Civiliniazation of War – Paramilitarization of Cyberspace and its implications for (civilian) infosec pros. A new framework for collaboration

by @rodsoto

What is war?

"An act of violence intended to compel our opponent to fulfill our will". Clausewitz

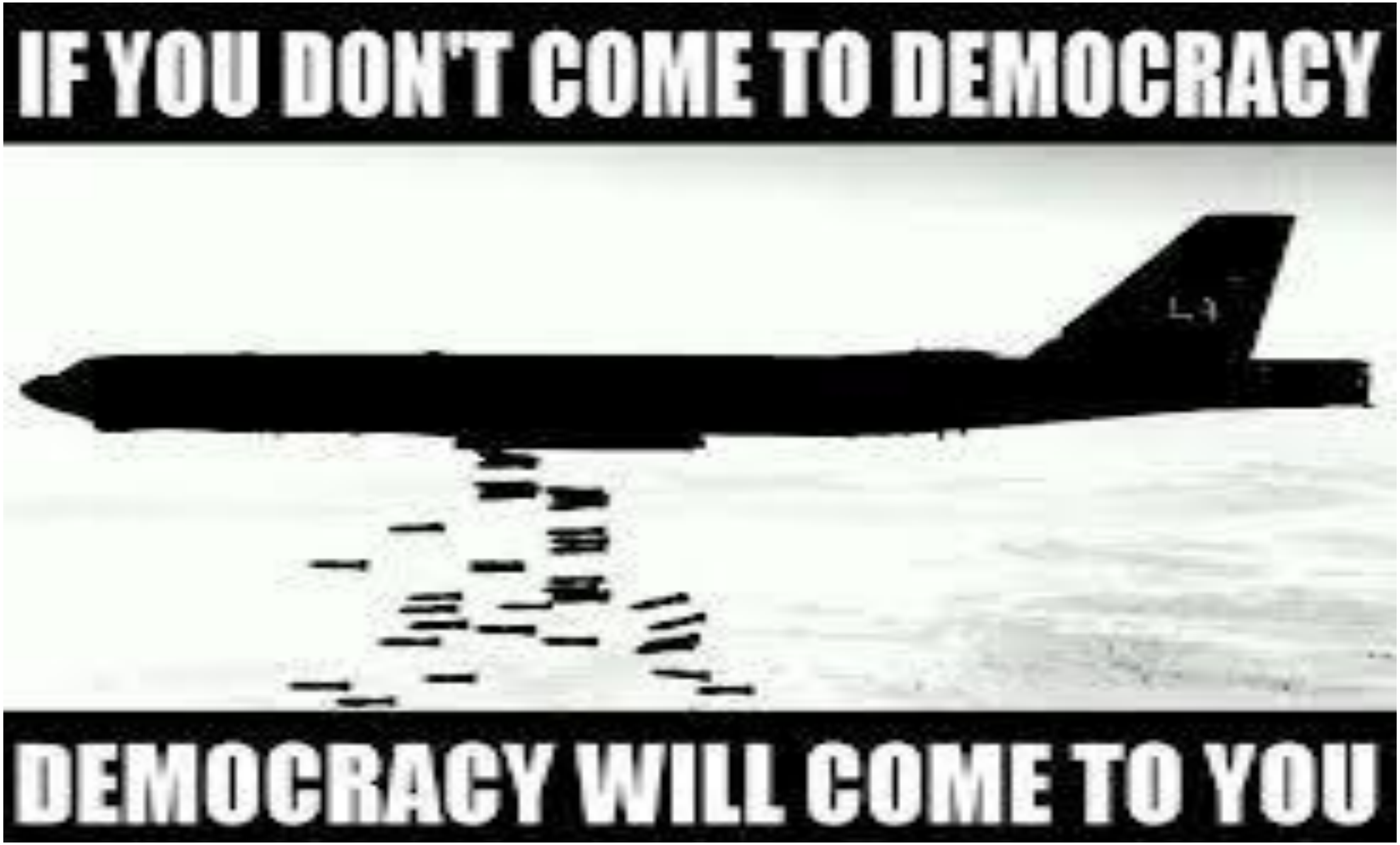
Characterized by focusing its operations on demarcated military personnel,
system and institutions.

Traditional concept of war delineates strictly civilians from military

Civilian: A person not in the armed forces services or police.

Military: the armed forces of a country.

America Power Supremo



Is the concept of war as we know it obsolete?

- The United States a military power supremo (Kilcullen)

- PLA Concept of “Unrestricted warfare”

- Decline of inter-state wars, growing role of civilians in high-technology warfare

- Military operations other than war (MOOTW) – Confrontation of NON-Combatants
  Non- Military war

- Last decade has seen a change in the involvement of civilians in war
  (Leviathan vs SysAdmin - Barnett)

- Widespread adoption of high tech and information technology. Growing relevance of intra-state armed conflict, the pervasiveness of civilian agencies in such conflicts, and the blurring of lines between civilians and combatants.

War is still WAR

“War which has undergone the changes of modern technology and the market system will be launched even more in atypical forms. In other words, while we are seeing a relative reduction in military violence, at the same time we definitely are seeing an increase in political, economic, and technological violence. However, regardless of the form the violence takes, war is war, and a change in the external appearance does not keep any war from abiding by the principles of war.”

Liang & Xiangsui
Unrestricted Warfare - 1999

Technological violence involves the INTERNET

- Use of Internet and information technology as a mean to gain advantage over adversary countries

- Theft of IP, ex-filtration of data, espionage

- Take over of essential services dependent on the use of IT and the Internet

- Deny, degrade, destroy ability of adversary to perform and provide essential services via aggressive digital attacks

- Inflict or exert power by amplifying effects of hostile actions blackmail or extortion by infecting millions of hosts with malware/spyware

Consider this...

The security and effective operation of U.S. critical infrastructure including energy, banking and finance, transportation, communication, and the Defense Industrial Base – rely on cyberspace, industrial control systems, and information technology that may be vulnerable to disruption or exploitation.*

Cyber threats to U.S. national security go well beyond military targets and affect all aspects of society.

National security is being redefined by cyberspace.*

Consider this

16 Industries considered Critical Infrastructure Sectors of the United States (DHS):

- Chemical Sector
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial
- Food & Agriculture
- Gov Facilities
- Health Care
- IT
- Nuclear
- Transportation Sys
- Water & Waste Water

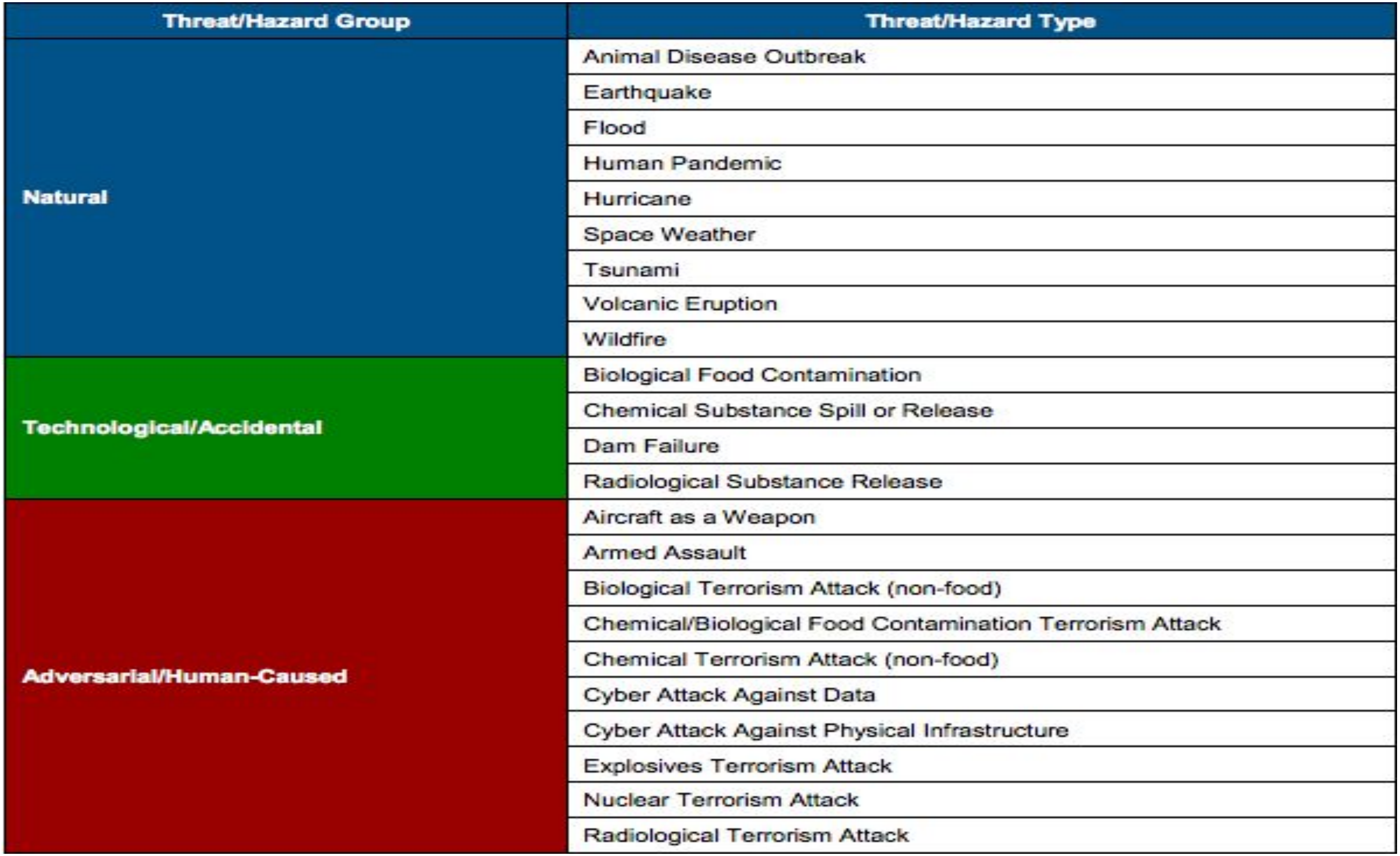
Cyber domain is also included in the scope of the National Protection Framework

- Critical Infrastructure Protection. Protecting the physical and cyber elements of critical infrastructure. This includes actions to deter the threat, reduce vulnerabilities, or minimize The consequences associated with a terrorist attack, natural disaster, or manmade disaster. Critical Infrastructure Protection is an element of critical infrastructure security and resilience as detailed in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.

- Cybersecurity. Securing the cyber environment and infrastructure from unauthorized or malicious access, use, or exploitation while protecting privacy, civil rights, and other civil liberties.

*Page 3
https://s3-us-gov-west-1.amazonaws.com/dam-production/uploads/1406717583765-996837bf788e20e977eb5079f4174240/FINAL_National_Protection_Framework_20140729.pdf

Cyber also included in the Strategic National Risk Assessment



Threat/Hazard Group	Threat/Hazard Type
Natural	Animal Disease Outbreak
	Earthquake
	Flood
	Human Pandemic
	Hurricane
	Space Weather
	Tsunami
	Volcanic Eruption
	Wildfire
Technological/Accidental	Biological Food Contamination
	Chemical Substance Spill or Release
	Dam Failure
	Radiological Substance Release
Adversarial/Human-Caused	Aircraft as a Weapon
	Armed Assault
	Biological Terrorism Attack (non-food)
	Chemical/Biological Food Contamination Terrorism Attack
	Chemical Terrorism Attack (non-food)
	Cyber Attack Against Data
	Cyber Attack Against Physical Infrastructure
	Explosives Terrorism Attack
	Nuclear Terrorism Attack
	Radiological Terrorism Attack

Cyberspace as a battlefield

"Every citizen **(Infosec Pro/Hacker)**is a soldier"? Mao Zhedong

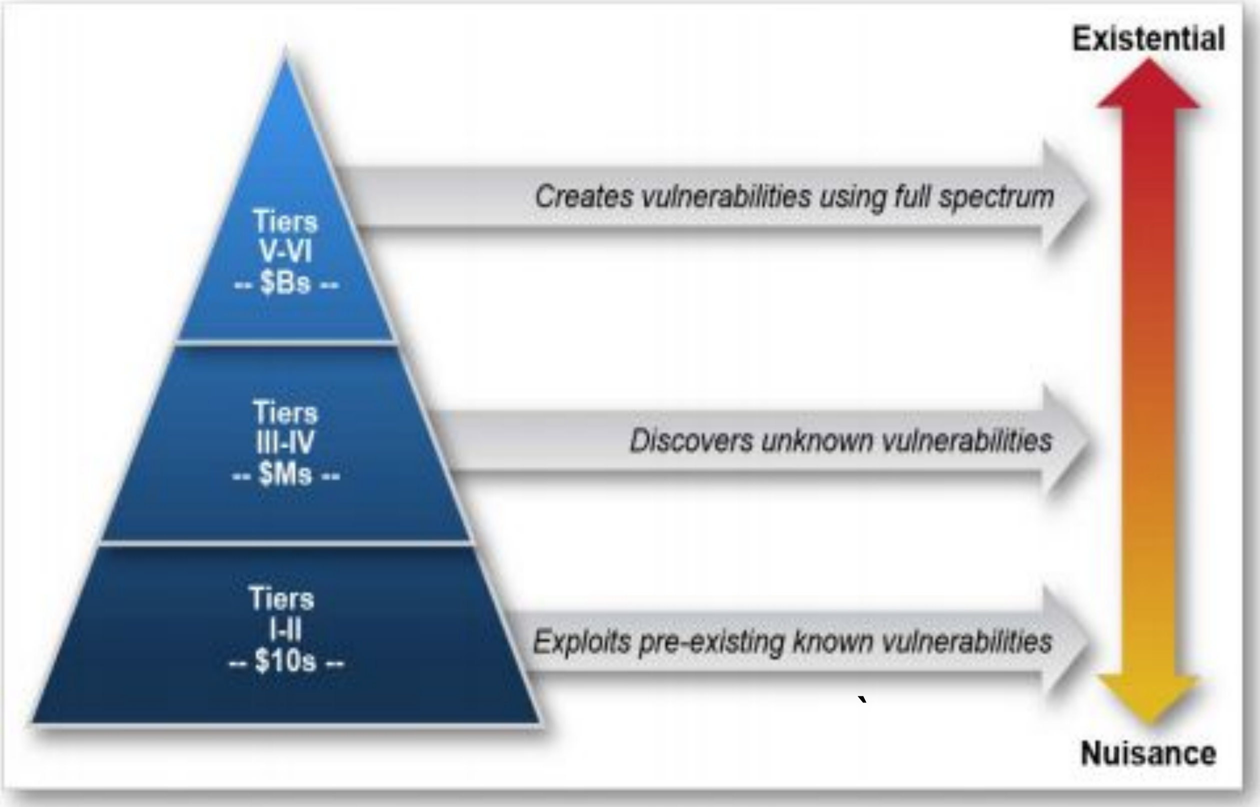
Para-militarization of Cyberspace

Paramilitary : (of an unofficial force) organized similarly to a military force.

- Increase and proliferation of “hackers for hire”, hacktivists and digital “insurgents”

- Infosec civilian professionals are facing threats in some cases against state sponsored military actors

Cyber Threat Taxonomy


Existential
Tiers
V-VI
-- $Bs --
Creates vulnerabilities using full spectrum
Tiers
III-IV
-- $Ms --
Discovers unknown vulnerabilities
Tiers
I-II
-- $10s --
Exploits pre-existing known vulnerabilities
Nuisance

Source DoD Defense Science Board

Examples of war in cyberspace

- Estonia 2007

- Stuxnet 2010

- Shamoon 2013

- Itsoknoproblembro 2011-2013

There are also NUMEROUS incidents involving the 16 verticals classified by DHS as critical infrastructure were there is allegedly state sponsored involvement

Existential Cyber Attack

“Existential Cyber Attack is defined as an attack that is capable of causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc.”*

*Department of Defense Science Board Report

War in cyberspace brings infosec civilans to the frontlines

- Current state of affairs has no framework that guides infosec professionals

- Title 10 United States code – DOD military operations (Army, Navy, Air Force)

- Title 50 United States code – Intelligence collection (NSA, DIA, CIA) – Civilian agencies. Civilian Federal Networks under DHS

- Corporations and Residential networks YOU ARE ON YOUR OWN. Under Title 10 & Title 50 specifications. Civilians CANNOT engage in cyber warfare. Keystrokes executed by military personnel only

War in cyberspace brings infosec civilians to the frontlines

- In this context war is no longer just military business

- Either you wanted or not you are in the trenches

- There are no clear rules of engagement

- No clear channels of communication with national security agencies

- No clear procedures of disclosure of such incidents

- Reaction and prosecution is based on $value and this may overlook the big picture when dealing with incidents that may affect other essential critical infrastructure companies

Civilians in the fog of war (cyber)

**The term seeks to capture the uncertainty regarding one's own capability,
adversary capability, and adversary intent during an engagement, operation, or campaign
*wikipedia.**

Are INFOSEC companies the equivalent of defense contractors?

In case you wonder? :) Are you a Mercenary?

Six conditions that must be cumulatively fulfilled:

- Special recruitment.
- Direct participation in hostilities.
- Desire for private gain as primary motivation.
- Neither a national of a party to the conflict nor a resident of territory controlled by a party.
- Not a member of the armed forces of a party to the conflict.
- Not sent by another State on official duty as a member of its armed forces.

For example,
consider a private company located in State A that is engaged by State B to conduct cyber
operations on its behalf in its armed conflict with State C. So long as the six criteria are
fully met, its employees who conduct the cyber operations are mercenaries, and thus
unprivileged belligerents. The same would be true with regard to a 'hacker for hire' who
meets the same criteria, even if operating alone and far from the battlefield.

It is clear that no person qualifying as a mercenary enjoys combatant status.
Source: NATO Tallinn Manual

Are INFOSEC companies the equivalent of defense contractors?

ABSOLUTLEY NOT

- No legal framework that supports such collaboration

- One of the things expressly prohibited to contractors:

“[p]rohibited contract functions include actions that directly result in disruptive and/or destructive combat capabilities including offensive cyber operations, electronic attack, missile defense, and air defense.”*
From the Law of Armed Conflict Desk book

- Contractors are entitled to self defense though.. ;)

War in Cyberspace brings infosec civilians to the front

- The curious case of going from “UNCLASSIFIED to CLASSIFIED”

- Limits in cooperation forced by private civilian/military gap outdated laws in computer crime leaves infosec professionals with no choice but to assume a passive posture after attack

- Lack of communication between national security agencies and infosec professionals prevents putting dots together

-The line between civilians and military is blurred in some cases biggest civilian responsibility in protecting critical essential infrastructure services

War in Cyberspace brings infosec civilians to the front-lines

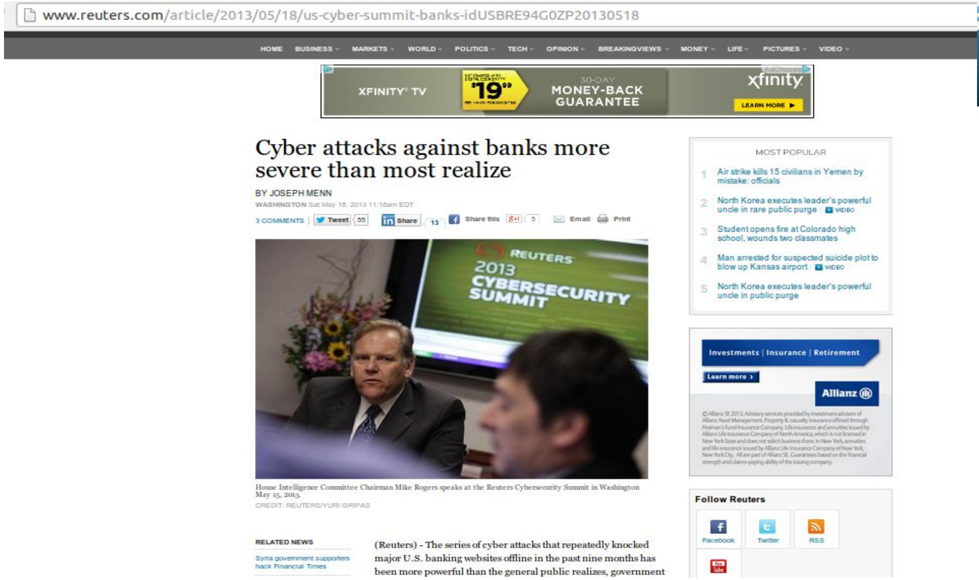
- Governments wants it both ways. They wont brief us yet they want us to identify and tell them what we do not know

- Wrongful approach of government agencies only in commercial damages

- Government CANNOT give you a computer and turn you into a cyber warrior in a boot camp. They need to embrace the civilian infosec professionals

- Once again YOU CANNOT ENGAGE IN COMBAT. As civilian you are likely to fall under “unprivileged enemy belligerents”, this term is used to refer to “terrorists” or participating in war but outside the law and not protected by LOAC, GC, etc.

The power supremo is already being tested



Cyber attacks against banks more severe than most realize

BY JOSEPH MENN

WASHINGTON Sat May 18, 2013 11:18am EDT

House Intelligence Committee Chairman Mike Rogers speaks at the Reuters Cybersecurity Summit in Washington May 15, 2013.

CREDIT: REUTERS/YURI GRIPAS

RELATED NEWS

Syria government supporters hack Financial Times

(Reuters) - The series of cyber attacks that repeatedly knocked major U.S. banking websites offline in the past nine months has been more powerful than the general public realizes, government

MOST POPULAR

1 Air strike kills 15 civilians in Yemen by mistake: officials

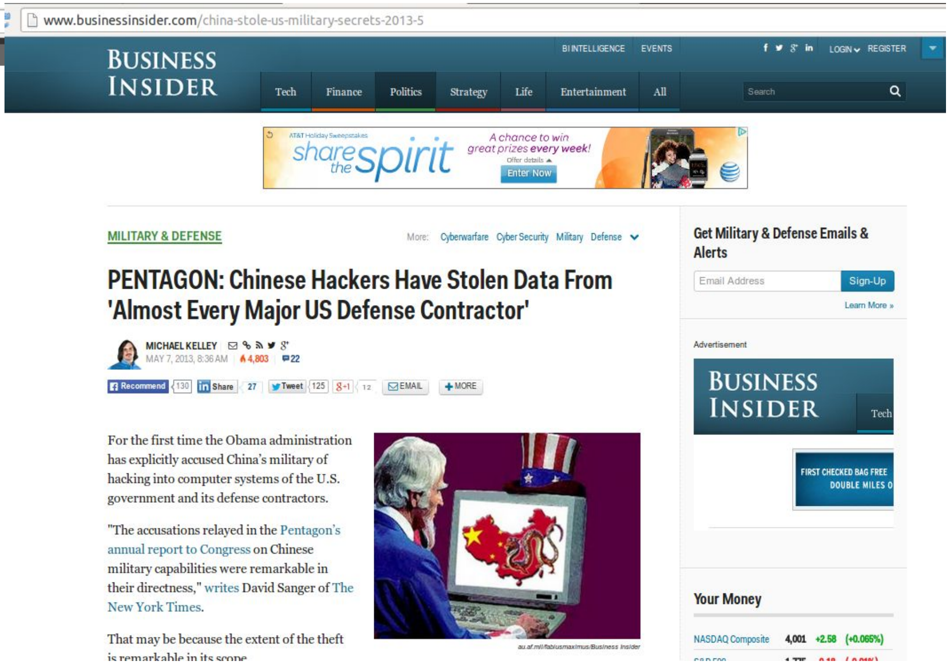
2 North Korea executes leader's powerful uncle in rare public purge VIDEO

3 Student opens fire at Colorado high school, wounds two classmates

4 Man arrested for suspected suicide plot to blow up Kansas airport VIDEO

5 North Korea executes leader's powerful uncle in public purge

Follow Reuters



MILITARY & DEFENSE

PENTAGON: Chinese Hackers Have Stolen Data From 'Almost Every Major US Defense Contractor'

MICHAEL KELLEY

MAY 7, 2013, 8:36 AM 4,803 22

For the first time the Obama administration has explicitly accused China's military of hacking into computer systems of the U.S. government and its defense contractors.

"The accusations relayed in the Pentagon's annual report to Congress on Chinese military capabilities were remarkable in their directness," writes David Sanger of The New York Times.

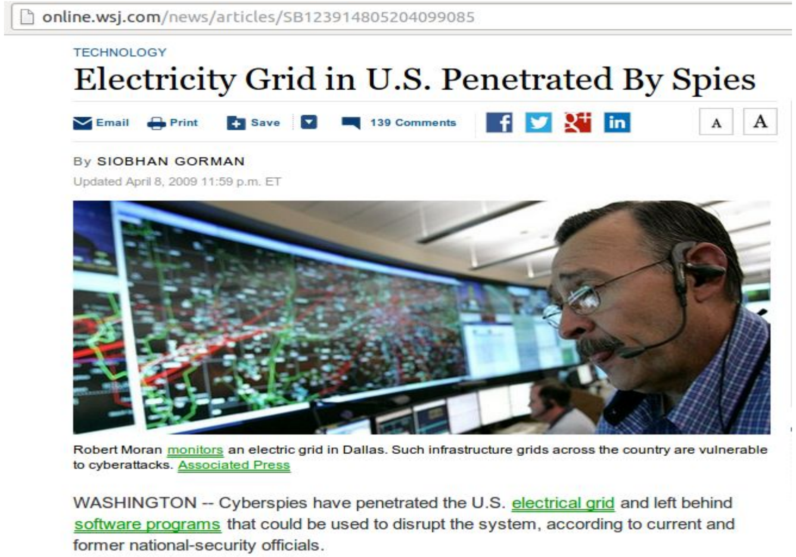
That may be because the extent of the theft is remarkable in its scope

au.af.mil/fabiusmaximus/Business Insider

Get Military & Defense Emails & Alerts

Your Money

NASDAQ Composite	4,001	+2.58	(+0.065%)



TECHNOLOGY

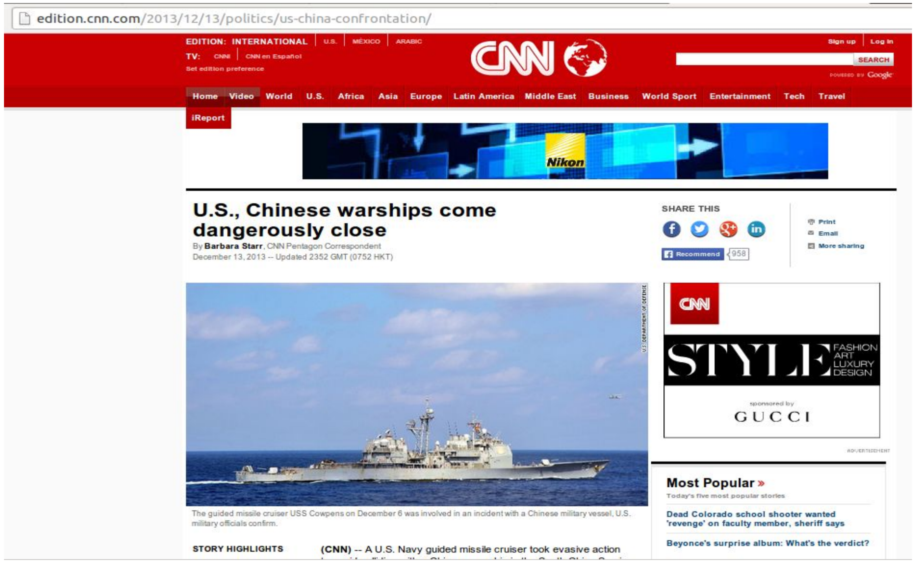
Electricity Grid in U.S. Penetrated By Spies

By SIOBHAN GORMAN

Updated April 8, 2009 11:59 p.m. ET

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks. Associated Press

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.



U.S., Chinese warships come dangerously close

By Barbara Starr, CNN Pentagon Correspondent

December 13, 2013 -- Updated 2352 GMT (0752 HKT)

The guided missile cruiser USS Cowpens on December 6 was involved in an incident with a Chinese military vessel, U.S. military officials confirm.

STORY HIGHLIGHTS

(CNN) -- A U.S. Navy guided missile cruiser took evasive action

Most Popular »

Today's five most popular stories

Dead Colorado school shooter wanted 'revenge' on faculty member, sheriff says

Beyonce's surprise album: What's the verdict?

The power supremo is already being tested

- Near critical levels of downtime in principal U.S financial institutions during 2013 DDos campaigns

- Widespread IP theft, probe and footprint of essential national infrastructure

- Regional powers able to reach military level enough to defy U.S. (2015). This may also reflect in an increase of digital operations. Regional powers using digital domain to exert power on businesses, organizations and individuals

- Opposing powers seem to have a clearer strategy or framework for military-civilian collaboration. They also seem to have a good grasp of using Cyber to counter military might imbalance

I brought you PEACE Internet

The power supremo is already being tested

- No actual cyberwar treaties. Geneva convention does not apply to cyberwar and even if forced, it would only be nominally

- Adversaries look at cyber as their way of countering overwhelming military, political and economic power, is not in their interest to regulate or establish balancing rules of conflict in cyber domain

- Internet as of now in terms of conflict is by nature asymmetric

and will continue to be, it may not be in our best interest to seek rules & regulation that may play against us in future conflicts

What to do as infosec professionals?

- Do not panic, become aware of your responsibilities and implications of your organization not only locally but nationally & Internationally

- Persist and persist in security awareness training at your organizations, families, communities

- Government must EMBRACE the infosec civilian community, nurture it and protect it NOT PROSECUTE IT

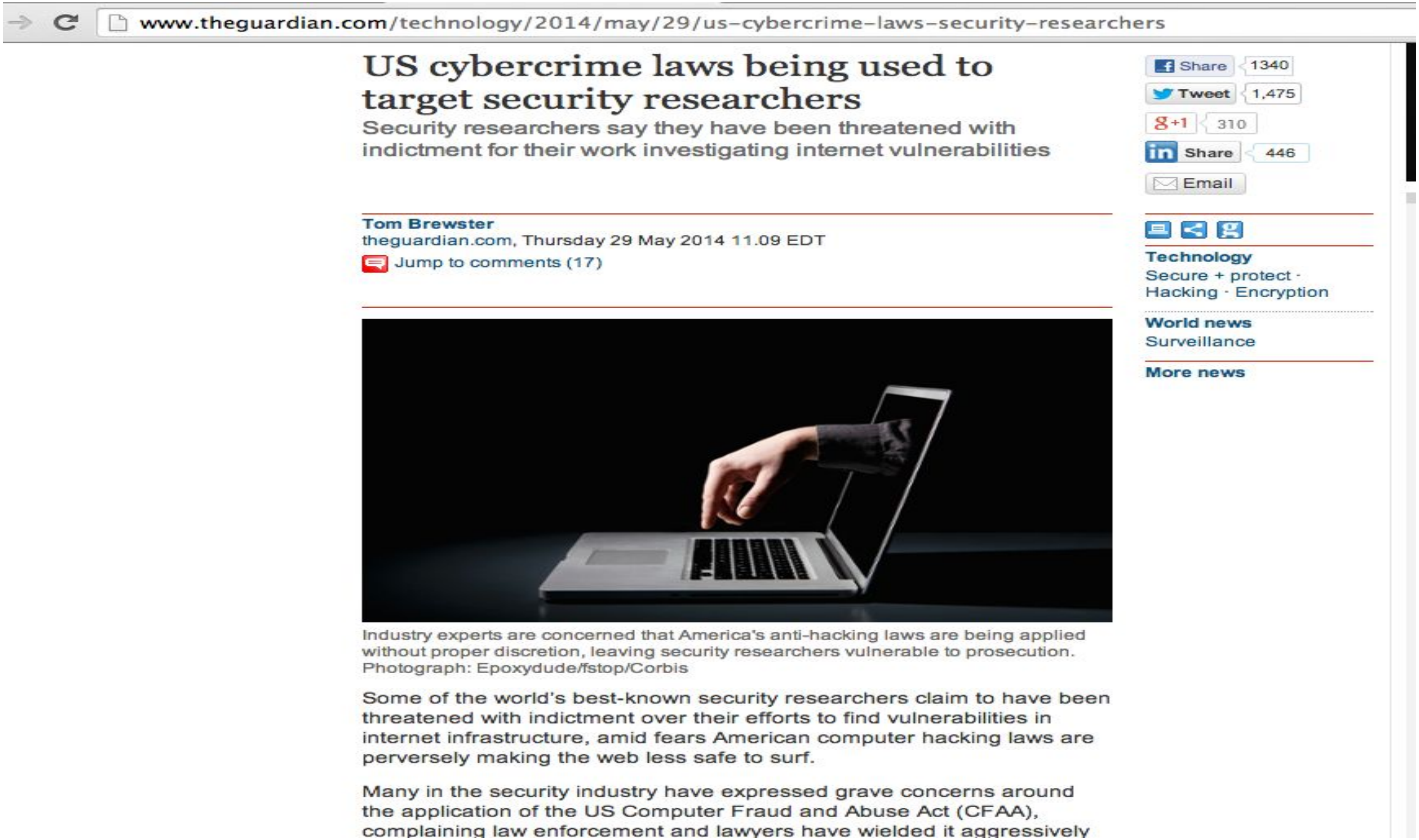
- Only through communication, collaboration and cooperation we will be able to avoid another "dots were no put together"

- Government must also clarify cyber domain chain of commands and rules of engagement (current laws unclear and outdated)

- Do not be a Neville Chamberlain . Being a vigilante is also not good, only organized community efforts will bring the attention of related government branches

- Participate in the community and help military/government understand cyber domain. It might be prudent re-open Office of Civilian Defense, closed in 1945. This office could be an effective mean of aggregating civilian infosec professionals skills to United States cyber force even if only for informational collaboration purposes

Some relevant developments, throughout this year



www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers
Share 1340
Tweet 1,475
+1 310
Share 446
Email
Technology
Secure + protect · Hacking · Encryption
World news
Surveillance
More news

US cybercrime laws being used to target security researchers

Security researchers say they have been threatened with indictment for their work investigating internet vulnerabilities

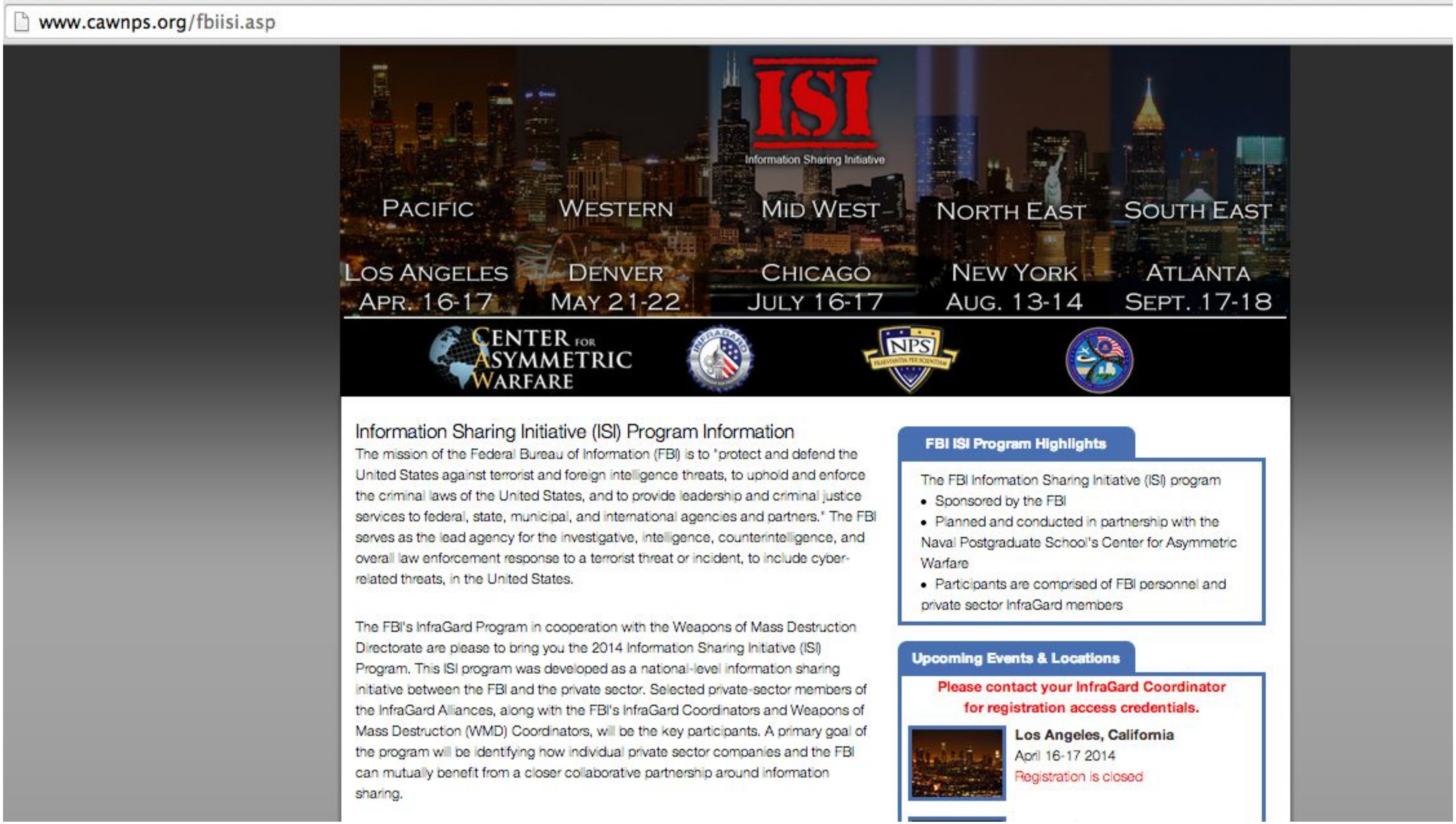
Tom Brewster
theguardian.com, Thursday 29 May 2014 11.09 EDT
Jump to comments (17)

Industry experts are concerned that America's anti-hacking laws are being applied without proper discretion, leaving security researchers vulnerable to prosecution. Photograph: Epoxydude/fstop/Corbis

Some of the world's best-known security researchers claim to have been threatened with indictment over their efforts to find vulnerabilities in internet infrastructure, amid fears American computer hacking laws are perversely making the web less safe to surf.

Many in the security industry have expressed grave concerns around the application of the US Computer Fraud and Abuse Act (CFAA), complaining law enforcement and lawyers have wielded it aggressively

Some relevant developments throughout this year



www.cawnps.org/fbiisi.asp

ISI

Information Sharing Initiative

Pacific	Western	Mid West	North East	South East
Los Angeles Apr. 16-17	Denver May 21-22	Chicago July 16-17	New York Aug. 13-14	Atlanta Sept. 17-18

Information Sharing Initiative (ISI) Program Information

The mission of the Federal Bureau of Information (FBI) is to "protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners." The FBI serves as the lead agency for the investigative, intelligence, counterintelligence, and overall law enforcement response to a terrorist threat or incident, to include cyber-related threats, in the United States.

The FBI's InfraGard Program in cooperation with the Weapons of Mass Destruction Directorate are please to bring you the 2014 Information Sharing Initiative (ISI) Program. This ISI program was developed as a national-level information sharing initiative between the FBI and the private sector. Selected private-sector members of the InfraGard Alliances, along with the FBI's InfraGard Coordinators and Weapons of Mass Destruction (WMD) Coordinators, will be the key participants. A primary goal of the program will be identifying how individual private sector companies and the FBI can mutually benefit from a closer collaborative partnership around information sharing.

FBI ISI Program Highlights

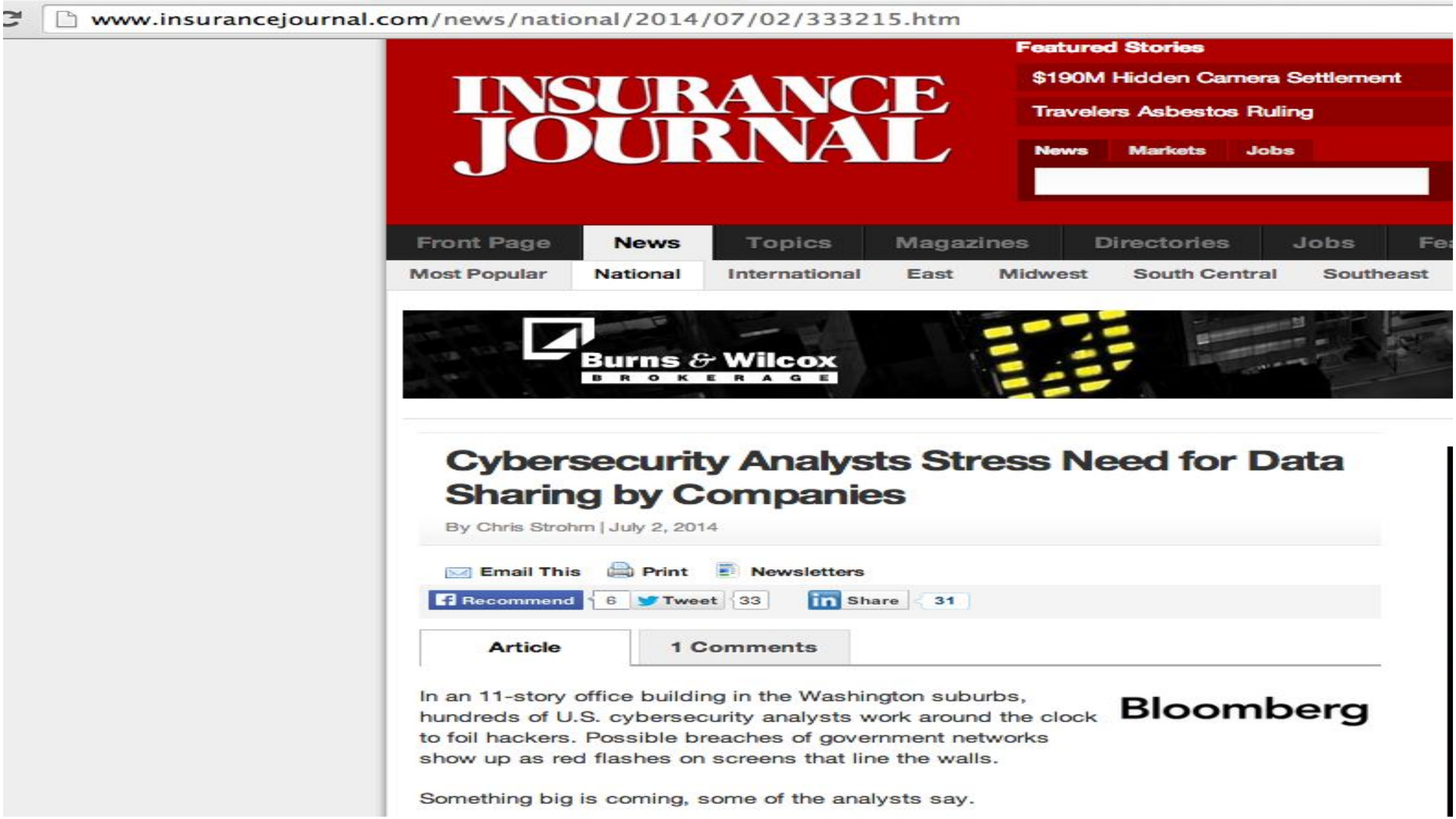
The FBI Information Sharing Initiative (ISI) program
- Sponsored by the FBI
- Planned and conducted in partnership with the Naval Postgraduate School's Center for Asymmetric Warfare
- Participants are comprised of FBI personnel and private sector InfraGard members

Upcoming Events & Locations

Please contact your InfraGard Coordinator for registration access credentials.

Los Angeles, California
April 16-17 2014
Registration is closed

Some relevant developments throughout this year



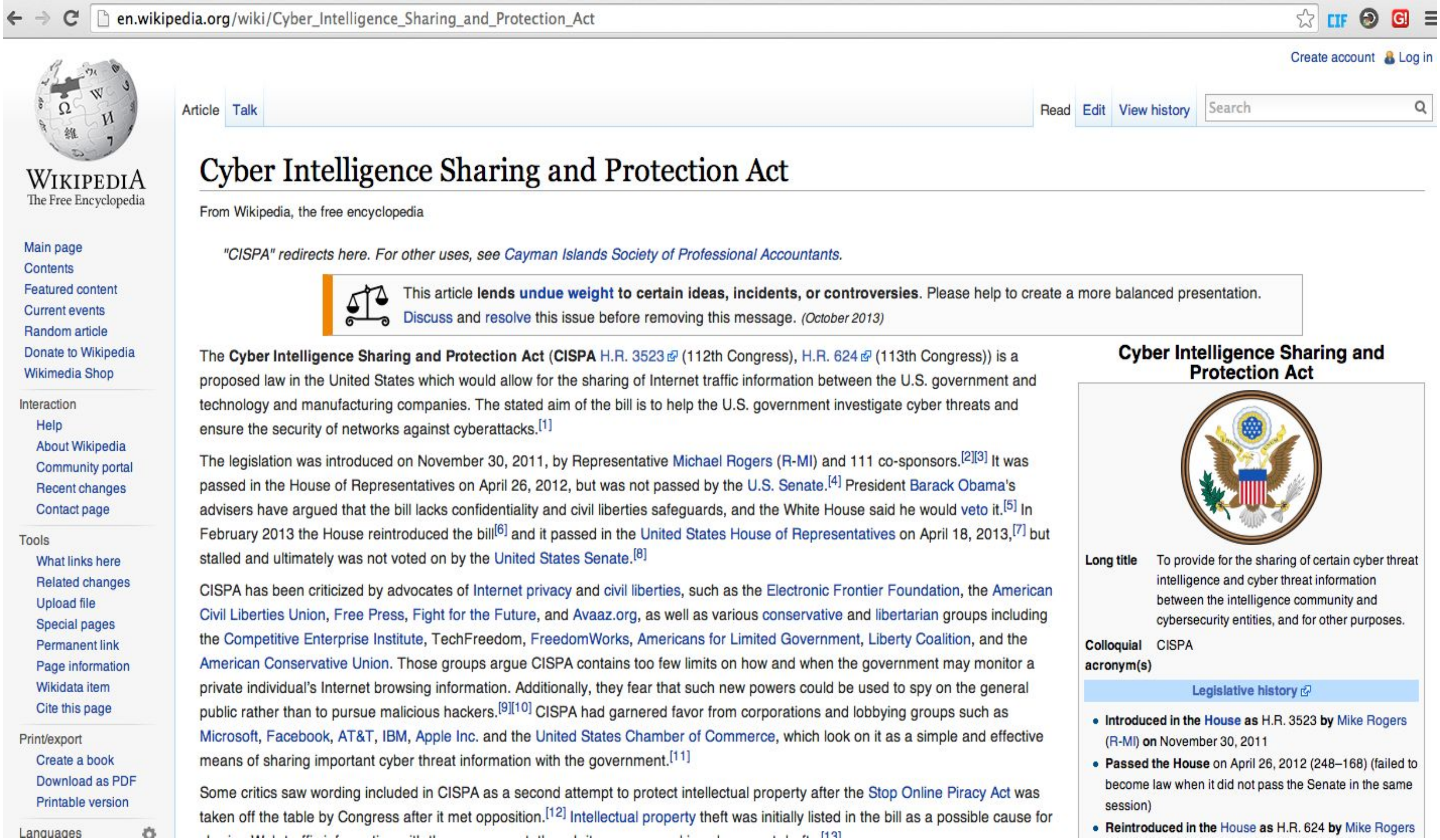
Cybersecurity Analysts Stress Need for Data Sharing by Companies

By Chris Strohm | July 2, 2014

In an 11-story office building in the Washington suburbs, hundreds of U.S. cybersecurity analysts work around the clock to foil hackers. Possible breaches of government networks show up as red flashes on screens that line the walls.

Something big is coming, some of the analysts say.

And of course there is THIS…



Cyber Intelligence Sharing and Protection Act

From Wikipedia, the free encyclopedia

"CISPA" redirects here. For other uses, see Cayman Islands Society of Professional Accountants.

This article **lends undue weight to certain ideas, incidents, or controversies**. Please help to create a more balanced presentation. Discuss and resolve this issue before removing this message. *(October 2013)*

The **Cyber Intelligence Sharing and Protection Act** (**CISPA** H.R. 3523 (112th Congress), H.R. 624 (113th Congress)) is a proposed law in the United States which would allow for the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. The stated aim of the bill is to help the U.S. government investigate cyber threats and ensure the security of networks against cyberattacks.[1]

The legislation was introduced on November 30, 2011, by Representative Michael Rogers (R-MI) and 111 co-sponsors.[2][3] It was passed in the House of Representatives on April 26, 2012, but was not passed by the U.S. Senate.[4] President Barack Obama's advisers have argued that the bill lacks confidentiality and civil liberties safeguards, and the White House said he would veto it.[5] In February 2013 the House reintroduced the bill[6] and it passed in the United States House of Representatives on April 18, 2013,[7] but stalled and ultimately was not voted on by the United States Senate.[8]

CISPA has been criticized by advocates of Internet privacy and civil liberties, such as the Electronic Frontier Foundation, the American Civil Liberties Union, Free Press, Fight for the Future, and Avaaz.org, as well as various conservative and libertarian groups including the Competitive Enterprise Institute, TechFreedom, FreedomWorks, Americans for Limited Government, Liberty Coalition, and the American Conservative Union. Those groups argue CISPA contains too few limits on how and when the government may monitor a private individual's Internet browsing information. Additionally, they fear that such new powers could be used to spy on the general public rather than to pursue malicious hackers.[9][10] CISPA had garnered favor from corporations and lobbying groups such as Microsoft, Facebook, AT&T, IBM, Apple Inc. and the United States Chamber of Commerce, which look on it as a simple and effective means of sharing important cyber threat information with the government.[11]

Some critics saw wording included in CISPA as a second attempt to protect intellectual property after the Stop Online Piracy Act was taken off the table by Congress after it met opposition.[12] Intellectual property theft was initially listed in the bill as a possible cause for

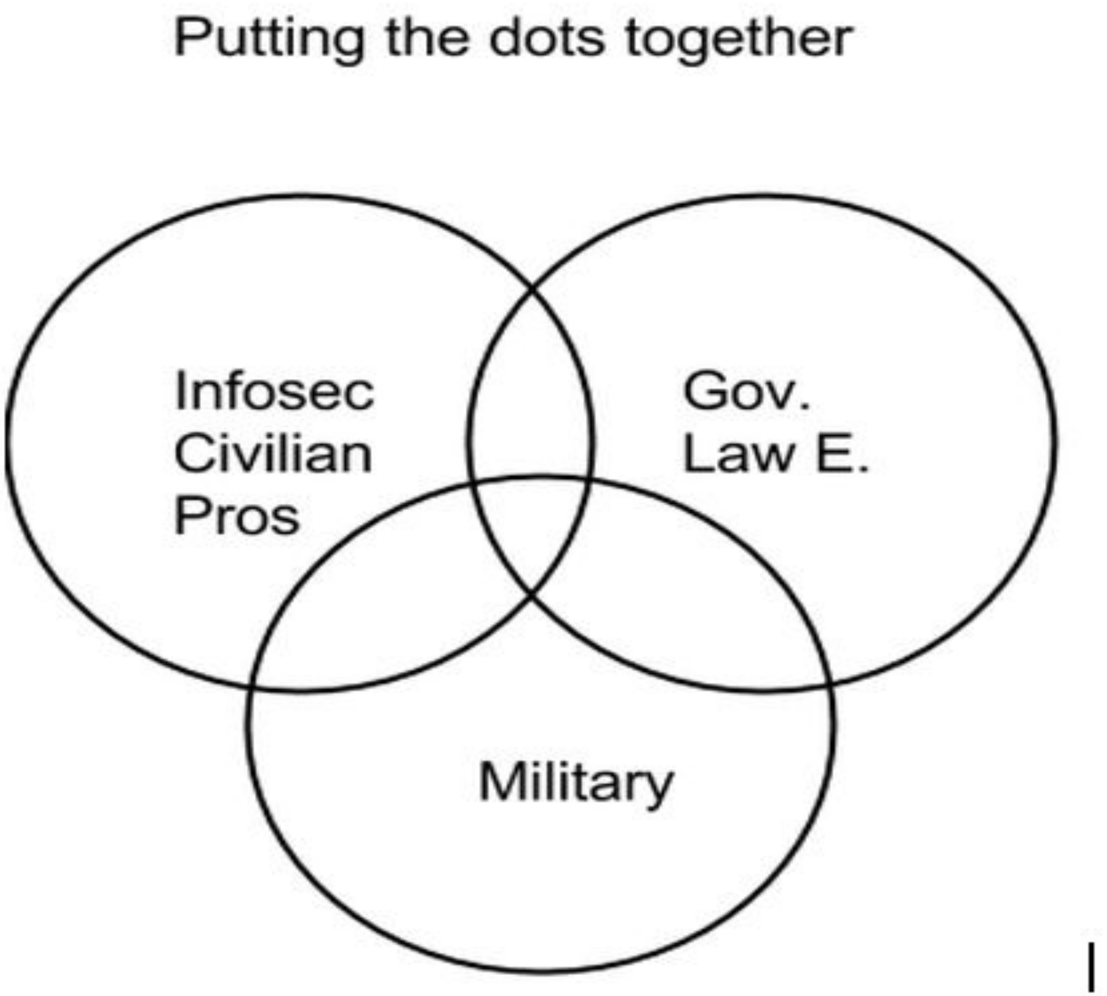
Cyber Intelligence Sharing and Protection Act

Long title	To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes.
Colloquial acronym(s)	CISPA

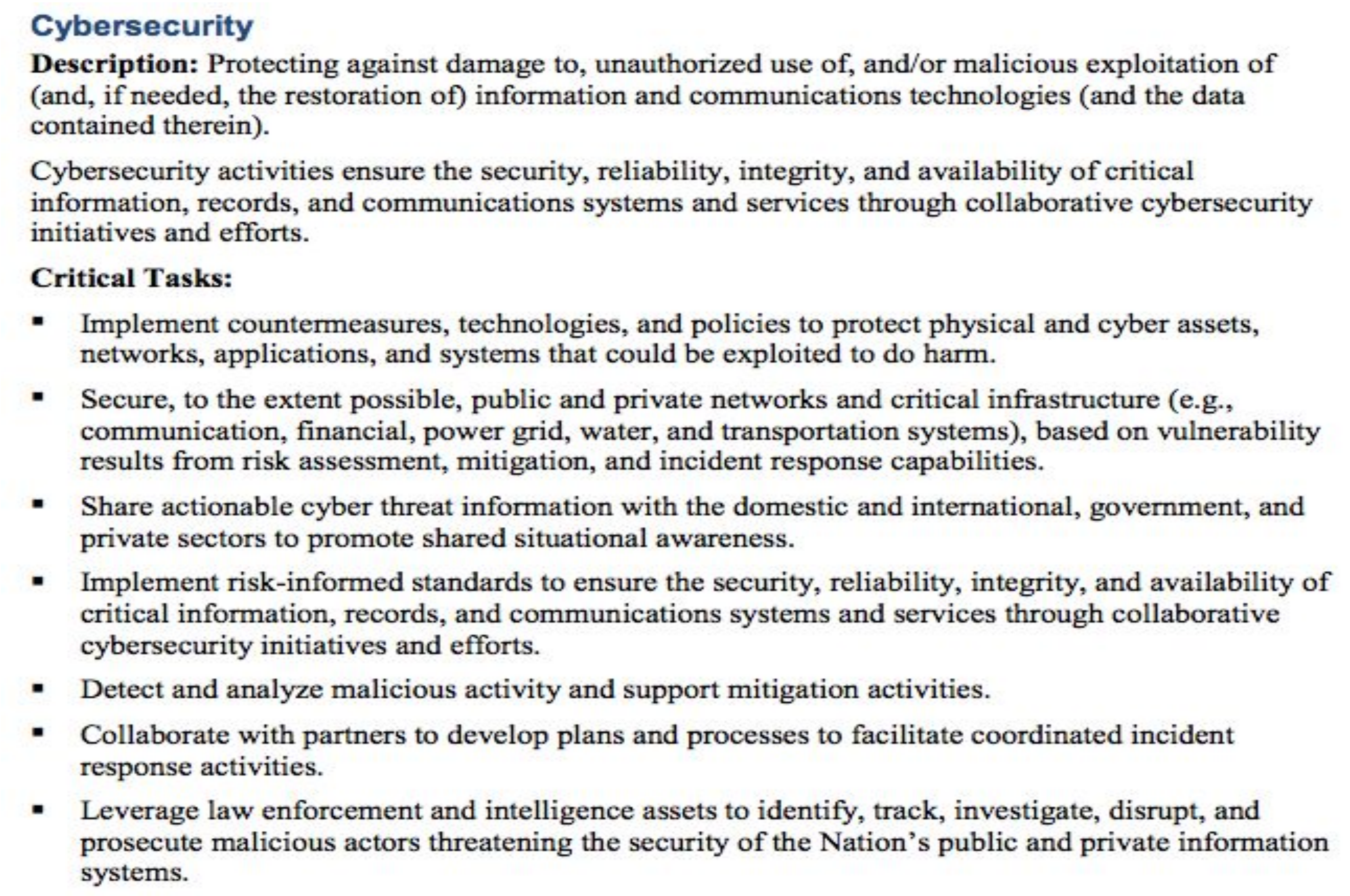
Legislative history

- **Introduced in the** House **as** H.R. 3523 **by** Mike Rogers (R-MI) **on** November 30, 2011
- **Passed the House** on April 26, 2012 (248–168) (failed to become law when it did not pass the Senate in the same session)
- **Reintroduced in the** House **as** H.R. 624 **by** Mike Rogers

A new framework for collaboration



Cybersecurity is included in the Core Capabilities Unique to Protection section included in the National Protection Framework – Page 17 of document NPF



Cybersecurity

Description: Protecting against damage to, unauthorized use of, and/or malicious exploitation of (and, if needed, the restoration of) information and communications technologies (and the data contained therein).

Cybersecurity activities ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.

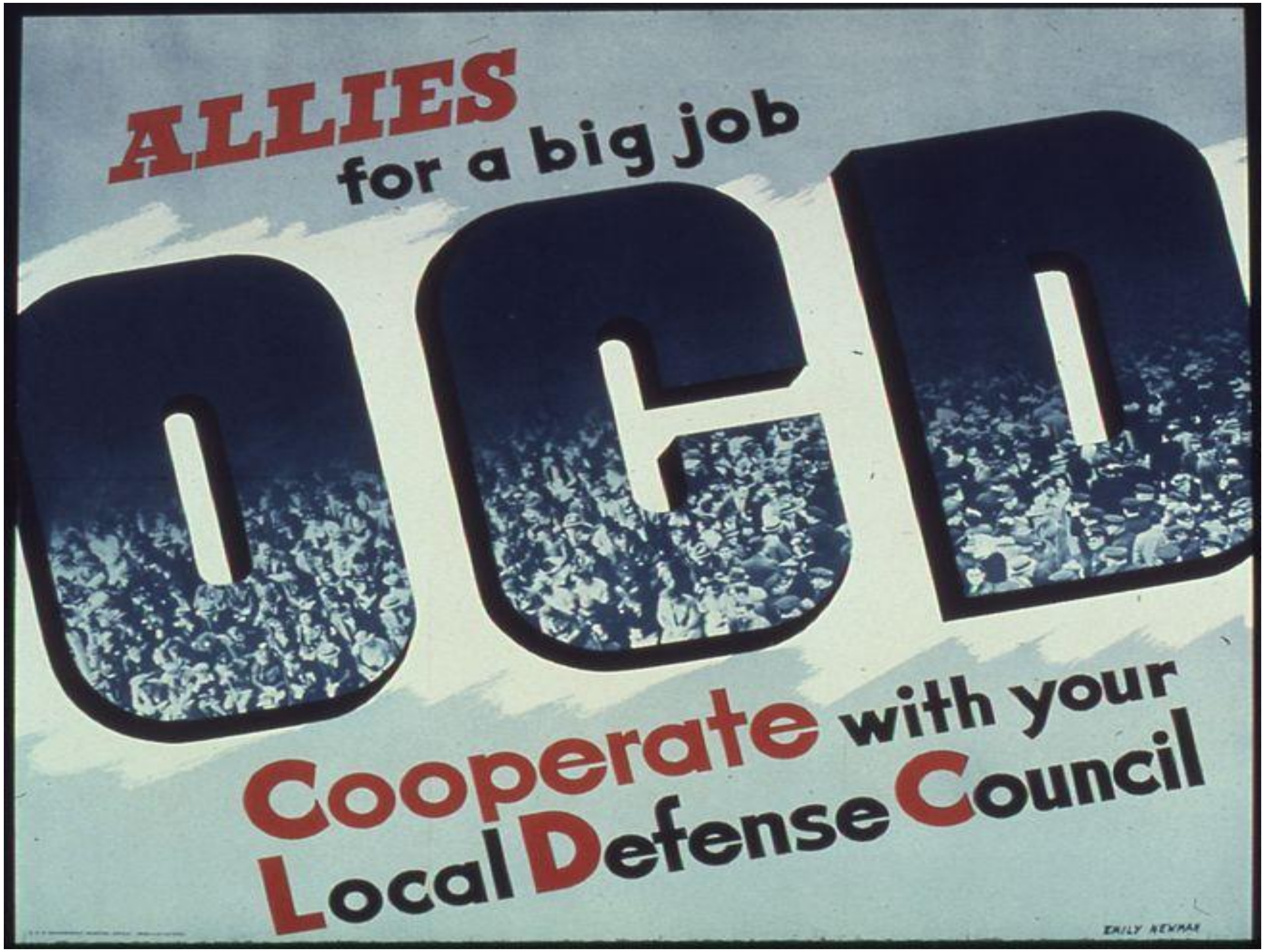
Critical Tasks:

- Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited to do harm.
- Secure, to the extent possible, public and private networks and critical infrastructure (e.g., communication, financial, power grid, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities.
- Share actionable cyber threat information with the domestic and international, government, and private sectors to promote shared situational awareness.
- Implement risk-informed standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts.
- Detect and analyze malicious activity and support mitigation activities.
- Collaborate with partners to develop plans and processes to facilitate coordinated incident response activities.
- Leverage law enforcement and intelligence assets to identify, track, investigate, disrupt, and prosecute malicious actors threatening the security of the Nation's public and private information systems.

This framework must address the following items:

- Disclosure procedures
- Rules Of Engagement
- Communication means
- Cross training with Military, Law Enforcement
- Incidents must not be approached from the monetary perspective
- Infosec civilian professionals must be trained in LOAC, GC
- Chain of command when dealing with National Security incidents
- Escalation Control/Matching procedures (For Cyber)
- Legal protections for Infosec civilian pros engaged
- Participation in National Protection Framework for Cyber
- Creation of an organization that oversees this framework

Office of Civilian Defense closed in 1945



Q&A

Your questions
reach me at rod@hackmiami.info
@rodsoto

References

http://www.defense.gov/news/d20110714cyber.pdf
http://en.wikipedia.org/wiki/Unrestricted_Warfare
http://en.wikipedia.org/wiki/Office_of_Civilian_Defense
http://en.wikipedia.org/wiki/Title_50_of_the_United_States_Code
http://en.wikipedia.org/wiki/Title_10_of_the_United_States_Code
http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf
http://www.amazon.com/Cyber-War-Threat-National-Security/dp/0061962244/ref=sr_1_1?ie=UTF8&qid=1396377212&sr=8-1&keywords=cyberwar+richard+clarke
http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
https://s3-us-gov-west-1.amazonaws.com/dam-production/uploads/1406717583765-996837bf788e20e977eb5079f4174240/FINAL_National_Protection_Framework_20140729.pdf