Niels Nagelhus Schia

Senior Research Fellow (NUPI)

Finse Cyber Winter School 2022

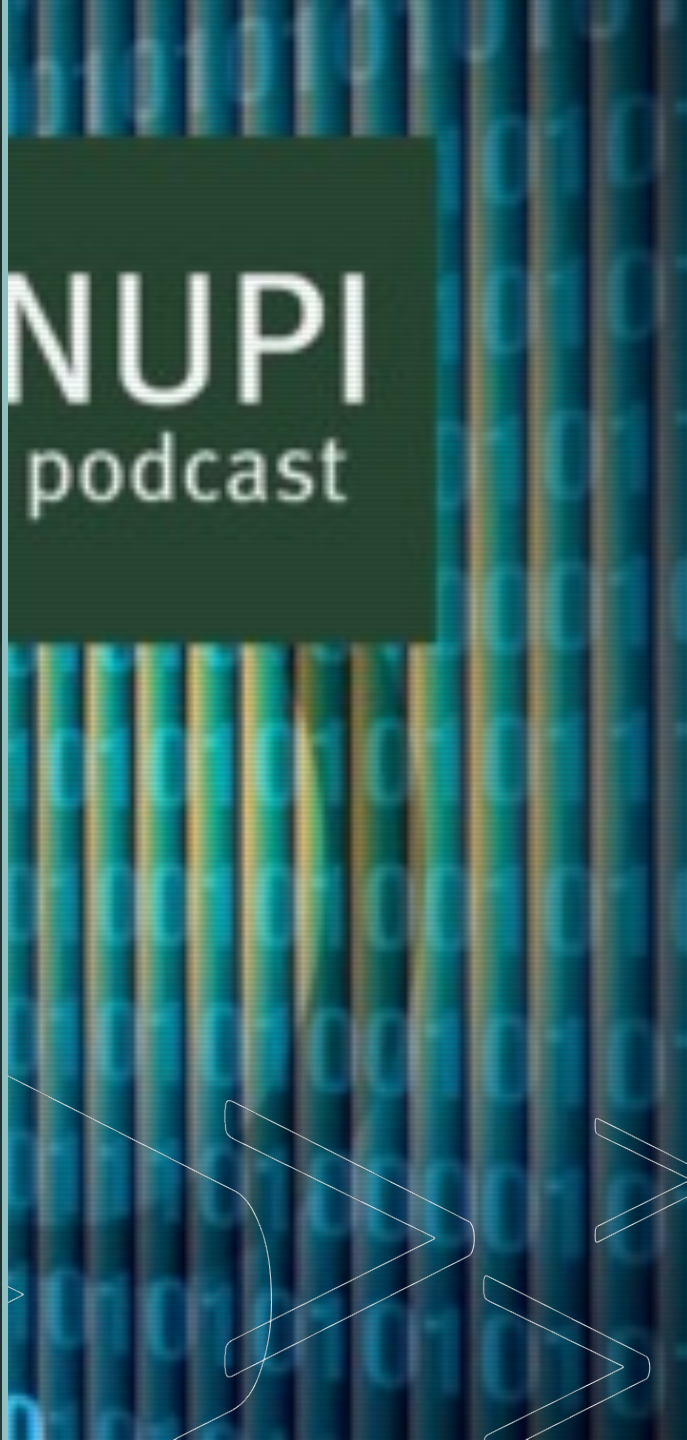
International politics, the UN and Cybersecurity

Three parts:

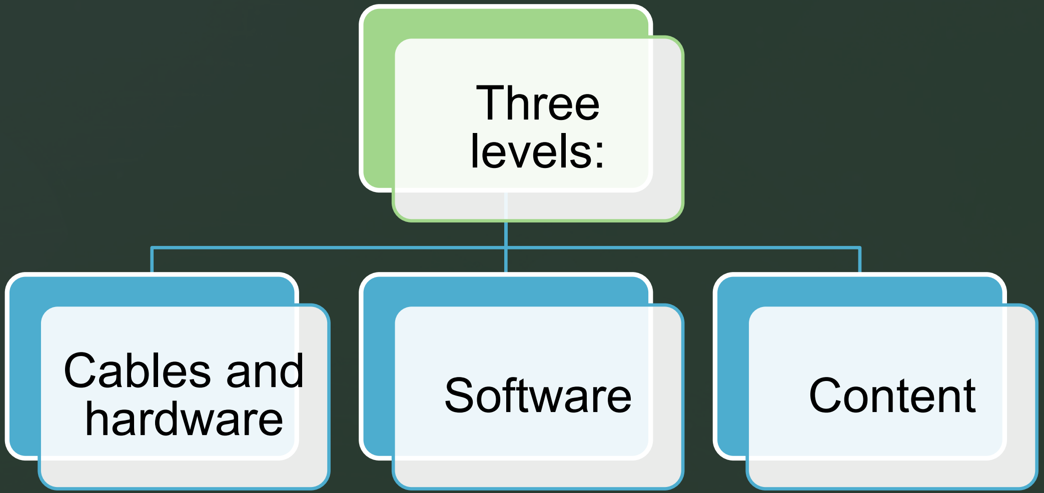
1. International politics and the Stuxnet-case
2. The digital battlefield – Ukraine
3. Cybersecurity and international organizations

NUPI's Research Centre on Digital Technology and Cybersecurity

- Cybersecurity capacity building
- Cyber sovereignty
- Digital technology – little brother / big brother
- International Organizations
- Cyber attacks
- Digital vulnerabilities and critical infrastructure
- Cloud services, global data flows and national autonomy



Social Science Perspective on Cybersecurity

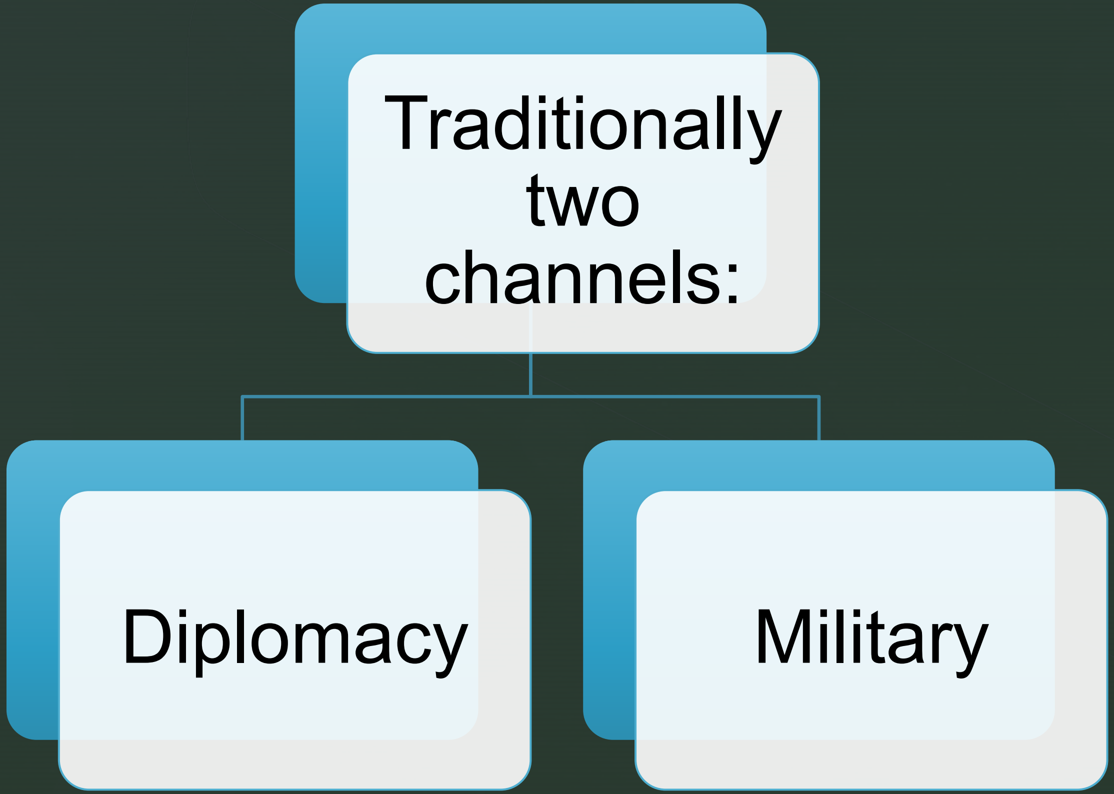


Three levels:

- Cables and hardware
- Software
- Content

Cybercrime vs cyberattacks/operations

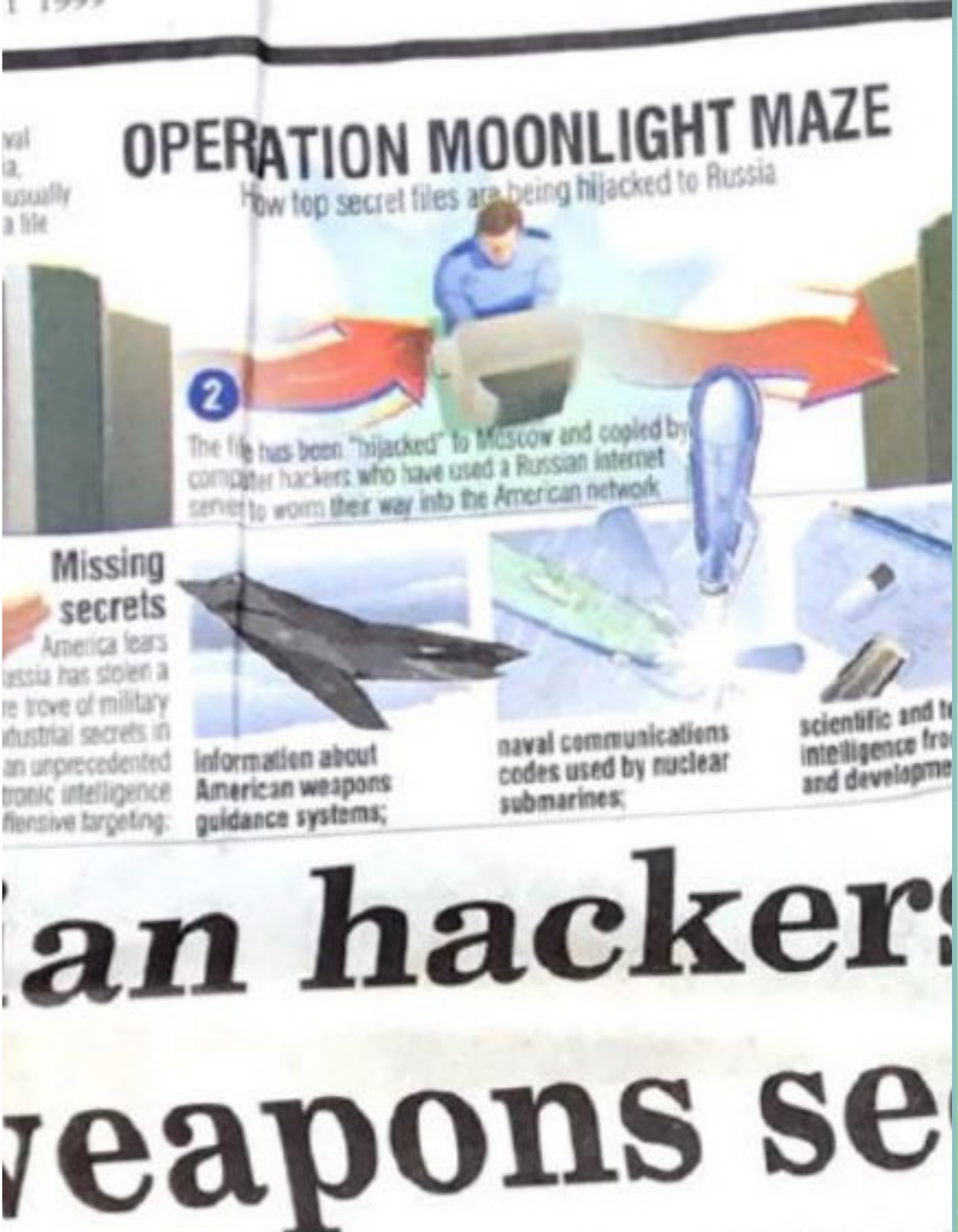
Part 1: International Relations = relations between states



Digital technology as a third channel of communication? Stuxnet as an example

Before Stuxnet

- Moonlight Maze 1996-1998
- Titan Rain 2003-2006
- Estonia 2007
- Iran’s nuclear programme



val
a,
usually
a file

OPERATION MOONLIGHT MAZE

How top secret files are being hijacked to Russia

2

The file has been "hijacked" to Moscow and copied by computer hackers who have used a Russian internet server to worm their way into the American network

Missing secrets

America fears
ssia has stolen a
e trove of military
dustrial secrets in
an unprecedented
tronic intelligence
ffensive targeting:

information about American weapons guidance systems;

naval communications codes used by nuclear submarines;

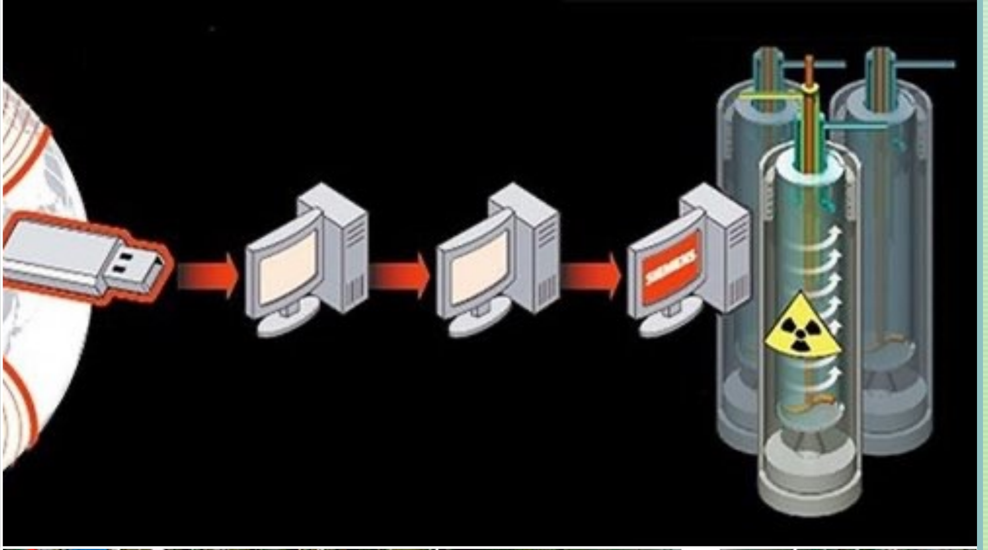
scientific and t
intelligence fro
and developme

an hackers

veapons se

Stuxnet – the world's first cyber weapon

- Where: Natanz, Iran, 2008 (publicly known 2010)
- What: Operation Olympic Games – kinetic damage (new)
- Whom: USA



Post Stuxnet: US vs Iran cyberoperations

Attacker	Victim	Year	Target	Consequences
USA and Israel	Iran	2010	Natanz nuclear facility	1000 centrifuges destroyed, delayes in technological development
Iran	Saudi-Arabia	2012	Saudi Aramco	Destruction of large amounts of data
Iran	USA	2012-2013	American banks	Lack of functionality in financial services
Iran	USA	2013	Sands Casino	Closed casino, financial losses
USA	Iran	2019	Iran's Armed Forces	Lack of functionality in control system for missiles
Iran	USA	2019	US authorities and critical infrastructure	Information security breach
Iran	Israel	2020	Israeli water treatment plants	Risk of chlorine poisoning, lack of functionality within irrigation
Israel	Iran	2020	Shahid Rajaee Harbor	Loss of functionality in computer systems, major delays in supplies
Israel	Iran	2021	Natanz nuclear facility	Power outages, centrifuges destroyed

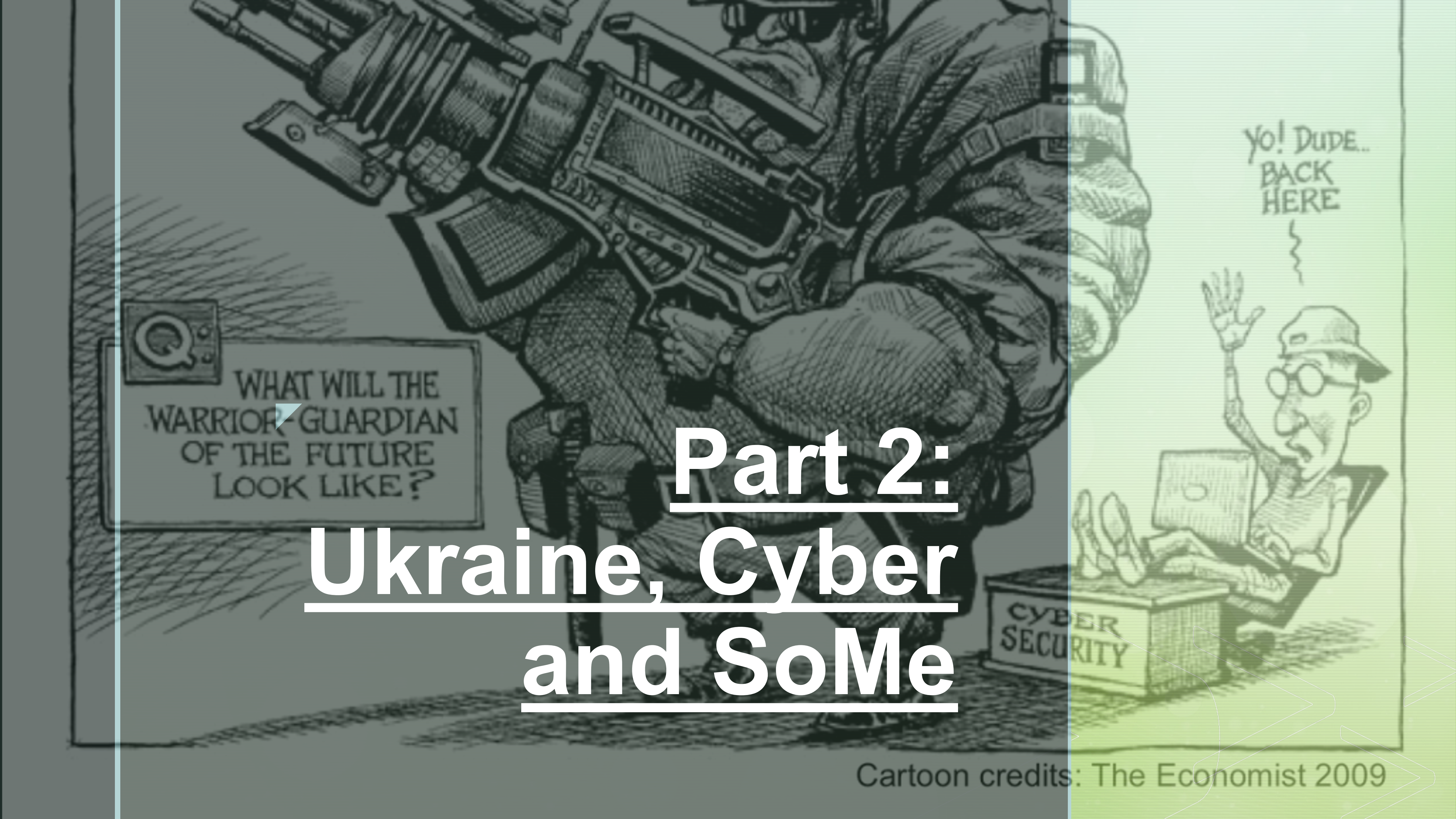
A paradigm shift?

- Kinetic
- Arms race
- States' strategic understanding of cyber threats and cybercapacities

The shift

1. Strategic Impact - Pressure release (Jervis & Healey 2020) Maschmeyer 2021.
2. States' perceptions of threats in the cyber domain
3. Defensive cyber capacities and critical infrastructure

-> Change in states' perceptions of cyber conflict and cyber capacities, cyber attacks can cause physical damage, third channel

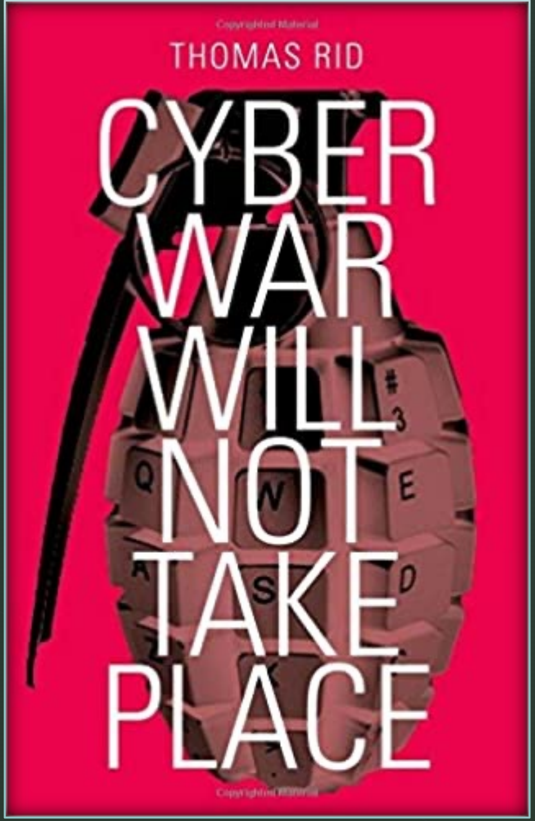


Part 2: Ukraine, Cyber and SoMe

Cartoon credits: The Economist 2009

“Cyber war will not take place”
T. Riid 2012

“*Secret cyber war in Ukraine*”
T. Riid 2022



The Economist
Why fairness is a bad idea
Rewriting Wall Street's rules
Who will run Brazil?
How Big Oil became Big Gas
The link between IQ and disease
Cyberwar
The threat from the internet

What has happened in Ukraine?

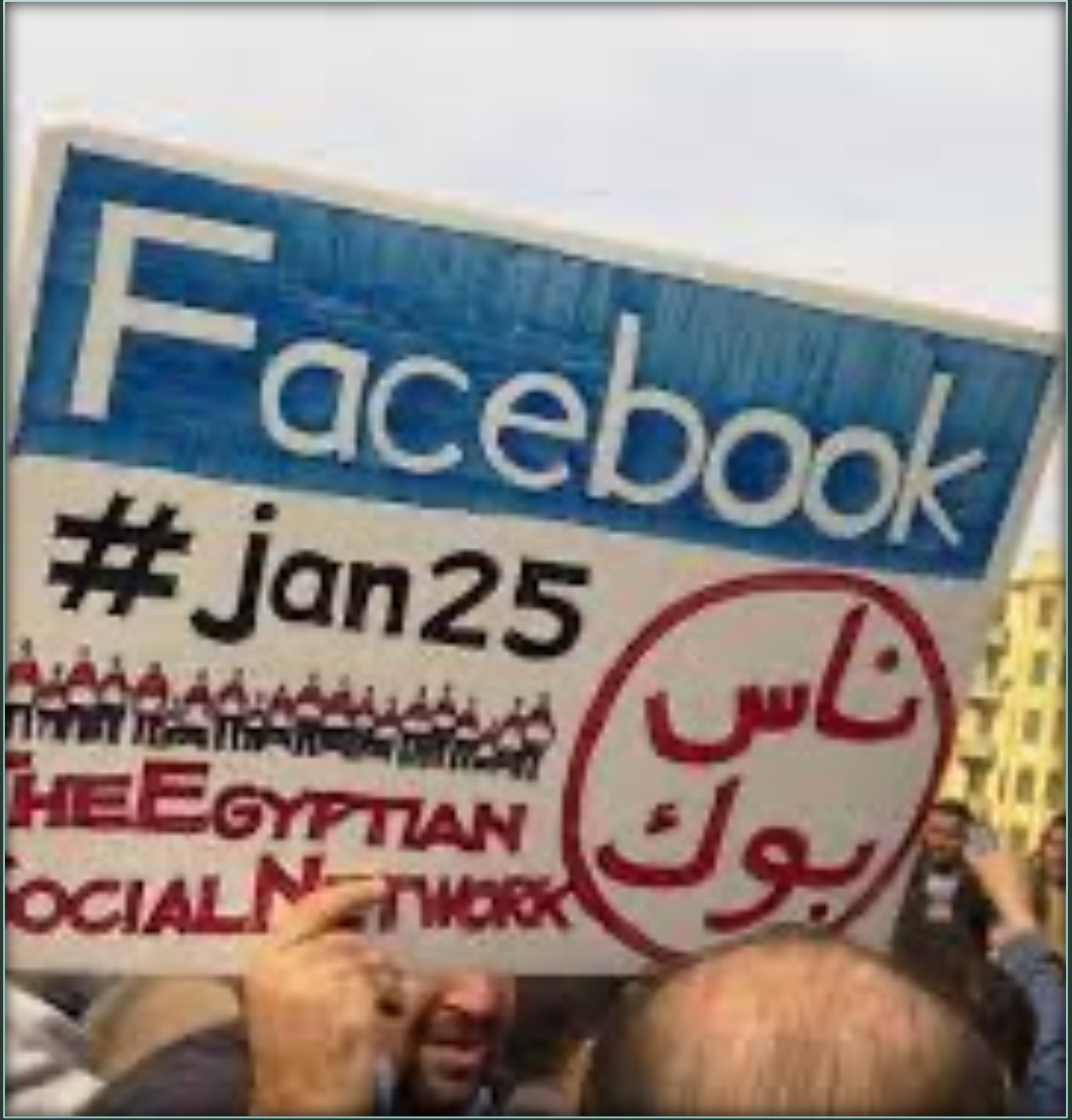
Cyberattacks and SoMe

Weapons of the weak
Old against new
Demokracy vs dictatorship

What we have seen so far

- DDoS on Government, Military, Financial, Telco
- Destructive wipers: WhisperGate (13 Jan 2022), HermeticWiper (22 Feb 2022)
- Espionage: Ukraine, also internationally CISA Alert (AA22-047A)
- Defacement of websites
- Supply chain attacks (Kitsoft)
- Influence operations / Disinformation using SMS message, social media, and other media
- Viasat

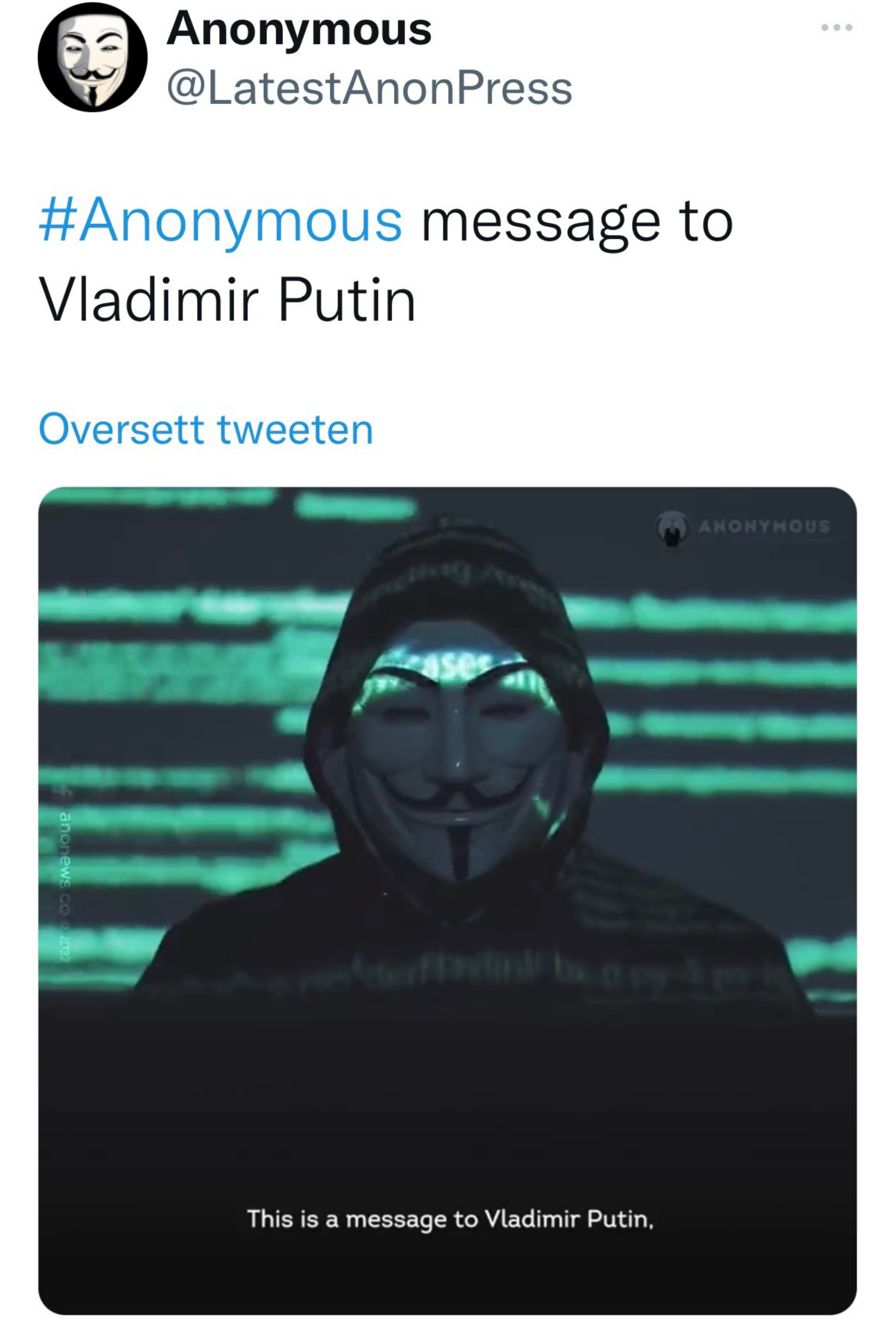
<u>Arabic spring</u>



Development since the Arab spring

- Facebook from 500 million to 3 billion users
- You Tube and Twitter has had similar growth
- New plattforms have emerged (Snapchat, Telegram, TikTok)

Anonymous



Anonymous
@LatestAnonPress

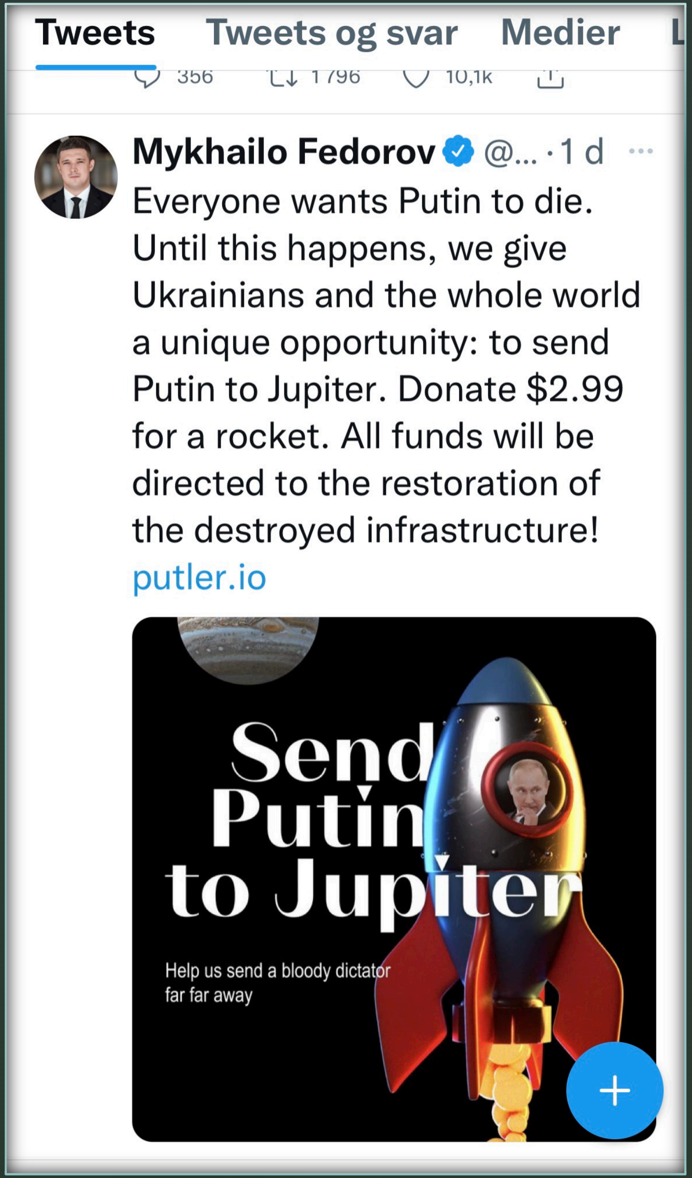
#Anonymous message to Vladimir Putin

Oversett tweeten

This is a message to Vladimir Putin,

Ukraina og Plattformene

- Facebook/ Meta
- Elon Musk
- YouTube
- Google
- Twitter
- Apple



Mykhailo Fedorov @... · 1 d

Everyone wants Putin to die. Until this happens, we give Ukrainians and the whole world a unique opportunity: to send Putin to Jupiter. Donate $2.99 for a rocket. All funds will be directed to the restoration of the destroyed infrastructure!

putler.io

In Russia

- Cyber capabilities
- Narratives
- Mass media controll
- Social media

Internet as a human right

- “*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers (…) The promotion, protection and enjoyment of human rights on the Internet*”
  The Universal Declaration of Human Rights, Art. 19.

Part 3
International Organizations

- The United Nations
- NATO

NATO Summit Warsaw 2016

Cyber space as the fifth domain

Cyberattacks and article 5

- High threshold
- Dependant of situation and political decision
- 3 examples:
  Stuxnet 2010
  Estland 2007
  NotPetya 2017

The United Nations

- Key processes:
- The Security Council
- The GGE
- The OEWG
- WSIS

working together towards
2025
World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015

WSIS

Responsible state behaviour in cyberspace at the United Nations

UN GGE

Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.

UN Open-Ended Working Group

INTERSESSIONAL
CONSULTATIVE MEETING

OEWG

The UN Security Council

- Maintain international peace and security
- Binding decisions
- Veto powers
- Cybersecurity?

Disagreements and challenges

- Slow start and cumbersom process
- Clear differences of opinion on the use of force in cyberspace
- Russia and China seek to negotiate a treaty
- US and the West: international law is sufficient

Future perspective on global governance and cybersecurity

Thank you very much !

- Niels Nagelhus Schia / Senior research fellow, NUPI
  Head of NUPI's Research centre on digital technology and cybersecurity.
- Email: nns@nupi.no