Alberto Cammozzo

Frontiers of digital citizenship
Technologies, Security and **Democracy**

University of Padova

Corso di laurea magistrale in Studi Europei
Second cycle degree in European Studies

Diritti Fondamentali e Cittadinanza Europea
Fundamental Rights And European Citizenship
2014/2015

Jun 4, 2015

1/ Technologies, Security and **Privacy:**
big data and web profiling
government surveillance
(activities in the public sphere citizens can directly affect)

2/ Technologies, Security and **Democracy:**
Censorship, Espionage
and Cyberwarfare
(activities we are less aware of/ involved in)

«You have **zero privacy** anyway.
Get over it. »

Scott McNealy,
Sun Microsystems, 1999

Should we?

What is /Privacy/ ?

PRIVACY AS CONTEXTUAL INTEGRITY

Helen Nissenbaum*

Abstract: The practices of public surveillance, which include the monitoring of individuals in public through a variety of media (e.g., video, data, online), are among the least understood and controversial challenges to privacy in an age of information technologies. The fragmentary nature of privacy policy in the United States reflects not only the oppositional pulls of diverse vested interests, but also the ambivalence of unsettled intuitions on mundane phenomena such as shopper cards, closed-circuit television, and biometrics. This Article, which extends earlier work on the problem of privacy in public, explains why some of the prominent theoretical approaches to privacy, which were developed over time to meet traditional privacy challenges, yield unsatisfactory conclusions in the case of public surveillance. It posits a new construct, "contextual integrity," as an alternative benchmark for privacy, to capture the nature of challenges posed by information technologies. Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it. Building on the idea of "spheres of justice," developed by political philosopher Michael Walzer, this Article argues that public surveillance violates a right to privacy because it violates contextual integrity; as

3 “Traditional” principles governing privacy in the US

Are they adeguate to “public surveillance”?

Principle 1: Protecting Privacy of Individuals Against Intrusive Government Agents

→ limiting government powers in the name of individual **autonomy** and **liberty**

“the net effect of computerization is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems.”

SEC’Y’S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP’T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973)

(Nissenbaum 2004)

Principle 2: Restricting Access to Intimate, Sensitive, or Confidential Information

people are entitled to their **secrets**

Protecting “the private life, habits, acts, and relations of an individual.”

Samuel D. Warren & Louis D. Brandeis,
The Right to Privacy , 4 H ARV . L. R EV . 193 (1890)

(Nissenbaum 2004)

Principle 3: Curtailing Intrusions into Spaces or Spheres Deemed Private or Personal

sanctity of certain spaces or places

"The common **law** has always recognized a **man's house as his castle**, impregnable, often, even to its own officers engaged in the execution of its commands."

Samuel D. Warren & Louis D. Brandeis,
The Right to Privacy , 4 H ARV . L. R EV . 193 (1890)

(Nissenbaum 2004)

“Unlike those cases, however, **public surveillance** does not involve government agents seeking to expand access to citizens; or collection or disclosure of sensitive, confidential, or personal information; or intrusion into spaces or spheres normally judged to be private or personal.”

(Nissenbaum 2004)

The outcome:

“the courts have ruled that there is no expectation of privacy in a **public setting**”

(in Nissenbaum 2004)

But:

«Observing the texture of people's lives, we find them not only crossing dichotomies, but moving about, into, and out of a plurality of distinct realms [contexts]. They are at **home** with families, they go to **work**, they seek **medical** care, visit **friends**, consult with **psychiatrists**, talk with **lawyers**, go to the **bank**, attend **religious** services, **vote**, **shop**, and more. »

(Nissenbaum 2004)

«I posit two types of **informational norms**: norms of **appropriateness**, and norms of **flow** or distribution. **Contextual integrity** is maintained when both types of norms are upheld, and it is violated when either of the norms is violated. »

(Nissenbaum 2004)

1. «norms of **appropriateness** dictate what information about persons is appropriate, or fitting, to reveal in a particular context »

Appropriate | not appropriate
behaviour for a given context

(Nissenbaum 2004)

2. «What matters is not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or flow, respects contextual **norms of information flow**.»

Free choice, discretion, confidentiality

(Nissenbaum 2004)

PRIVACY is a set of social norms that regulate,

in a given **context**,

{

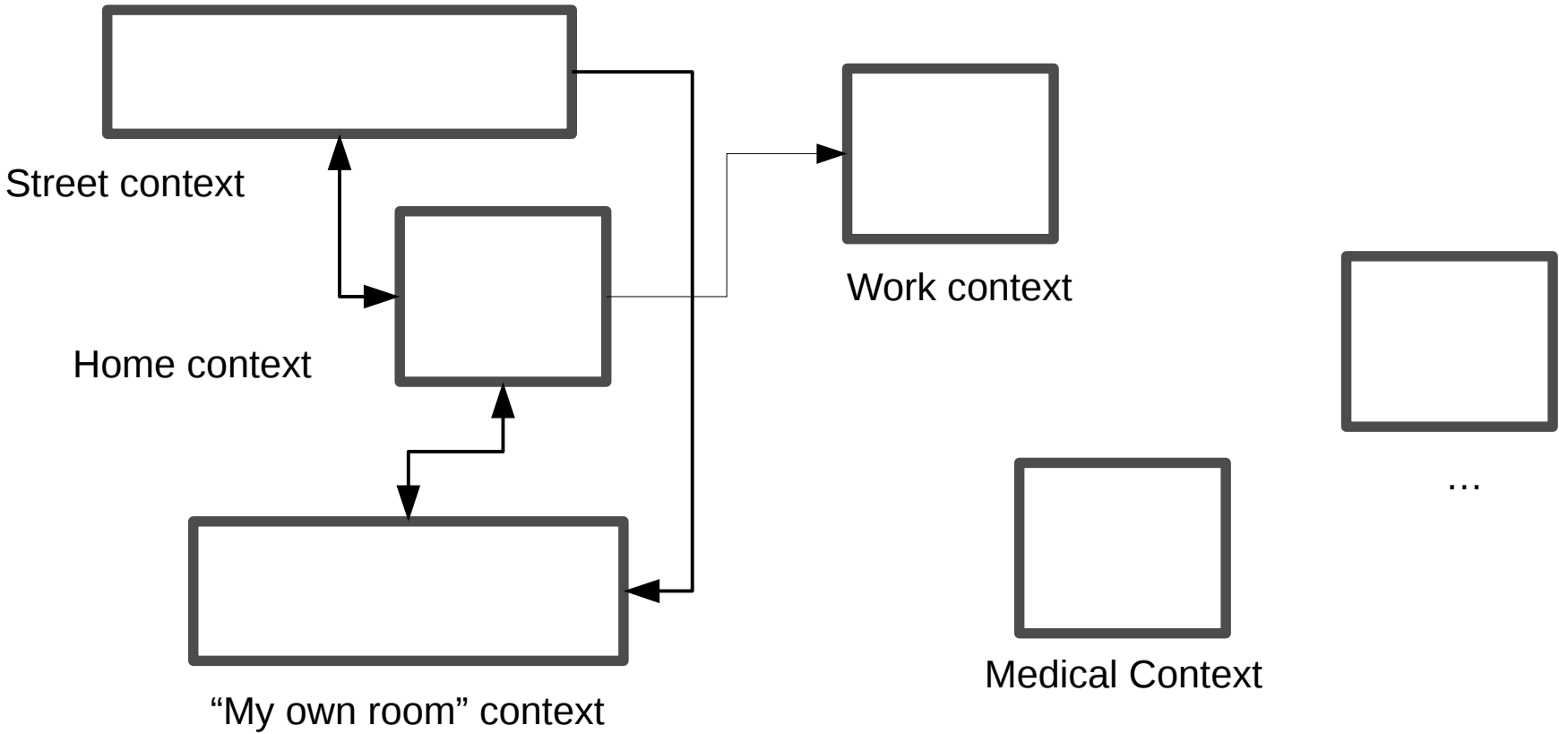
1. which information **it is appropriate to disclose**

2. the flow of information between different parties

(from Nissenbaum 2004)

“Traditional” privacy

“Contextual” privacy



When [...] the availability of public records online, is viewed through the lens of contextual integrity, certain aspects of the **change in placement** from locally kept records (whether hardcopy or electronic) to Web-accessible records, are highlighted in novel ways. The change in placement, [...] is significant because it constitutes a breach of entrenched norms of flow. As such, it demands scrutiny in terms of **values**.

(Nissenbaum 2004)

Example:

university or high school exam results

To avoid “under the counter” agreements or partiality

1st principle: *Transparency*

“Exams should be public
Results should be public”

The exam should not be webcasted, nor exam results be available forever in web search engines

2nd principle: *Privacy*

“Results should be public *for those attending to class or course, and held in public records*” (the appropriate context)

In this case, *privacy* norms
restrict the **scope**
of the *transparency* principle
and help to confine the circulation of information
in the appropriate context

The proportionality principle

Action should be:

/1/ **legitimate**
/2/ **suitabile** and appropriate for the goal
/3/ **necessary:** implying minimal sacrifice for competing interests
/4/ **reasonable**, proprtionate, quantitatively adequate in satisfying protected interests (sufficient but not excessive)

See: SVILUPPI RECENTI DEL PRINCIPIO DI PROPORZIONALITA' NEL DIRITTO AMMINISTRATIVO ITALIANO
Umberto Fantigrossi, Liuc Papers n. 220, 2008 on "Teoria dei tre gradini": idoneità, necessarietà e adeguatezza

P.P.: articulable relationship between means and ends, specifically that the means chosen [...] be **suitable or appropriate**, and **no more restrictive than necessary** to achieve a lawful end.

the scrutiny as to whether the invasion of the fundamental right is as non-invasive as possible

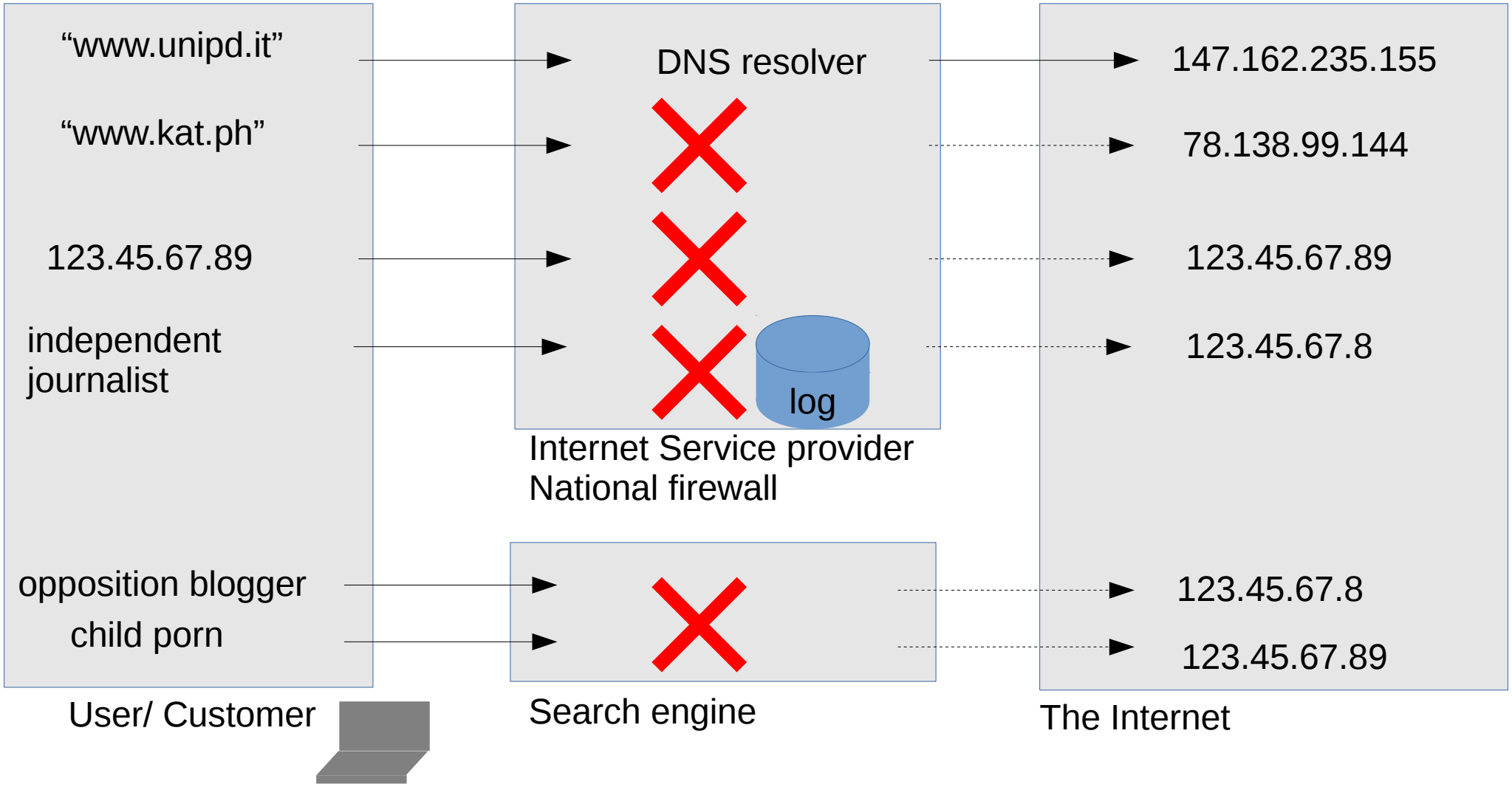
Least restrictive means analysis (US)

Engle, Eric, The History of the General Principle of Proportionality: An Overview (July 7, 2009). 10 Dartmouth Law Journal 1-11 (2012).. Available at SSRN: http://ssrn.com/abstract=1431179

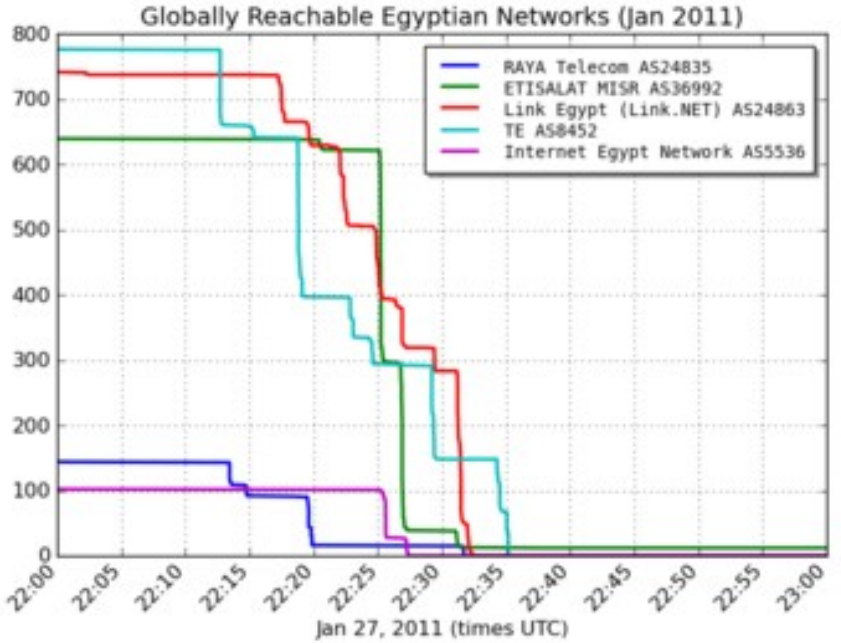
1/ Technologies, Security and **Privacy:**
big data and web profiling
government surveillance
(activities in the public sphere citizens can directly affect)

2/ Technologies, Security and **Democracy:**
Censorship, Espionage
and Cyberwarfare
(activities we are less aware of/ involved in)

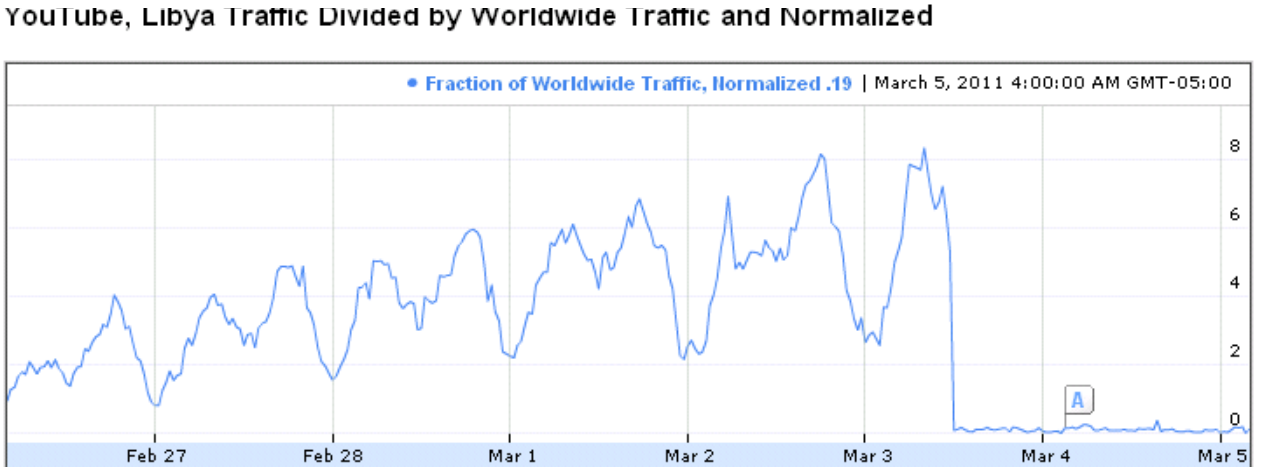
Censorship


“www.unipd.it”
“www.kat.ph”
123.45.67.89
independent journalist
opposition blogger
child porn
User/ Customer
DNS resolver
log
Internet Service provider
National firewall
Search engine
147.162.235.155
78.138.99.144
123.45.67.89
123.45.67.8
123.45.67.8
123.45.67.89
The Internet

Jan 2011 – Egypt:
BGP routes
withdrawal



March 2011 – Libya
“warm standby mode”:
Unique State ISP
First chokes traffic
Then withdraws
BGP routes



GREATFIRE.ORG

SEARCH | TEST URL | TEST KEYWORD | FAQ | NEWS | 中文

tank man | All | Search

CENSORSHIP OF TANK MAN IN CHINA

Title	Tested Since	Censored*	Tags
keyword: tank man	May 2012	67%	Keywords
keyword: tiananmen tank man	Jul 2013	33%	Keywords
www.google.com/search?q=tiananmen tank man	Jul 2013	100%	Blocked, Google Searches, URLs
s.weibo.com/weibo/tiananmen tank man	Jul 2013	100%	URLs, Weibo Searches
www.baidu.com/s?wd=tank man	Apr 2012	100%	Baidu Searches, URLs
s.weibo.com/weibo/tank man	May 2012	0%	URLs, Weibo Searches
s.weibo.com/weibo/the tank man	Aug 2013	0%	URLs, Weibo Searches
www.baidu.com/s?wd=tiananmen tank man	Jul 2013	0%	Baidu Searches, URLs
s.weibo.com/weibo/the tank man?cron_key=HW_OMiF...	Feb 2015	0%	URLs, Weibo Searches
www.google.cn/search?q=tank man	Jul 2013	0%	URLs

* Blocked, censored, or restricted, in the last 90 days. Red = a URL that is blocked, or a keyword that is censored on one or more websites. Yellow = a URL that is throttled or self-censored. For more info, click an individual entry or check out or FAQ.

COMMENTS

Submitted by DrBen, ceo of D... on Fri, Mar 25, 2011

The websites www.drben.net and www.chinareport.com have been blocked from mainland China since 2002. I am the owner, so I know.

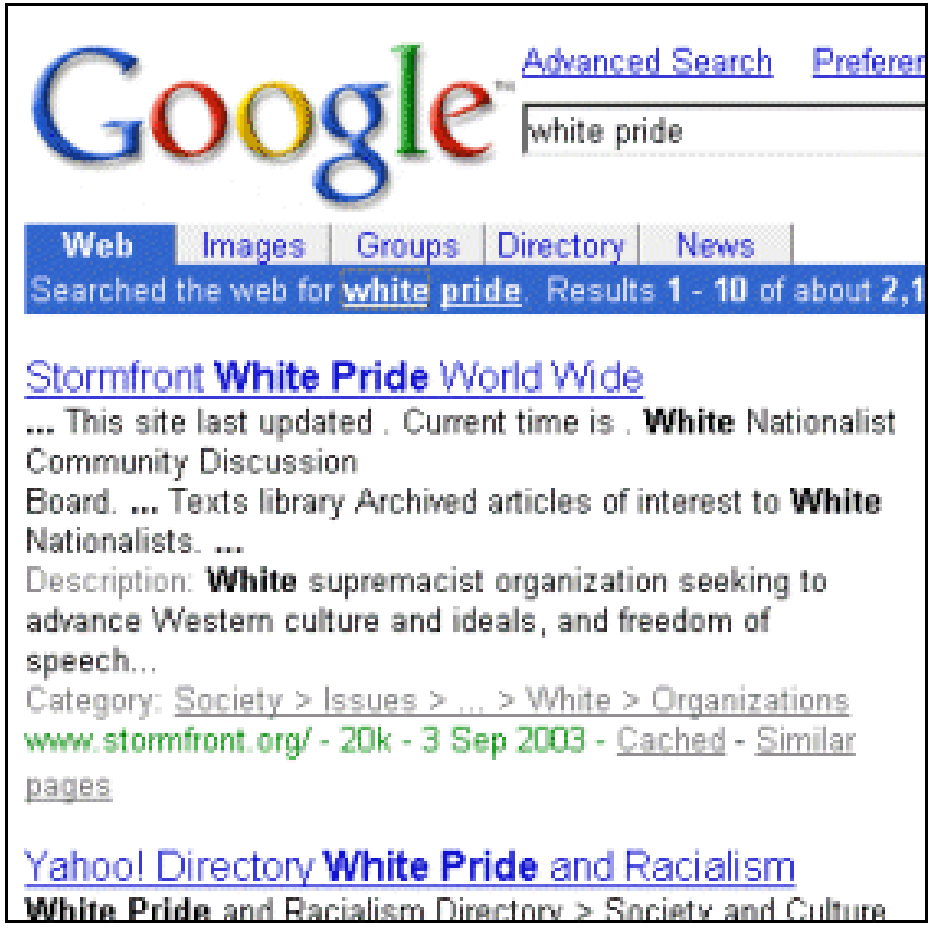
Submitted by chandru on Thu, Sep 22, 2011

HI,
Can You Please explain me your Site ..
What you do and etc..
chandru.rt@gmail.com

Submitted by sanjay kumar thakur on Mon, Mar 28, 2011

my gmail and orkut is not opening in firefox

US-Google



Censored Google Germany

http://blogoscoped.com/archive/2003_09_04_index.html

Zittrain, Jonathan; Edelman, Benjamin.
"Localized Google search result exclusions: Statement of issues and call for data." http://cyber.law.harvard.edu/filtering/google/results1.html
Harvard Law School: Berkman Center for Internet & Society. October 22, 2002.

2010
Wikileaks “Cablegate”

This webpage is not available

chromium

The server at **wikileaks.net** can't be found, because the DNS lookup failed. DNS is the web service that translates a website's name to its internet address. This error is most often caused by having no connection to the internet or a misconfigured network. It can also be caused by an unresponsive DNS server or a firewall preventing Chromium from accessing the network.

Here are some suggestions:

- Reload this web page later.
- Check your internet connection. Reboot any routers, modems, or other network devices you may be using.
- Check your DNS settings. Contact your network administrator if you're not sure what this means.
- Try disabling DNS prefetching by following these steps: Go to **Wrench menu > Preferences > Under the Hood** and deselect "Use DNS pre-fetching to improve page load performance."
- Try adding Chromium as a permitted program in your firewall or antivirus software's settings. If it is already a permitted program, try deleting it from the list of permitted programs and adding it again.

Wikileaks shutdown attempts – Dec, 2010

DynDNS and **Amazon** AWS end support to Wikileaks.org

PayPal restricts account used by WikiLeaks due to a "violation of the PayPal Acceptable Use Policy"

Mastercard and **Visa** withdraw ability to make donations to WikiLeaks

Apple removes an unofficial WikiLeaks app from the iTunes App Store

Postfinance, the Swiss postal system, shuts Assange's bank accounts

French minister Eric Besson warns Internet providers of "consequences" for those helping to keep WikiLeaks online

US access to Wikileaks banned in selected locations (eg **Library of congress**)

DDOS attacks ...

Espionage






Explain and Send Screenshots

Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.
18 USC 1 note.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

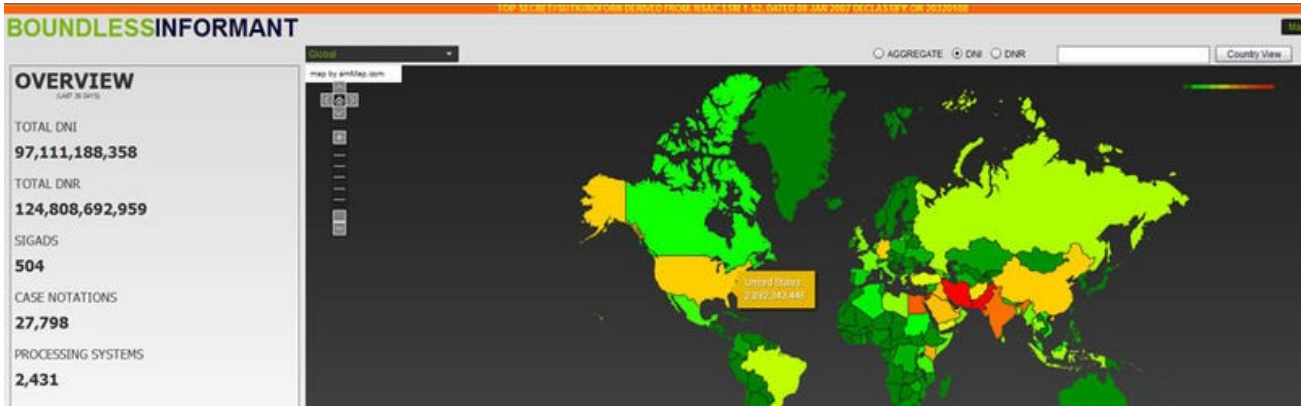
SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

undefined

Edward Snowden, June 2013



1. data collection

- International fiberoptic exchanges interception (voice & data)

  STORMBREW OAKSTAR BLARNEY FAIRVIEW TEMPORA SOCIALIST RAMPART-A

- Infiltrations and/or cooperation with ICT industry

  Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple

  PRISM, MUSCULAR Xkeyscore, SCISSORS, BOUNDLESS INFORMANT

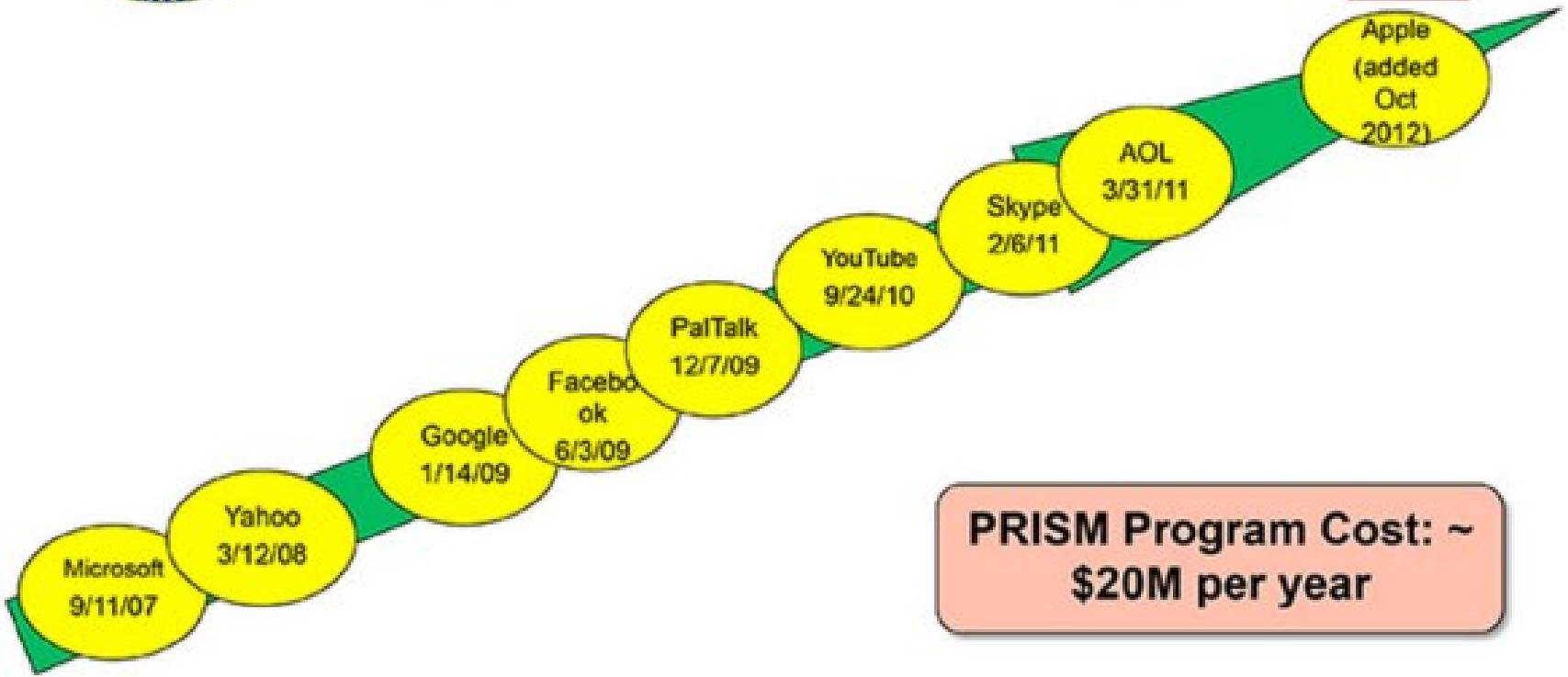
- US Phone conversations metatdata collection

  Verizon, AT&T e Sprint Nextel

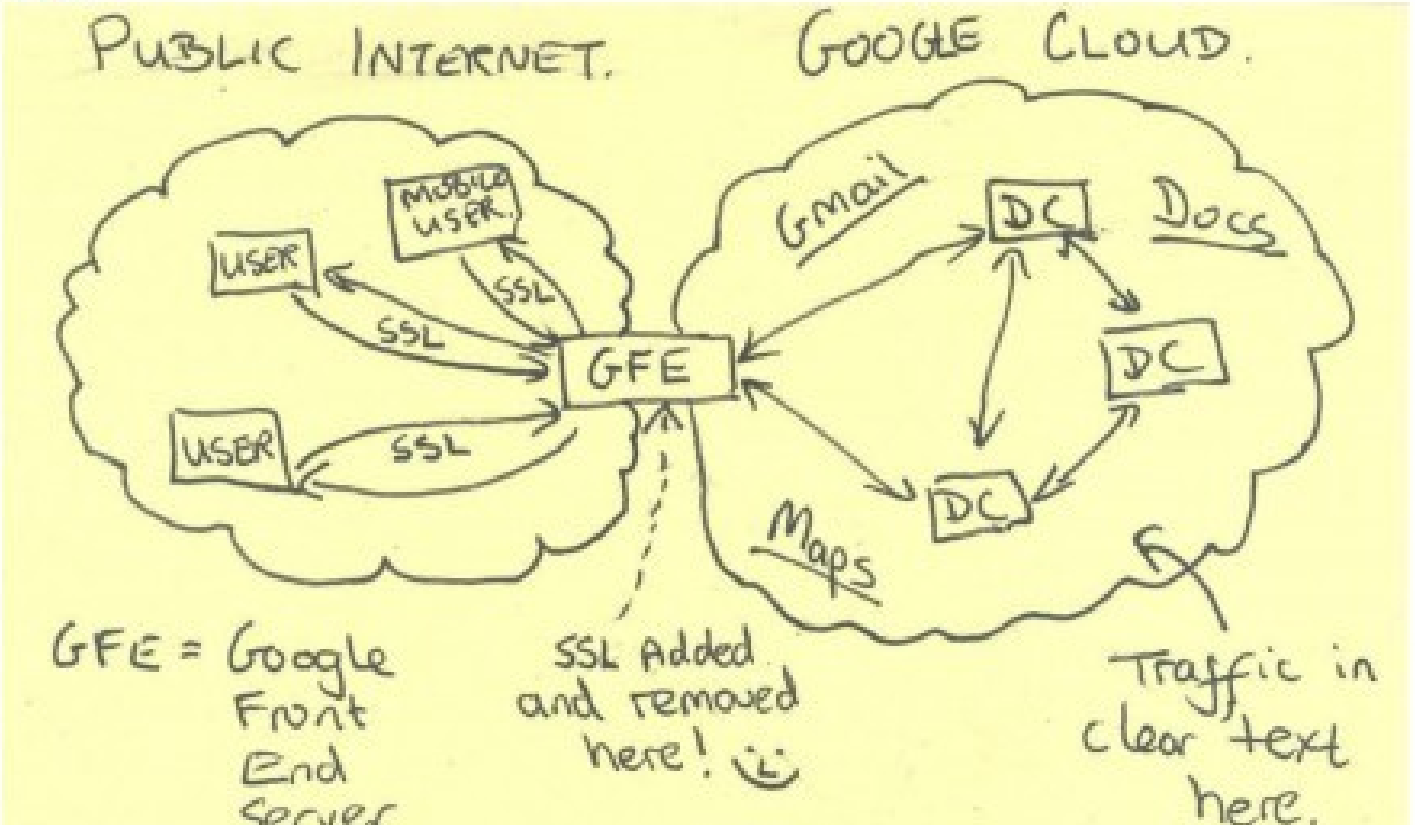
  MAINWAY, STELLARWIND

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

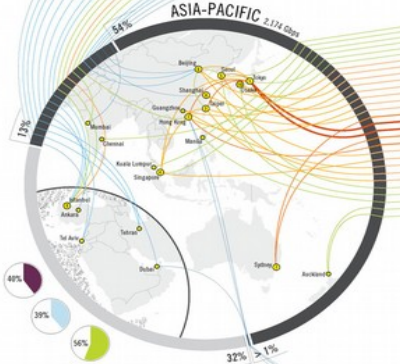


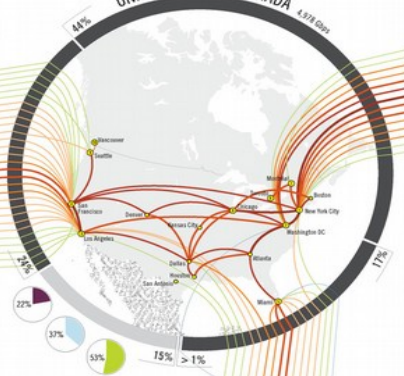
Current Efforts - Google

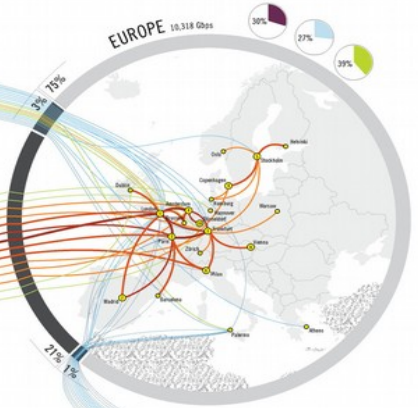


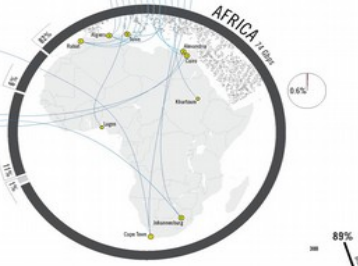
2009 GLOBAL INTERNET MAP

TeleGeography





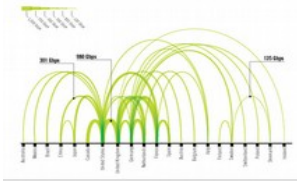




INTERNATIONAL INTERNET BANDWIDTH BY COUNTRY

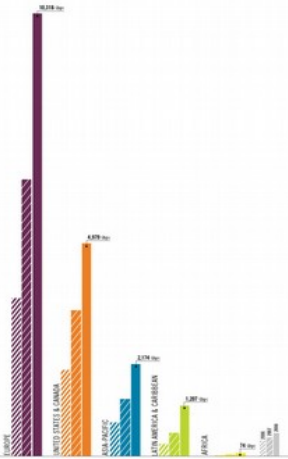
CARRIERS

In mid-2000, the Internet's international geography was the sum of 540 individual international IP carriers who owned, leased, or otherwise managed cross-border network capacity. TeleGeography has divided these carriers into three groupings—Global, Regional, and National—around which Internet backbone providers cluster. "Global" IP carriers sell wholesale Internet connectivity (IP transit) in at least two regions and in all four) two countries in each of three regions using their own backbone. "Regional" carriers specialize in selling backbone connectivity to customers within a single world region. Although these carriers concentrate on intraregional links, many operate at least a few links that cross regional borders. "National" IP carriers, the most common type of backbone carrier, include Internet backbone providers that primarily focus on a single country.



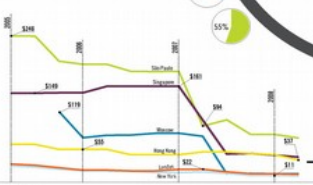
COUNTRY ROUTES

The highest-capacity country-to-country Internet routes link major European countries with each other and with the United States. In 2000, the big route was United Kingdom-United States, with a capacity of 900 Gbps.



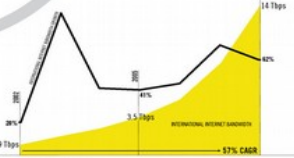
REGIONAL CAPACITY

How much does Internet backbone capacity vary from region to region? A lot. The international Internet capacity connected to Africa is but a fraction of the capacity connected to Europe and other regions. How bandwidth growth in Africa is going to ease in 2009 and 2010, however, as new submarine cables on both coasts of the continent will introduce considerable amounts of cheap, high-quality capacity.



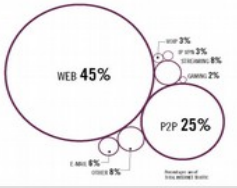
PRICING

Internet backbones are global, but Internet capacity prices are local, determined by competition, total available capacity, and the cost of regional transport capacity to a city. While the median monthly price per Mbps for a GigE Port differs greatly between cities in the U.S. and Western Europe and the more remote São Paulo and Singapore, price differences have narrowed.



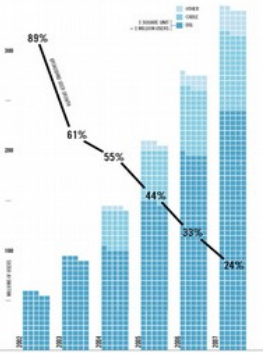
CAPACITY GROWTH

Between 2002 and 2008 the capacity of international Internet links increased at a compound annual growth rate of 57 percent. Although this pace may not seem particularly robust, the actual amount of new capacity that is added each year is staggering. In 2008 alone, over 5.8 Tbps of new international Internet capacity was added.



TRAFFIC BY APPLICATION

Internet capacity is used to carry a wide variety of applications and services, but video content has emerged as the primary driver of Internet traffic. The most commonly used applications by Internet video content are the Web (which includes HTTP-based video), peer-to-peer (P2P) applications, and streaming protocols.



BROADBAND USER GROWTH

The total amount of traffic generated by end-users has increased dramatically as consumers have switched from dial-up modems to higher-bandwidth technologies such as digital subscriber line (DSL), cable modem, and fiber to the home (FTTH). Broadband users tend to spend more time using the Internet and use bandwidth-intensive applications more frequently than non-broadband users. During 2007, the total number of broadband subscribers in the world rose 24 percent, to more than 260 million.

ABOUT THE MAIN PROJECTION

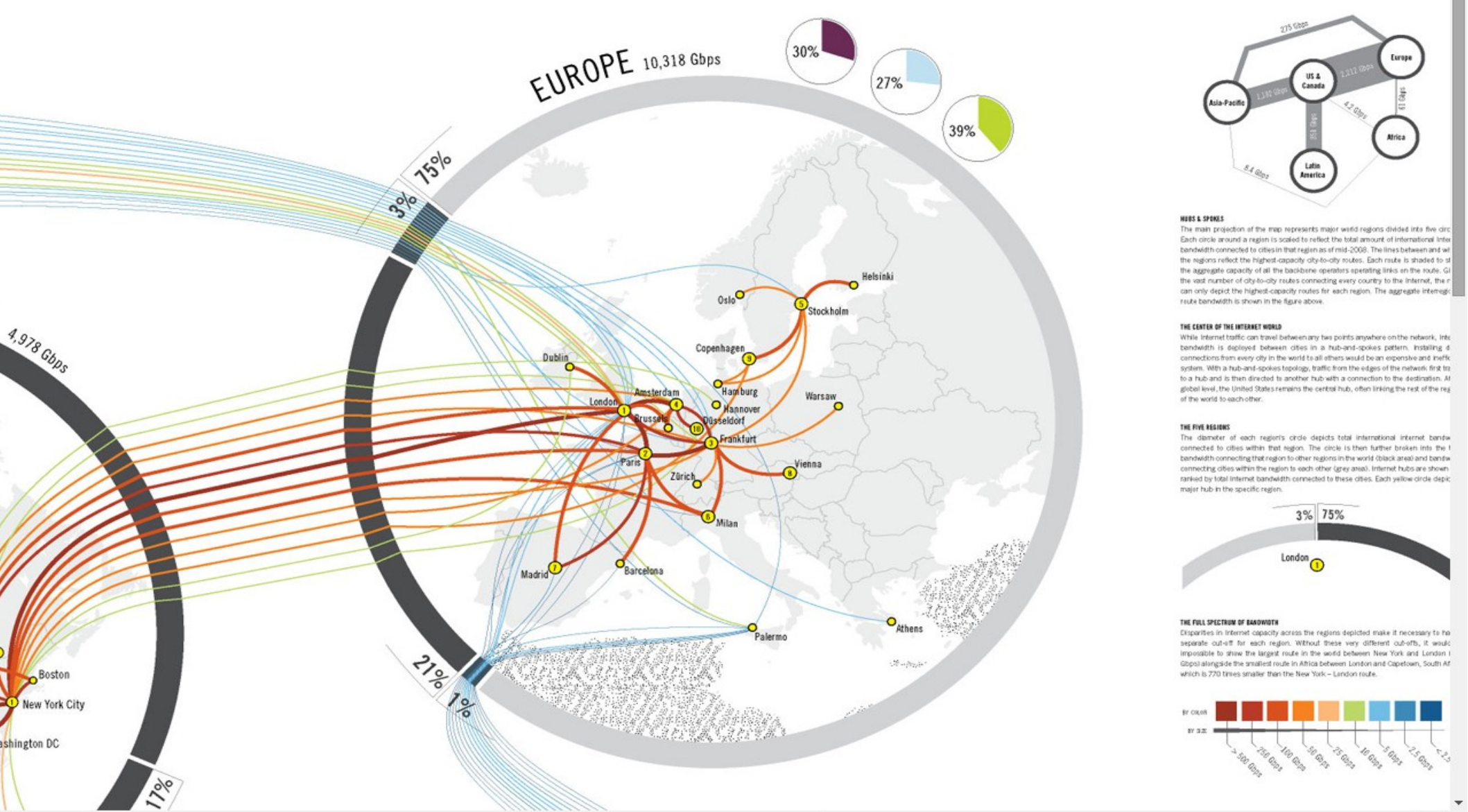
REGIONAL GRAPHICS

Region's Percent of World's Broadband Users
This graph represents the percentage of the total world's broadband subscribers residing within a region. The subscribers can be using any technology.

Average Utilization of Regional Bandwidth
This graph represents the average utilization of international Internet capacity connecting to or within the region. Average utilization is the sum of all traffic across a node in the month divided by the capacity of that node.

Peak Utilization of Regional Bandwidth
This graph represents the peak utilization of international Internet capacity connecting to or within the region. Peak utilization is measured at the 95th percentile. This statistic is calculated by dividing one month's traffic into 5 minute increments, ranking the traffic levels of each increment, and removing the top 5 percent, then dividing by the capacity of the node.

https://www.telegeography.com/


EUROPE 10,318 Gbps
30%
27%
39%
75%
3%
21%
1%
17%
4,978 Gbps
Helsinki
Oslo
Stockholm
Copenhagen
Dublin
Amsterdam
London
Hamburg
Hannover
Brussels
Düsseldorf
Frankfurt
Warsaw
Paris
Zürich
Vienna
Milan
Madrid
Barcelona
Palermo
Athens
Boston
New York City
ashington DC
275 Gbps
Europe
US & Canada
2,112 Gbps
1,102 Gbps
Asia-Pacific
4.2 Gbps
Africa
Latin America
5.4 Gbps
HUBS & SPOKES
The main projection of the map represents major world regions divided into five circ
Each circle around a region is scaled to reflect the total amount of international Inte
bandwidth connected to cities in that region as of mid-2008. The lines between and wi
the regions reflect the highest-capacity city-to-city routes. Each route is shaded to st
the aggregate capacity of all the backbone operators operating links on the route. Gi
the vast number of city-to-city routes connecting every country to the Internet, the r
can only depict the highest-capacity routes for each region. The aggregate interregi
route bandwidth is shown in the figure above.
THE CENTER OF THE INTERNET WORLD
While Internet traffic can travel between any two points anywhere on the network, Inte
bandwidth is deployed between cities in a hub-and-spokes pattern. Installing d
connections from every city in the world to all others would be an expensive and ineffic
system. With a hub-and-spokes topology, traffic from the edges of the network first tra
to a hub and is then directed to another hub with a connection to the destination. At
global level, the United States remains the central hub, often linking the rest of the reg
of the world to each other.
THE FIVE REGIONS
The diameter of each region's circle depicts total international Internet bandw
connected to cities within that region. The circle is then further broken into the t
bandwidth connecting that region to other regions in the world (black area) and bandw
connecting cities within the region to each other (grey area). Internet hubs are shown
ranked by total Internet bandwidth connected to these cities. Each yellow circle depic
major hub in the specific region.
3%
75%
London
1
THE FULL SPECTRUM OF BANDWIDTH
Disparities in Internet capacity across the regions depicted make it necessary to ha
separate cut-off for each region. Without these very different cut-offs, it would
impossible to show the largest route in the world between New York and London
Gbps) alongside the smallest route in Africa between London and Capetown, South Af
which is 770 times smaller than the New York – London route.
BY COLOR
BY SIZE
> 500 Gbps
250 Gbps
100 Gbps
50 Gbps
25 Gbps
10 Gbps
5 Gbps
2.5 Gbps
< 2.5

2. Targeted operations

- Interception:
  - Embassies (38), Government offices (Fr), media (Al Jazeera),
  - Foreign political leaders and head of State (Br, Mx, De),
  - International organizations (ONU, IAEA, UE? – tramite Belgacom)

    DROPMIRE, SOCIALIST
- Computer intrusion with viruses and malware

  GENIE, T.A.O.
- Attack to anonimyzing products such as Tor

  (EgotisticalGiraffe).

3. Targeting infrastructures

- Weakening standard encryption standards
  - "Differential Workfactor Cryptography" (Lotus Notes)
  - Dual_EC_DRBG standard: (RSA)

    BULLRUN, EDGEHILL, Sigint Enabling

  → Computer security uprooting
  - Also on proprietary products: Crypto AG, Windows

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

This Exhibit is SECRET//NOFORN									
	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

[1]Includes enacted OCO funding. Totals may not add due to rounding.

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

(TS//SI//REL TO USA, FVEY) This Project supports the Comprehensive National Cybersecurity Initiative (CNCI) by investing in corporate partnerships and providing new access to intelligence sources, reducing collection and exploitation costs of existing sources', and enabling expanded network operation and intelligence exploitation to support network defense and cyber situational awareness. This Project contains the SIGINT Enabling Sub-Project.

(U) Base resources in this project are used to:

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers

4. **opaque juridical framework**

- FISA (Foreign Intelligence Surveillance Act)
- Foreign Intelligence Surveillance Court
  - Blanket legal approvation [?]
  - Warrantless intercepts
- *NSA letters with nondisclosure provisions*: recipient can't divulge the content of the order.

NSA surveillance on EU data

- Abuse of bilateral agreements
  - PNR (Passenger Name Record)
  - TFTP (Terrorist Finance Tracking Program) agreement
    intra-EU financial transaction information to the US
  - Safe Harbour
  - Council of Europe's Budapest Convention on Cybercrime transborder access to stored computer data
- Cooperative intelligence activities with UE governments
  (eg RAMPART-A started 1992)
- Covert intelligence activities = spying
  (eg SOCIALIST)

UE response (so far)

UE response so far

4 July 2013 – European Parliament
“Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU **citizens' privacy**” → LIBE Inquiry on electronic mass surveillance of EU citizens

21 February 2014 – LIBE Report “Protecting **fundamental rights** in a digital age”

12 March 2014 – European Parliament
“Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU **citizens’ fundamental rights** and on **transatlantic cooperation** in Justice and Home Affairs”

Procedures 2013/2682(RSP), 2013/2188(INI)

EP resolution of 12 March 2014

- **“compelling evidence** of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of **all citizens around the world**, on an unprecedented scale and in an **indiscriminate** and non-suspicion-based manner;”
- **“trust has been profoundly shaken**: trust between the two transatlantic partners, trust between citizens and their governments, trust in the functioning of democratic institutions on both sides of the Atlantic, trust in the respect of the rule of law, and trust in the security of IT services and communication”
- “data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible **existence of other purposes including political and economic espionage**, which need to be comprehensively dispelled”
- **“secret laws and courts violate the rule of law”**

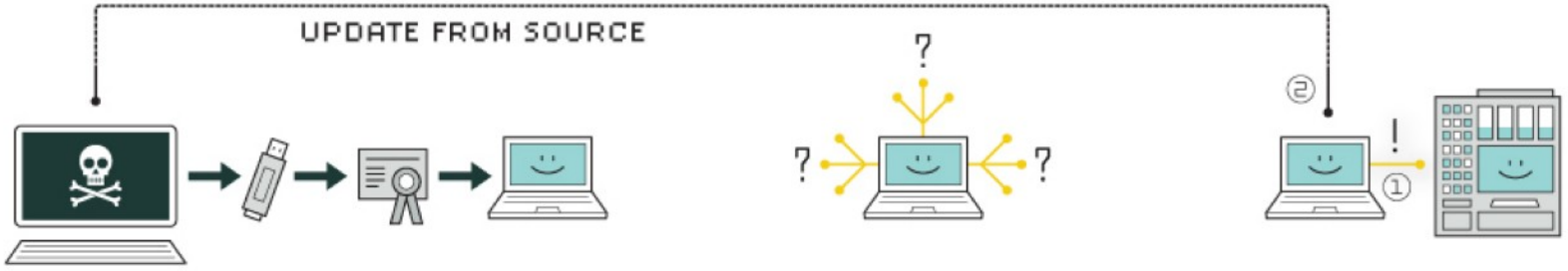
EP resolution **Priority Plan**
A European Digital Habeas Corpus

1. Adopt the **Data Protection Package** in 2014;
2. Conclude the **EU-US Umbrella Agreement** guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens, including in the event of data transfers from the EU to the US for law enforcement purposes;
3. **Suspend Safe Harbour** until a full review has been conducted and current loopholes are remedied, making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with the highest EU standards;
4. **Suspend the TFTP** agreement until [...]
5. **Evaluate any agreement**, mechanism or exchange with third countries involving personal data in order to ensure that the right to privacy and to the protection of personal data is not violated due to surveillance activities, and take necessary follow-up actions;
6. **Protect the rule of law** and the fundamental rights of EU citizens, (including from threats to the **freedom of the press**), the right of the public to receive impartial information and professional confidentiality (including lawyer-client relations), as well as ensuring **enhanced protection for whistleblowers**;

Cyberwarfare (Cyberterrorism)

Jan 2010: Stuxnet worm infects PC globally, targeting Iran's Plutonium programme, making Siemens enrichment turbines fail

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

May 2015

World | Fri May 29, 2015 2:59pm EDT

Related: WORLD, NORTH KOREA, ISRAEL

Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed - sources

SAN FRANCISCO | BY JOSEPH MENN

The United States tried to deploy a version of the Stuxnet computer virus to attack North Korea's nuclear weapons program five years ago but ultimately failed, according to people familiar with the covert campaign.

The operation began in tandem with the now-famous Stuxnet attack that sabotaged Iran's nuclear program in 2009 and 2010 by destroying a thousand or more centrifuges that were enriching uranium. Reuters and others have reported that the Iran attack was a joint effort by U.S. and Israeli forces.

According to one U.S. intelligence source, Stuxnet's developers produced a related virus that would be activated when it encountered Korean-language settings on an infected machine.

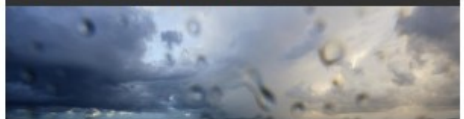
But U.S. agents could not access the core machines that ran Pyongyang's nuclear weapons program, said another source, a former high-ranking intelligence official who was briefed on the program.

The official said the National Security Agency-led campaign was stymied by North Korea's utter secrecy, as well as the extreme isolation of its communications systems. A third source, also previously with U.S. intelligence, said he had heard about the failed cyber attack but did not know details.

TRENDING ON REUTERS

1 Greece, creditors agree on need for quick deal as talks continue
2 Senate to let NSA spy program lapse, at least temporarily
3 Senate lets NSA spy program lapse, at least for now
4 Joe Biden's son Beau dies of brain cancer | VIDEO
5 Obamas visit Biden family after death of vice president's son | VIDEO

PHOTOS OF THE DAY



http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

Privacy is important for **democracy**

May 2014 – **International Principles on the Application of Human Rights to Communications Surveillance**

Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognised under international human rights law.

Communications Surveillance interferes with the right to privacy among a number of other human rights. As a result, it may only be justified when it is **prescribed by law**, **necessary** to achieve a legitimate aim, and **proportionate** to the aim pursued.

https://necessaryandproportionate.org/

« We are **not fully ourselves** if too many of our decisions are not taken by us, but by agents, automata, or superiors.

On the other side, sometimes it is our duty, our moral duty if you like, to **accept authority**»

Autonomy  Authority

Joseph Raz "The Problem of Authority: Revisiting the Service Conception", 2006

« Sometimes –for example, on the scene of an accident– **coordination**, which in the circumstances requires recognizing *someone as being in charge* of the rescue, is essential if lives are to be saved.

We must yield to the **authority**, where there is someone capable of playing this role.
There are in the *political sphere* many less dramatic analogues of such situations, where **a substantial good is at stake**, a good that we have moral reasons to secure for ourselves and for others but that can in the circumstances be best secured by yielding to a coordinating authority. These cases justify **giving up deciding for oneself**, and pose no threat to the authenticity of one's life, or to one's ability to lead a self-reliant and self-fulfilling life. »

Joseph Raz "The Problem of Authority: Revisiting the Service Conception", 2006

Security principle in our society tends to prevail on other principles, such as free speech, autonomy, …

“For your security...”
“To save lives...”

Democracy comes also from the preservation of social context integrity, that is, privacy.

Yet, deliberative **democracy** requires more than shoppers; it demands **speakers** and **listeners**.

[...]

when widespread and secret **surveillance** becomes the norm, the act of speaking or listening takes on a different social meaning.

Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 V AND . L. R EV . 1607 (1999)

Thank you!

Questions?

alberto @ cammozzo.com
http://cammozzo.com
Twitter: tagMeNot

Additional slides

UE & Cybercrime

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE OF THE
EUROPEAN UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity[4] incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU economy is already affected by cybercrime[5] activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cyber-security strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity[4] incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU economy is already affected by cybercrime[5] activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cyber-security strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity[4] incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU economy is already affected by cybercrime[5] activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cyber-security strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

Cybercrime: “*broad range of different criminal activities where computers and information systems are involved either as a* ***primary tool*** *or as a* ***primary target***.

Cybercrime comprises:

– traditional offences: fraud, forgery, identity theft

– content-related offences: on-line distribution of child pornography or incitement to racial hatred

– offences unique to computers and information systems: attacks against information systems, denial of service and malware”

STRATEGIC PRIORITIES AND ACTIONS

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

Actors involved

- ENISA European Network and Information Security Agency (114 TFEU):
  - CERT (Computer Emergency Response Team)
  - CII (critical information infrastructures) Protection & Resilience
  - Identity & Trust (consumer & payments)
  - Risk Management (Threat Landscape)
- Europol European Cybercrime Centre (EC3):
  - Payment Fraud
  - High-Tech Crimes
  - Child Sexual Exploitation
  - Cyber Intelligence
- EDA
  - Cyber defence project [?]
- EUROJUST, CEPOL

Budapest convention on Cybercrime

- Council of Europe's Budapest Convention on Cybercrime
  - Total number of signatures not followed by ratifications: 8 (incl GR, IR, SW)
  - Total number of ratifications/accessions: 45 (incl. USA, Australia, Japan)

EP resolution of 12 March 2014

- UE & US: prohibit blanket mass surveillance activities
- asks the Commission for the suspension of the TFTP Agreement;
- react to concerns that three of the major computerised reservation systems used by airlines worldwide are based in the US and that PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy
- “Safe Harbour principles do not provide adequate protection for EU citizens” & “Commission has failed to act to remedy the well-known deficiencies of the current implementation of Safe Harbour”
- accelerate their work on the whole Data Protection Package (Data Protection Regulation and the Data Protection Directive) to allow for its adoption in 2014
- 'privacy by design' and 'privacy by default' are a strengthening of data protection and should have the status of guidelines (esp. ‘Big Data’ and new applications such as the ‘Internet of Things’)
- development of European clouds and IT solutions as an essential elemen
- EP may only consent to TTIP agreement provided the agreement fully respects, inter alia, the fundamental rights recognised
- oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate
- threats to the freedom of the press and the chilling effect on journalists of intimidation by state authorities, in particular as regards the protection of confidentiality of journalistic sources
- European whistleblower protection programme,