Imposing and Evading Cyber Borders
The Dilemma of Sovereignty

pirate security conference psc

Alessandro Guarino

2017 Pirate Security Conference - *Munich 16/2/2017*

The Speaker

15+ Years in Information/Cyber Security Consultancy

StudioAG
Consulting & Engineering

Speaker Author

CyCon International Conference on Cyber Conflict — 2013

iSSE 2016 — 2013-2016

E-PRIVACY XX — 2016

IET Events The Institution of Engineering and Technology

Standards

UNINFO

ETSI

CEN CENELEC

2011 →

Introduction: Cyber?

- The Internet changed any facet of society – The cliché that is nevertheless true…
- Cyberspace: a cool world from Neuromancer to the NATO Warsaw doctrine
- Cliché so true that Cyber-* (operations, warfare, conflict) is now part of statecraft, security, strategy conversation.
- While cyberspace is a complex, socio-technical system where many different actors have stakes, Nation-States are still relevant, arguably the most relevant.
- We will explore the dilemma: global common or sovereign entities.

Introduction: Cyber?

- Why borders? The border is symbol and one of the fundamental attributes of a sovereign Westphalian State (no need to stress the recurrence of “protecting our borders” in the current political climate)
- Does it translate to cyber?
- How does sovereignty and the other attributes of states work when dealing with “cyberspace”: peace, security, war, international norms...

A Bit of History

The relatively sudden and widespread diffusion of Internet access was the result of a series of converging political and technical factors.

It’s likely that none of the actors involved predicted exactly what would happen and how disruptive an innovation it was going to be.

This holds also for conflict (and warfare) in cyberspace: it’s not new, we have decades of history to look back to (and hopefully learn from).

A Bit of History

- Breaking up of monopolies in the telecommunication market in the U.S.
- Decision by the FCC (Federal Communications Commission) to reclassify “data processing” – machine-to-machine digital communications – as a “value-added” enhanced service → companies were mainly concerned with voice services and saw this as a small price to pay...
- The consequence was the creation of an unregulated and open market for digital services, at first in North America but later a wave of liberalisations spilled over to Europe as well.
- Free Software Movement – The Free Licences were an enabling Factor for the Commercial Internet

A Bit of History – Technological Factors

- Packet-switching architecture of the network
  - Decentralised by nature
- TCP/IP Protocol suite
  - Standard, open specifications
  - Local routing
- Robust, free, easy to use stacks for commercial use of the Internet
- xDSL Technology.

The Tension of Governance

- We have seen from history the two poles:
  - Cyberspace as an immaterial realm, where geography (and laws) do not matter
    - *“Governments of the Industrial world, you weary giants […], I come from Cyberspace, the new home of Mind […], You have no sovereignty where we gather.”*
  - The Sovereignty Argument
    - Cyber is only an extension of telecommunications networks, just a new telehgraph, a matter for inter-governmental fora…
    - One of the oldest modern international organizations was established just for that purpose.

The Tension of Governance

- The potential for creating and maintaining transnational social networks with ease, flexibility, and relative anonymity has been seen as a threat not only to state sovereignty, but also to national security itself.

- This perception has increased since the beginning of this century (another true cliché) and informed nation-state policy, in their quest to regain control.

The Tension of Governance

- It's true that "cyber" or "the cloud" does not actually exist – it's physical, it's located somewhere (in someone's territory).
- When it's not (as his the case for submarine cables) it's heavily regulated by international laws and treaties.

The Tension of Governance

- Governance and (National) Cybersecurity
- State actual practices vs. Cooperation
  - Formally the tension between the two poles resulted in different governance models
  - Classic inter-governmental fora (e.g. the ITU)
  - Network governance models (inclusive of non-states)
- Some sort of network governance model was already in place when states began to realise the potential of cyberspace and to reestablish traditional sovereignty. The Internet Corporation for Assigned Names and Numbers (ICANN) and the decentralised management of the Domain Name System (DNS) are striking examples. Decentralised governance made the Internet incredibly successful at various levels.

The State of the Art

- We are witnessing a resurgence of the Nation-State at all levels.
- Some manifestations:
  - European Union Crisis and Brexit
  - U.S. new isolationism / protectionism (but world domination…)
  - China
  - “Imperial” Russia
- Back to cyber: states want to reaffirm sovereignty, defend their borders, control their people – at the same time operate outside and deter adversaries…

State of the Art – Defining Cyberspace

- U.S. Department of Defense

  “domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures.”

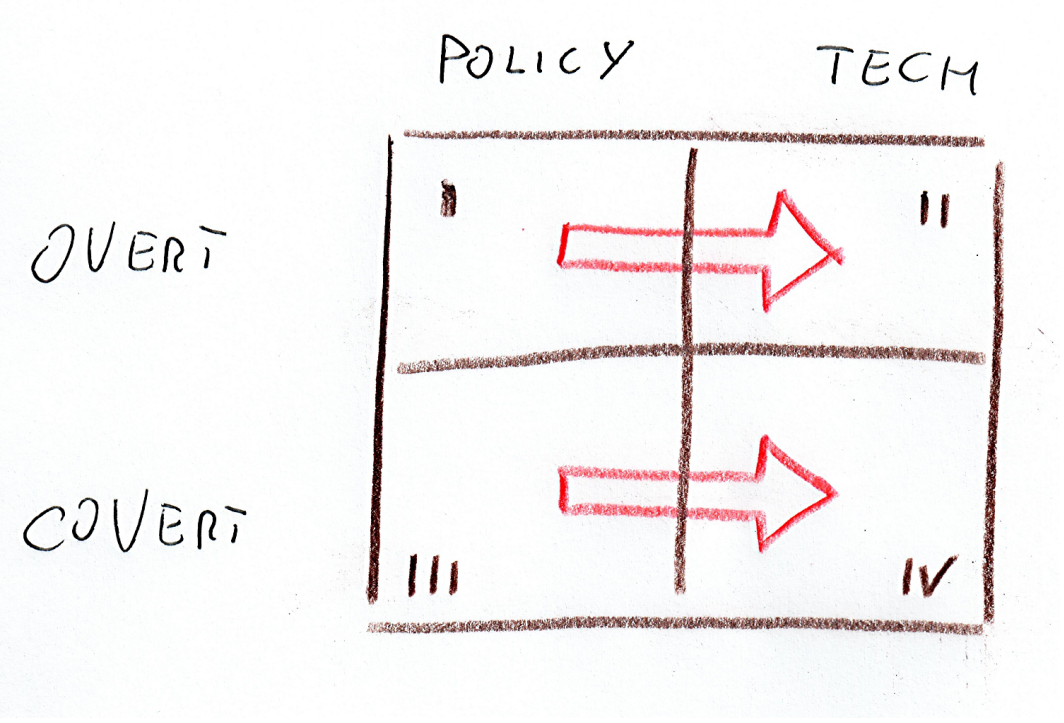
- Russia

  Information space is “the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself.”

- China

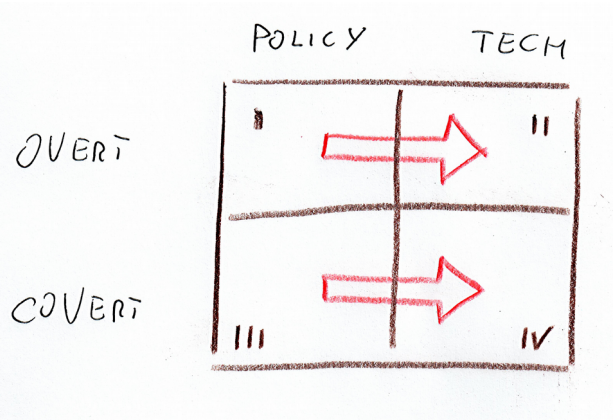
  “The main function of the information space is for people to acquire and process data… a new place to communicate with people and activities, it is the integration of all the world’s communications networks, databases and information, forming a “landscape” huge, interconnected, with different ethnic and racial characteristics of the interaction, which is a three-dimensional space.”

How it's done? Imposing Borders



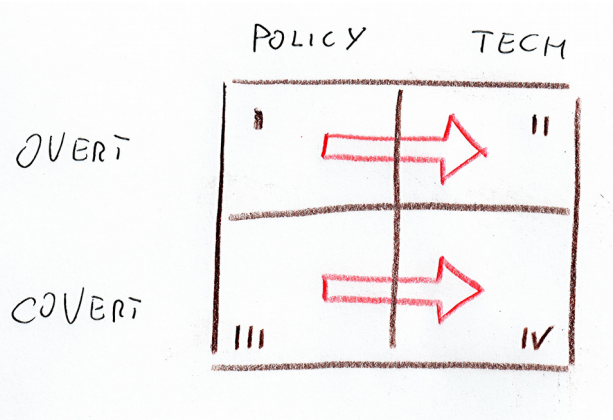
How it's done? Imposing Borders

- The "overt" arsenal…
  - All attempts to bring back cyber governance under state control
  - Control of the "physical" (e.g. Egypt Block of the Internet in 2011)
  - Policies informing technical means (e.g. "The Great Firewall)



How it's done? Imposing Borders

- The "covert" arsenal…
  - Content monitoring on the web and social networks by security agencies
  - "Moral Suasion" (And National Security Letters) on ISPs and network operators.
  - Mass surveillance and bulk collecting
  - Cyber defence of public and private networks



How: Evading Borders

- The technology that enables borders
  - For non-state actors (good and bad)and individuals but also…
- For Nation-States themselves
  - Deterrence? Does it work?

How: Evading Borders

- Some examples of the technology that help evading borders:
  - Strong encryption
  - Onion routing (plus pluggable transports)
  - Virtual Private Networks / Proxies
  - Cryptocurrencies
- It’s dual-use at best:
  - Individual privacy
  - Investigative Journalists
  - Cyber Crime
  - National Cyber Security – Government themselves use it
- Some riddles to solve: deterrence and how to solve the cyber security dilemma

The Tribulations of Cyber Diplomacy

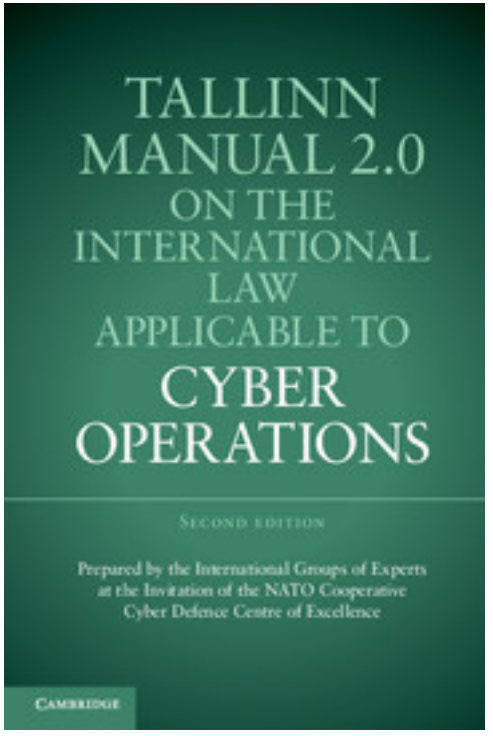
- The Security Dilemma in Cyber
  - Critical because the realm is offence-dominated
  - And No Clear Distinction between offence and defence
- Struggle to reach consensus – State Practice vs. International Norms
  - Basic Definitions
  - Cyber Operations / Cyber Conflict Rules
  - Internet Governance
  - Definition of Information Weapons
- Sovereignty: the key to the future evolution of cyber norms

The Tribulations of Cyber Diplomacy

- Political climate and state practices also contribute to nations themselves undermining and evading borders.
- Russia is a good example:
  - Permissive environment for cyber criminals (as long as they comply and occasionally help…)
- While the U.S. ostensibly condemns the use of “proxy” hacker groups, it more or less secretly makes good use of them
  - “The Jester”
  - Privatisation of Cyber Security and “Active Defence”
  - Global Mass Surveillance does not help.

The Tribulations of Cyber Diplomacy

- Cooperation in fighting Cybercrime
  - Still sketchy, even it's improving.
  - Parties to the Budapest Convention are increasing.
- Cyber International Law
  - Cyberspace is NOT "The Wild West"
  - Law exists and is applicable, just because of the sovereignty principle.
  - State practices however still rule.
  - Tallinn Manual 2.0



Case Study: China

- The People's Republic could well be considered the champion of the sovereignty argument.
- Beijing sought to establish as clear lines of sovereignty in cyberspace as there were for land, sea, and air, since at least 2010.
- Countries should respect other countries' rights in developing a cyber governing path forward for its own citizens (Position expressed by Xi and also by the Chinese ambassador to the UK at Chatham House Cyber Conference in 2016, inter alia).
- Cyber sovereignty is a fundamental part of national sovereignty and also a mean to counteract perceived "cyber hegemonic" behaviours by other powers.

Case Study: China

- China has been leveraging the UN Charter as justification to extend the principle of sovereign equality to cyberspace.
- Chinese experts were part of the international group of experts that developed Tallinn Manual 2.0
- This achieves two important objectives for Beijing: it demonstrates China's intent on using existing applicable international law to support its proposal, and it shows China's desire to raise such issues to a government level and in an international forum.

Case Study: China

- 2015 – Anti Terror Law
  - Compels technology companies to help decrypt information giving Chinese authorities access to encrypted data
- 2015 – National Security Law
  - Provides a framework for China's security considerations in the face of emerging threats. Overlapping security considerations demonstrates Beijing's perspective that national security is an inherently integrated process.

Case Study: China

- July 2016 – Overseas Non-Government Organisation Management Law
  - All NGOs are required to get approval from a supervisory unit to operate in China. Prohibits any Chinese organisation from conducting activities on behalf of or with non-authorised NGOs.
    While the law is not specifically cyber-related, it is safe to assume that NGOs properly registering with Chinese authorities would be required to comply with any acceptable technology use policies set forth by the Chinese government in other legislation.
- November 2016 – Cyber Security Law
  - Increases the government's powers to record and impede the dissemination of information deemed "illegal". Two key reoccurring themes are stressed: 1) the ability to monitor and control information, and 2) the compliance of foreign enterprises with the rules set forth

Conclusions

- Nation-States will be main actors in any cyber international order.
- Sovereignty is and will be a key principle:
  - Hardware is clearly subject to it (or regulated...)
  - Data will be probably deemed an “Object” as well – it’s an open issue in IL – States have duty to protect, attack is forbidden etc etc
- But: enforce sovereignty could undermine own cyber operations as well…
  - Cyber Deterrence and “Nobody But Us” do not work so well and can backfire but are extremely attractive, especially for America.
- Expect the ambiguity to continue.
- No sovereignty without borders…
- Need to involve non-state actors to preserve the advantage of the Internet.

Thank You For Your Attention

Any questions?

a.guarino@studioag.eu

@alexsib17

Slides available on:
www.studioag.pro

This Presentation is Based on a Paper Co-Authored with Emilio Iasiello – Cyber Security Consultant and Researcher – Arlington, VA

(Some) References

A. Guarino, E. Iasiello - Imposing and Evading Cyber Borders: the Dilemma of Sovereignty – 2017, in pre-publication

International Law and Cyber Operations - Launch of the Tallinn Manual 2.0 – Feb 8 2017 – Atlatntic Council - https://www.youtube.com/watch?v=riP4kStBBJs

J.P. Barlow – A Declaration of the Independence of Cyberspace – Crypto Anarchy, Cyberstates and Pirate Utopias, ed. Ludlow, Cambridge 2001

A. Guarino – Cyberspace Does not Exist – Strange Loops 15/1/2015 – http://www.strangeloops.pro/en/2015/01/la-nuvola-non-esiste

M.L. Mueller – Network and States – MIT Press – Cambridge 2010

Pictures Credits

Slide 4 – Daily Kos – http://www.dailykos.com/
Slide 10 – Wired – https://www.wired.com/2012/10/ff-inside-google-data-center/