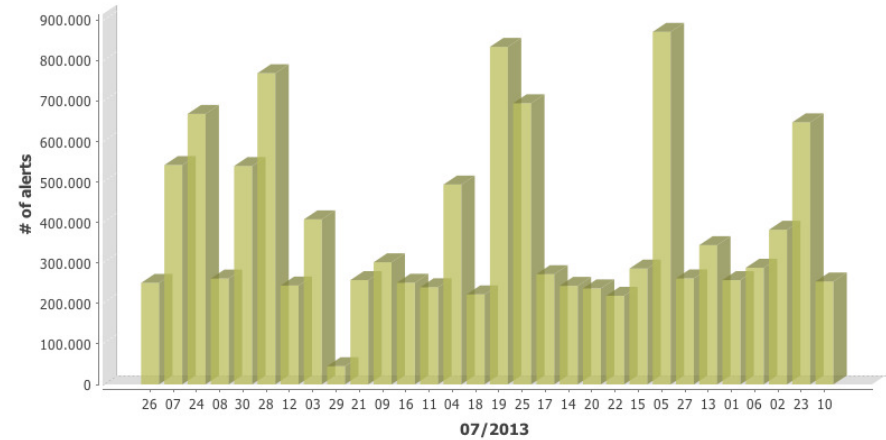
<http://sicherheitstacho.eu/>

Recorded Cyberattacks

March 2013



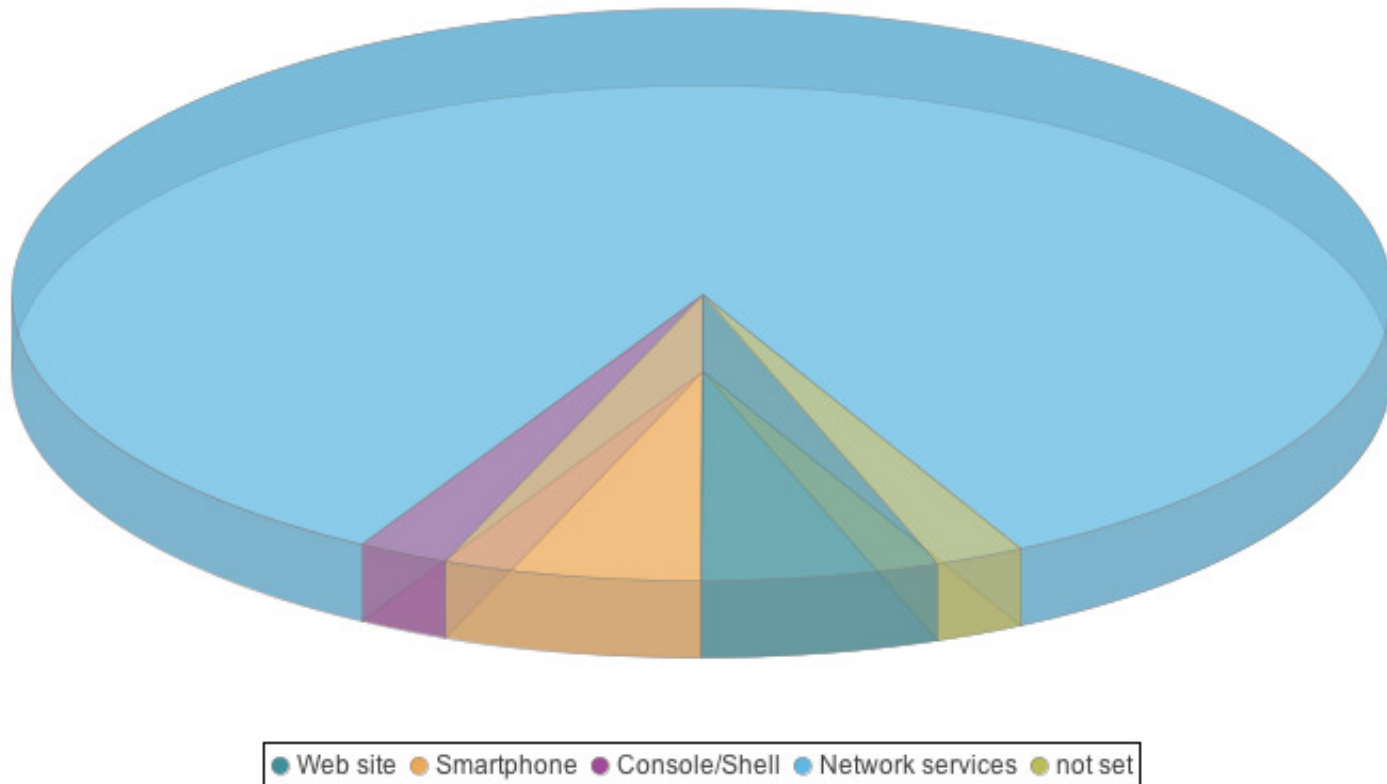
July 2013



<http://sicherheitstacho.eu/>

Types of Targets for Cyberattacks

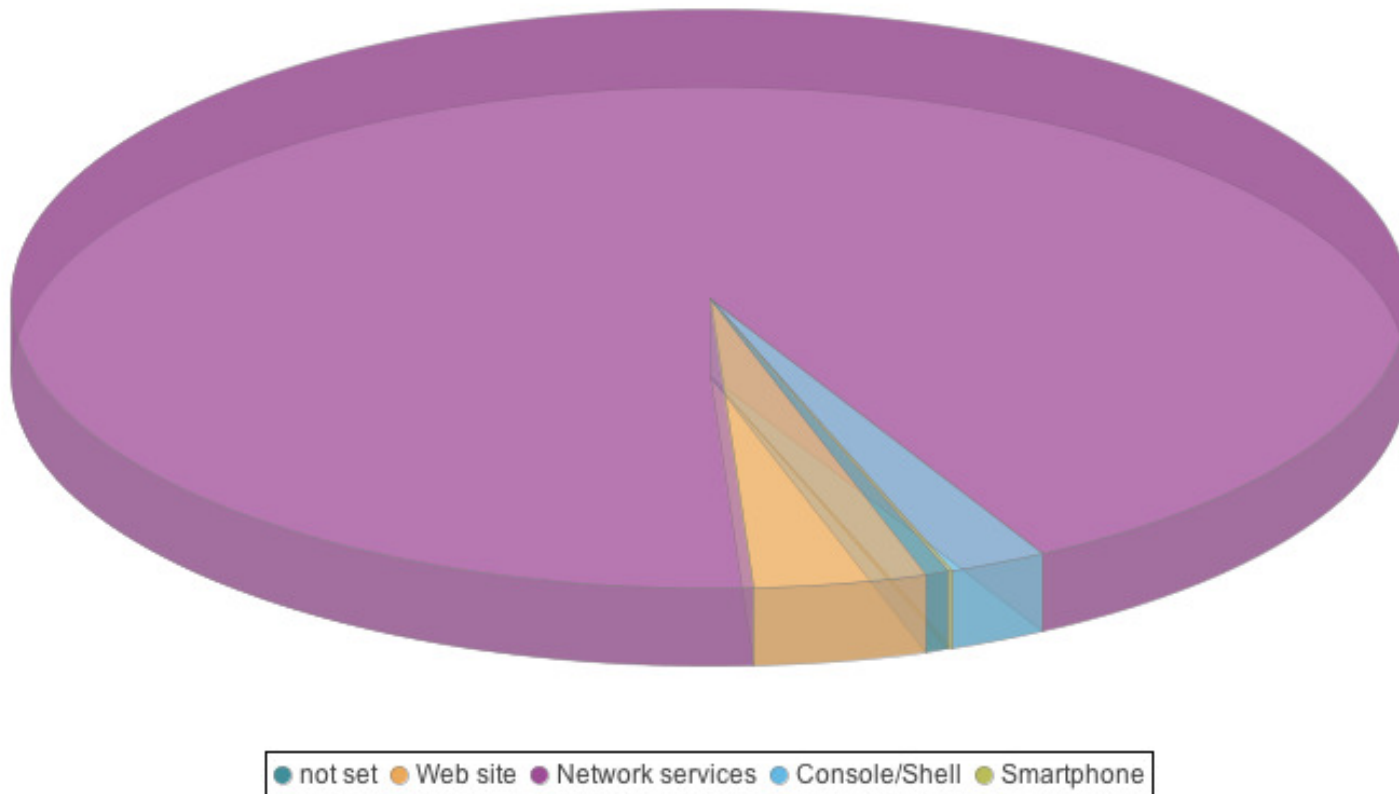
March 2013



<http://sicherheitstacho.eu/>

Types of Targets for Cyberattacks

July 2013



<http://sicherheitstacho.eu/>

Some Worst Case Scenarios

- Espionage and lost trade secrets
- DDoS attacks on banks and other financial institutions
- Attacks on SCADA systems
- Attacks on banks and the financial system
- Catastrophic attacks on critical infrastructure facilities and targets



Experts Suspect North Behind SKorea Computer Crash



Depositors try to use automated teller machines of Shinhan Bank while the bank's computer networks are paralyzed at a subway station in Seoul, South Korea, Wednesday, March 20, 2013. (AP Photo/Ahn Young-joon)



What Is the U.S. Government Doing to Defend the American Population?

- U.S Cyber Command, June 23, 2009
- Policies that describe the U.S.'s interest in protecting and defending cyberspace
- Several Cyberwarfare units created in the U.S. Military
- Internet "Kill Switch", September 2012
- Presidential Policy Directive 20, November 14, 2012
- Presidential Policy Directive 21, February 12, 2013
- Executive Order on Cybersecurity and Critical Infrastructure, February 12, 2013
- New Sophisticated Offensive Cyberweapons
- Cooperation, agreements, and exchange of information with allies and organizations
- The Federal Government will spend over \$65 Billion will be spent on Cybersecurity, 2013 – 2018.



Motto in MD5 Hash 9ec4c12949a4f31474f299058ce2b22a

"USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."



Mission of U.S. Cyber Command

"USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."



Mission in MD5 Hash `9ec4c12949a4f31474f299058ce2b22a`

A Quick Review of Some Previous and Current OBAMA Administration Policies Related to Cybersecurity

- 2009 – Critical Review of National Infrastructure – Cyberspace is strategic and critical - declared our digital infrastructure a strategic national asset and made protecting this infrastructure a national priority.
- 2010 – U.S. Cyber Command created and staffed
- 2011 – Presidential Policy Review - We will defend Cyberspace
- 2012 - President Obama's Defense Strategic Guidance 2012 - Sustaining Global Leadership: Priorities for 21st Century Defense
- 2012 – PPD 20
- 2013 – U.S. Cyber Command to be expanded five-fold
- 2013 – PPD 21
- 2013 – Executive Order 13636 on Cybersecurity-related initiatives and Information Sharing
- March 12, 2013 report Worldwide Threat Assessment of the US Intelligence Community by Director of National Intelligence, James Clapper, gives a clear and current summary of the Cyberthreats and the Actors. What's most interesting is that for the first time, Cyberthreats are now at the **top of the list of global threats to the U.S.**

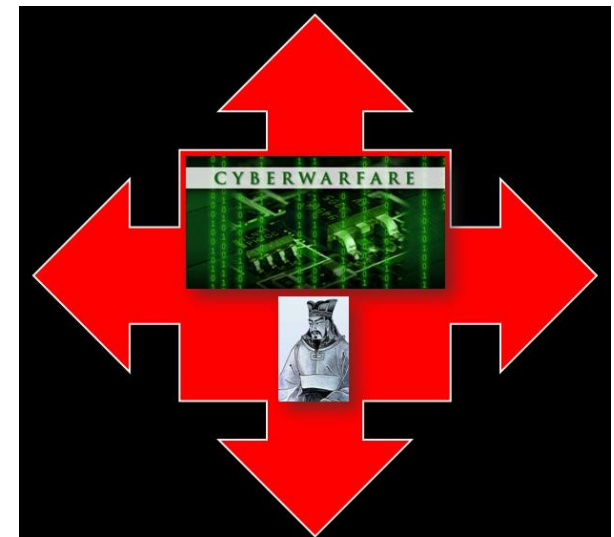
- Also... March 2013 – Tallinn Cyberware Operations Document (Hackers and Hacktivists may now be killed)

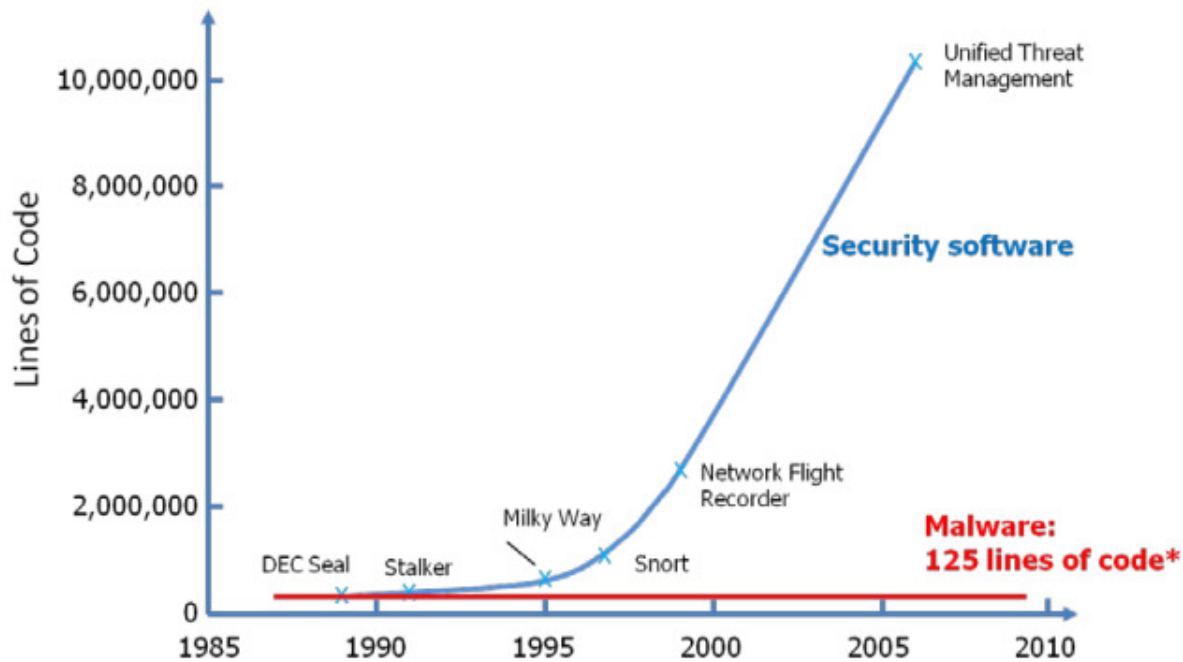
Some Other Laws and Policies

Date	Law or Policy	Impact	Impact of Freedom(s)
May 2011	USA PATRIOT Act (Renewed)	Provides the Government sweeping powers to gather and use previously protected private information from private citizens	Impacts the First and Fourth Amendments
December 2011	NDAAs	Indefinite Detainment without due process	Impacts the First, Sixth, and Eighth, Amendments
January 2012	Surveillance of Social Media by DHS, FBI, NSA, etc.	Early identification of possible threats	No Fourth Amendment protection during Internet use
March 2012	Executive Order 13603	The Executive Branch can legitimately seize control of all water, food (human and animal), medicine, fuel, fertilizer. etc.)	Makes Americans think of a Totalitarian Communist Dictatorship
December 2012	Warrantless Wiretap Act (Renewed)	Allows surveillance of all electronic communications	No Fourth Amendment protection during phone calls or Internet use
March 2013	U.S. Cyber Command will guard certain private organizations	Better cybersecurity for certain private organizations	N/A However, the Federal Government will no doubt be accused of showing favoritism towards some organizations and indifference or disrespect to others.
April 2013	ATF Seeks 'Massive' Database of Personal Info: 'Assets, Relatives, Associates and More'	The system will be utilized by staff "to provide rapid searches on various entities for example; names, telephone numbers, utility data and reverse phone look-ups, as a means to assist with investigations, and background research on people, assets and businesses."	(No comment. Connect the dots yourself and draw your own conclusions.)

Cyberwar and Cyberattacks – Some Present Challenges to Resolution

- The lack of international definition and agreement on what constitutes an act of cyberwar (Markoff and Kramer, 2009).
- The lack of the ability to clearly attribute the source of an attack (Turzanski and Husick, 2012).
- The ability for non-state actors to conduct potent cyberattacks (Turzanski and Husick, 2012).
- The inability to clearly define what the exact nature of critical infrastructure targets (Turzanski and Husick, 2012).
- The massive proliferation and reliance on ubiquitous, highly insecure, vulnerable systems based on SCADA technologies during the 1980s and 1990s (Turzanski and Husick, 2012).
- The continually changing landscape of information technology including the vulnerabilities and threats related to systems that are obsolete, yet remain in operational use for several years past their intended useful life.
- Consider the following slide that defines the complexity of defense...





Defense becomes more and more complex, yet still outmatched by offense

*DARPA Brief to DSB, May 2011

* Malware lines of code averaged over 9,000 samples

Figure 3.2 Graphic Illustration of the Complexity of Software Required to Defend and Attack our Systems. Very Small Changes (Even Single Bits) Can Cause Major Impacts to the Operation of a System

There is no single silver bullet to solve the threat posed by cyber-attack or warfare. Solving this problem is analogous to previous complex national security and military strategy developments including counter U-boat strategy in WWII, nuclear deterrence in the Cold War, commercial air travel safety and countering IEDs in the Global War on Terrorism. The risks involved with these challenges were never driven to zero, but through broad systems engineering of a spectrum of techniques, the challenges were successfully contained and managed. (U.S. Department of Defense, 2013)



HACKING

The NSA Is Training 13 Teams of Covert Hackers to Attack Other Countries

 [Kyle Wagner](#) 

For the first time, the United States has officially disclosed plans to develop counterattack measures against foreign nations' cyberattacks. General Keith Alexander, chief of the military's Cyber Command and the NSA, told Congress yesterday the military is [training 13 teams of programmers and computer experts](#) to carry out offensive attacks.

(Wagner, 2013)

Recent Developments – March 2013

- **Global Threat Assessment** lists Cyber Threats as No. 1 threat to U.S. – March 12, 2013
- NATO's Tallinn **Manual for Cyberwarfare Operations** released – March 19, 2013 (authorizes killing hackers and hacktivists!)
- Rand Beers, Under Secretary of DHS for Cybersecurity releases **12-page report about Cybersecurity, Critical Infrastructure, EO 13636 and PPD21** – March 20, 2013
- S. Korea banking organizations and other businesses endure massive cyberattack and N. Korea is the primary suspect – March 20, 2013.
- Most massive DDoS Attack ever – CyberBunker v. SpamHaus – March 27, 2013

The Future of Cyberwar and Cyberattacks

- Increasing intensity and frequency
- Greater capacities to inflict damage
- Better Intelligence
- Faster Response
- Tighter Integration and Automation
- More complex offensive cyberweapons
- Better cyberdefense and deterrence will be necessary
- Better analysis and think-tank groups
- Possibly more secret Policy Directives (i.e. PPD 20)
- Possible loss of personal freedoms



What Can You and Your Organization Do Today?

- Continually Educate yourself, friends, colleagues and family
- Adopt and implement, and follow a security compliance framework, such as ISO 27001
- Continually improve your security controls and your security posture
- Report incidents that result in more than \$5000 damage to the Internet Crime Complaint Center www.ic3.gov
- Defend yourself (ask me more about this later)
- Do not attack or return fire
- Remain vigilant

How does Title 10 of the U.S. Code Affect Cyberwarfare and the Average U.S. Citizen?

- American Citizens are legally prohibited from responding offensively to cyberattacks

Career Opportunities?

- Yes – The U.S. Government is hiring Cybersecurity Professionals
- Private Industry will be picking up more and more Cybersecurity experts



Career Development Opportunities?

Illinois Institute of Technology

- M.S. in Cyber Forensics and Security

<http://www.itm.iit.edu/cybersecurity/index.php>



Bellevue University

- M.S. in Cybersecurity
- B.S. in Cybersecurity

<http://www.bellevue.edu/degrees/graduate/cybersecurity-ms/>



Conclusion – Part 1

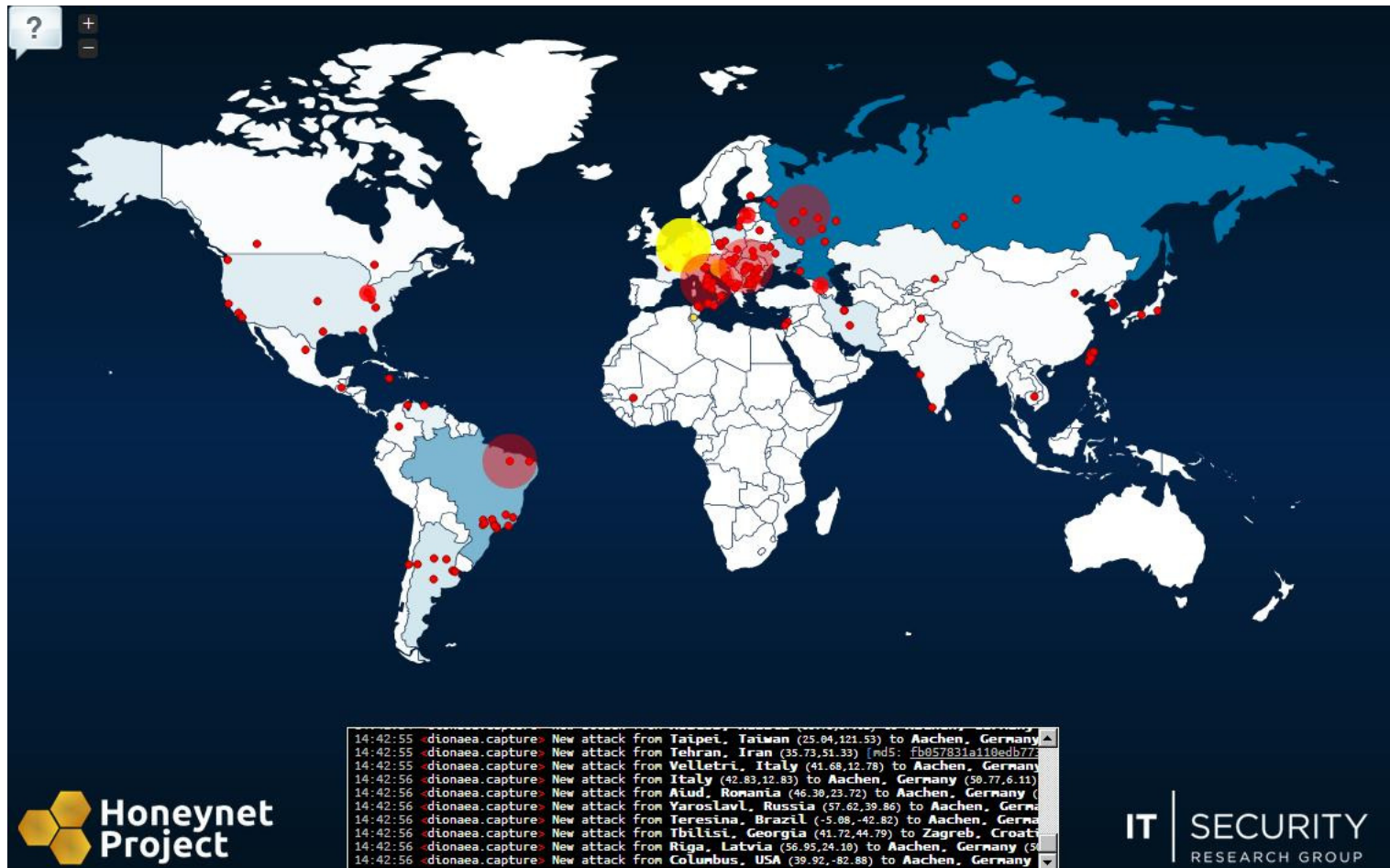
- In 2013, cyberattacks, cyberweapons, and cyberwarfare events are growing in number, frequency, and sophistication
- Due to our dependence on Cyberspace, we are living in dangerous times because of the current and worsening cyberthreat landscape



Conclusion – Part 2

- When Doing Your Research and Analysis About Cyberwarfare...You must:
 - Go national and international
 - Use MANY resources
 - Consider the perspectives and orientation, motives, of the sources (example: India will report capabilities and events about Israel's IDF Unit 8200 that the U.S. will not)
 - Do plenty of critical thinking
 - Remember that
 - Attribution is hard
 - Verification is hard because “evidence” can be manufactured
 - There is a LOT of propaganda and hype

We Will Be Living in Interesting Times From Now On...



August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

74

Questions?



Send e-mail to William F. Slater, III: slater@billslater.com

William F. Slater, III

August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

75

Resource Website

<http://billslater.com/cyberwar>

- **Writing**
- **Presentations**
- **References**

e-mail slater@billslater.com

Web: <http://billslater.com>

Twitter: <http://twitter.com/billslater>

LinkedIn: <http://www.linkedin.com/profile/view?id=713787>

Facebook: <http://www.facebook.com/billslater>



William F. Slater, III



Thank You, Thank You Very Much!!!

-William F. Slater, III
slater@billslater.com
<http://billslater.com/cyberwar>

August 8, 2013

Suppose They Gave a Cyberwar and Everybody Came ? (version 1.0)

77

References

- Beidleman, S. W. (2009). Defining and Deterring Cyber War - Homeland Security Digital Library. Retrieved from <https://www.hsdl.org/?view&did=28659> on March 18, 2013.
- Bousquet, A. (2009). The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York, NY: Columbia University Press.
- Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.
- Crosston, M. (2011). World Gone Cyber MAD: How “Mutually Assured Debilitation” Is the Best Hope for Cyber Deterrence. An article published in the Strategic Studies Quarterly, Spring 2011. Retrieved from <http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf> on October 10, 2012.
- Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from <http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf> on September 30, 2012.
- Hagestad, W. T. (2012). 21st Century Chinese Cyberwarfare. Cambridgeshire, U.K.: IT Governance.
- Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.
- Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.
- Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.
- Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from <http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all> on June 28, 2009.

References

- Obama, B. H. (2012). Defense Strategic Guidance 2012 - Sustaining Global Leadership: Priorities for 21st Century Defense. Published January 3, 2012. Retrieved from http://www.defense.gov/news/Defense_Strategic_Guidance.pdf on January 5, 2012.
- Technolytics. (2012). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict, third edition. Purchased and downloaded on September 26, 2012.
- Turzanski, E. and Husick, L. (2012). "Why Cyber Pearl Harbor Won't Be Like Pearl Harbor At All..." A webinar presentation held by the Foreign Policy Research Institute (FPRI) on October 24, 2012. Retrieved from <http://www.fpri.org/multimedia/2012/20121024.webinar.cyberwar.html> on October 25, 2012.
- U.S. Army. (1997). Toward Deterrence in the Cyber Dimension: A Report to the President's Commission on Critical Infrastructure Protection. Retrieved from http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf on November 3, 2012.
- U.S. Department of Defense. ((2013). Department of Defense - Defense Science Board – Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, published January 2013. Retrieved from <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf> on March 16, 2013.
- Wagner, K. (2013). The NSA Is Training 13 Teams of Covert Hackers to Attack Other Countries. An article published on March 13, 2013. Retrieved from <http://gizmodo.com/5990346/the-nsa-is-training-13-teams-of-covert-hackers-to-attack-other-countries> on March 19, 2013.
- Articles at <http://www.cyberwarzone.com>
- Papers at <http://billslater.com/writing>

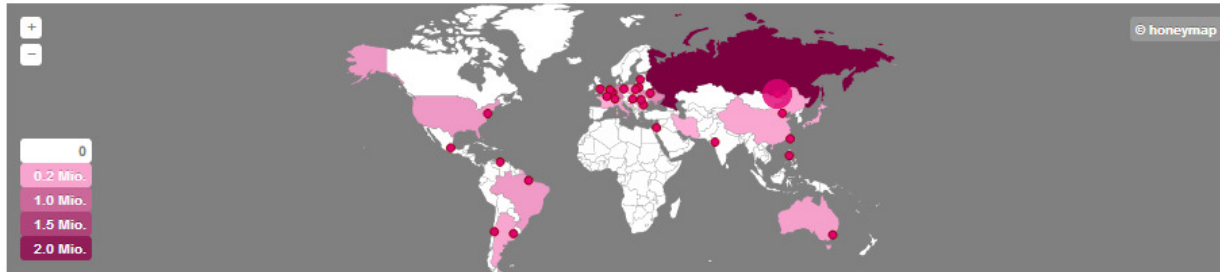
References

<http://sicherheitstacho.eu/>

Realtime World wide cyberattack monitoring service launched by Germany's Deutsche Telekom Besides a real-time overview of current attacks, recorded by a total of 97 sensors, the website also provides statistics such as the top 15 source countries, distribution of attack targets, total number of attacks per day and overall sum of attackers per day.



Overview of current cyber attacks (logged by 97 Sensors)



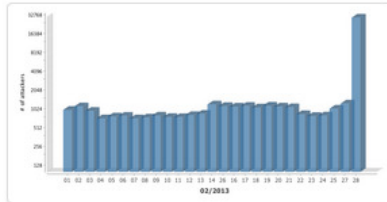
Live-Ticker

Date	Source	Attack on	Parameter
2013-03-19 03:18:48	Russia	Network services	dionaea.smbd.port.445
2013-03-19 03:18:48	United Kingdom	Network services	dionaea.smbd.port.445
2013-03-19 03:18:45	Ukraine	Network services	dionaea.smbd.port.445
2013-03-19 03:18:46	Chile	Network services	dionaea.smbd.port.445
2013-03-19 03:18:44	Ukraine	Network services	dionaea.smbd.port.445

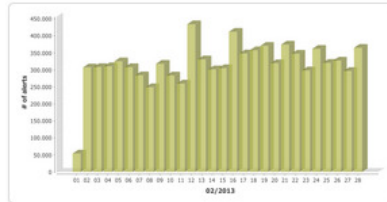
Top 15 of Source Countries (Last month)

Source of Attack	Number of Attacks
Russian Federation	2,402,722
Taiwan, Province of China	907,102
Germany	780,425
Ukraine	566,531
Hungary	367,966
United States	355,341
Romania	350,948
Brazil	337,977
Italy	288,607
Australia	255,777
Argentina	185,720
China	168,146
Poland	162,235
Israel	143,943
Japan	133,908

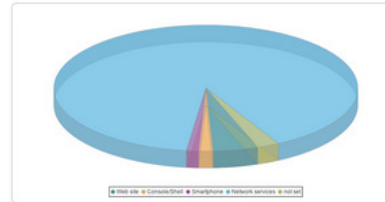
Overall sum of attackers per Day (Last Month)



Overall sum of attacks per Day (Last Month)



Distribution of Attack Targets (Last Month)



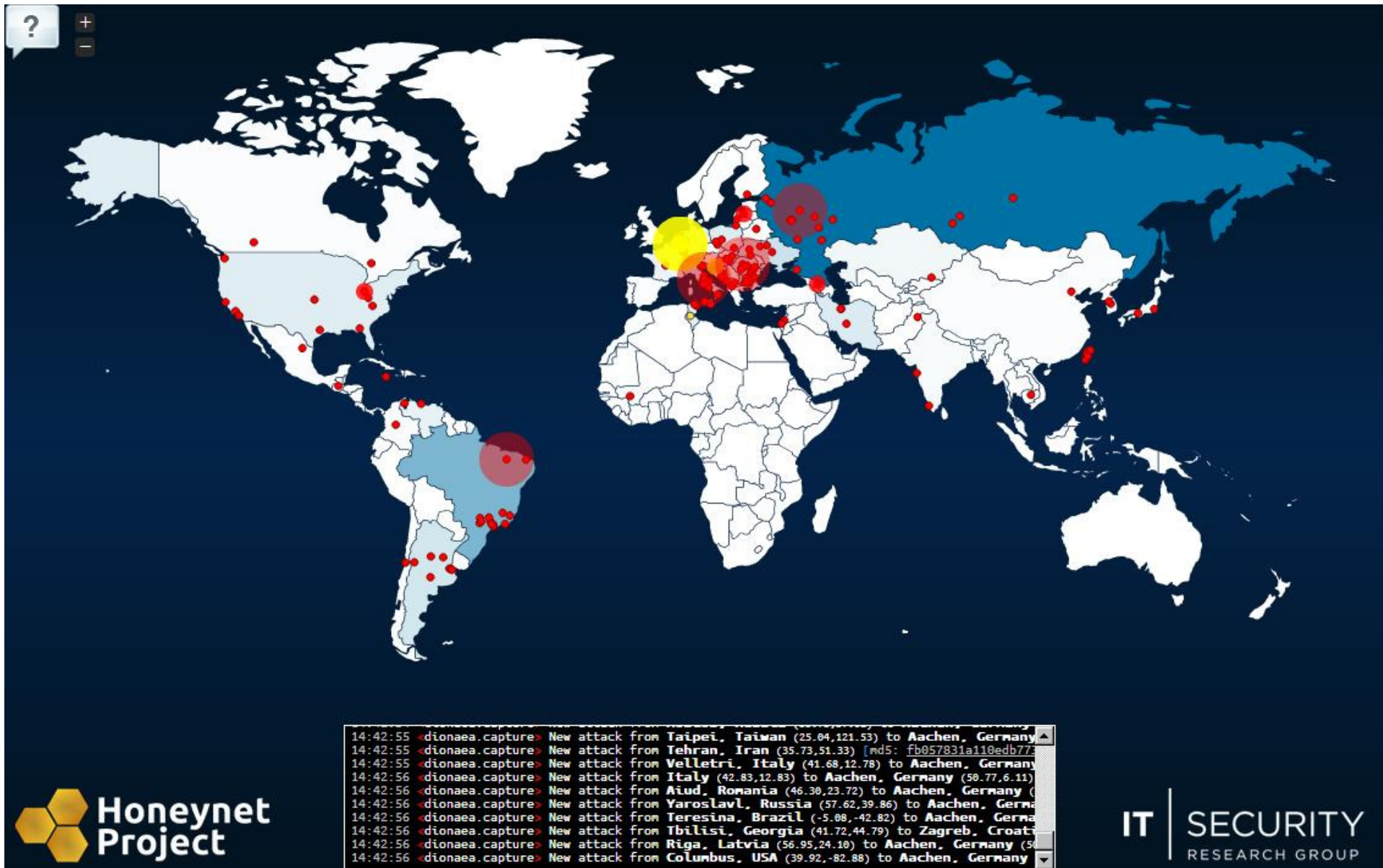
Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	27,327,356
Attack on Netbios protocol	937,476
Attack on Port 33434	687,446
Attack on SSH protocol	669,589
Attack on Port 5353	522,671

References

<http://map.honeynet.org/>

Realtime World wide cyberattack monitoring service launched by the Honeynet Project.



References

<https://isc.sans.edu/dashboard.html>

Internet Storm Center



Threat Level: GREEN YELLOW ORANGE RED

[Storm Center](#) [Tools](#) [Data/Reports](#) [My ISC](#) [Contact](#)

Dashboard: 2013-03-28

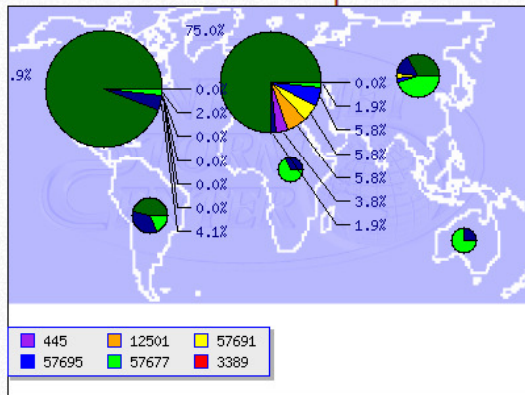
Handler on Duty:
John Bambenek
[Contact Us](#)

[Suggest a Dashboard Block](#)

Current Date (UTC): **Thu, 28 Mar 2013 14:49:27 +0000**

Refresh page every -or-

World Map



Today's Diaries

- [Where Were You During the Great DDoS Cybergeddon of 2013?](#)
- [ISC StormCast for Thursday, March 28th 2013](#)
<http://isc.sans.edu/podcastdetail.html?id=3211>

Top 10 Source IPs

IP Address	Reports	Target IPs	First Seen	Last Seen
069.175.126.170 (US)	2,214,645	167,399	2012-07-11	2013-03-28
061.142.106.034 (CN)	188,184	115,432	2012-11-10	2013-03-28
115.095.166.247 (KR)	172,008	104,571	2012-08-26	2013-03-28
061.147.119.186 (CN)	287,733	98,312	2012-11-15	2013-03-28
176.010.035.241 (IS)	660,258	98,029	2013-01-26	2013-03-28
094.142.155.123 (IS)	399,685	93,739	2013-03-05	2013-03-28
069.175.054.106 (US)	1,501,920	92,325	2012-07-14	2013-03-28
178.255.087.241 (GB)	93,349	83,306	2012-05-15	2013-03-28
060.214.139.074 (CN)	419,102	82,009	2013-02-01	2013-03-28
074.216.195.099 (CA)	80,554	80,054	2012-12-04	2013-03-28

[View Top Sources Page](#)

Search Internet Storm Center

site/port/ip search:



Top Attacker: 60.214.233.220
Top Port Attacked: 445 Last Updated 28-Mar-2013 02:28 pm UTC

DSHield.org

Top 10 Ports

by Reports		by Targets		by Sources	
Port	Reports	Port	Targets	Port	Sources
179	1013643	5900	82339	20612	36889