# The Dimension of the Challenge: The Hacked World Order

Magdalena Adamczyk, Patryk Gałczyński, Piotr Gawryś, Dominik Katszer, Konrad Najder, Mateusz Nowotyński

11.05.2018

# Agenda

1. Year Zero – Piotr Gawryś
2. World order today – Mateusz Nowotyński
3. The pervasive influence of Cyber Conflicts – Magdalena Adamczyk
4. Cyber Power Anatomy – Patryk Gałczyński
5. The Sources of Cyber Power – Dominik Katszer
6. The New International Order – Konrad Najder

# Year Zero

1. approx. 75% of the world's population has access to mobile phones.
2. approx. 2.7 billion people are connected through the Internet.

# Year Zero

Is it outside any supervision?

# Year Zero

1. June 2012 - June 2013 – Year Zero in the battle over cyberspace.
2. Many cyber attacks and information theft made public.

# Year Zero

USA and Israel were trying to stop Iran's nuclear program for many years using tools such as:

1. Diplomatic pressure.
2. Financial sanctions.
3. Assasinations.
4. ...and cyberattacks.

# Year Zero

USA and Israel were trying to stop Iran's nuclear program for many years using tools such as:

1. Diplomatic pressure.
2. Financial sanctions.
3. Assasinations.
4. ...and cyberattacks.

# Stuxnet malware

In June 2012, US officials leaked details of a computer attack on Iran's nuclear program using **Stuxnet** malware.

# Stuxnet malware

1. Aimed to speed up and slow down motors in Iranian machines used for enriching uranium to cause malfunctions.
2. Provided false feedback to avoid suspecting cyber attack.
3. Very sophisticated – used five "zero days".
4. Configured only to work on very specific machines.

# Stuxnet malware

1. Supposedly resulted in about 1000 destroyed machines.
2. Some say it could set back Iran's nuclear program up to 2 years.
3. Other say it actually helped Iran because Iranian scientists apart from fixing the issues also introduced improvements in performance.

# Stuxnet malware consequences

1. Strategic turn in use of cyber attacks – not only stealing or corrupting the data but also affecting actual physical equipement.
2. Large amount of funding committed to developing cyber capabilities.

# Iran's counterattack

1. Iran declared intent to develop cyber forces.
2. Between September 2012 and June 2013, an activist group called Izz ad-Din al-Qassam Cyber Fighters took credit for roughly two hundred DDoS attacks on USA's financial institutions.
3. In August 2012, the Shamoon malware struck Saudi Aramco, Riyadh's state oil giant corrupting thousands of hard drives. Responsibility was claimed by Cutting Sword of Justice.

# Iran's counterattack - Shamoon malware

Attacking big oil and gas suppliers was big escalation of the cyber threat.

# Meanwhile in China...

1. Massive cyber theft campaign against USA companies.
2. Stealing secrets from weapon programs, financial institutions, media centers...
3. Stolen information estimated to $250 billion and another $114 billion in related expenses.

# Summit in California

In June 2013, USA's Presient Barack Obama and China's top leader Xi Jinping met in California to talk about Chinese attacks.

# Year Zero culmination

Two day's before Summit in California, Edward Snowden's first leaks went public exposing USA spying on its own citizens.

# Year Zero culmination

"They demonstrate that the United States, which has long been trying to play innocent as a victim of cyber-attacks, has turned out to be the biggest villain in our age" – China's Xinhua news agency

# Lack of borders

In current cyber age there are almost no borders. In oppose to the beginning of Cold War physical distance and obstacles make no difference. Any country can attack, using the Internet, their neighbor or country on another side of the globe.

# Uncountable power

Conventional power was quite easy to calculate. It could be represented as GDP and military spending. Currently, we don't know what creates main economical power. Whats more unlike conventional weapons, like tanks, planes, missiles etc., cyber weapons cannot be counted.

# Global access

1. Only a few countries were able to build a nuclear bomb and even today only a few possess it.
2. Almost every country or even some individuals can perform digital assault.

# Lack of self-stabilization

1. During Cold War, attacker identity will be known and counter-attack will be performed before launched missile will land, a rule known as "whoever shoots first, dies second".
2. Origin of cyber attacks is hard to detect. What's more once used cyber weapon becomes obsolete so there is pressure to use it or it may be neutralized and useless

# Risk of spreading

Cyber weapons once used can be evaluated and repurposed and used by others. For example, Stuxnet malware is now available to download by almost everyone

# Unpredictable route of attack

Since in conventional war geographical features performed big role there were only a few possible routes of attack, but cyber attack may be performed from any place. What's more attacker can easily hide their identity or even conduct "false flag" attack that is designed to look like it was performed by someone else.

# Evolution of malware

Even if malware was at first created to perform one task usually it can be remotely updated to do something completely different

# Government or criminals

Tracking source of attack with precision to the country is hard on its own, but it's even harder to discover if attack was executed by some criminals or government of given country.

# The pervasive influence of Cyber Conflicts

1. New meaning of the word war
2. Space between war and peace
3. April 2013, SEA attack

# Division between the public and the private

What is the government's responsibility and what remains the responsibility of companies? Does such a division exist?

# Source of cyber power

Why Israel has more companies listed on the NASDAQ than any country outside the United States?
Private-sector, government, and universities cooperate!

# America's soft power

"Ability to influence and attract through ideas, institutions, and culture rather than to coerce through force"

Tech-companies are trying to have a more personal contact with the client following every aspect of the user's life.

# Digital sovereignty

Refers to the twentieth century version of state control.
The old world is trying to embrace the virtual world with its laws.
"de-Americanization of the Internet"

# Surveillance society

By whom we are under surveillance
- Government
- Hackers
- Corporations

...and why it is getting worse
- Greater possibilities of collecting and storing information

# What is Cyber Power?

# Conventional war analogies

1. Guns, nukes?
2. Critical infrastructure?
3. Borders?
4. Crowd control?
5. Amount of malware?
6. Hardware?
7. Server location?
8. Limiting information?

# Cyber Power

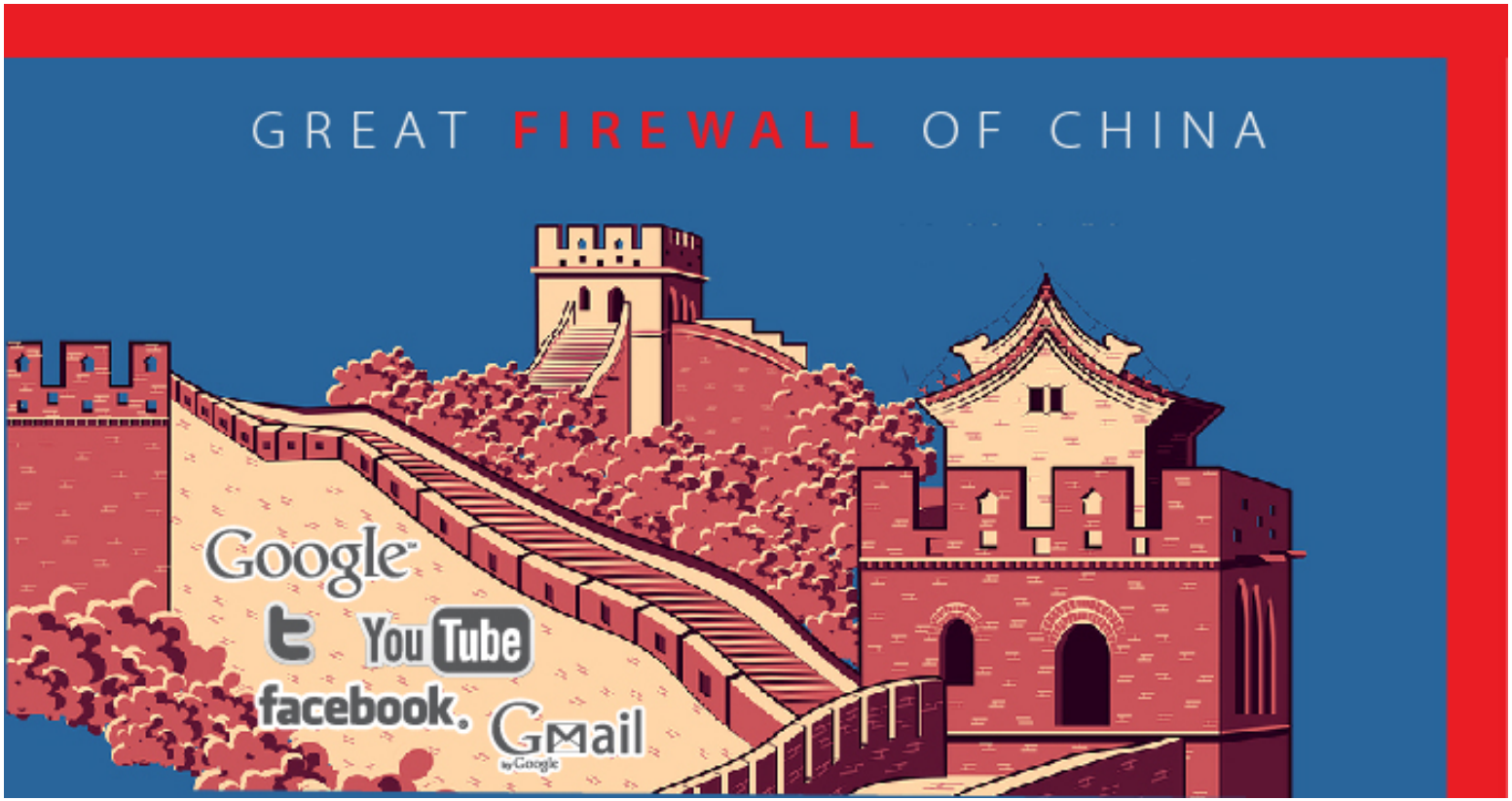
It (cyberspace) offers **all actors** speed and reach, anonymity and protection, and the ability to create and participate in virtual economies and wield cyber weapons, all with a low buy-in cost. This **drastically alters the power equation**. - *The anatomy of a cyber power, Jill Rowland, Mason Rice, Sujeet Shenoi*

# In the hacked world order, new strategic cultures of cyber power are emerging.

Some see cyber attacks as a limited tool to use carefully; others view them as a much broader political weapon to wield against a range of adversaries.

# Back to China again - border and access to information

# Back to China again - border and access to information



# Back to China again - firepower

https://github.com/greatfire/wiki

# Back to China again - firepower

## Large Scale DDoS Attack on github.com

Mar 27, 2015 jnewland Engineering

We are currently experiencing the largest DDoS (distributed denial of service) attack in github.com's history. The attack began around 2AM UTC on Thursday, March 26, and involves a wide combination of attack vectors. These include every vector we've seen in previous attacks as well as some sophisticated new techniques that use the web browsers of unsuspecting, uninvolved people to flood github.com with high levels of traffic. Based

**GitHub Status**
@githubstatus

After 113 hours of sustained DDoS attacks our defenses are holding. We will keep our status at yellow until the threat has subsided.

9:32 PM - Mar 30, 2015

368 587 people are talking about this

I can't change who you are but I have the power to choose my friends

One person's Internet freedom is another's Internet imperialism.

Join us in building up a peaceful, safe, and open and co-operative cyberspace.

*Lu Wei - Head of Internet Information Office*

# Cyber meaning

- Definition
  Term was introduced as a Greek transaltion which means governing or stering, however currently it has a lot of definitions depending on context.
- Daily life
  The internet is everywhere, everything is getting more smart and barier between offline and online life disappears

# Cyber layers

- Hardware
  Each hardware like e.g. router, cables gives a control of data flow through internet.
- Software
  Every kind of malware and even subsidizing operating systems and search engines like Google
- Fake social account
  It can be easily used for spreading disinformation. Nowadays it is hard to distiguish true facts from fake or blured news.

# Components of cyber power

- Size
- Shared mission and private sector
- Adventurous and inventive military and intelligence agencies
- Attractive narrative of cyberspace

## Size

How would your life look like without Google or Facebook ?

# Size

- The more hardware (phones, serwers, routers) state produce the better. It makes customer addicted to specific company or state.
- Currently US dominates internet economy.
- Worth to remember that the more your country is active in the internet the more influence it exerts on foreign companies and governance.
- sophisticated technology is also a source of vulnerability, everything can be a target of cyberattack.

# Size

Example of hardware dominating:

Data passed via internet is mainly passed by US for example email from Brazil to Peru can be transported through California, so they can take advantage of this fact.

# Shared mission and private sector

**Relationship between government and private sector**

- State secure technology company through law, money , idealogy etc
- State can even cooperate with foreign parters and enforce some regulations abroad.
- In return they got antyviruses, technological development and data.

# Shared mission and private sector

"Surveillance is the business model of the Internet." - Google, Facebook, Twitter collect personal data, mails etc. we think that everything is free but it is wrong, we pay with our personal data then they e.g .can personalize adverts .

Nowadays most of companies try to collect as much data as possible , and this is the reason why big data field in computer sciencie is still growing up.

# Shared mission and private sector

**National cybersecurity has to be a shared mission** - *Barack Obama*

He said that because a lot of critical infrastructures are in private sector where he dont have direct access. Government and private sector are interdependenced.

If governance want to harness the energy and innovation of the private sector then they are making business abroad.

# Military and intelligence agencies

- Making real impact which does not only rely on breaking into machine, is not easy.
- US spends three to four times more on cyber offense than it does on defense.
- What is more, the more intense the military competition, the more rapid the innovation and development will be.

We don't have to look far for surveillance example. Facebook, Tweeter, FBI, CIA. Different between social media and organisations like CIA is about how they get data. In social media we give them freely.

## Military and intelligence agencies

How sophisticated surveillance or cyberattack can be ?

# Military and intelligence agencies

Everything is possible if you have enough budget, time and specialists.

*"any sufficiently advanced technology is indistinguishable from magic"* – Arthur C. Clarke

# Attractive narrative of cyberspace

It is very important, because in that way government is convincing users to itself.

US :
United States will work toward an “open,interoperable, secure, and reliable information and communications infrastructure.” which is a bit hypocritical because of how US is engaged in extensive surveillance. US tryes to have one global network which can be controlled by them.

# Attractive narrative of cyberspace

China:
China is not of an open global platfrom but rather of one fragmented bynational jurisdictions and regulations. They even use technology for inspection of internet content by checking send packages. examines the content of the messages, scanning for sensitive key words and blocking access to sites

Europe:
Privacy as a fundamental right has translated into widely copied trade policies and regulatory models. promote the protection of online rights.

# True Cyber Superpowers

- China and the United States are the only true cyber superpowers which managed to put all four of the building blocks together.
- Russia is almost there without one block. They lose the competition in producing technologies and services which are shaping cyberspace.
- Other countries also are significant in the this field, however they are more restraint.
- There also exists states which citizens have doesnt have free access to the internet so surveillance is limited. Some countries also are not very well technologically developed so they are at the end of rate.

# Which country has the best hackers ?

# Cyberspace usage motivations

While Cyberspace is hard to compare to anything we've seen before, we can outline state's motivations:

- increase access to information and communication technologies to spark economic growth,
- protect their own information assets and citizens...
- but at the same time exploit and damage those of other countries,
- access the data of their own citizens for intelligence and law enforcement.

# Cyberspace usage classification

Each state has a different road to reach its desires.
Five fundamental questions determine the culture of country's user of cyber power, how a nation-state:

1. interprets threats,
2. uses force,
3. exerts influence,
4. spurs innovation,
5. delineates the national good.

# Internal and External Hazards

**What is the balance between internal and external threats?**
Both the liberal democracies and authoritarian states collect data to prevent terrorist attack (external), but authoritarian regimes collect much more data about their own citizens.

- USA advocates for open internet, argumenting that societies get stronger the freer information flows,
- China sees controlling information as a primary security concern,
- Russia is trying to remove Western influence from the Web.

# Disruption and Destruction

**How do you use force and military power in cyberspace?**

- what happens in cyberspace is mostly out of the sight of the public
- offense in cyberspace is considered the best defense

The USA uses cyberattacks in two different ways:

- surgical and precise, like Stuxnet, requiring much preparation and military intelligence,
- small attacks, like stealing data from a company, DDoS attack on country's banks.

# Space between

*"You have diplomacy, economic sanctions... and then you have military action. In between there's this space, right? In cyber, there are a lot of things that you can do in that space between that can help us accomplish the national interest."* – Eric Rosenbash, Assistant Secretary of Defence

# Diplomats and Trolls

**How to excert influence in the digital age?**

- digital age brought more public diplomacy,
- "war of narratives" on social media, and on the internet in general,
- flooding the internet with disinformation and propaganda.

# Silicon Valley, Beijing and Brussels

**What model of technological competition is best adapted for the future?**

Based on Sillicon Valley, Beijing and Brussels models

# Silicon Valley

- innovation and entrepreneurship
- highly focued on private sector
- hoping on being the most competitive

# Beijing

- government controlling long-term goals
- minimizing dependence on foreign technology

# Brussels

- more managerial than Silicon Valley, and less interventionalist than the Beijing one
- protecting privacy, managing inequality, promoting social welfare
- regulation to the market, using the gravity of the European market to shape technological trajectories.

# The social contract

**What is the balance between individual rights and state interests in the digital age?**

- highly debated topic nowadays, with individual's right to privacy,
- every society is confronting the question of what to do with the massive amounts of data,
- in liberal democracies the access to data by the state is considerable, but limited,
- authoritarian states mostly see their citizens data as tool to use for their advantage.

# Conclusion

## Conclusion