PPD 01

PPD 02

PPD 03

PPD 04

PPD 05

PPD 06

PPD 07

PPD 08

PPD 09

PPD 10

PPD 11

PPD 12

PPD 13

PPD 14

PPD 15

PPD 16

PPD 17

PPD 18

PPD 19

PPD 20

PPD 21

What's in Presidential Policy Directive 20 (PPD 20)?
How It Will Probably Affect America and Americans and Why You Should Care

William F. Slater, III, M.S. MBA, PMP, CISSP, CISA

A Presentation for Forensecure 2013

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

What's in PPD 20? How It Will Affect America and Americans and Why You Should Care

Agenda

- Introduction
- Disclaimers and Primary Sources
- Definitions of Threats, Vulnerabilities, and Critical Infrastructure
- A Quick Look at the Present Cyberthreat Landscape and the Probable Present Capabilities
- A Quick Review of Previous OBAMA Administration Policies Related to Cybersecurity
- How does Title 10 of the U.S. Code Affect Cyberwarfare and the Average U.S. Citizen?
- Probable Contents of the PPD 20
- Other Content Topics that Should Be Considered
- The Classification of PPD 20 and the Necessity for Secrecy
- So Why PPD 20 and Why Now?
- How Will PPD 20 Affect America the Average American
- What Can You and Your Business Do **Today**?
- The Future of Cyberwar and Cyberattacks
- Conclusion
- Questions

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

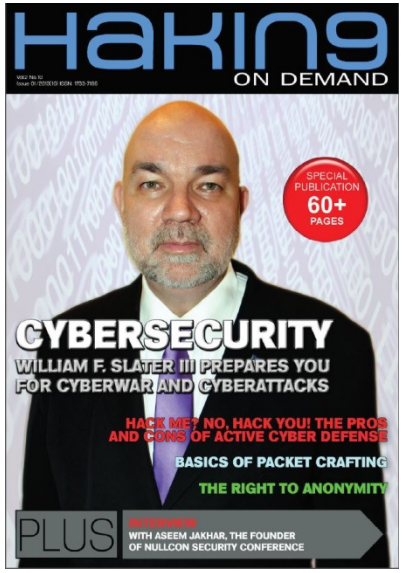
The Speaker

William F. Slater, III

- Adjunct Professor at the Illinois Institute of Technology
- Career IT Professional since 1977 with extensive experience in IT Security, Data Centers, Project and Program Management in Infrastructure, System Development, and Services (including the United States Air Force)
- Published author on Cyberwarfare and Cyberdeterrence issues in 2012 and 2013
- Graduated with M.S. in Cybersecurity from Bellevue University in March 2013, and has more the 20-security related certifications, including CISSP, SSCP, and CISA

July 1977

January 2013



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

Disclaimers and Primary Sources

- I started my IT career as a young computer systems staff officer in the United States Air Force supporting the command control information systems that provided real-time information to the Strategic Air Command Battle Staff
- 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.
- Researched publicly available sources
- I do not have an active secret security clearance
- I did not access any classified documents to create this presentation

.

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

DEFINITIONS OF THREATS, VULNERABILITIES, AND CRITICAL INFRASTRUCTURE

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

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 cyber-attacks, 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**

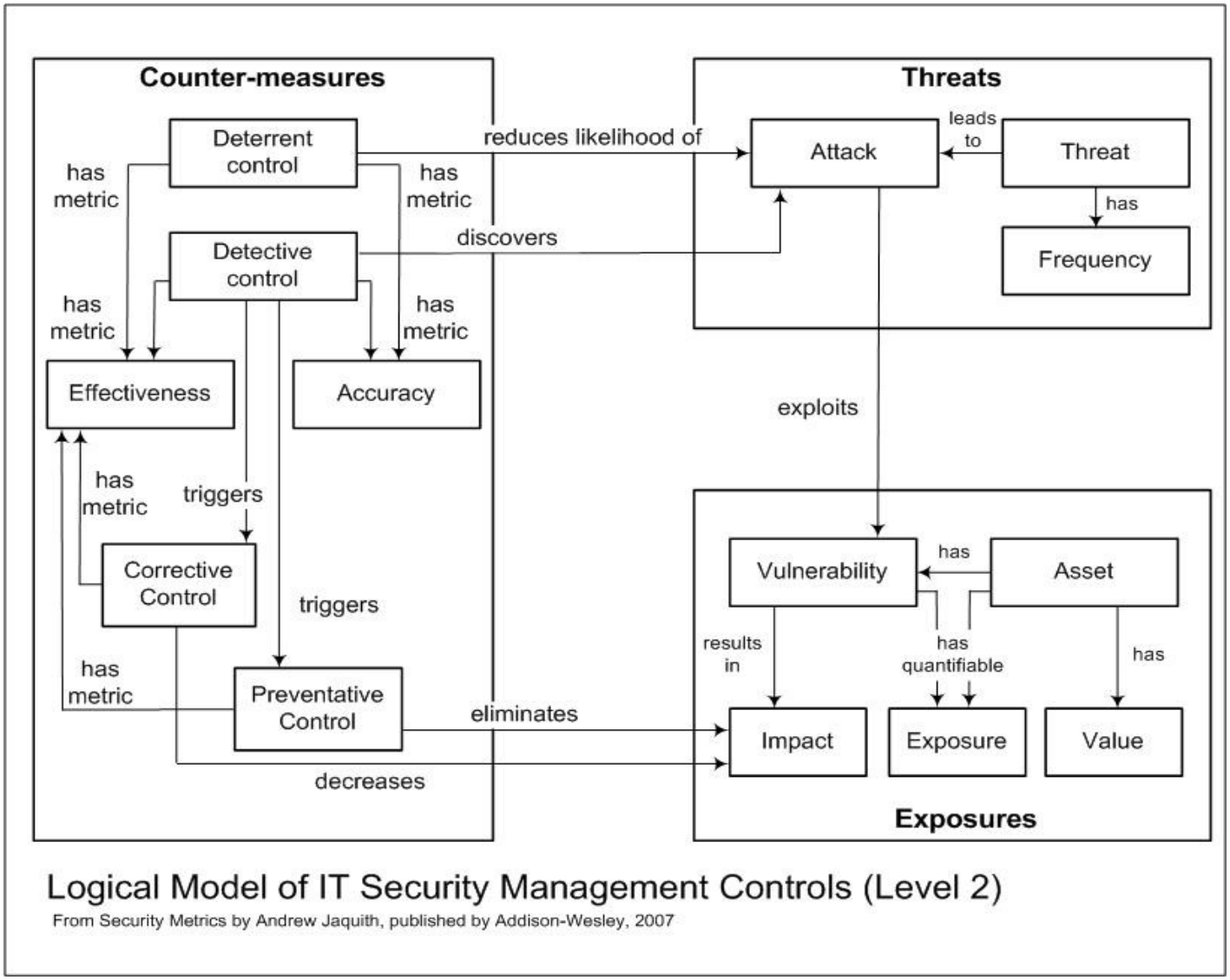
  The efficacy of cyber deterrence relies on the ability to impose or raise costs and to deny or lower benefits related to cyber attack in a state's decision-making calculus. Credible cyber deterrence is also dependent on a state's willingness to use these abilities and a potential aggressor's awareness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

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

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?



Logical Model of IT Security Management Controls (Level 2)

From Security Metrics by Andrew Jaquith, published by Addison-Wesley, 2007

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.

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

What Makes Cyberwarfare Difficult to Analyze and Understand?

- Lack of Agreement 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

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

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.

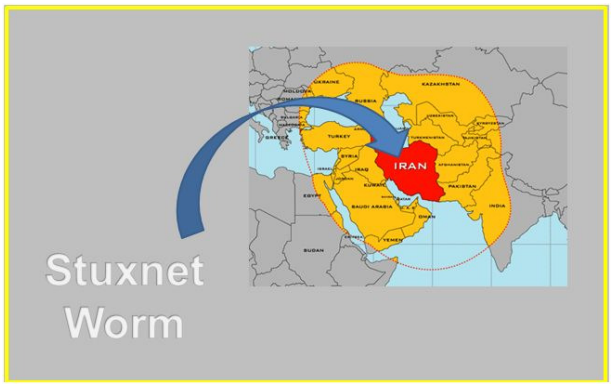
Copyright 2013 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

A QUICK LOOK AT THE PRESENT CYBERTHREAT LANDSCAPE AND THE PROBABLE PRESENT CAPABILITIES

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

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
- Disclosure of 140+ Chinese Cyber Espionage Attacks – February 2013
- March 13, 2013 - Unfortunately, according to James Rickards, a top financial-threat adviser to the Pentagon, CIA, and Director of National Intelligence, **an "economic Pearl Harbor" is quickly approaching**.
- Cyberattacks on S. Korean Banks and other businesses on March 20, 2013



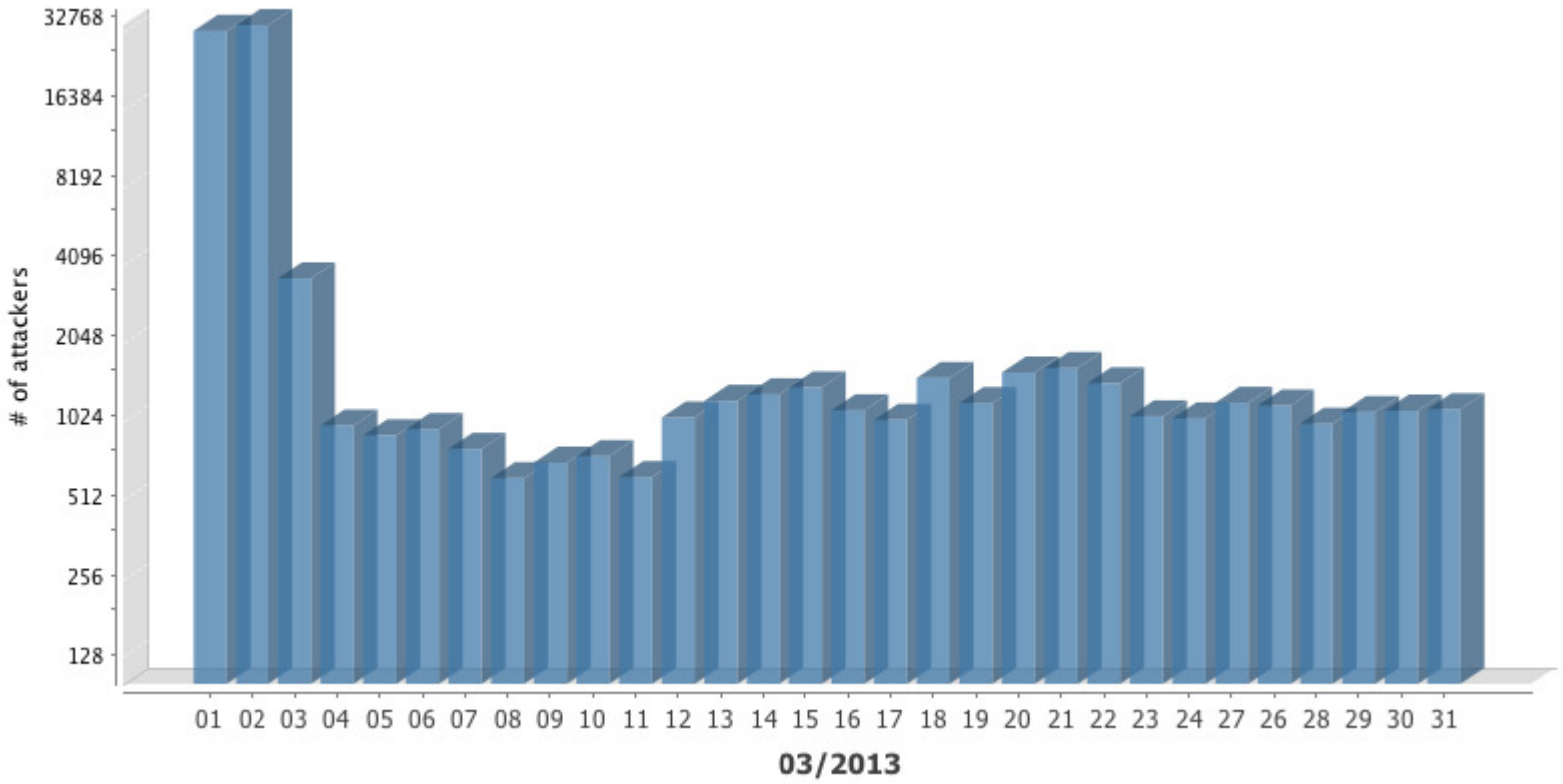
Copyright 2013 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

Most 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
- 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

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

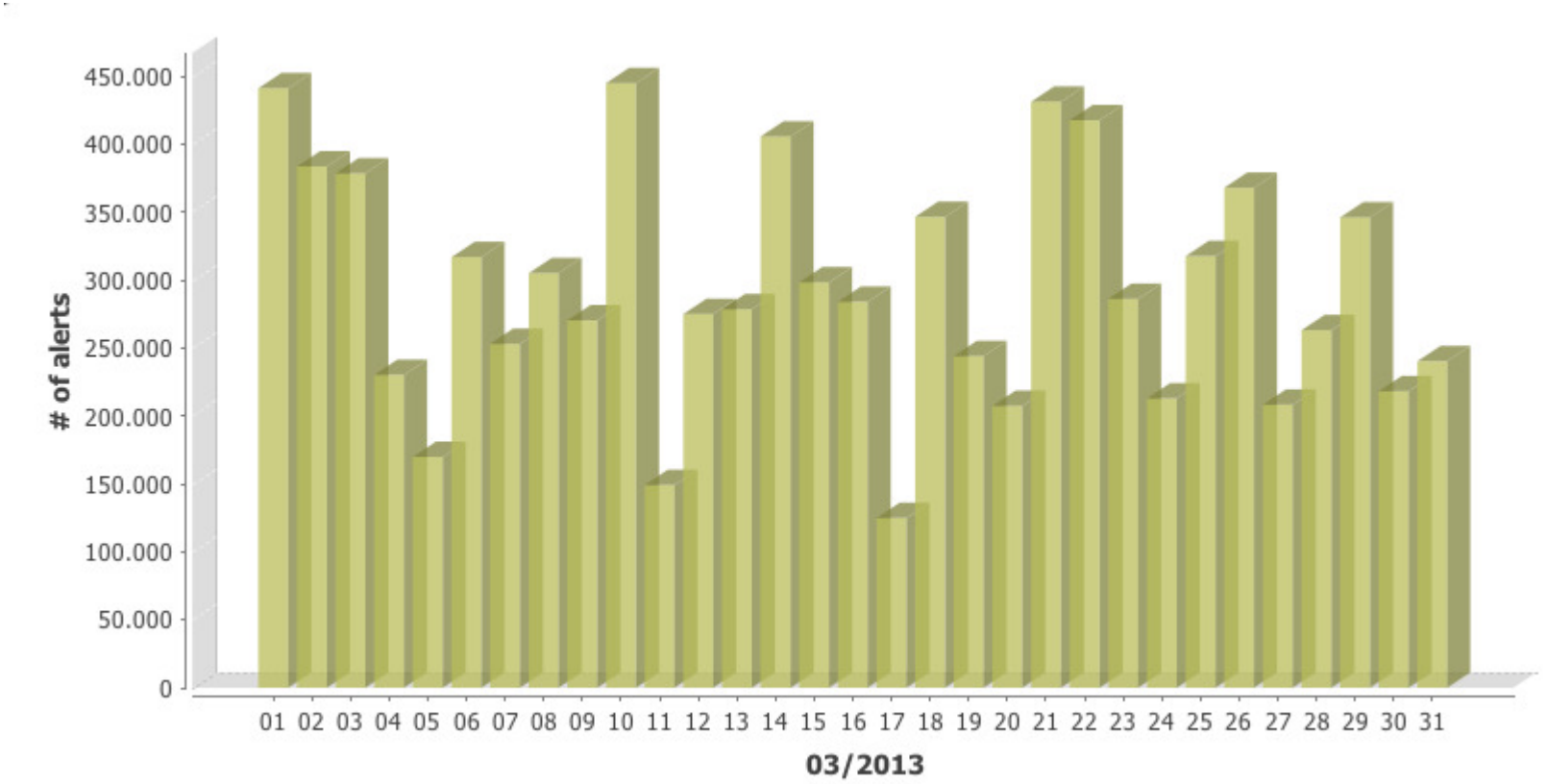
Recorded Cyberattacks



http://sicherheitstacho.eu/

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

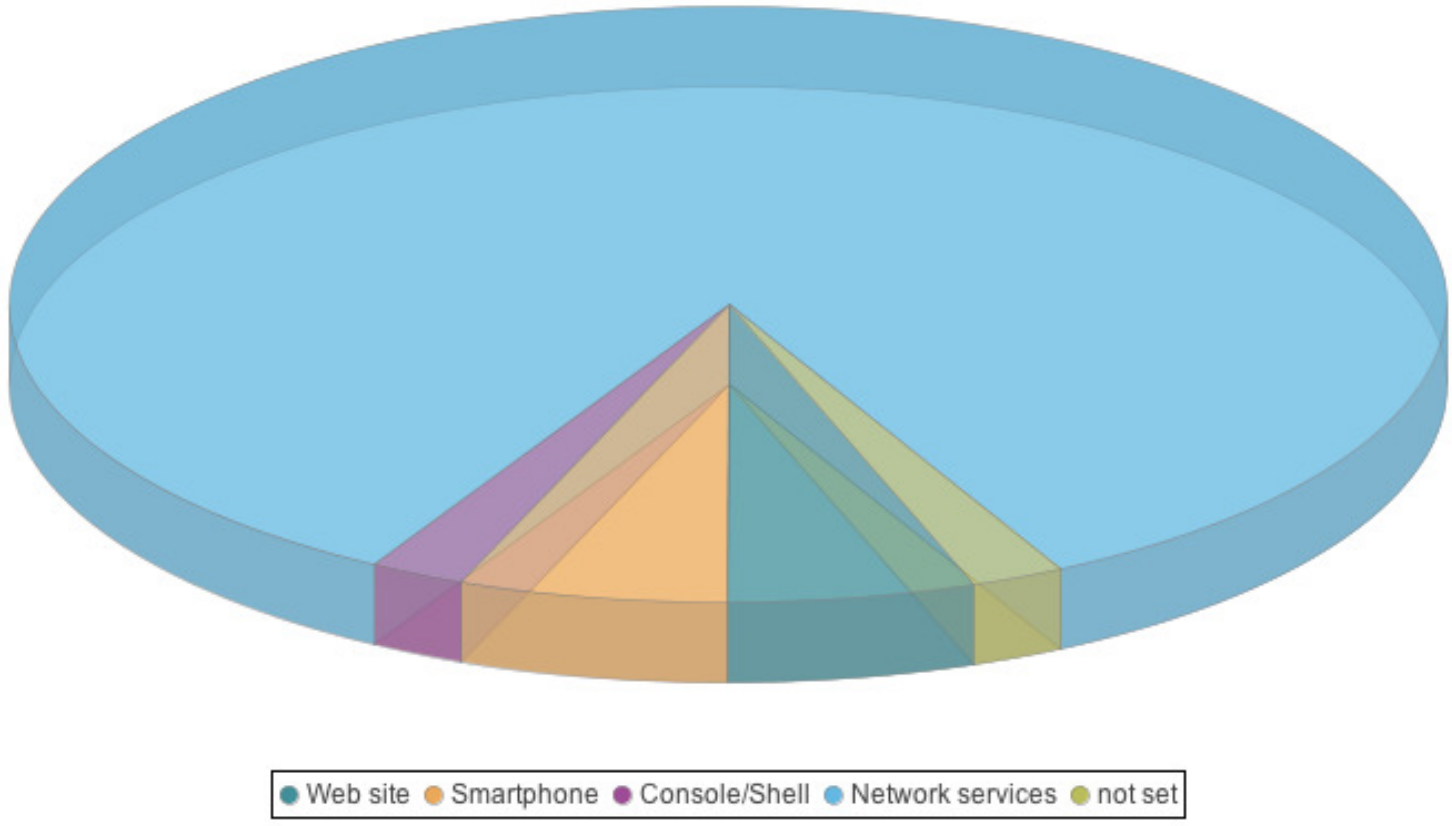
Recorded Cyberattacks



http://sicherheitstacho.eu/

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

Types of Targets for Cyberattacks



http://sicherheitstacho.eu/

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

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. (Saini, 2012)."	Strategies are still under development, but will follow the guidance of policies related to the conduct of war. (Saini, 2012)

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

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

Cyber Military Capabilities 2009	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)

Copyright 2012 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

WHO IS DOING THIS AND WHY?

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

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)

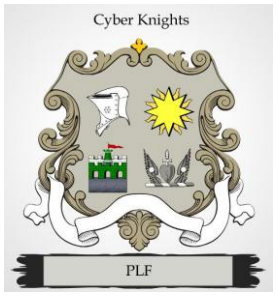
Description	Number of Attacks
Attack on SMB protocol	31,077,005
Attack on Netbios protocol	1,108,033
Attack on Port 5353	921,115
Attack on SSH protocol	919,145
Attack on Port 33434	687,446

http://sicherheitstacho.eu/

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

Cyberadversaries:

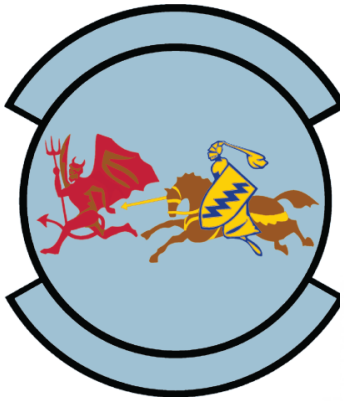
Organized, Capable, Equipped, Talented, and Determined – From Nation States and Non-State Actors



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

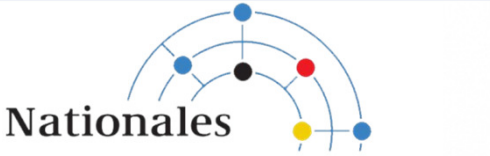
Cyber Good Guys:

Also Organized, Capable, Equipped, Talented, and Determined – From Nation States



8200 יחידה

KÜBERKAITSELIIT
ESTONIAN CYBER DEFENCE LEAGUE



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

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

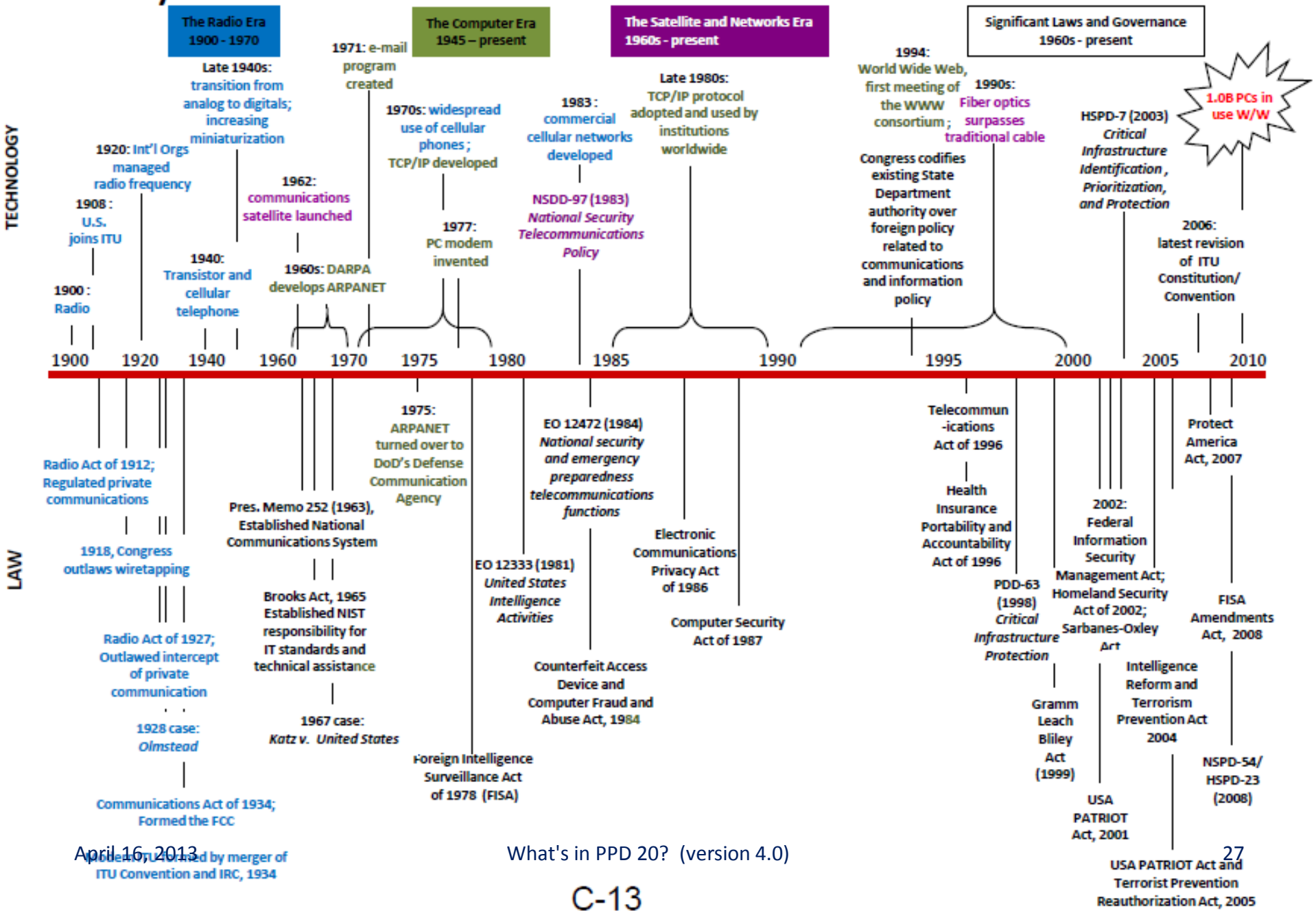
Depositors try to use automated teller machines of Shinhan Bank while the bank's computer networks are paralyzed at a subway station in Seoul, South Korea, Wednesday, March 20, 2013. (AP Photo/Ahn Young-joon)

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

A QUICK REVIEW OF SOME PREVIOUS AND CURRENT OBAMA ADMINISTRATION POLICIES RELATED TO CYBERSECURITY

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

History Informs our Future



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

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."

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

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."

Misson in MD5 Hash 9ec4c12949a4f31474f299058ce2b22a

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

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)

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

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	**NDAA**	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.)

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

The Bill of Rights

Ratified December 15, 1791

Article I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Article II

A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

Article III

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Article IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Article V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any Criminal Case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Article VI

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining Witnesses in his favor, and to have the Assistance of Counsel for his defence.

Article VII

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury shall be otherwise reexamined in any Court of the United States, than according to the rules of the common law.

Article VIII

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishment inflicted.

Article IX

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Article X

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

The Bill of Rights

Ratified December 15, 1791

Article I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Article II

A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

Article III

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Article IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Article V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any Criminal Case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Article VI

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining Witnesses in his favor, and to have the Assistance of Counsel for his defence.

Article VII

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury shall be otherwise reexamined in any Court of the United States, than according to the rules of the common law.

Article VIII

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishment inflicted.

Article IX

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Article X

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

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

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

PROBABLE CONTENTS OF THE PPD 20

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

Offensive Cyberweapons and Tactics

- PPD 20 authorizes the creation, maintenance and use of cyberweapons that can be used offensively
  - DDoS
  - Espionage
  - Reconnaissance
  - Sabotage

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

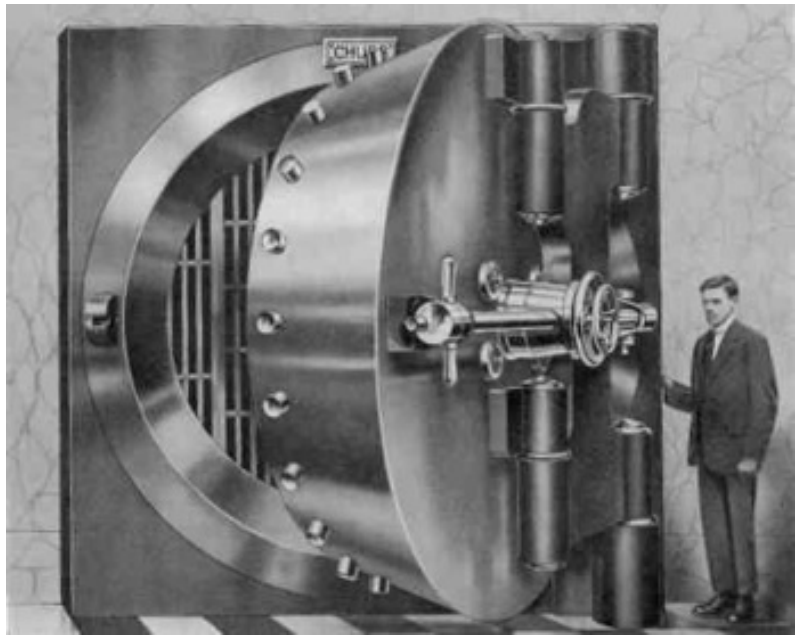
Probable Contents of the PPD 20

- PPD 20 Provides Guidance and Streamlined Directives for
  - Definition of Critical Assets
  - Ongoing Risks Assessments
  - The Creation and Maintenance of Operational Plans for Offensive and Defensive Operations
  - The Creation and Maintenance and Use of Offensive and Defensive Cyberweapons
  - Rapid response
  - The Creation and Maintenance and Use of Contingency Plans in the Event of a National Emergency
  - U.S. Cyber Command's Roles and Responsibilities related to offensive and defensive cyberwarfare operations and cyberdeterrence
  - DHS's Roles and Responsibilities related to offensive and defensive cyberwarfare operations and cyberdeterrence
  - Cyber operations with Allies (i.e. Israel and the U.K.)
  - How the U.S. will protect its interests and the interests of its Allies in Cyberspace
  - Probable shutdown of the public Internet inside the U.S. in the event of an extreme set of cyberattacks or emergency **(external or internal)**

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

The Classification of PPD 20 and the Necessity for Secrecy

- PPD 20 is classified as **Top Secret** because
  - It protects the plans and actions of the Federal Government and the U.S. Military
  - It protects our Allies
  - It prevents unfriendlies (state and non-state actors) from gaining an advantage
  - It prevents the American public from getting excited



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

So Why PPD 20 and Why Now?

- CISPA legislation failed to get passed in 2012 by the 112th Congress
- The Obama Administration recognition that the protection of Cyberspace and the Internet is vital to our national interests and to the interests of our Allies
- The alarming increase of cyberattacks, both in frequency and sophistication, make it imperative for President Obama to act, sooner than later

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

How Will PPD 20 Affect America the Average American

- America will be more secure
- Americans will be under greater surveillance
- The Federal Government will react more swiftly and efficiently to cyber events
- More and more data will be collected and analyzed
- Americans will have less “freedom”

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

What Can You and Your Business Do Today?

- Educate yourself your family, colleagues and your organization about Threats and Vulnerabilities related to Cyberattacks and Cyberwarfare
- Adopt or create a security compliance framework… and use it
- Act Responsibly
- Practice Self Restraint and Self Censorship
- Protect Yourself, your family, colleagues and your organization
- Do not take matters into your own hands and go on the offensive
- Social Media Monitoring, Watch your Employees, the Government is Watching
- Remember: These Rights from the Bill of Rights have become greatly limited or disappeared completely: 1, 4, 6, and 8
- Watch this space, it's only going to get more interesting

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

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 Cybersecurity

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

ILLINOIS INSTITUTE OF TECHNOLOGY

Bellevue University

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

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

BELLEVUE UNIVERSITY

THE FUTURE OF CYBERWAR AND CYBERATTACKS

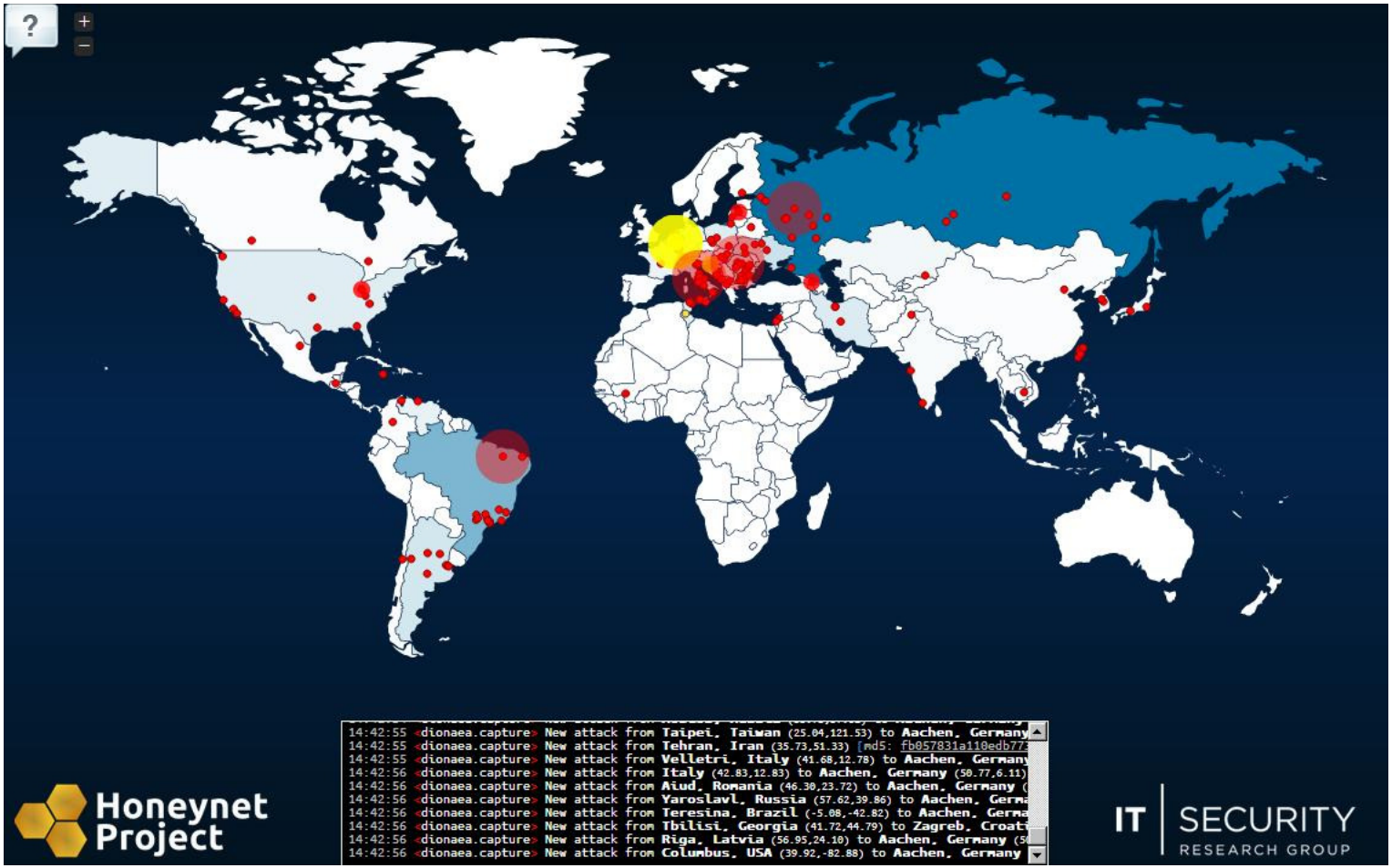
Copyright 2013 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

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 cyber defense and deterrence will be necessary
- Greater dangers from both state and non-state actors
- Better analysis and think-tank groups
- Possibly more secret Policy Directives (i.e. PPD 20)
- Possible loss of more personal freedoms

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

We Will Be Living in Interesting Times From Now On…



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

Conclusion

- The unique nature of cyberattacks and cyberwarfare, combined with the facts that cyberspace is so critical to business and that there are so many people who use it, makes it a complex area to protect
- The Obama Administration is extremely tech savvy and committed to defending cyberspace and the Internet for America and its Allies, and in the absence of Congressional support, the Obama Administration will act decisively

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

Questions

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

Copyright 2012 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

Website

http://billslater.com/cyberwar

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

William F. Slater, III

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

Copyright 2012 by William F. Slater, III, Chicago, IL, U.S.A.. All rights reserved nationally and internationally

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.
- 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.

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

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. And 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

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

More References

Rand Beers is the current Under Secretary of Homeland Security for National Protection and Programs. Beers was appointed as Under Secretary by President Barack Obama on June 19, 2009.

March 20, 2013, he delivered this 12-page report, a Statement for the Record Before the United States House of Representatives Appropriations Committee Subcommittee on Homeland Security. It gives unusually detailed review of how the Executive Branch, particularly the Department of Homeland Security sees its role in defining and protecting Critical Infrastructure, both physical and virtual from cyber threats related to cyberattacks. It also discusses the contents the contents and intent of PPD 21, EO 13636, both of which are related specifically to cybersecurity and protection of critical infrastructure.

For your edification:
http://appropriations.house.gov/uploadedfiles/hhrg-113-ap15-wstate-beersr-20130320.pdf

More information:

EO 13636
http://blog.zwillgen.com/wp-content/uploads/2013/02/CybersecurityEO-201302122.pdf

PPD 21
http://blog.zwillgen.com/wp-content/uploads/2013/02/PPD21-201302124.pdf

Update Presentation on the OBAMA Administration Priorities on DHS Highlights Efforts to Strengthen Cybersecurity for the Nations Critical Infrastructure
http://www.dhs.gov/news/2013/02/13/dhs-highlights-efforts-strengthen-cybersecurity-nations-critical-infrastructure

Commentary:
http://blog.zwillgen.com/2013/02/13/for-obama-a-cybersecurity-triple-play/

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