Internet Governance
Controversial Issues

Virgilio Almeida
Harvard University

Cambridge, September 2016
References


Controversial Issues

• Deep Packet Inspection
  – For traffic management
  – For political and economics rationales
• Kill Switch
  – Technical anatomy
  – Case studies
• Delegate censorship
• Denial of service attacks vs human rights
Deep Packet Inspection (DPI)

- DPI is a label for a collection of technologies and applications that detect and shape live traffic on a network.
- DPI recognize patterns in and across network packets. The primary technical capability here is the ability to recognize(*).
  - Packet manipulation is the ability to act on the detection, by blocking, prioritizing or de-prioritizing, or otherwise regulating the flow of certain traffic.
  - Packet notification concerns actions around the information that can be extracted from detection, such as generating reports, alarms or billing incidents.

- DPI is a controversial technology
- Question: Which force is stronger in DPI deployment: commercial incentives of ISPs to manage bandwidth, or external regulatory and consumer concerns about privacy?
  - What are the commercial incentives?
  - What are the risks?

- (*) Cybersecurity via Intermediaries, PhD Dissertation, Hadi ASGHAR, 2016
  Cyberspace Governance, Harvard 2016
Deep Packet Inspection

- From a governance standpoint:
  - Benefits for ISPs: bandwidth management (e.g., blocking or throttling BitTorrent) and ad-injection, network quality monitoring and per application billing
  - Benefits for other actors: government surveillance, content regulation, copyright enforcement and malware detection.
  - Risks: legal (depending on national laws) and reputational risks (i.e., privacy concerns and competition).
  - Costs: include equipment and software costs, operational costs, etc.
- Most ISPs use DPI for bandwidth management including many liberal democracies(*).
- DPI use was lower in countries with better privacy safeguards (i.e., constitutional and statutory protections, privacy enforcement, and other safeguards).

(*) Cybersecurity via Intermediaries, PhD Dissertation, Hadi ASGHAR, 2016
Internet control points: kill switch

• The distributed architecture of the internet provides some sort of protection against widespread outages when compared to centralized architectures.
  • The monolithic term “kill switch” is a misnomer: there exist numerous points where outage can occur;
  • There are many control points that can produce different types of outage.

• Between 2005 and 2015, several governments attempted to shut down the Internet: authoritarian regimes, hybrid regime and well-consolidated democracy.
  • Justification:
    – democratic and hybrid regimes justified their actions to control the Internet infrastructure by citing unclear legislations concerning telecommunications and national security.
    – Internet viewed as the main threat to the stability of the nation-state, but the decision to shut down the Internet corresponds to a single authority, usually the president.
Internet control points: kill switch

• Between 1995 and 2011, there were over 600 instances of government control over digital networks made by consolidated and unconsolidated democracies, authoritarian regimes and fragile states.

• Actions of governmental control -> internet shutdown

• Forms of control (*):
  – by governments to deprive their own population from having Internet access
  – by governments to deprive different populations (other than their own) from having Internet access (as tool of cyber-warfare)
  – by private citizens or organizations to deprive specific populations from Internet access.

• Shutting down the Internet is defined as a government attempt to stop all Internet activity, and is colloquially known as the “Internet kill switch”

(*) P. Vargas Leon, Addressing the ultimate form of cyber security control: a multiple case study for the Internet kill switch

Cyberspace Governance, Harvard 2016
Figure 1. Internet Shut Down Cases

Cyberspace Governance, Harvard 2016
How Can the Internet Be Shut Down?

- Governments "can" order ISP to shut down their networks
- Other ways:
  - Landlocked "Pipes"
  - Undersea "Pipes"
  - Network Components (Servers, Switches, F/W, etc)
  - Wireless Towers/Cellular
  - Capacity
  - Crossroads: e.g., ISP’s, USA Ingress/Egress Points
  - Human Element
  - DoS Attacks and Similar
Cell Phone Blocking: the Bart case

After Cellphone Action, BART Faces Escalating Protests

By ZUSHA ELINSON  AUG. 20, 2011
Cell Phone Blocking: the Bart case

• BART officials acknowledged that they had switched off the transit system's underground cell phone network, from 4 to 7 p.m. to prevent protesters from coordinating plans to stop trains.

• Move to disrupt protesters' plans blasted as violation of free speech
• Hackers of the group Anonymous attacked San Francisco's BART website, on Sunday. The attack came after BART blocked cell service to thwart a protest on Thursday.

• Several internet governance issues:
  – Security, hacking,
  – Freedom of expression, privacy
  – Law enforcement
Egypt Leaders Found ‘Off’ Switch for Internet

By JAMES GLANZ and JOHN MARKOFF
Published: February 15, 2011

Epitaphs for the Mubarak government all note that the mobilizing power of the Internet was one of the Egyptian opposition’s most potent weapons. But quickly lost in the swirl of revolution was the government’s ferocious counterattack, a dark achievement that many had thought impossible in the age of global connectedness. In a span of minutes just after midnight on Jan. 28, a technologically advanced, densely wired country with more than 20 million people online was essentially severed from the global Internet.

The blackout was lifted after just five days, and it did not save President Hosni Mubarak. But it has mesmerized the worldwide technical community and raised concerns that with unrest coursing through the Middle East, other autocratic governments — many of them already known to interfere with and filter specific Web sites and e-mails — may also possess what is essentially a kill switch for the Internet.
China presses for Internet ‘kill switch’

China is pressing forward with a plan to control the Internet, even striding toward development of an online “kill switch” that would allow the communist country to basically shut down web access within its borders.

The Wall Street Journal said the nation’s just passed a security law that boosts its cyber defenses and presses for technological advances that give government the power to control Internet access. Specifically, the law includes a mandate for China companies to use local technology vendors when possible and to help create an Internet “kill switch” in times of national emergency.
Censorship, bias and discrimination in the transition from the physical world to virtual world

A- transported from the real world (data and procedures)
B- created by algorithms of the virtual world
C- new and unknown (e.g. Created in the virtual world due to new quantification)
Beijing Seeks to Tighten Reins on Websites in China

If the rule applies to all websites, it will have major implications and will effectively cut China out of the global Internet. By creating a domestic registry for websites, the rule would create a system of censorship in which only websites that have specifically registered with the Chinese government would be reachable from within the country.
China demands stricter rules for live streaming

© 19 August 2016 | China
Iran’s Web Spying Aided By Western Technology

European Gear Used in Vast Effort to Monitor Communications

By CHRISTOPHER RHOADS in New York and LORETTA CHAO in Beijing
Updated June 22, 2009 11:59 p.m. ET

The Iranian regime has developed, with the assistance of European telecommunications companies, one of the world’s most sophisticated mechanisms for controlling and censoring the Internet, allowing it to examine the content of individual online communications on a massive scale.

The monitoring capability was provided, at least in part, by a joint venture of Siemens AG, the German conglomerate, and Nokia Corp., the Finnish cellphone company, in the second half of 2008, Ben Roome, a spokesman for the joint venture, confirmed.
China's internet regulator has demanded stricter controls over the popular practice of live streaming, as part of a range of new requirements for sites.

As well as asking sites to step up control of live broadcasts, the Cyberspace Administration of China wants the content monitored full-time.

It is the latest move by authorities to clamp down on what it sees as "inappropriate" content online.

Live streaming is particularly popular among Chinese youth.

There are an estimated 80 platforms in use around the country, with some gaining notoriety for hosting live broadcasts of stunts that have gone viral.

The People's Daily reported that the CAC statement asked sites to "strengthen security evaluation of new products like live broadcast". It also said the the new requirements would apply to "bullet-screens" - where online user comments pop-up on top of live videos.

It is just one of a range of new requirements placed on websites to better regulate themselves, including putting the onus on them to set up 24-hour monitoring of their online content.

In April, the Ministry of Culture announced it was investigating a number of popular live-streaming platforms for allegedly hosting pornographic or violent content that "harms social morality".
Internet Companies Shouldn't Be Censors

By Leonid Bershidsky

PayPal blocked an account set up by Russian activists seeking to collect funds for the publication of a report on Russia's involvement in eastern Ukraine. The U.S. online payment company explained that it didn't "provide the option of using its system to receive donations to political parties or causes in Russia." It's just the latest example of an Internet giant cast in a role for which it is ill-equipped.

Companies such as Google, Twitter, Facebook and even Paypal are ruling on matters of free speech. The decisions are made by business executives, who are essentially performing the function of editors in traditional media. But their organizations aren't professional media: They are conduits for other people's content, products and money, and their ability to make value judgments should be as limited as a water company's power to shut off service on a whim.
Google Transparency Reports

Removal requests by the numbers

See all data
Google Transparency Reports

Cyberspace Governance, Harvard 2016
Facebook: content removal requests

France Requests for Data
We respond to valid requests relating to criminal cases. Each and every request we receive is checked for legal sufficiency and we reject or require greater specificity on requests that are overly broad or vague.

<table>
<thead>
<tr>
<th>Total Requests</th>
<th>Users / AccountsRequested</th>
<th>Percentage of requests where some data produced</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,711</td>
<td>2,894</td>
<td>54.22%</td>
</tr>
</tbody>
</table>

France Content Restrictions
We restricted access in France to content reported under laws prohibiting Holocaust denial and condoning terrorism, as well 32,100 instances of a single image related to the November 2015 terrorist attacks in Paris that was alleged by OCLCTIC to violate French laws related to the protection of human dignity.

Number of pieces of content restricted

37,695
Twitter: content removal requests

Removal requests worldwide

REQUESTS:
- 1 - 47
- 48 - 476
- 477 - 2493
- Other Data Available

Map by @trebor

Cyberspace Governance, Harvard 2016
Attacks as Human Rights Suppression

• DDoS: goal is to stop flow of information;
• Governments have used DDoS attacks to block access to alternative media;
• Communities @ Risk: Targeted Digital Threats Against Civil Society, a report by the Citizen Lab;
  – In the digital realm, CSOs face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.
  – Targeted digital threats undermine CSOs’ core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety.
  – Targeted digital threats extend the “reach” of the state (or other threat actors) beyond borders and into “safe havens.”
Targeted Digital Threats Against Civil Society

While governments and businesses are often highlighted as victims, malware attacks against ethnic minority groups in China including Tibetans and Uighurs, and religious groups such as Falun Gong, go back to at least 2002, and possibly earlier.

The lessons we draw from the Syrian case align with those from the formal study. Namely, attackers exploit the pervasive, constant use of mass market communications tools by the opposition, just as do threat actors that target participants in our study.

- APT1 (Reported by Mandiant)
  - Targeted 141 organizations from 20 industry sectors
  - Targeted Tibet Group 1, compromised Rights Group 1

- DTL Campaigns (Reported by FireEye)
  - Targeted government and 11 industry sectors
  - Targeted Tibet Groups 1, 2, 3, and 4

- NetTraveler (Reported by Kaspersky)
  - Targeted 350 organizations from NGOs, government, and industry
  - Known to target Tibetan and Uyghur CSOs
  - Targeted Tibet Groups 1, 2, 3, 4, and 5; China Group 3

- PlugX Campaigns (Reported by TrendMicro, AlienVault)
  - Targeted companies in Asia and US, and Tibetan CSOs
  - Targeted China Groups 1 and 2; Tibet Groups 1 and 2
Communities @ Risk: Targeted Digital Threats Against Civil Society is the culminating report of a multi-year, multi-group study on targeted digital threats. We define targeted digital threats as persistent attempts to compromise and infiltrate the networked devices and infrastructure of specific individuals, groups, organizations, and communities.

The study involved 10 civil society organizations (CSOs) that shared suspicious emails, network traffic, and other data with Citizen Lab researchers who conducted detailed, confidential analysis over a four year period. Citizen Lab researchers also paid site visits to the participating CSOs and interviewed them about their perceptions and the impacts of the digital attacks on their operations. Data from both the technical and contextual aspects of the research informs the report’s Key Findings:

- In the digital realm, CSOs face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.
- Counterintuitively, technical sophistication of malware used in these attacks is low, but the level of social engineering employed is high.
- Digital attacks against CSOs are persistent, adapting to targets in order to maintain access over time and across platforms.
- Targeted digital threats undermine CSOs’ core communications and missions in a significant way, sometimes as a nuisance or resource drain, more seriously as a major risk to individual safety.
- Targeted digital threats extend the “reach” of the state (or other threat actors) beyond borders and into “safe havens.”
References

• The 2016 Federal Cybersecurity Research and Development Strategic Plan, Executive Office of the President, National Science and Technology Council, Feb 2016.

• [Link](https://www.whitehouse.gov/blog/2016/02/08/national-challenges-and-goals-cybersecurity-science-and-technology)

  [http://www.nap.edu/21833](http://www.nap.edu/21833)
THANKS!

Valmeida@cyber.law.harvard.edu