

CE876 - Information Security Mng. & Eng.

Lecture 14: International Aspects of Cybersecurity

Seyedeh Atefeh Musavi / Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology
Spring 1400

S4Lab



Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content.

Why International-level?

- The trans-border nature of the internet and its integration have made it a global infrastructure around which all kinds of conflicts of norms – of legitimacy, of power, of culture – develop.
- The multifunctional nature of the internet has also enabled it to transform itself into an essential infrastructure for a wide set of social, cultural, economic and political activities and sectors.
- The “end-to-end” architecture of the network – i.e. its distributed architecture – favors the development of decentralized collective action

Internet governance ecosystem

1. The administration of critical Internet resources such as names and numbers.
2. The establishment of Internet technical standards (e.g. TCP/IP, HTTP).
3. Access and interconnection coordination.
4. Cybersecurity governance.
5. The policy role of private information intermediaries.
6. Architecture-based intellectual property rights enforcement.

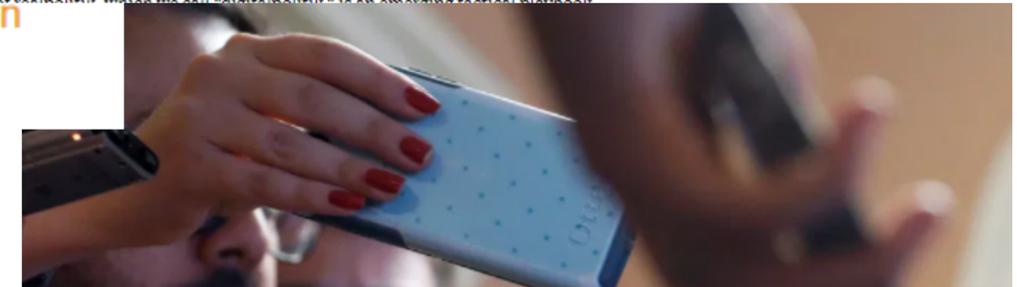


THE WAR-TORN WEB

A once-unified online world has broken into new warring states.

BY SEAN McDONALD AND AN XIAO MINA
ILLUSTRATIONS BY DOUG CHAYKA AND JASON LI FOR FOREIGN POLICY
DECEMBER 19, 2018

The global internet continues to fragment. Governments, in particular, are using their influence to shape the ways that digital companies, markets, and rights connect us online. This new form of territoriality, which we call "digital territoriality," is an emerging tactical playbook.



TECHTANK

U.S. government should not reverse course on internet governance transition

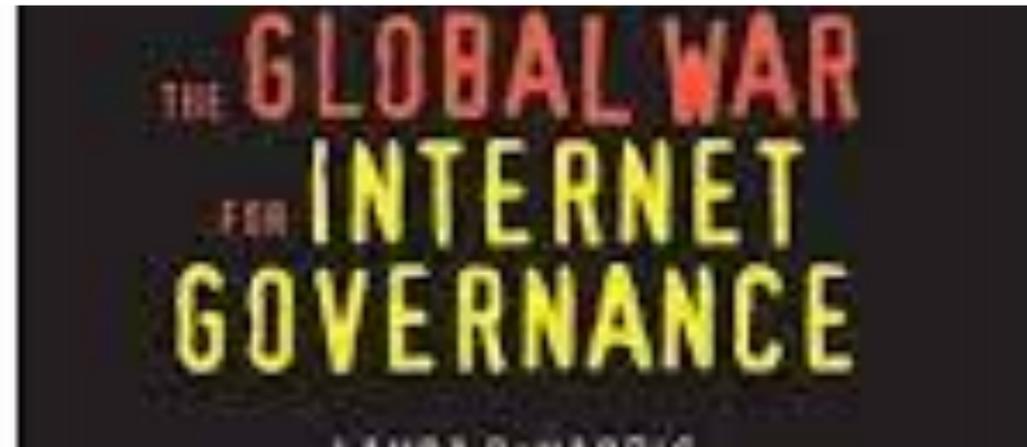
Paris Peace Forum. The summit had a lofty goal, according to its mission: to generate support and collective action at a time when "countries are turning inward." The global political context turned out that the timing was too, as the divide between President Donald Trump and Angela Merkel was on full display during **Trump's visit to France** for the centennial commemorations. Trump was boarding a **flight back to Washington** as the forum began.

Aug 9, 2012, 02:10am EDT

Why is the UN Trying to Take over the Internet?



Larry Downes Former
Cybersecurity
Best-selling author on technology policy



THE WALL STREET JOURNAL

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ Magazine

Subscribe | Sign In

Search

How China Is Taking Over International Organizations, One Vote at a Time

China's decadelong campaign to secure more clout at the United Nations is now helping shield Beijing from international scrutiny

Who wins?

- So There is a war between different stakeholders for Internet governance.
- But how they follow this aim is important.
- The more in depth realization of the Internet ecosystem, the better governance decisions ...

During the legislative deliberations about the proposed modifications to Internet governance structures, it became clear that some policymakers were unfamiliar both with how basic technologies of Internet governance work and with how global coordination works among the institutions that manage these systems. Considering the complexity of these technological and institutional frameworks, this might not be sur-

experts. *Roll Call* reported that one of the sponsors of SOPA was generally dismissive of criticism of the bill as “completely hypothetical” and suggested that “none of it is based in reality.”³



Rejection of exclusivity

- There exist a global trend toward rejection of exclusivity and support for openness can be seen in:
 - Open source licenses.
 - Network neutrality.
 - Support for unlicensed radio spectrum.
 - The construction of a global governance regime for the internet.

Rejection of exclusivity (con't)

- These (GPL, NN, open Internet...) take the logic of the “commons” into new territory.
- Its political demands pertain not to pure informational goods, such as software and digital content, but to networks and bandwidth – resources that, unlike software or digitized information, are subject to physical scarcity and are not non-rival in consumption.
- A reliance on commons over private property rights for certain kinds of resource allocation; and a valorization of openness and freedom over exclusion.
- The dialogue on internet governance participates fully in the ongoing debate over “commons” and “property” in communication information policy.

Tragedy of commons (overuse)



[Image: <http://blogs.strategygroup.net/>]

Garrett Hardin, 1968, the US ecologist and philosopher warned that “the inherent logic of the commons remorselessly generates tragedy”, adding gloomily that, “Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons.”



- One can think of Russian political ads, extremist videos, fake news and all the rest is as the polluters of common resources, albeit ones that are privately owned.
- The term for this is the tragedy of the commons.
- Open ecosystems that are openly shared by entire communities tend to get despoiled.

Self-interest on commons

- Hardin's prime example was the overgrazing of common land, when the number of farmers and shepherds seeking to use the resource of free feed for animals becomes too high.
- He also cited companies polluting the environment with sewage, chemical and other waste rather than cleaning up their own mess. Rational self-interest led to the commons becoming barren or dirty.
- People and organizations who exploit free resources for money or other motives.
- These are polluters of the digital commons and with them come over-grazers: people guilty of lesser sins such as shouting loudly to gain attention or attacking others.
- The digital commons fosters great communal benefits that go beyond being a publisher in the traditional sense.
- The fact that YouTube is open and free allows all kinds of creativity to flourish in ways that are not enabled by the entertainment industry. The tragedy is that it also empowers propagandists for terror.

What to do with selfishness?

- Hardin was a pessimist about commons, arguing that there was no technical solution and that the only remedy was “mutual coercion, mutually agreed upon by the majority”.
- The equivalent for Facebook, Twitter and YouTube would be to become much more like publishers, imposing tight rules about entry and behavior rather than their current openness.
- They resist this partly because it would bring stricter legal liability and partly because they want to remain as commons.
- But every time a scandal occurs, they have to reinforce their editorial defenses and come closer to the kind of content monitoring that would change their nature.
- More than 75 per cent of extremist videos taken down by YouTube are identified by algorithms, while Facebook now finds automatically 99 per cent of the Isis and al-Qaeda material it removes.

Selfishness in commons

- Commons can be easily regulated.
- BTW, some think this is like having an automated fence around a territory to sort exploiters from legitimate entrants.
- Machines cannot solve everything, though. If they could exclude all miscreants, the commons would turn into something else.
- The vision of an unfettered community is alluring but utopias are always vulnerable.
-

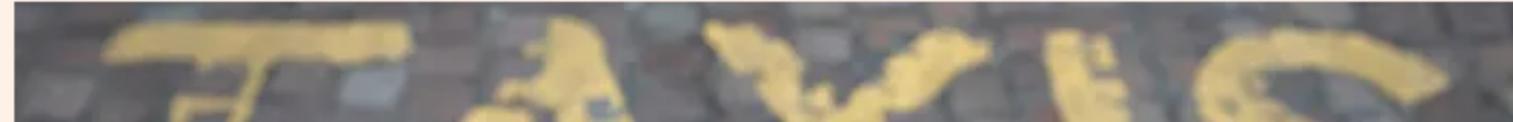


[Image: <https://i.pinimg.com/>]

Uber Tragedy

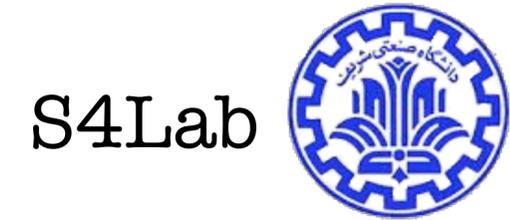
Uber exemplifies the Tragedy of the Commons

From Tad Borek, San Francisco, CA, US — Wednesday's most read letter



- Within driving distance of San Francisco are millions of potential drivers. The city is a hub of tourism and business travel.
- The result is overgrazed roads with the anticipated tragic outcomes: inadequate driver wages from oversupply, which results in high turnover and lower driver quality; and negative externalities such as traffic congestion and increased air pollution.
- There's more. Uber's data breach has implications.
 - Robo-taxis will become popular and will be involved in fatal accidents. It will be then necessary to review data. Did a sensor fail, or code break? All related data will be owned by the same company.

Private and common property debates



- On one side of the debate, “the commons” is presented as something large, public-spirited and inclusive while the role of private property rights is either ignored or denigrated as enclosed, restrictive, selfish.
- On the other side of the political spectrum, “commons” is equated with an all-embracing economic communism or overbearing regulation, and “the market” defended rigidly as if it were the answer to all problems.

Privatization

- How do we solve such an overuse tragedy?
- Often, by creating private property.
- Private owners tend to avoid overuse because they benefit directly from conserving the resources they control.

ICANN example

- Till 1 October 2016, ICANN was under US government oversight.
 - Given up as a result of Edward Snowden's NSA leaks.
- Opponents were unwilling to give ICANN complete control over the internet's naming system.
- They argue that the root file, the big directory of domain names and their associated servers, was US government **property** - and therefore required congressional approval before being "given away."
- Giving up the power amounts to handing it over to countries like China and Russia.
- It could use that power to disrupt and censor communications online.



[Image: <https://www.cfr.org/>]

[[Has the US just given away the internet?](#), Dave Lee, BBC, 2016]

Bandwidth example

- Net Neutrality – the demand for turning bandwidth into a commons.
 - Fears that bandwidth suppliers would become vertically integrated into the supply of content and applications, and that that integration would give them incentives to discriminate against independent suppliers.
- Opponents of net neutrality, on the other hand, see bandwidth as a private resource, one that is supplied most efficiently if exclusive owners take responsibility for managing and conserving it, and are able to optimize its value by exerting control over the content and applications it conveys.
- The NN debate is often framed as a clash between advocates of “regulation” and advocates of a “free market.”
 - Guess who is who?!

Tragedy of anti-commons

- Private owners tend to avoid overuse because they benefit directly from conserving the resources they control.
- Unfortunately, privatization can overshoot. Sometimes we create too many separate owners of a single resource.
- Each one can block the others' use. If cooperation fails, nobody can use the resource.
- Everybody loses in a hidden tragedy of the anti-commons.



[Image: <https://wikimedia.org/>]

	Commons	Anticommons
Privilege to use	many	none
Right to exclude	none	many
Consequence	overuse	underuse

[Table: [The Tragedy of Anticommons, Michael Heller, 2014](#)]

Commons or properties?

- In practice dynamic interplay between privatization and common spaces occurs.
- The “tragedy of the anti-commons” provides an important clue as to how commons can support markets, and vice versa.
- Notion of property-preempting investments :
 - “Firms and individuals are increasingly injecting information into the public domain with the explicit goal of preempting or undermining the potential property rights of economic adversaries.”
 - “Strong rights lead to investments in the public domain” and that these represent a “private ordering response to the phenomenon of the anti-commons.”
- In the case of software, it is not just the possibility of an anti-commons that has led to the embrace of open-source software by the likes of IBM, Sun Microsystems and other major IT interests; it is also (if not primarily) the market dominance of a rival firm, Microsoft.

An interplay example: TCP/IP

- The internet is based on global and nonproprietary standards that can be freely adopted by anyone. These standards constitute a global commons.
 - Patented technologies are unwelcome in both the IETF and the W3C.
- Unlike the standards and software protocols, The internet is a network of privately owned and administered networks. The bandwidth resources supplied by these entities are not non-rival.
- Open standards and private networks are linked together via the end-to-end argument.
- At the end points, the internet is private and exclusive; at the core standards level, it is nonproprietary and open.
- This permits the network to serve as a relatively neutral and transparent platform for the widest possible variety of applications and services

An interplay example: TCP/IP 2

of power equilibrium among peers. As Peter Cowhey and Milton Mueller (2009) put it:

[R]etaining the IETF as the locus of [internet] standards governance allayed the worst fears of the three major industrial regions. For the US Government, the worry was that the European Union or Japan might belatedly become tempted to engage in industrial policy to overcome the de facto boost to the US computer industry emerging from the Internet computing revolution. For the EU and Japan, the IETF was an instrument for keeping the computer industry away from the consolidated dominance of Microsoft.

- the internet's unique mixture of open, nonproprietary standards, private networks and private content, applications and services was welcomed because it offered a more open and neutral alternative to powerful and potentially threatening actors such as IBM, Microsoft, and the ITU.

Delegated governance

- Some forms of privatized Internet governance are directly delegated from government authorities to corporations.
 - Particularly prevalent in the Internet context because private companies, rather than public entities, serve as information intermediaries.
 - E.g. Delegated censorship, delegated surveillance, delegated copyright enforcement, and delegated law enforcement
- This phenomenon of privatization and delegation is not unique to Internet control issues but is part of broader political conditions.
 - Global phenomenon of the privatization of functions traditionally performed by the state.

Governmental privatization of state functions

- Much of Internet governance is enacted by private corporations and non-governmental entities.
- Private corporations enact policy not only in carrying out their core functions but also as actors responding to events on a larger political stage.
- WikiLeaks example:
 - Free DNS resolution services decided to stop providing these services, temporarily erasing its online presence. Amazon stopped hosting WikiLeaks sites on its computers, citing a violation of its terms of service.
 - Financial companies severed the flow of money to WikiLeaks.
 - The WikiLeaks saga serves as an exemplar of the political power of private intermediaries.

Self-regulation in private sector

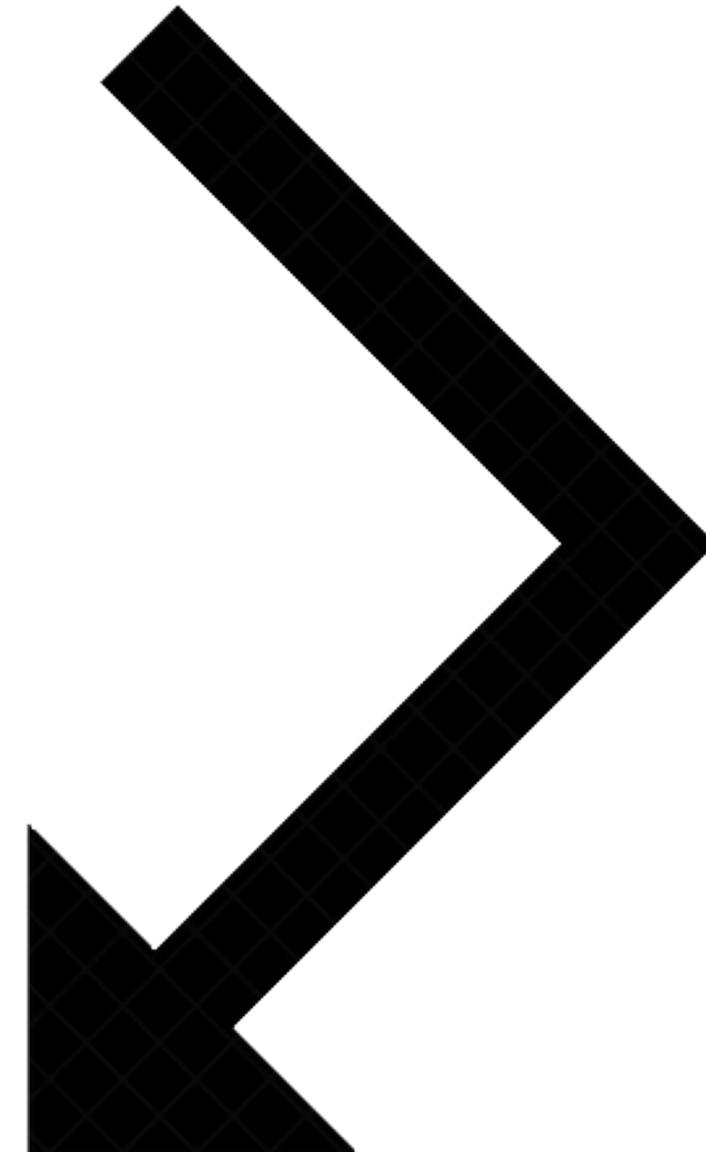
- Another broader context is the global influence of multinational corporations on regulatory decisions across industries including pharmaceuticals, telecommunications, entertainment, and energy.
- They set de facto global public policy via their approaches to labor practices, environmental impacts, health care for employees, fair trade, and human rights.
- Multinational corporations, via this cross-cultural decision making, enact global governance.
- Hence, one can see corporations as forces of public policy interventions.
 - Governmental orders
 - Or alternatively develop voluntary and self-regulatory business practices that adhere to certain ethical standards and social values

Let's see another idea

Offensive cyber security

Cyber deterrence

- Passive deterrence:
 - “Deterrence by denial (the ability to frustrate the attacks)”
- Active deterrence
 - “Deterrence by punishment (the threat of retaliation)”
 - Hack-back



Comparison with nuclear

- Cyber deterrence by the threat of retaliation works differently than that of nuclear deterrence.
- The particularities of the bi-polar world and the extraordinary damage potential of nuclear weapons, made defense strategies less feasible.
- Cyber deterrence is multipolar and takes place between asymmetric opponents. Cyber capabilities are mostly opaque and easily proliferate.
- Multiple challenges should be solved.
- Can you guess some?

Non-State Actors

- The spectrum of actors ranges from script kiddies with low level skills to cyber criminals with medium abilities to cyber mercenaries with considerable capabilities.
- Cyber-criminal activity is the largest group of cyber threats and one of the most difficult to effectively deter.
- Hacktivists are activists motivated by politics or religion or the desire to expose that of a wrongdoing or exact revenge.
- Violent nonstate-sponsored organizations such as terrorist groups.
- State-sponsored groups can be effectively deterred.
- Even proxy actors.

[\[Is Cyber Deterrence Possible?,
Timothy M. McKenzie, AUP, 2017\]](#)

Attribution

- When A cyber attacks D, D does not automatically know that it was A.
- If D retaliates digitally, again A does not necessarily know that it was D.
- There is barely a target in digital space that is attacked by only one actor.
- Misperceptions are therefore quite common.
 - Also the risk that attackers may act under a false flag or claim to be responsible for attacks they did not carry out.
- All-source attribution “is a process that integrates information from all sources, not just technical sources at the scene of the attack, to arrive at a judgment (rather than a definitive and certain proof) concerning the identity of the intruder.

[\[Is Cyber Deterrence Possible?,
Timothy M. McKenzie, AUP, 2017\]](#)

Proportionality and Appropriateness

- It is well researched in political science, that escalation spirals are often a consequence if a retaliation is perceived as inappropriate or too painful. In these cases, deterrence fails.
- Determining the correct measure is highly complex and also a function of the attribution problem.

Demonstration Problem

- An attacker must be able to weigh up the costs of a potential punishment by D. Thus, A must be able to assess the damage potential of D's cyber capabilities.
- For this very reason, military parades display kinetic weapons to the world and weapons tests are conducted for the whole world to see.
 - This transparency principle does not readily apply to cyber capabilities.
- Demonstrating of cyber capability for reasons of damage threat jeopardizes the functioning of the capability.
 - If a defender knows about the attack vector, he can adapt, which then makes an attack less useful.
- Offensive cyber abilities follow the law of diminishing returns: any deployment of ability increases the chances that it will be less effective in the future.
- 0-day capabilities cannot be credibly demonstrated without compromising their effectiveness.

[Cyber deterrence is overrated: analysis of the deterrent potential of the new cyber doctrine and lessons for Germany's "Active Cyber Defense", Schulze, Matthias, SWP, 2019]

Lack of Controllability

- It is complicated, although not impossible, to limit cyber capabilities to one target and to avoid collateral damage.
- Even attacks such as Stuxnet (2010), which were carefully tailored to specific targets, also infected other systems world-wide.
- Collateral effects such as WannaCry or NotPetya (both 2017) are habitual in cyber conflicts.
- No one can realistically estimate where else a certain system configuration is in use.

Active Cyber Defense Certainty Act (ACDC)

S4Lab



The proposed legislation (whose full text can be found at the bottom of the story) would amend an existing US law, the Computer Fraud and Abuse Act (CFAA), to let firms and individuals hack back to locate persistent attackers. They would also be able to monitor the hackers' systems and disrupt their operations.

4. The bill would inevitably lead to damaging reprisals

The draft legislation says those who hack back should try hard not to escalate hostilities. But hackers aren't going to take attacks on their own systems lightly. Having already found chinks in victims' digital defenses, they might well exploit more of them if provoked.

5. Private companies could find themselves confronting nation-states

Countries like North Korea, Russia, and Iran are thought to be behind some of the biggest cyberthreats facing businesses today. It certainly would not be advisable for a single company to take them on.

Computing / Cybersecurity

Five reasons “hacking back” is a recipe for cybersecurity chaos

A new US bill would make it legal for private companies to chase hackers across the internet. It's a terrible idea that simply will not die.

by **Martin Giles**

June 21, 2019

Avoiding a World War Web

- Parallel efforts by private and governmental sectors, Examples:
 - “Cybersecurity Tech Accord” -> 34 company ,2017
 - Siemens -> May 2018, “Charter of Trust”



[Image:<https://www.widgit.com/>]

Supporters of the Paris Call are therefore committed to working together to:

- > Protect critical individuals and infrastructures from malicious cyber activities;
- > Protect the availability and integrity of the Internet;
- > Prevent interference aimed at undermining electoral processes;
- > Defend intellectual property from cyber threats;
- > Prevent the proliferation of malicious software and practices;
- > Strengthen the security of digital products and processes;
- > Improve cyber hygiene for all;
- > **Prevent non-state actors, including the private sector, from hacking-back;**
- > Strengthen international norms of responsible behaviour and confidence-building measures.

QA