Introduction to cyberwarfare: a crash course

and why is this relevant?

Hack.LU, Luxembourg, 2023

Lukasz Olejnik, PhD

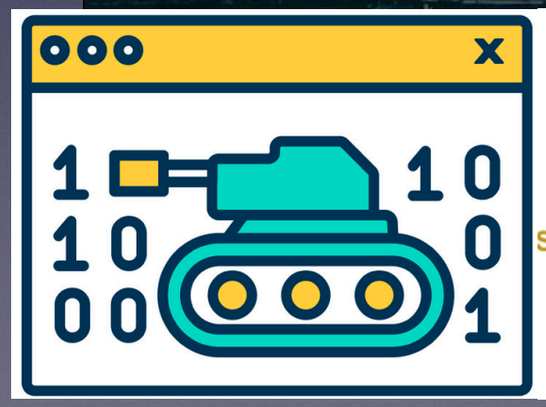
Who am I?

- Security and privacy research (independent)
- Consultant. Advisor.
- PhD, INRIA (France).
- Strategic tech communication.
- Technology & technology policy
- Former advisor on cyberwarfare at International Committee of the Red Cross
- Author of papers, reports.
- Book “Philosophy of Cybersecurity”

@lukOlejnik
@LukaszOlejnik@Mastodon.Social
blog.lukaszolejnik.com
lukaszolejnik.com
me@lukaszolejnik.com

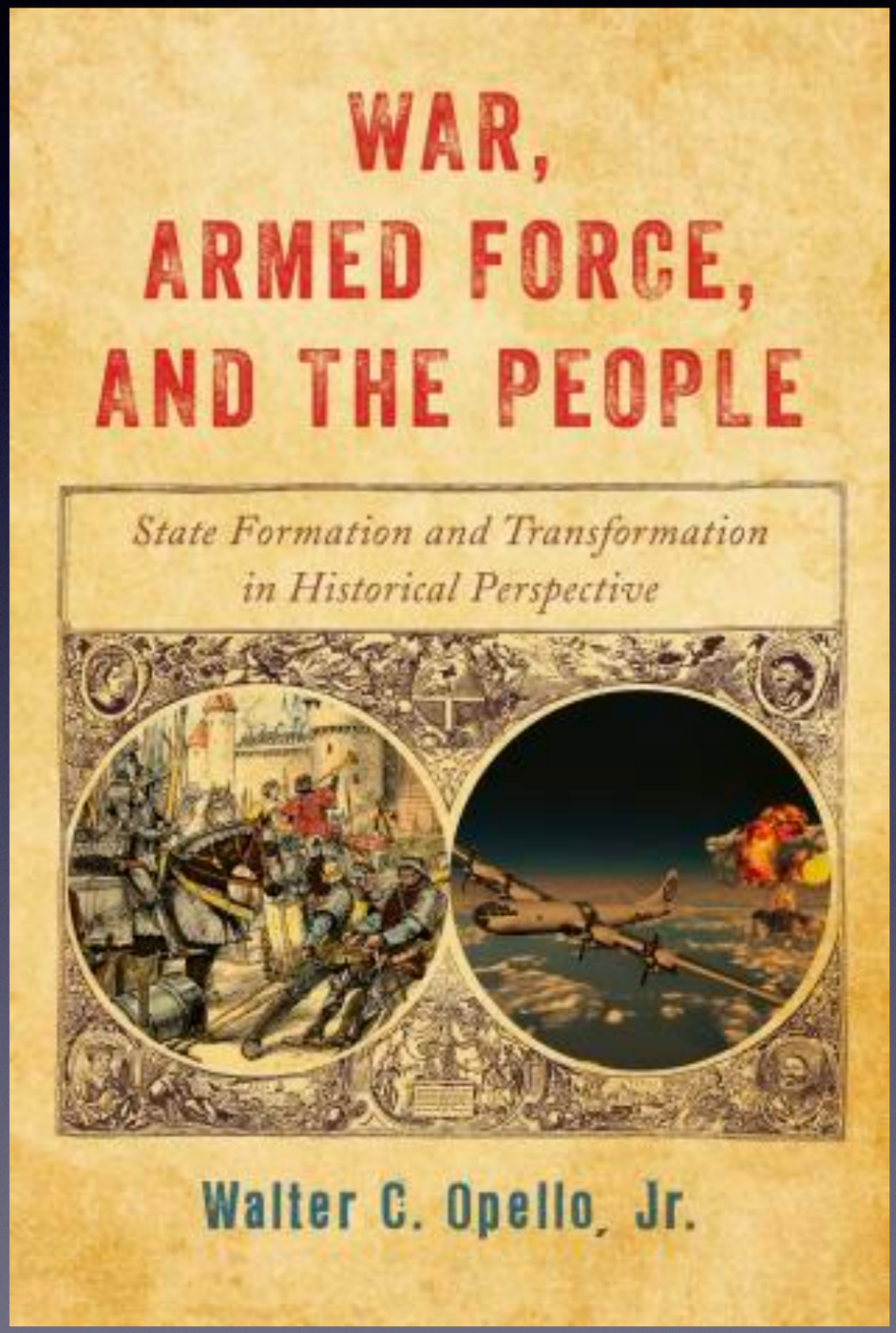
Facts vs Fiction
How to understand “Cyberwarfare”?

- War only “in, over, internet, and with cyber tools”?
  - **NO**: not realistic, wars happen in multiple domains
- **Cyber capabilities integrated with other tools and activities in other domains? THIS.**
  - Operations can be limited to “cyber”
  - Fully-fledged conflicts involve many domains **including cyber**



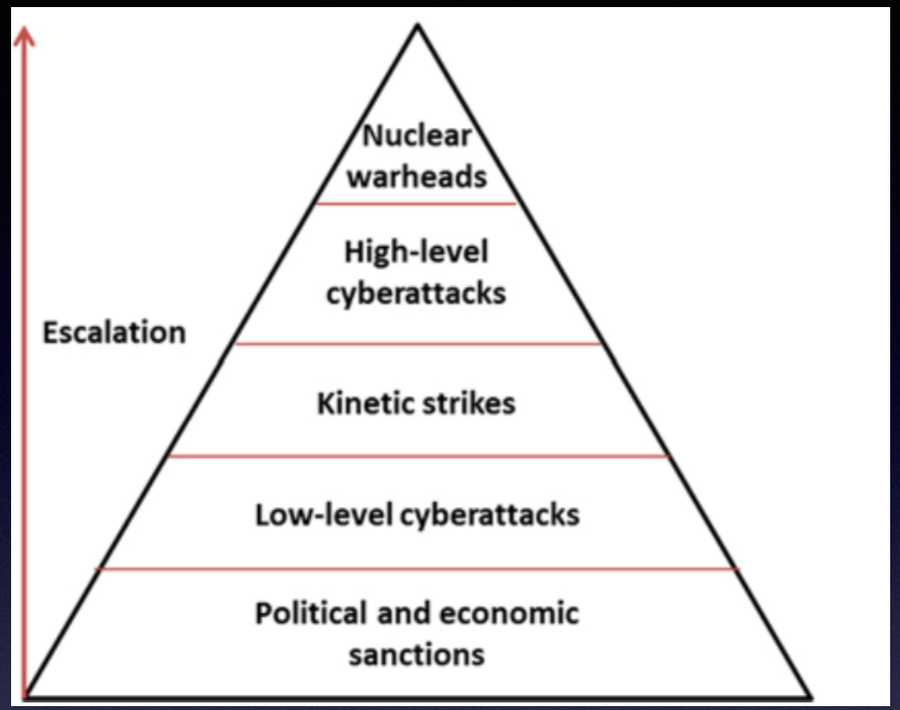
Cyber as "**use of force**"?

- article 2(4) of UN Charter:
  - *All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state …*
    - *Except when authorised or in self-defence*
- Cyberattack can be a "**use of force**" (~war). Effects count:
  1. **Physical destruction, killings. intentional**
  2. Attributed to a State (v. important)
- Almost none so far (since 2000).
- High intensity = "armed aggression" (war)



Surprise! Cyberattack is not an *attack*

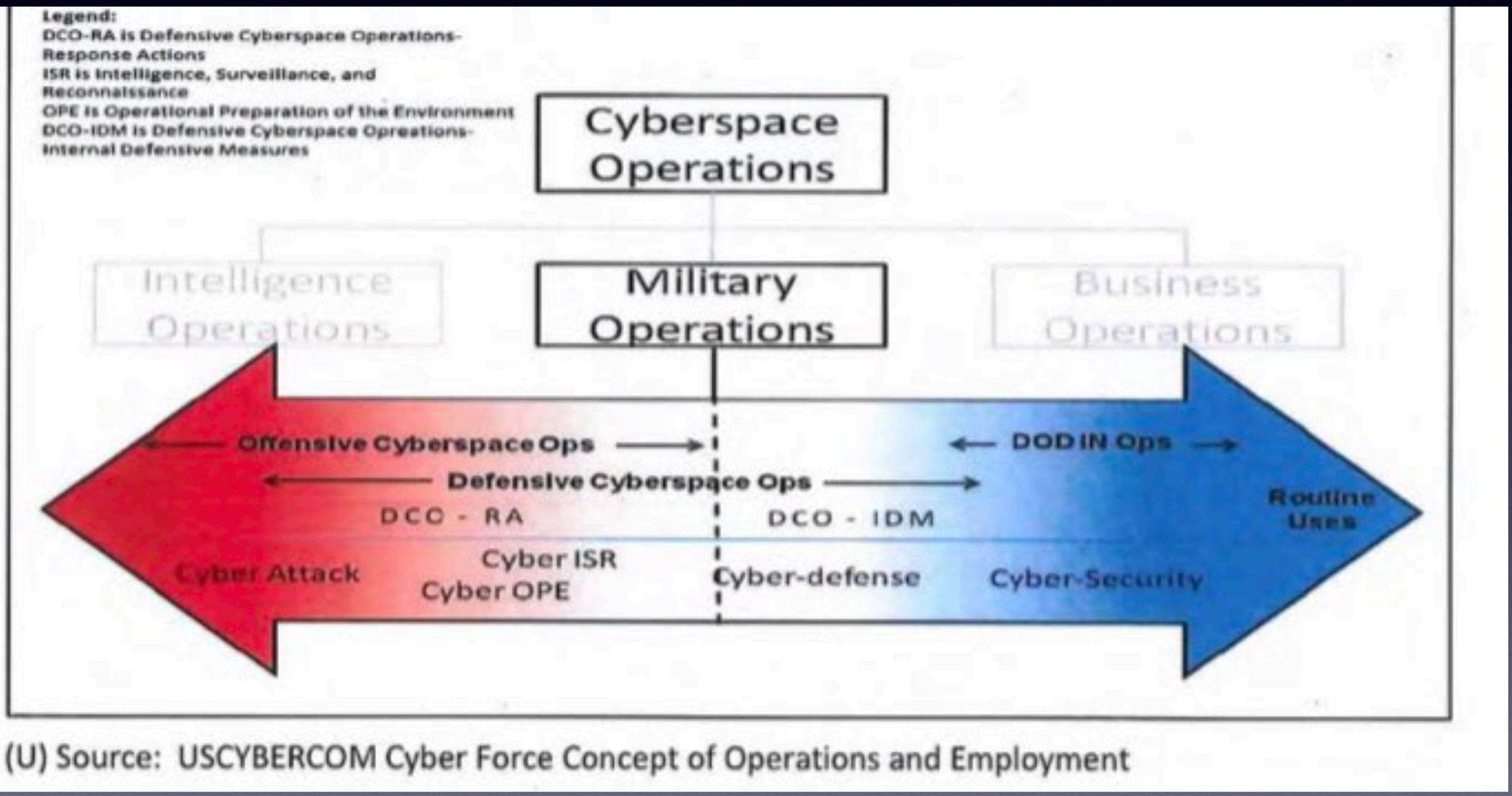
- "Attack" term not often used in international law
- UN Charter art. 51 ("*armed attack*").
  - Attacks only possible in self-defence
  - "*type of weapon used* ***immaterial*** *to the application of Articles 2(4) and 51*" (ICJ). CYBER COUNTS.
- Geneva Conventions, Additional Protocol I.
  - some lawful, others not



Article 49 — Definition of attacks and scope of application

1. "Attacks" means acts of violence against the adversary, whether in offence or in defence.

Avoid the term "*cyberattack*"!
Better: **cyber operations.**



(U) Source: USCYBERCOM Cyber Force Concept of Operations and Employment

DCO - defensive. **OCO** - offensive. **ISR** - intelligence/reconnaissance.

Some international law "rules"

- **Example theoretical cyber norm during peacetime**: do not attack CERTs.
- **Example practice during war**: *Russian army coerces telecommunication operator employee to give access to infrastructure*
- **Cyber norms not applicable during wartime?**

42. With regard to this norm, ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public can have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population, and can be escalatory, possibly leading to conflict.

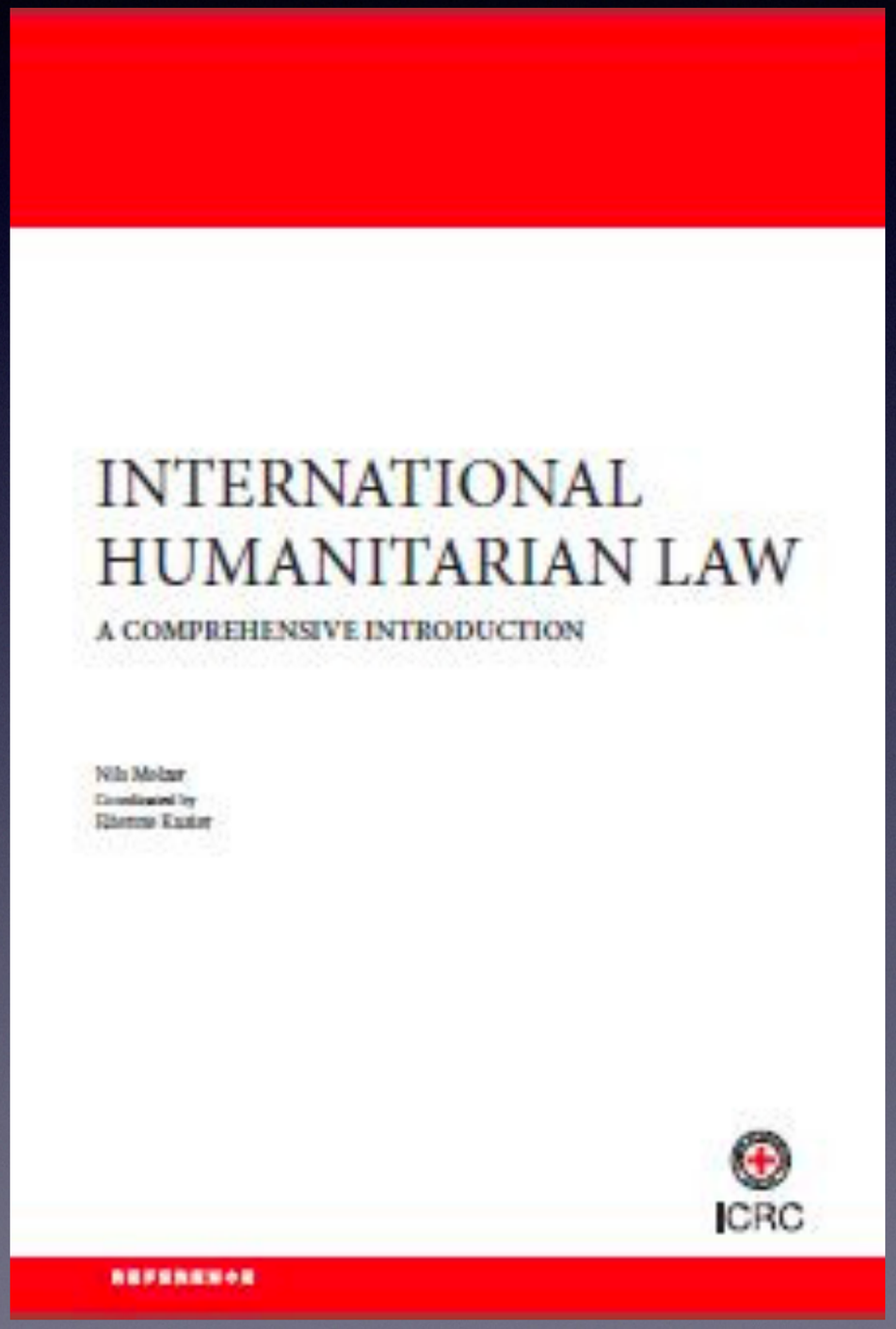
43. This norm also points to the fundamental importance of critical infrastructure as a national asset since these infrastructures form the backbone of a society's vital functions, services and activities. If these were to be significantly impaired or damaged, the human costs as well as the impact on a State's economy, development, political and social functioning and national security could be substantial.

Norm 13 (c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

29. This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate

Laws of Armed Conflict applicable to cyberwarfare

- Distinction. Proportionality and precaution.
  - Sparing civilian targets (people/objects)
  - Assessing legality of tools
- Practice during war
  - **Cyber operations vs civilian targets** in Ukraine and in Russia.
  - Cyber activities **by** civilians.
- None of them reach “attack”-level. (*Except Viasat?*)



So, cyberwarfare…?

- ICT/digital tools **to achieve effects**
- Effects **in IT**/“cyber”/internet
- **In support** of information operations
- **In support of other units** (combined arms,special ops, electronic warfare, land like tanks, etc…)

- In Ukraine cyberwarfare, **not seen**:
  - “blowing up stuff”
  - “killing with cyberattacks”
  - “paralysing critical infrastructure”
  - “hacking weapons systems”
- *Cyberwarfare vs CYBERFIREWORKS*.
- Forget about Cyber Pearl Harbor, Cyber 9/11, etc… Useless.

Reports of lethal effects of cyberattacks?

- Cybersecurity in healthcare a *life and death* issue.
- Establishing causality is **difficult**.
- German hospital case (2020)
  - **Refuted:** Ransomware infection in hospital systems did not cause person's death.
- American hospital case (2021), similarly.
- Security breaches at hospital/medical facilities linked with increased mortality.
  - Increased security adds friction in the use of IT systems.
  - Stretch: does not mean that cyberattacks kill

> In anesthesiology, the absence of medical records "put lives at risk," said Jeffrey Planchard, an anesthesiologist who worked at Springhill during the outage and now works at Mount Sinai Hospital in Chicago. "Having access to previous anesthesiology records is crucial. What kind of airway are you looking at? What kind of allergies that they may or may not remember?" he said.
>
> The hospital didn't say anything about an attack at first, saying instead, in response to an

> Time from door to ECG significantly increased after a breach and the elevated time to ECG persisted at 4 years after the breach. Security typically adds inconvenience by design—making it more inconvenient for the adversary. For example, stricter authentication methods, such as passwords with two-factor authentication, are additional steps that slow down workflow in exchange for added security. Lost passwords and account lockouts are nuisances that may disrupt workflow. The persistence in the longer time to ECG suggests a permanent increase in time requirement due to stronger security measures.

Choi et al/2019

> It is submitted that all operations expected to cause death, injury or physical damage constitute attacks, including when such harm is due to the foreseeable indirect or reverberating effects of an attack, such as the death of patients in intensive-care units caused by a cyber attack against the electricity network that then cuts the hospital electricity supply.

ICRC report/2019

But **could** cyberattacks kill?

- Yes.
- Risk to implants, pacemakers?
- Secondary or tertiary effect.
  - E.g. following some explosion?
- Chemical/water poisoning?
  - Would violate Chemical Convention.

3. RISK EVALUATION

Successful exploitation of these vulnerabilities may allow an attacker with adjacent short-range access to one of the affected products to interfere with, generate, modify, or intercept the radio frequency (RF) communication of the Medtronic proprietary Conexus telemetry system, potentially impacting product functionality and/or allowing access to transmitted sensitive data. Successful exploitation requires: (1) an RF device capable of transmitting or receiving Conexus telemetry communication, such as a monitor, programmer, or software-defined radio (SDR); (2) to have adjacent short-range access to the affected products; and (3) for the products to be in states where the RF functionality is active. Before the device implant procedure and during follow-up clinic visits, the Conexus telemetry sessions require initiation by an inductive protocol. Outside of these use environments, the RF radio in the affected implanted device is enabled for brief periods of time to support scheduled follow-up transmissions and other operational and safety notifications. The result of successful exploitation of these vulnerabilities may include the ability to read and write any valid memory location on the affected implanted device and therefore impact the intended function of the device.

2. "Toxic Chemical" means:

Any chemical which through its chemical action on life processes can cause death, temporary incapacitation or permanent harm to humans or animals. This includes all such chemicals, regardless of their origin or of their method of production, and regardless of whether they are produced in facilities, in munitions or elsewhere. (For the purpose of implementing this Convention, toxic chemicals which have been identified for the application of verification measures are listed in Schedules contained in the Annex on Chemicals.)

Chemical Weapons Convention, Article 2(2)

Cases that are **not** cyberwarfare

- US allegedly engaged a Russian target ("Troll Farm"/FNA) around 2018?
- RU Federal News Agency:
  - *"On November 5, 2018 at about 22:00 Moscow time, the RAID controller of the internal office was destroyed and two out of four hard drives were disabled. The hard drives on servers in Sweden and Estonia were formatted."*
- Dutch intelligence operators hacked into APT29, have seen it launch cyberoperations aimed at US elections, and also linked it to the SVR?
- Russian SVR hacked Dutch police systems. In context of investigating the shooting down of MH17 plane.

- Cyber/info ops in US (2016) and French (2017) elections.
- Alleged China-linked group APT31 conducting cyber operations vs Russian targets.
- Alleged Indian cyberattacks vs Chinese targets. Also Chinese vs Indian.
- Supply-chain compromise of Solarwinds in US, reaching many targets.

Ukraine war and cyberwarfare.

Multiple targets: State systems, critical infrastructure, databases, etc…

Many novel events. Some examples **that stand out**.

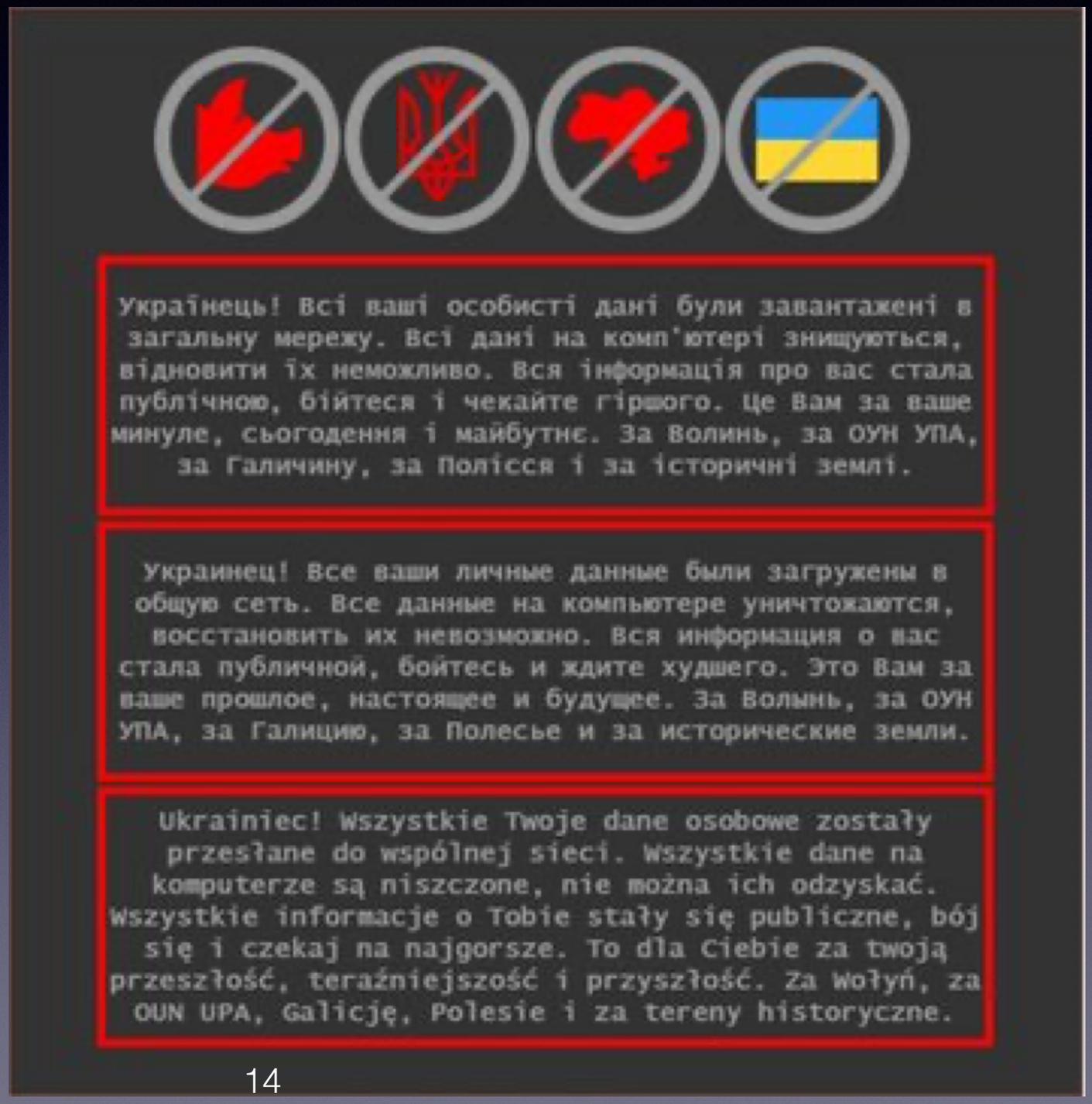
Practice goes **contrary to some** analysts expectations'.

All in line with definitions/considerations of this talk.

Prelude to Russian war in Ukraine happened over cyber

Russian Cyber ops **prepared** since 2021

Important cyber-enabled InfoOp launched January/2022

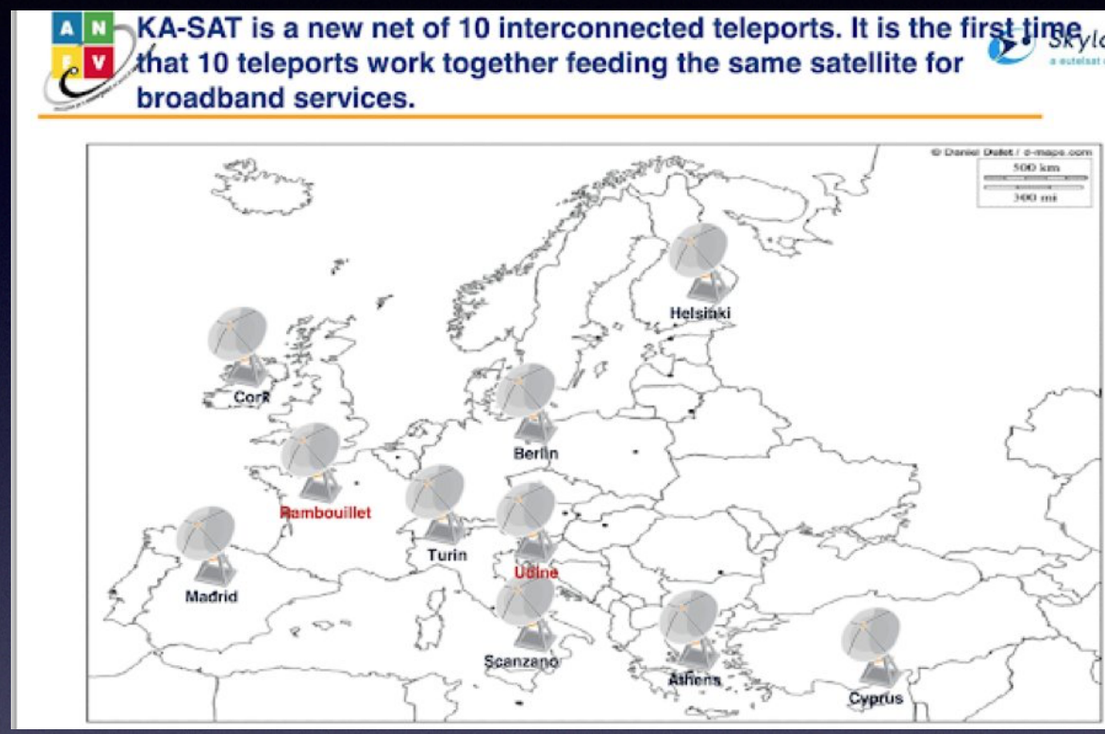


Cyber in Russian war in Ukraine

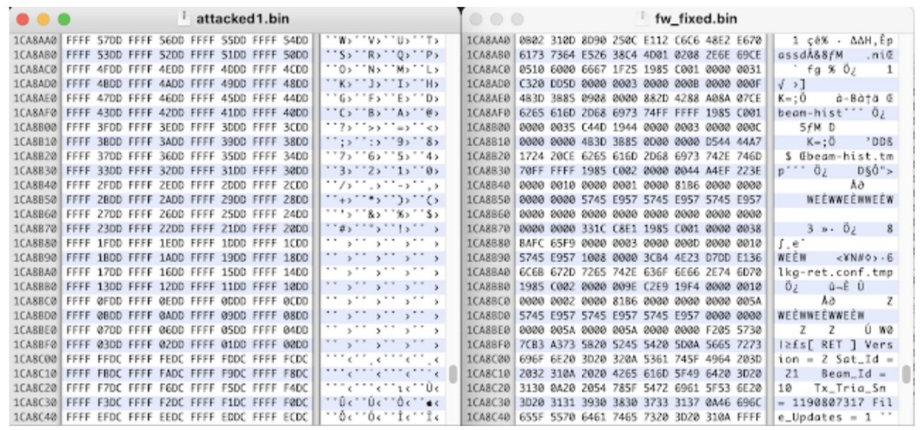
- Wipers, DDoS. Whatever.
- **Russia side**
  - Hacking UA government systems/businesses
  - Information operations (on the cheap)
  - Changing internal regulations.
- **Ukraine side** (by who?):
  - **defence**,
  - setting up working information operations activity, “IT Army”(?), making data of local operatives public, making public data of RU soldiers, publicising pictures of soldiers, etc.
    - Hacked UA smartphone devices
    - Moving data outside the country.
- **3rd-cauntries**:
  - Prestige. Logistical/transportation companies affected (PL/LT/UA)
  - Viasat.

“Typical” cyberwarfare. KA-SAT

- Coincided with a land invasion
- Bricked satellite comms equipment in Europe
    - Affected NATO countries. France (emergency services like firefighting/ ambulance!), Germany (wind turbine controls), Poland, etc.
- AcidRain ('malware designed to wipe modems and routers’). Overwrote firmware with ***0xffffffff***s.
- Affected Ukraine army (users of KA-SAT)
    - Clear example of cyberwarfare activity
    - Ukraine had backup comms channels (resiliency) so no general impact
- EU/UK/US said: this was Russia.



were pretty clear. In the following picture you can see 'attacked1.bin', which belongs to the targeted modem and 'fw_fixed.bin', coming from the modem in working conditions.



A destructive pattern, that corrupted the flash memory rendering the SATCOM modems inoperable, can be observed on the left, confirming what Viasat stated yesterday.

Databases

- Simple stealing data and leaking them may be irrelevant, but…
- Potential aim of cyberwarfare operations on Ukraine?
  - "*extensive details on much of Ukraine's population*".
- Potentially useful to identify/locate Ukrainians likely to "resist"?
  - *"and potentially target them for internment or worse". Tangible gains...*
- Beware of loosing databases with sensitive or **otherwise useful** information
  - For example: registered gun owners?

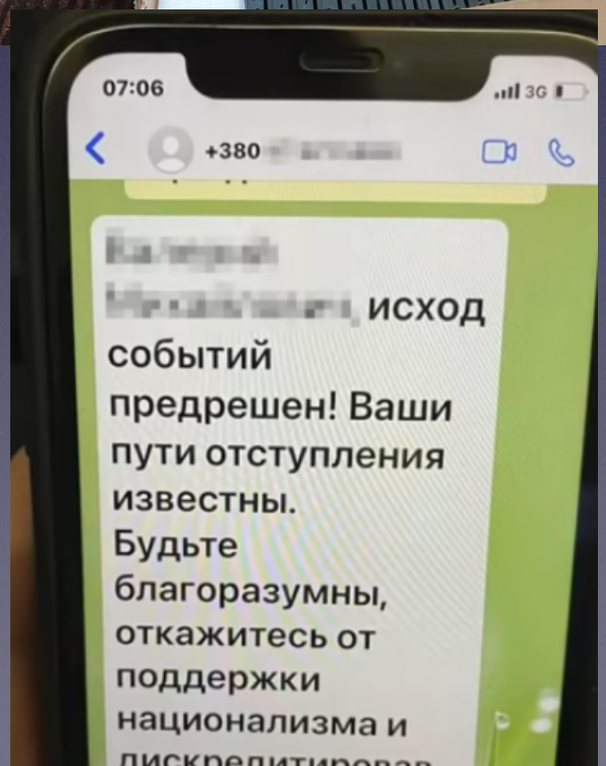
BOSTON (AP) — Russia's relentless digital assaults on Ukraine may have caused less damage than many anticipated. But most of its hacking is focused on a different goal that gets less attention but has chilling potential consequences: data collection.

Ukrainian agencies breached on the eve of the Feb. 24 invasion include the Ministry of Internal Affairs, which oversees the police, national guard and border patrol. A month earlier, a national database of automobile insurance policies was raided during a diversionary cyberattack that defaced Ukrainian websites.

"Make them scared that when the Russians take over, if they don't cooperate, the Russians are going to know who they are, where they are and come after them"

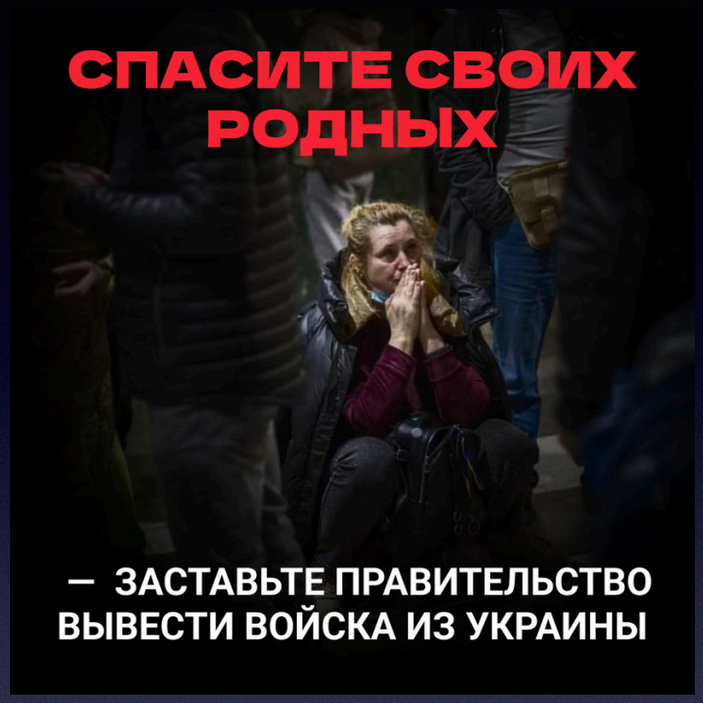
Example disruption of information operations infrastructure

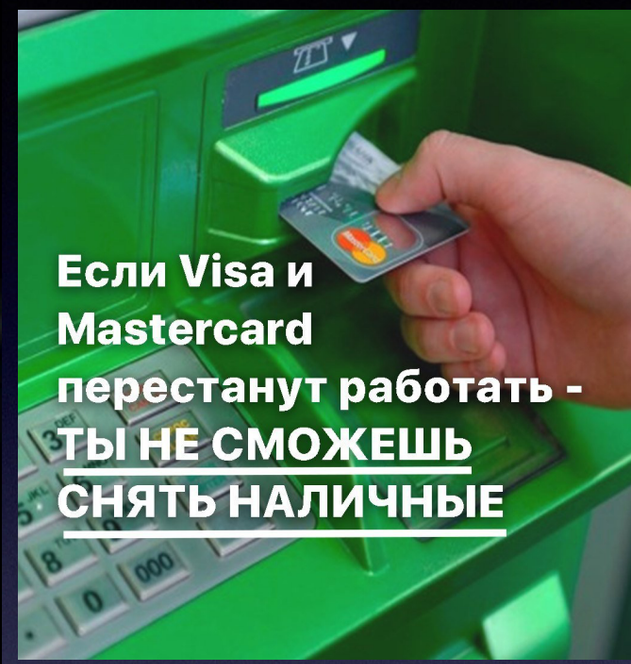
- Operating locally, in Ukraine
  - “*targeted UA military and law enforcement officers through sending SMS with proposals to surrender and defect to the occupiers*”
- Russian bot farms dismantled



Example use of ad networks to bypass Russian info filters

- Someone used ad infrastructures to pierce through the information filter-bubble in Russia
- Information about the war directed/presented/displayed in websites/social networks
- Ultimately, e.g. Google ads became banned by Russian authorities! (“spreading “”lies””).
- New laws for citizens: “15 years in prison for fakes about the actions of the Russian Armed Forces”



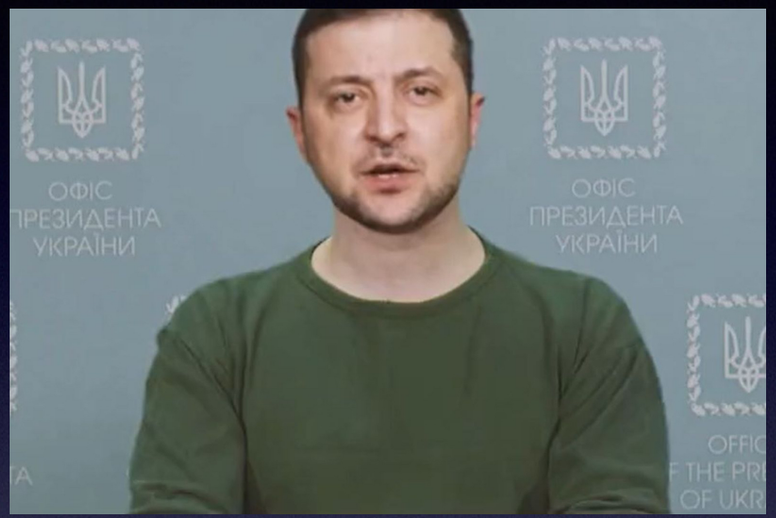


Example attempt to hack energy grid elements

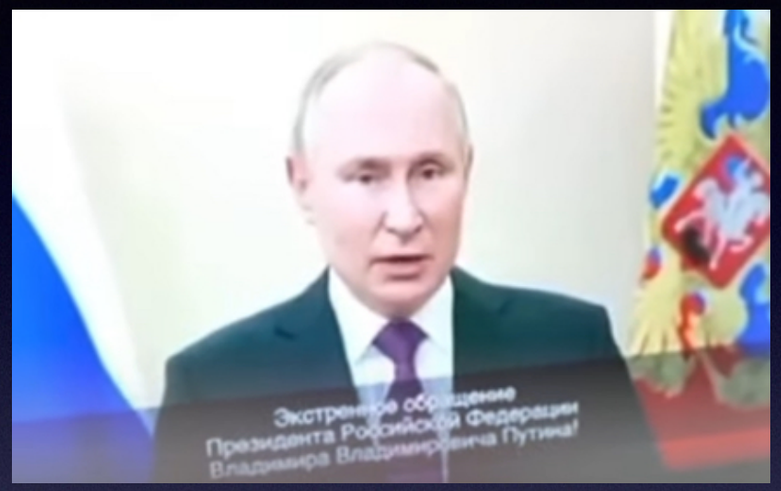
- 9 substations hacked. No impact/effect reached.
- If successful: could be used by offensive propaganda
- was a failure, so: used in defensive/supportive propaganda :)

- We know this only because it was leaked.
- (Kinetic strikes more effective)

Deepfake uses - legal under Geneva Conventions!



- “Zelensky Deepfake”
- Spread early during the war in 2022 on social media. Provenance unclear.
- Synthetic content calling UA soldiers to surrender.
- **Impact: 0**. It only reached some audience because… media covered it. It also excited Western analysts.



- “Putin Deepfake”
- Spread over hacked Russian TV Stations. Provenance unclear.
- Synthetic content announcing war and military drafts
- **Impact: unclear**, seems to be 0, still.
- (But: superior to “Zelensky deepfake” use. Putin’s deepfake disseminated over actual channels to actual viewers)

Beware the Info fog

- We still don’t know a lot. Cyber in the “shadows”. War is ongoing.
- Needs of war propaganda.
- Morale boosting in Ukraine/Russia means that some information may not be given.
    - This is normal.
- We’re in the West so we side with the West, and we accept information as given Ukraine (with some notable exceptions).
    - Again, this is normal.
- Let’s hope that some analysts see the objective picture :-)

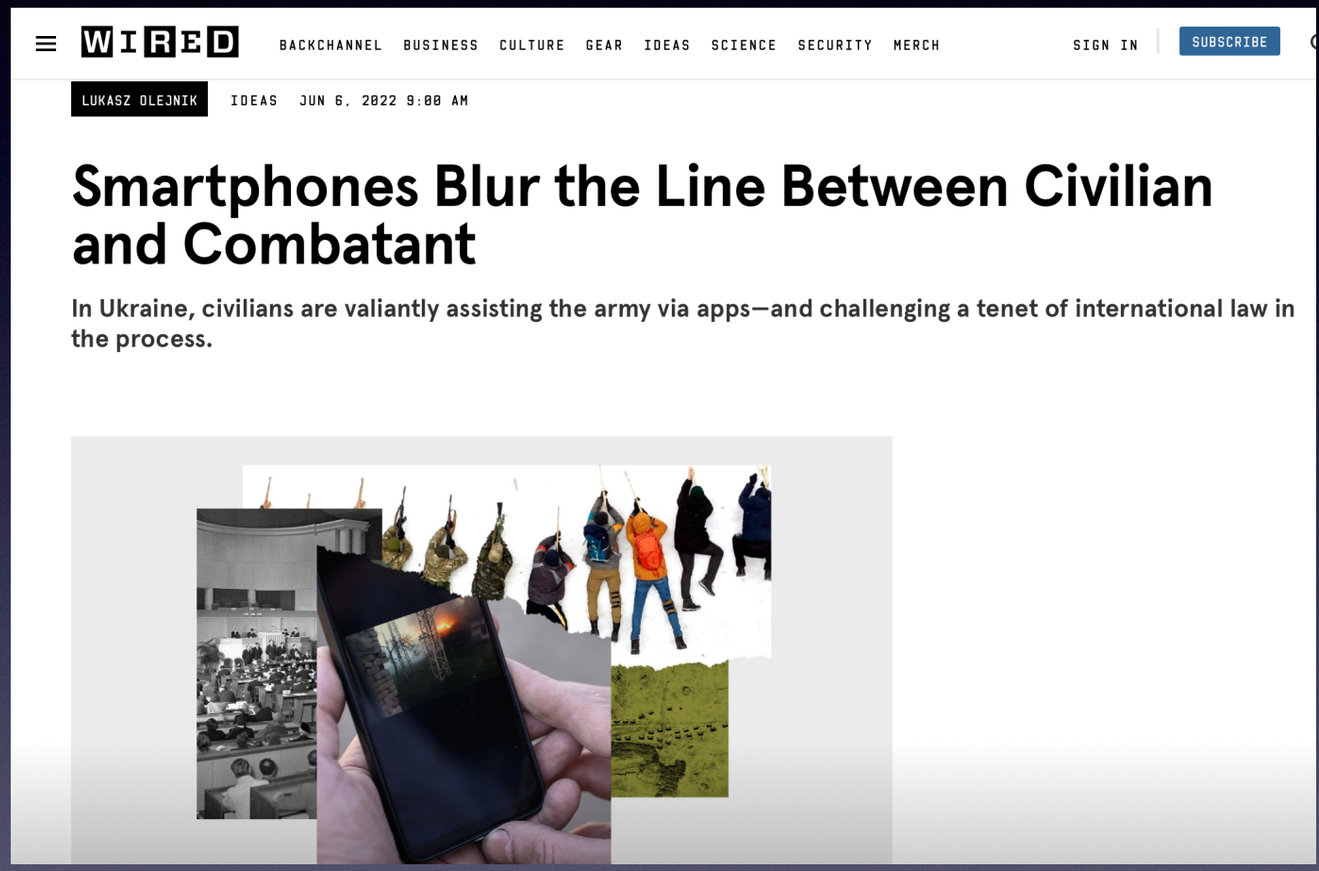
Company Threat Model for unstable times

- **Outside Armed Conflict (AC) zone**
- Basic cybersecurity as usual
- Tighter isolations/etc if having activity in places where AC takes place
- Take care of employees if they’re affected
- Prepare for potential crises (if a country is non-neutral). Prepare for unstable world.
- May be indirectly impacted.

- **Inside AC zone (Ukraine)**
- Basic cybersecurity as usual
- **Full backups in the cloud in non-AC zone.** Of data and infrastructure.
  - Ukraine government: migration to Azure/Amazon
- May be directly impacted.
- What about employees?

What if you’re in warzone.

- Personal safety. Food. Electricity. Backups (to cloud/portable disk). Power bank. Fully charged batteries. Basic cyber hygiene.
- Follow advice of crisis response guides, including by the government.
- If engaging in war-related activities (by using apps, or hacking), make sure you are aware of the stakes,
  - Loosing protected civilian status. Not fun when caught.



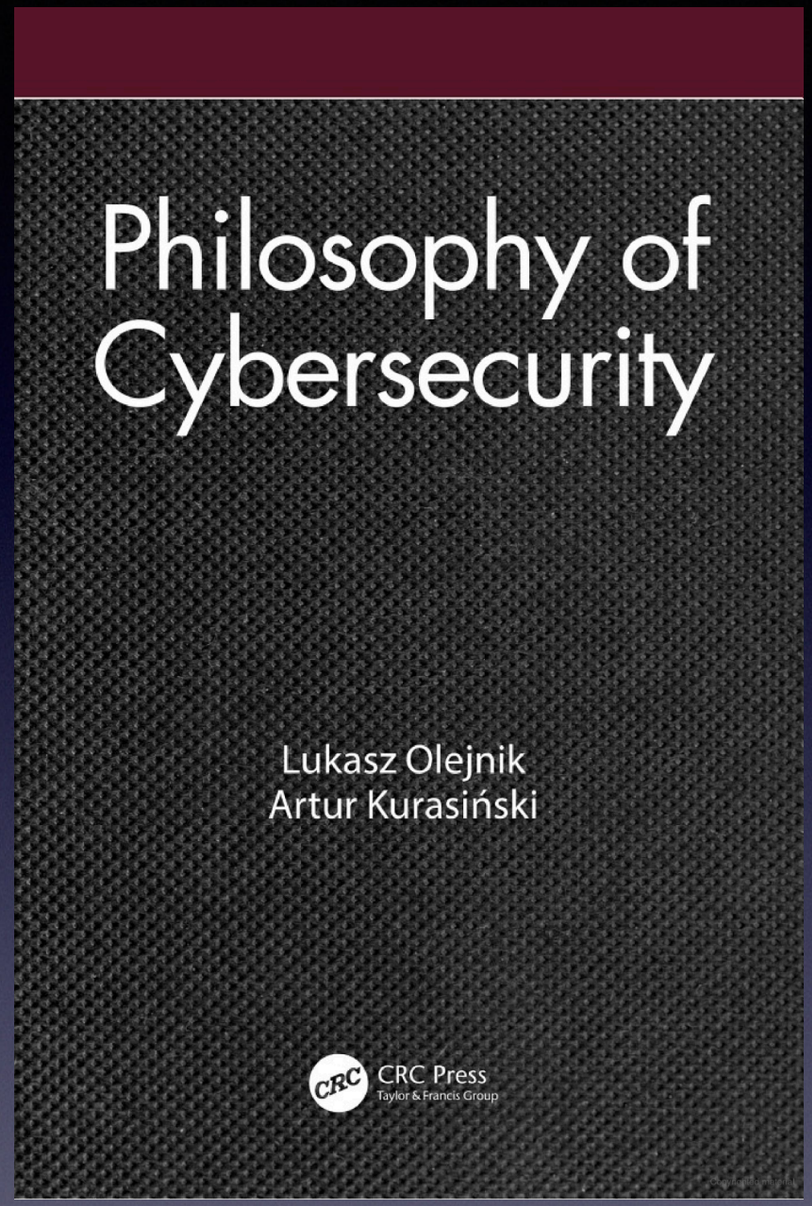
Playing with cyber-fires…

- Case study: user hacking an war side while being **outside** the war zone country
- Likely breaks domestic laws of that user State
  - E.g. hacking Russia while being in EU
  - Prosecution in EU unlikely… But the responsibility is yours.
- Case study: hacking a State at war while being **outside** the warzone…
- Case study: user hacking a State at war while being **inside** the warzone
  - E.g. hacking Russia while being in Ukraine or in Russia
  - Examples of people detained
- Depends if it has a nexus to the war
- If it does, you may be forfeiting protected (i.e. Geneva Conventions) status. Combatants have rights. You would not…

Thank you.

Some take-aways

- Cyberwar in Ukraine will have long-term consequences.
- Cyberwar affects companies and people inside warzone, but may also affect outside.
- Consequences for “Responsible behavior in cyberspace”?
- There are/were rules. They are currently evolving. Long-term process. Expect less protection?



@lukOlejnik
@LukaszOlejnik@Mastodon.Social
blog.lukaszolejnik.com
lukaszolejnik.com