Governments Pwn the Web:
A Constitutional Right to IT-Security?

Co-Creating An Agenda for Research, Policy and Activism

Berkman Luncheon Series 18.03.14

https://www.axelarnbak.nl
2013/14 Fellow Berkman Center & CITP

#berkman

@axelarnbak

"In almost every issue of weekly [Computerworld] is an article detailing a case of computer fraud, embezzlement or sabotage (…). Over 100 different articles from mid 1971."

1. P. Browne, *Computer security: a survey,* ACM SIGMIS, vol. 4/3, 1972
2. A. Westin, *Databanks in a free society; computers, record-keeping, and privacy*, New York: Quadrangle Books 1972.

Socio-technical Change

THE CRYPTO WARS

FBI/NSA:
“GOING DARK”

How the Code Rebels Beat the Government—Saving Privacy in the Digital Age

STEVEN LEVY

AUTHOR OF *HACKERS*


1110 Coachella Canal Road
92259
WE REMEMBER FREEDOM
SLAB CITY
INTERNET
CAFE

NEWS

How the NSA Plans to Infect 'Millions' of Computers with Malware

By Ryan Gallagher and Glenn Greenwald 12 Mar 2014, 9:19 AM EDT 122

One presentation outlines how the NSA performs "industrial-scale exploitation" of computer networks across the world.

ABOUT THE AUTHORS


Ryan Gallagher
Reporter: Read more


Glenn Greenwald
Editor: Read more

The Washington Post

Back to previous page

FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance

By Craig Timberg and Ellen Nakashima, Published: December 6

"The most powerful FBI surveillance software can covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers, say court documents and people familiar with this technology."

Plausible deniability is gone. We know:

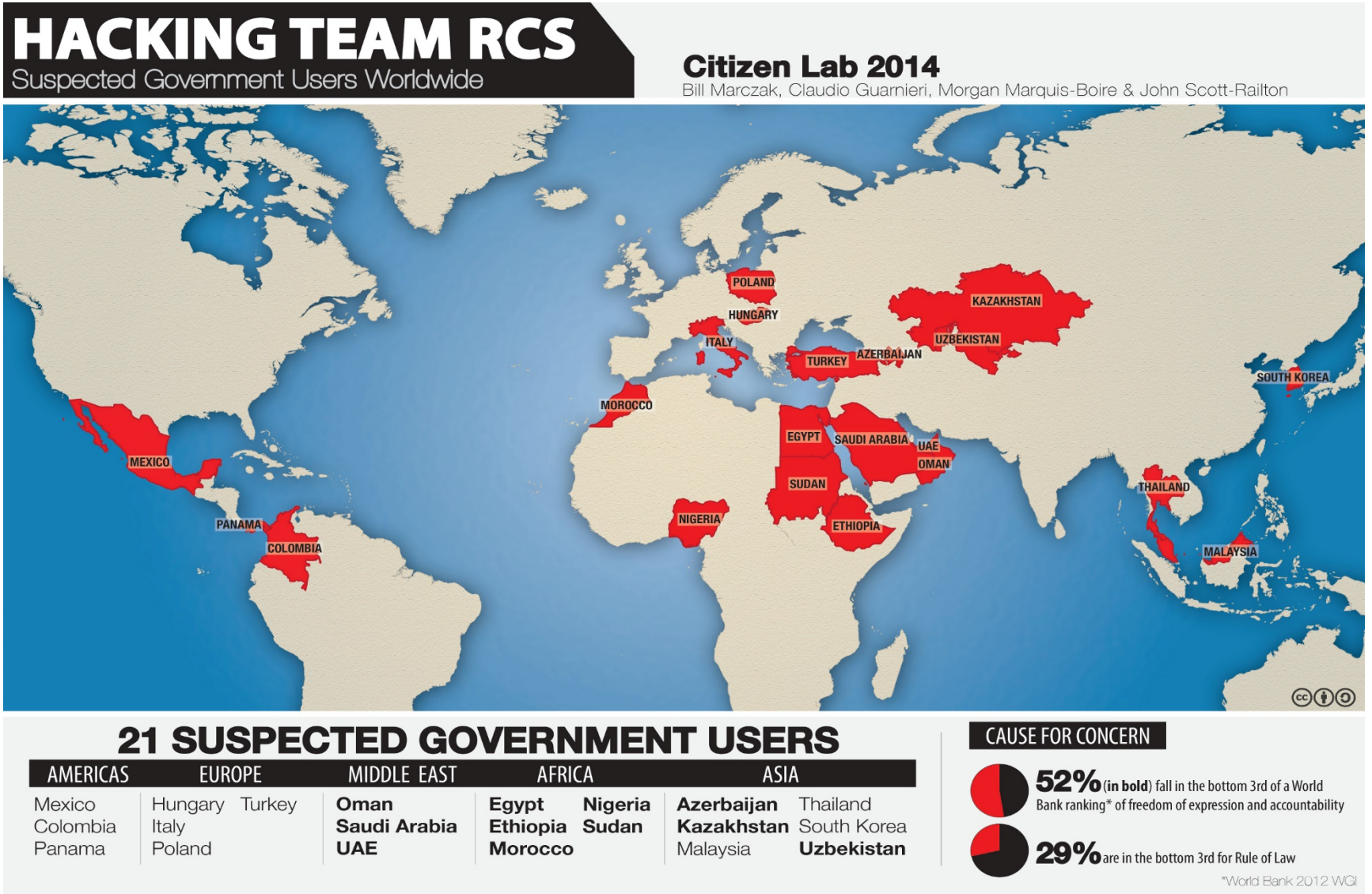
“It’s happening”
“It’s increasing”
“It’s problematic”

Today's talk about 'Western' Governments:

How to understand their hacking efforts?
How to respond to them?

Goal: co-create an agenda for research, policy and activism

TODAY: NOT DIRECTLY ABOUT..



History of dual-use regulation / Great work being done / Easy to condemn for hegemons

Check at the fantastic Citizen Lab: https://citizenlab.org/

OUTLINE

Hacking Cases by ‘Western’ Governments

11+ Problems with Government Hacking

A Constitutional Right to IT-Security?

Elements of a Research Agenda: Discussion!

OUTLINE

Hacking Cases by ‘Western’ Governments

11+ Problems with Government Hacking

A Constitutional Right to IT-Security?

Elements of a Research Agenda: Discussion!

YALE LAW SCHOOL

The Information Society Project

Law Enforcement & Hacking:
When Cops Control your Webcam

1:10 pm
Tuesday, Feb. 18
Levinson Auditorium
Law School

Panel 1: The Hacking Technologies Used by Law Enforcement

Kevin Poulsen, Investigations Editor, Wired (moderator)
Christopher Soghoian, Principal Technologist, ACLU
Morgan Marquis-Boire, Citizen Lab
Ashkan Soltani, Independent Consultant
Matt Blaze, Associate Professor, University of Pennsylvania
Axel Arnbak, Researcher, Institute for Information Law, University of Amsterdam

Panel 2: The Legal and Policy Implications of Hacking by Law Enforcement

Jennifer Valentino-Devries, The Wall Street Journal (moderator)
Magistrate Judge Steve Smith
Professor Laura Donahue, Georgetown University Law Center
Stephanie Pell, Principal, SKP Strategies LLC
Justin Rood, Senate Committee on Homeland Security and Governmental Affairs
Ahmed Ghappour, Clinical Instructor, The National Security Clinic, UT Law School

3 Cases of Government Hacking

1. Law Enforcement Investigation

2. Botnet prosecution and mitigation

3. Ubiquitous Intelligence Gathering

3 Cases of Government Hacking

1. Law Enforcement Investigation

2. Botnet prosecution and mitigation

3. Ubiquitous Intelligence Gathering

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN RE WARRANT TO SEARCH A TARGET COMPUTER AT PREMISES UNKNOWN	§	CASE NO. H-13-234M

MEMORANDUM AND ORDER

The Government has applied for a Rule 41 search and seizure warrant targeting a computer allegedly used to violate federal bank fraud, identity theft, and computer security laws. Unknown persons are said to have committed these crimes using a particular email account via an unknown computer at an unknown location. The search would be accomplished by surreptitiously installing software designed not only to extract certain stored electronic records but also to generate user photographs and location information over a 30 day period. In other words, the Government seeks a warrant to hack a computer suspected of criminal use. For various reasons explained below, the application is denied.

Magistrate Judge Smith, Apr. 2013, turns the FBI hacking request down:

1. *Identity and location of device owner not known*
2. *Search* **for** *and* **of** *computer*
3. *4th Amendment video surveillance criteria not met*

NB. Prof. Donahue (Georgetown):
dozens of cases from California to New York sealed, no public scrutiny

BUNDESTROJANER


BUNDESVERFASSUNGSGERICHT

German Cons

Chaos Computer Club

beta

SEARCH

home
Topics
Events
Support
Regional CCC
Publications
Contact
Imprint
Club

Deutsch

Chaos Computer Club analyzes government malware

2011-10-08 19:00:00, admin

The largest European hacker club, "Chaos Computer Club" (CCC), has reverse engineered and analyzed a "lawful interception" malware program used by German police forces. It has been found in the wild and submitted to the CCC anonymously. The malware can not only siphon away intimate data but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the internet.

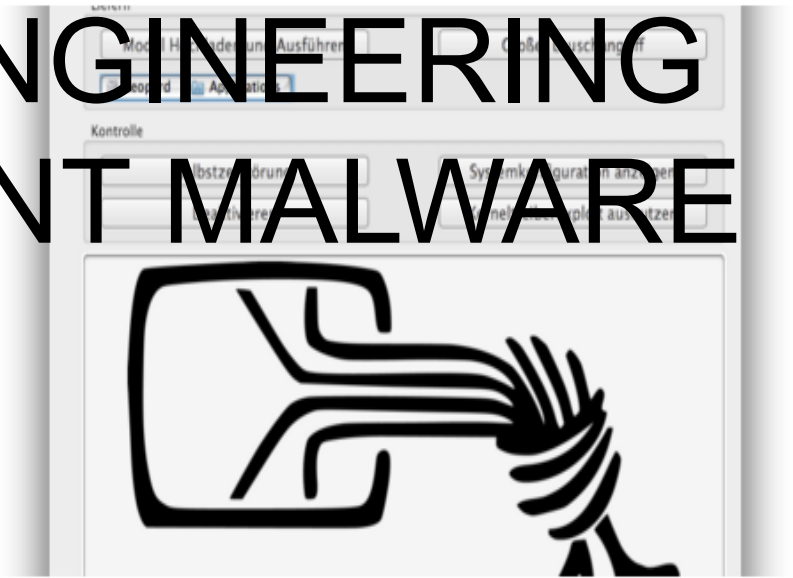
Tags

update
pressemitteilung
staatstrojaner

Featured

CHAOSRADIO

REVERSE ENGINEERING GOVERNMENT MALWARE



2014-02-27

2014-02-27
Chaosradio

2014-03-05
C-RaDaR
Darmstadt

3 Cases of Government Hacking

1. Law Enforcement Investigation

2. Botnet prosecution and mitigation

3. Ubiquitous Intelligence Gathering

Your computer is infected! - Mozilla Firefox

Bestand Bewerken Beeld Geschiedenis Bladwijzers Extra Help

http://teamhightechcrime.nationale-recherche.nl/nl_infected.php

Google

Meest bezocht Aan de slag Laatste nieuws

Your computer is infected!

Mozilla Firefox is gratis en opensourcesoftware van de Mozilla Foundation.

Ken uw rechten...

BREDOLAB

Your computer is infected!

If this Browser has opened automatically then your computer has been infected with malware. Your computer has become part of a bot network.

This message has been sent to you by the High Tech Crime Team of the Dutch National Crime Squad and aims to notify all owners of infected computers.

Dutch National Crime Squad takes down infamous botnet
On October 25th 2010, the High Tech Crime Team of the Dutch National Crime Squad took down a very large botnet, containing at least 30 million infected computer systems worldwide since July 2009. These computers were infected with the malicious Bredolab trojan, through infected websites. Through these botnets, cybercriminals can spread large amounts of other viruses and create new botnets.
In close cooperation with a Dutch hosting provider, The Dutch Forensic Institute (NFI), the internet security company Fox-IT and GOVCERT, the computer emergency response team of the Dutch government, shut down 143 computer servers today.

More information:

For more information about removing Bredolab from your computer, visit:
https://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/Ontmanteling+Bredolab.html.

FOX-IT EXPERTS IN IT SECURITY GOVCERT.NL OPENBAAR MINISTERIE LANDELIJK PARKET POLITIE Korps landelijke politiediensten Netherlands Police Agency

Klaar

BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN

VACATURES WORD DONATEUR en / nl

HOME • DOE MEE • ONS WERK • OVER ONS • CONTACT • PERS BLOG ZOEK

FOIA SOURCE CODE

```
program OpenTHTCPage;
uses
  Window,
  ShellApi;
begin
   try
   ShellExecute(0, 'open',
'http://teamhightechcrime.nationale-
     recherche.nl/nl_infected.php', nil,
nil, SW_SHOWNORMAL);
   except
     // ignore
   end
end
```

not encrypted, not signed!!

- Insert vulnerabilities, fx. phishing / new botnet

3 Cases of Government Hacking

1. Law Enforcement Investigation

2. Botnet prosecution and mitigation

3. Ubiquitous Intelligence Gathering

NEWS

How the NSA Plans to Infect 'Millions' of Computers with Malware

By Ryan Gallagher and Glenn Greenwald 12 Mar 2014, 9:19 AM EDT 122

One presentation outlines how the NSA performs "industrial-scale exploitation" of computer networks across the world.

ABOUT THE AUTHORS


Ryan Gallagher
Reporter: Read more


Glenn Greenwald
Editor: Read more

(U) There is More Than One Way to QUANTUM

TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live Tested	**N/A**
CND				
QUANTUMSMACKDOWN	Pevents target from downloading implants to DoD computers while capturing malicious payload for analysis.	Oct 2010	Live Tested	**N/A**

TS//SI//REL

OUTLINE

Hacking Cases by ‘Western’ Governments

11+ Problems with Government Hacking

A Constitutional Right to IT-Security?

Elements of a Research Agenda: Discussion!

1

no reliable data

2

no clear separation
wiretap/search

3

with lies, and no laws
oversight is hard

4

insecure malware
infosecurity disaster

5

hacking creates bad security incentives

6

scope undebated:
user / device / router /
isp / botnet / world

7

jurisdiction: within / across borders?

8

geopolitical tension:
cybercrime convention

9

constitution: protection across borders?

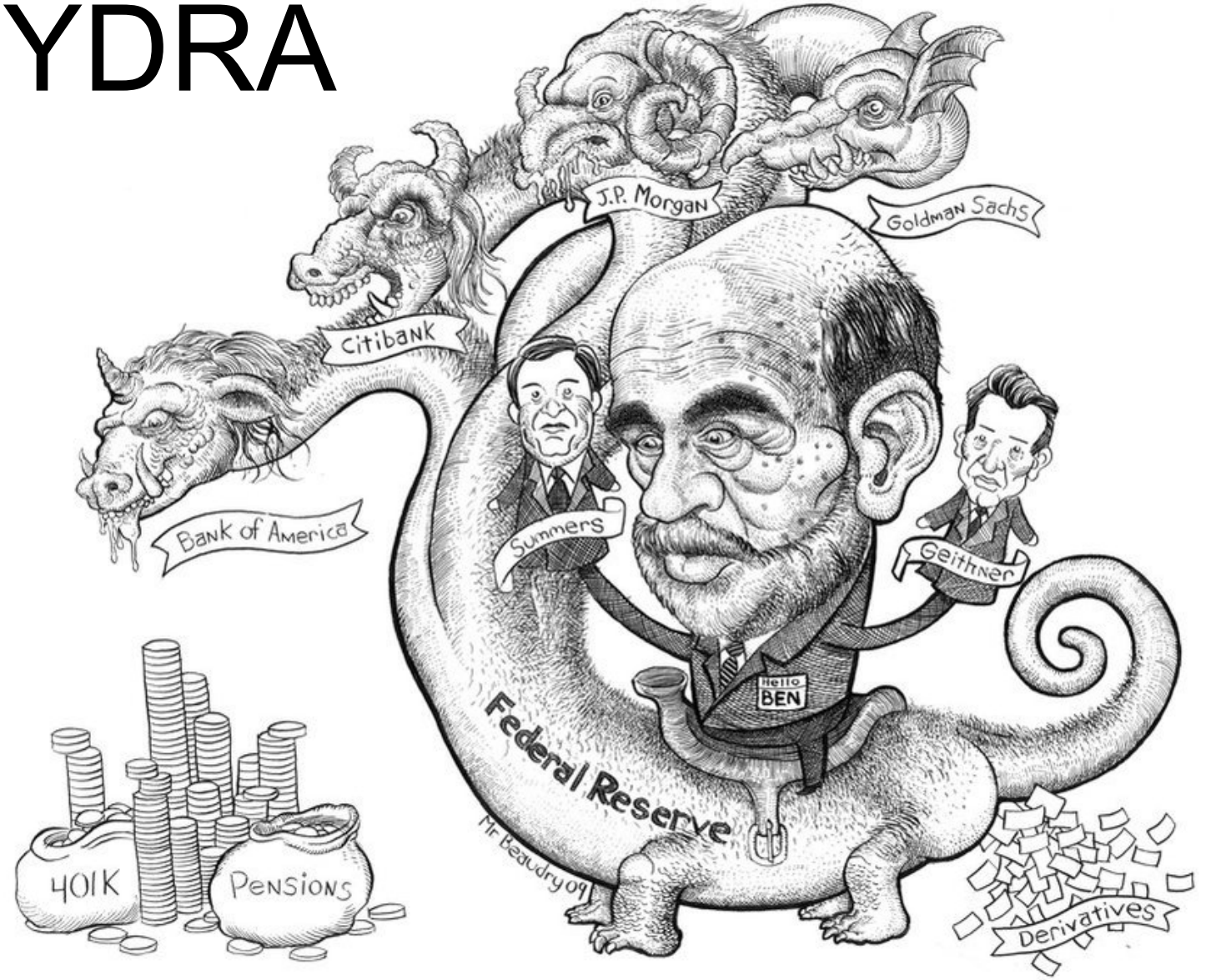
10

parallel construction:
NSA hack – FBI arrest

11

hacking necessary?
utopia: undercover job

GOVERNMENT HACKING HYDRA



For every apparent benefit, a problematic policy issue emerges

OUTLINE

Hacking Cases by ‘Western’ Governments

11+ Problems with Government Hacking

A Constitutional Right to IT-Security?

Elements of a Research Agenda: Discussion!

BUNDESTROJANER


CONSTITUTIONAL COURT
GERMANY

According to BVerfG, NJW 2008, 822 (849).

- IT-systems particularly sensitive
  - Separates systems, communication, data
  - Systems deserve particular protection
    - We structure our life
    - All-stop-shop for government access
  - Network, 'cloud‘ exacerbates privacy intrusion
    - 3rd parties & data centralised

- Hacking IT violates core of privacy, personality
  - Beyond 'Communication', Beyond the Home

Human Right:
Confidentiality & Integrity IT-Systems

- Broad scope: general storage device
  - Internet of Things, ‘Cloud’, RAM
  - Not on public device, but also on public wifi
  - Regardless of technical expertise user
- Integrity: manipulation of data also covered

- Not absolute, but strictest legal criteria
  - Stricter than house search
    - But: ‘Foundations of the State’
    - And: ‘Prevention’ with ‘High Probability’
  - Core of private life cannot be restricted
    - If such data found, immediate deletion!

EUROPEAN COURT OF HUMAN RIGHTS

Conclusion

The court finds that the Government's warrant request is not supported by the application presented. This is not to say that such a potent investigative technique could never be authorized under Rule 41. And there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology. But the extremely intrusive nature of such a search requires careful adherence to the strictures of Rule 41 as currently written, not to mention the binding Fourth Amendment precedent for video surveillance in this circuit. For these reasons, the requested search and seizure warrant is denied.

Signed at Houston, Texas on April 22, 2013.

Stephen Wm Smith
United States Magistrate Judge

OUTLINE

Hacking Cases by ‘Western’ Governments

11+ Problems with Government Hacking

A Constitutional Right to IT-Security?

Elements of a Research Agenda: Discussion!

RESEARCH

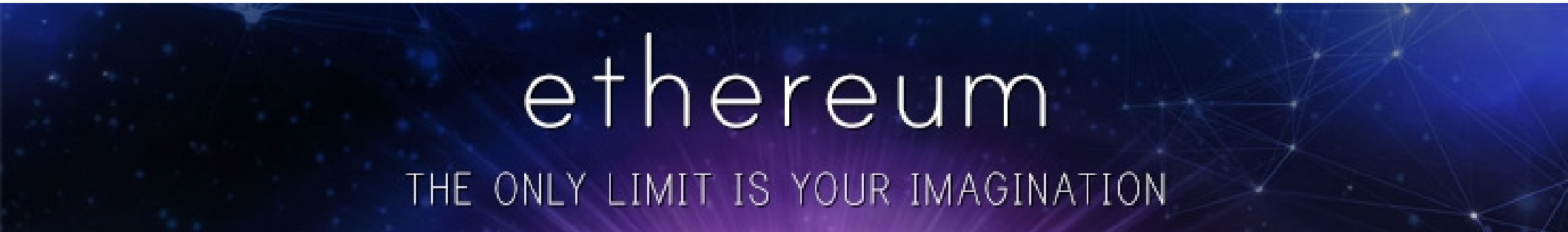
ROOT CAUSES OF CYBERCRIME? GAME THEORY: LARGE SCALE VULNS

Where Do All The Attacks Go?

Dinei Florêncio and Cormac Herley
Microsoft Research
One Microsoft Way
Redmond, WA, USA

"Many attacks cannot be made profitable, even when many profitable targets exist."

HUMAN RIGHT IT-SECURITY: AGAINST COMPANIES?



POSITIVE HUMAN RIGHT TO IT-SECURITY?

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF I v. FINLAND

(Application no. 20511/03)

JUDGMENT

(U) There is More Than One Way to QUANTUM

TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live Tested	**N/A**
CND				
QUANTUMSMACKDOWN	Pevents target from downloading implants to DoD computers while capturing malicious payload for analysis.	Oct 2010	Live Tested	**N/A**

TS//SI//REL

ARTIFICIAL INTELLIGENCE ETHICS

“consider the Trojan itself as a digital police officer, subject to the same restrictions but also powers that its physical counterparts posses.”

Source: http://www2.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.pdf

POLICY

"We Must Do Something.
Hacking Is Something.
Therefore, We Must Do It"

DEMAND RELIABLE DATA FOR INFORMED POLICYMAKING

Measuring the Cost of Cybercrime

Ross Anderson [1] Chris Barton [2] Rainer Böhme [3] Richard Clayton [4]
Michel J.G. van Eeten [5] Michael Levi [6] Tyler Moore [7] Stefan Savage [8]

"As a striking example, the botnet behind a third of the spam sent in 2010 earned its owners around US$2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars. We are extremely inefficient at fighting cybercrime"

http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf


his website has been seized
ggvow6fj3sehlm45.onion
Startpa
ALTERNATIVES TO HACKING?
POLITIE
This hidden service has been seized.
by the Dutch National Police
Just Weeks Ago: UTOPIA (undercover job)

TECHNOLOGY-SPECIFIC SURVEILLANCE LAWS

SURVEILLANCE LAW
NOT TECHNOLOGY-NEUTRAL

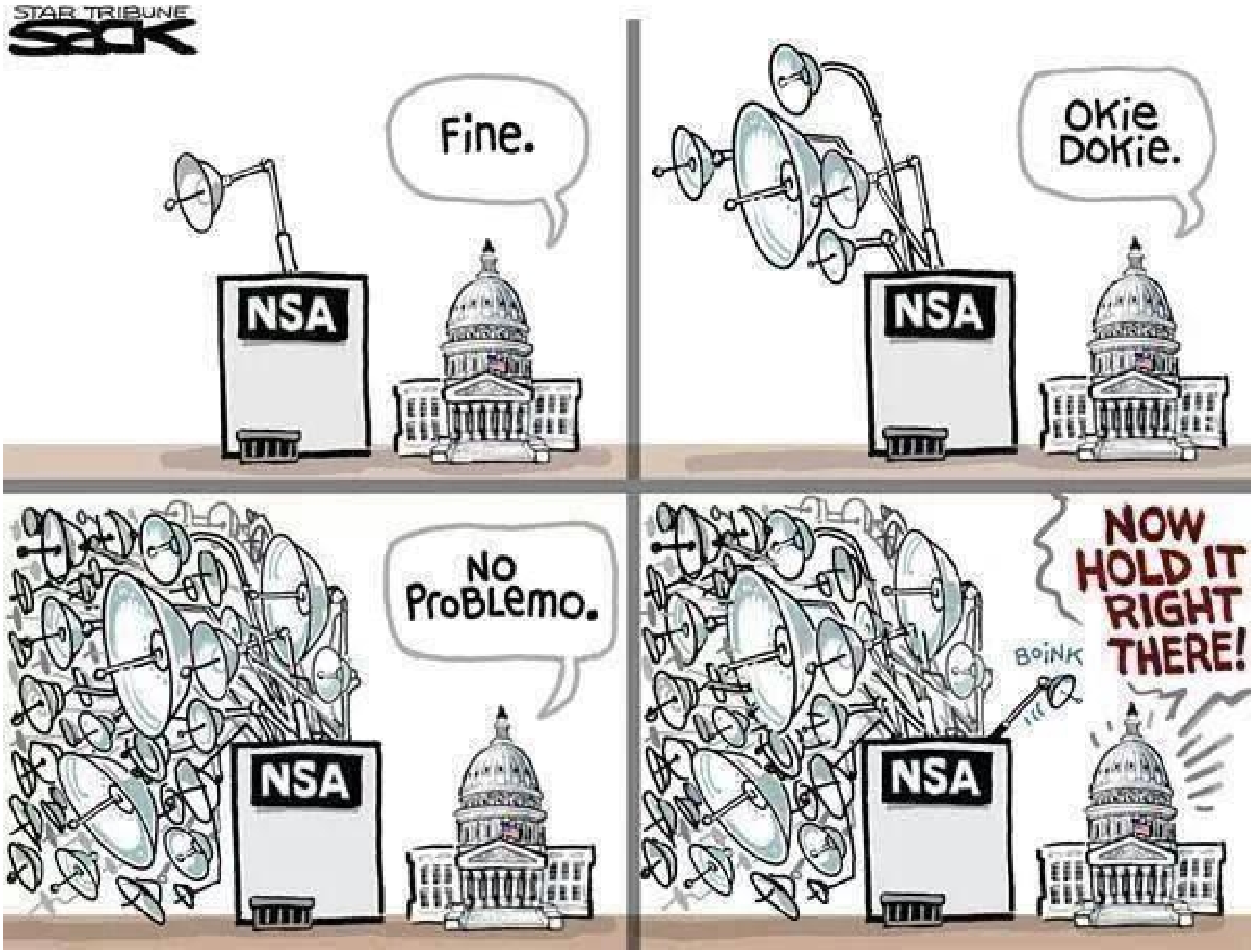
(U) There is More Than One Way to QUANTUM

TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live Tested	**N/A**
CND				
QUANTUMSMACKDOWN	Pevents target from downloading implants to DoD computers while capturing malicious payload for analysis.	Oct 2010	Live Tested	**N/A**

TS//SI//REL

REAL OVERSIGHT NEEDED



NATURE | NEWS

The best time to wage cyberwar

Maths model calculates whether it is worth waiting to hit enemies at their most vulnerable.

GAME THEORY: ESCALLATION

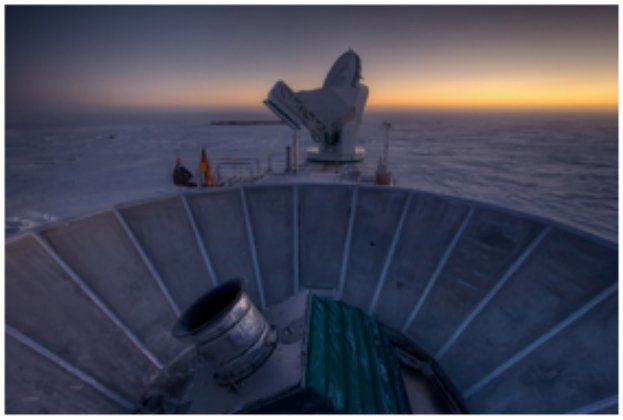
Regina Nuzzo

13 January 2014

If you discover a way to hack into your enemy's computers, do you strike while the iron is hot, or patiently wait for a better opportunity to arise? Wait too long, and a vigilant enemy might spot its vulnerabilities and fix them. Strike too soon, however, and you will have blown your chance to wreak havoc when you might really need it.

A new mathematical model, built on analyses of double-agent spies and code-breaking during the Second World War[1], provides a way to calculate the ideal timing of a surprise cyberattack. The

Top Story



The gravitational-wave revolution

Results from a South Pole observatory unleash a new kind of astronomy that can peer all the way back to the Big Bang.

E-alert RSS Facebook Twitter

Recent Read Commented Emailed

1. First hints of waves on Titan's seas
   Nature | 17 March 2014
2. Pests worm their way into genetically modified maize
   Nature | 17 March 2014
3. How astronomers saw gravitational waves from the Big Bang


AUGUST 25, 200
CNN
EXCLUSIVE
LANCE ARMSTRONG SPEAKS OUT
CNN
CANCER SURVIVOR, 7-TIME TOUR DE FRANCE
CYCLING CHAMP DENIES DRUG ALLEGATIONS
Live

HACKING TEAM RCS

Suspected Government Users Worldwide

Citizen Lab 2014

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire & John Scott-Railton

21 SUSPECTED GOVERNMENT USERS

AMERICAS	EUROPE	MIDDLE EAST	AFRICA	ASIA
Mexico	Hungary	**Oman**	**Egypt**	**Azerbaijan**
Colombia	Italy	**Saudi Arabia**	**Ethiopia**	**Kazakhstan**
Panama	Poland	**UAE**	**Morocco**	Malaysia
	Turkey		**Nigeria**	Thailand
			Sudan	South Korea
				Uzbekistan

CAUSE FOR CONCERN

52% (**in bold**) fall in the bottom 3rd of a World Bank ranking* of freedom of expression and accountability

29% are in the bottom 3rd for Rule of Law

*World Bank 2012 WGI

CHALLENGES DISARMAMENT (ALONG WITH ATTRIBUTION PROBLEM)

BUT NEEDED, ALONG WITH DUAL USE TRADE RESTRICTIONS

ACTIVISM

PRIVACY INTERNATIONAL

MUNK SCHOOL OF GLOBAL AFFAIRS
UNIVERSITY OF TORONTO
THE CITIZEN LAB

REVERSE-ENGINEERING TRACEROUTES PORT SCANS CONFERENCES WHAT'S GOING ON?

AMERICAN CIVIL LIBERTIES UNION

FACT-FINDING:
FOIA MALWARE
UNSEAL CASES
ROLE INDUSTRY
FIND WHISTLE-
BLOWERS

OPPOSE LAWS
11+ PROBLEMS
ALTERNATIVES

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

HOME • DOE MEE • ONS WERK • OVER ONS • CONTACT • PERS BLOG

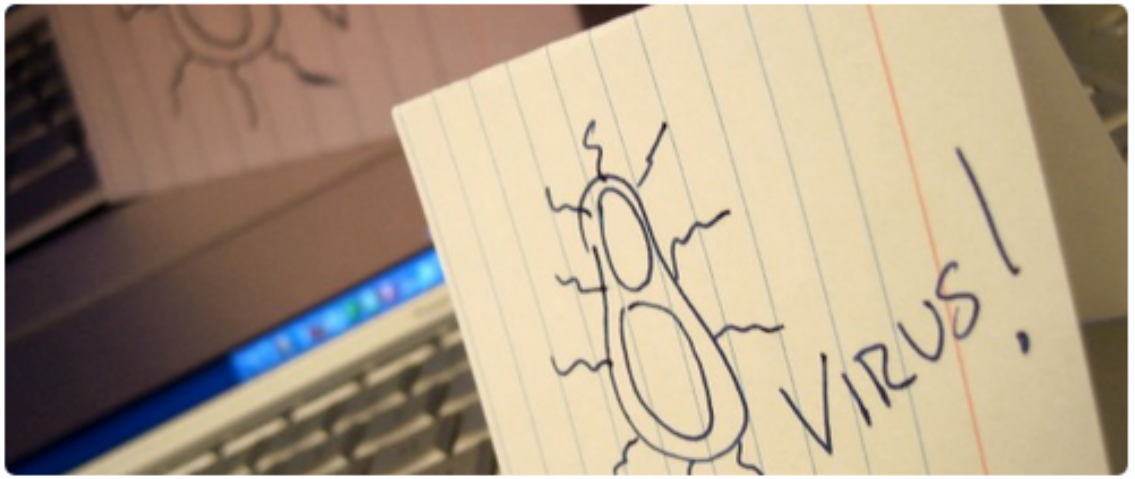


Image based on Computer Virus by talksrealfast (licentie: CC BY-NC-SA 2.0)

25 oktober 2013 21:40
Door Ton Siedsma

English

EXPERTS CALL UPON THE VENDORS OF ANTIVIRUS SOFTWARE FOR TRANSPARENCY

An international coalition of more than 25 civil rights organizations and security experts is concerned about the level of security provided by antivirus software companies. "The users of this software should be ably to rely on the security of their systems. We fear this might be a false feeling of security." says Ton Siedsma of the Dutch digital rights organization Bits of Freedom.

According to the coalition, these companies have a vital position in providing security and maintaining the trust of internet users engaging in sensitive activities such as electronic banking. There should be no doubt that your antivirus software provides the security needed to maintain this trust.

In the letter the coalition asks the antivirus companies for transparency on whether there have been any requests by governments to not detect the

WARNING FOR DANGEROUS DYNAMIC HUMAN RIGHT TO LEGITIMIZE HACKING POST-SNOWDEN: “LAWFUL / AUTHORIZED”

DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Saturday, June 08, 2013

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

June 8, 2013

DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

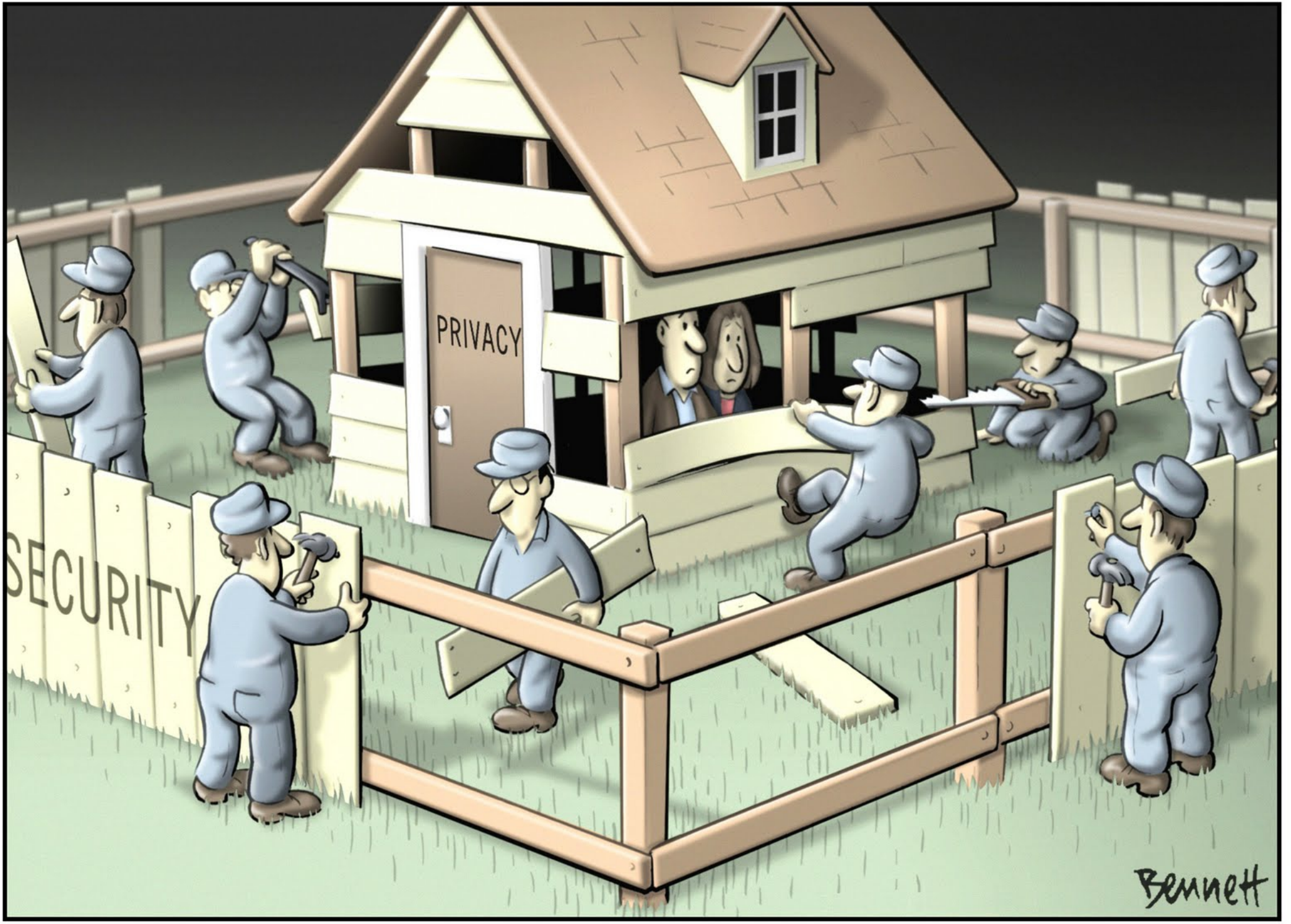
Over the last week we have seen reckless disclosures of intelligence community measures used to keep Americans safe. In a rush to publish, media outlets have not given the full context–including the extent to which these programs are overseen by all three branches of government–to these effective tools.

In particular, the surveillance activities published in The Guardian and The Washington Post are lawful and conducted under authorities widely known and discussed, and fully debated and authorized by Congress. Their purpose is to obtain foreign intelligence information, including information necessary to thwart terrorist and cyber attacks against the United States and its allies.

DEVELOP RICH VOCABULARY:
“BUNDESTROJANER” / “SABOTAGE”

DON’T ASSUME ‘TARGETTED SURVEILLANCE’ IS MORE OKAY:
“ALL VPN CONNECTIONS ORIGINATING IN A COUNTRY”

NEVER USE ‘CYBERSECURITY’:
IT’S A MILITARY CONCEPT


PRIVACY
SECURITY
Bennett

Governments Pwn the Web: A Constitutional Right to IT-Security?

Co-Creating An Agenda for Research, Policy and Activism

Berkman Luncheon Series 18.03.14
https://www.axelarnbak.nl
2013/14 Fellow Berkman Center & CITP