NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD

Cyberspace

The battlefield of the digital age

4 June 2025

Mr. Mario Beccia

NATO Deputy Chief Information Officer
beccia.mario@hq.nato.int

1970 - 2000

- HW and SW "massification"
- Personal computing
- Telco explosion
- Business ICT
- Sophisticated AI algorithms have no corresponding infrastructure
- Government and Defence drive ICT requirements

2001 - 2015

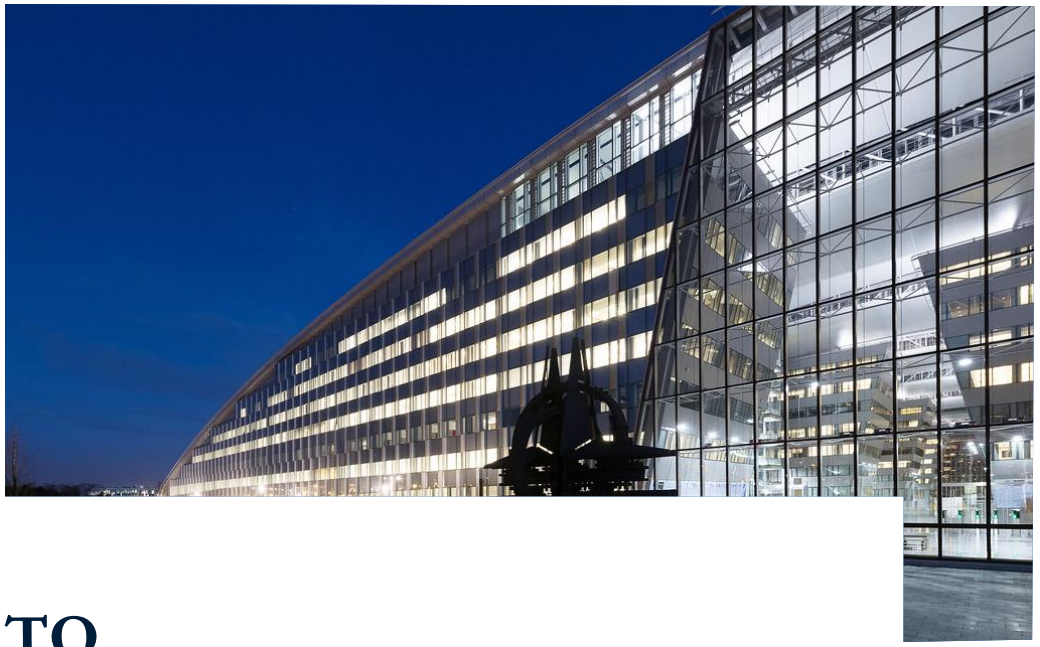
- Advent of the cloud
- Networks coverage
- Big data and storage
- Social media as mass-market product
- Moore's law crisis
- Estonia incidents
- Government and Defence commercialization

2016 - 2020

- Incidents in the EU (WannaCry, NotPetya)
- Attacks on Ukraine's critical infrastructure
- Cyberspace as a military domain
- Ransomware and DDoS
- ICT and Cybersecurity drive government and Defence requirements

2021 - 2025

- Satellite communications
- Advent of ML and GenAI
- ML training sets become massive
- AI driven increase in cloud computing market
- DeepFake attacks
- Digital Infrastructure as strategic asset



NATO

Washington Treaty

32 Member nations

Purpose is to guarantee freedom and security of its members through political and military means

Cyber at NATO

Embedded in NATO's core tasks

Threats are increasing in frequency and sophistication

Cyberspace is a military domain

Focus on

- Protecting our networks
- Conducting defensive operations in cyberspace
- Helping Allies enhance national resilience
- Providing a platform for consultation and collective action

Dynamics in the ecosystem

Strong presence of asymmetry

- Attacker investment and risk = low
- Defender investment and risk = high

Method 1: Inflict damage on attacker

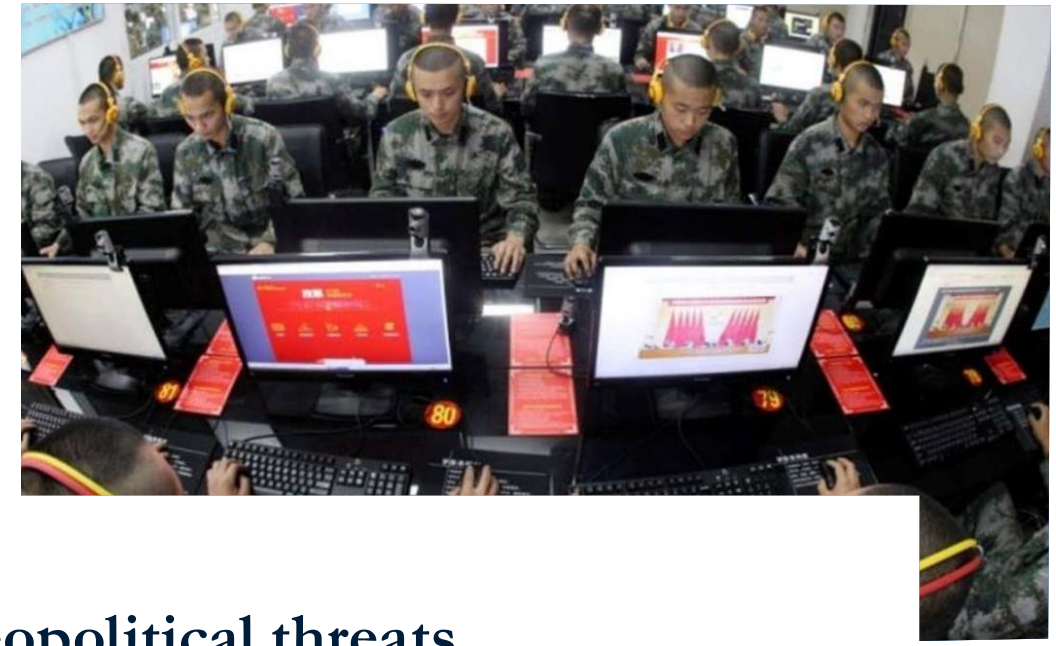
- Disruption or destruction – Offensive Cyber Operations (prerogative of nations – not private industry, not NATO)
- Public attribution – technically difficult, politically sensitive, and only marginally effective
- Sanctions – impose economical damage (nations)

Method 2: Deny benefits for attacker

- Cyber Resilience
- Knowledge of your environment
- Step-up defense through technology

In the movies

In real life



Geopolitical threats

Russia

China

North Korea

Iran

Russia

800% increase of attacks immediately after invasion

Massive disinformation campaigns

China

Biggest global threat

40 "Advanced Persistent Threat" groups

North Korea

Wide-ranging financial activities (>$1B per year)

Iran

Increased threat tied to Iran and Hezbollah

The Alliance:
– is able to defend itself in cyber-space as effectively as it does in Air, on Land, and at Sea; and

– has integrated cyberspace into its coordinated, cross-domain approach, ensuring all joint operational effects support its core tasks, and support and strengthen NATO's broader deterrence and defence posture.

– Military Vision and Strategy on Cyberspace as a Domain of Operations, 2018

We reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.

– NATO Warsaw Summit Communiqué, 2016

- NATO recognised cyberspace as a domain of military operations in 2016
- This recognition:
  - Assists in the integration of cyberspace into planning and operations at all levels
  - Provides a framework to better manage resources, skills, capabilities, planning, and decision making
  - Supports broader deterrence and defence mission (es. Art.5 applicability to Cyberspace)
- This recognition, however, does not change:
  - NATO's defensive mandate
  - NATO's commitment to act in accordance with international law
- Notable achievements:
  - Cyberspace Operations Centre (CyOC)
  - Framework mechanism for the integration of voluntary sovereign cyber effects

We are further accelerating the modernisation of our collective defence and are Establishing the NATO Integrated Cyber Defence Centre to enhance network protection, situational awareness, and the implementation of cyberspace as an operational domain throughout peacetime, crisis and conflict; and developing a policy to augment the security of NATO's networks.

NATO's deterrence and defence posture is based on an appropriate mix of nuclear, conventional, and missile defence capabilities, complemented by space and cyber capabilities. We will employ military and non-military tools in a proportionate, coherent and integrated way to deter all threats to our security and respond in the manner, timing, and in the domain of our choosing.

– NATO Washington Summit Communiqué, 2024

- With the decision taken at the Summit 2024, NATO started building the NATO Integrated Cyber Defence Centre (NICC)
- The Centre aims at:
  - Establishing better situational awareness in cyberspace, integrating red, blue and white pictures
  - Integrating existing resources to enhance Enterprise network protection (cyber resilience)
  - Supporting SACEUR's deterrence and defence mission, by further implementing cyberspace as an operational domain throughout peacetime, crisis and conflict
- The Centre integrates military and civilian resources:
  - Co-led by a civilian and a military leader
  - Brings together cyber specialists acting in the operational, technical and political areas
  - Acts as a hub to integrate industry- and Allies- provided tools and products
- The Centre integrates the NATO Enterprise with Allies, Industry and Academia:
  - Allies provide specialized personnel, and enable direct information sharing
  - Industry provides specialized services, such as Cyber Threat Intelligence, Incident Response and Auditing services

Cooperation Tools for Cyberspace

VCISC

Cyber Defence MoU

Improved integration with National Entities

A mechanism for NATO to work as an interconnecting and cooperation hub between Allies in case of a severe Cyber incident

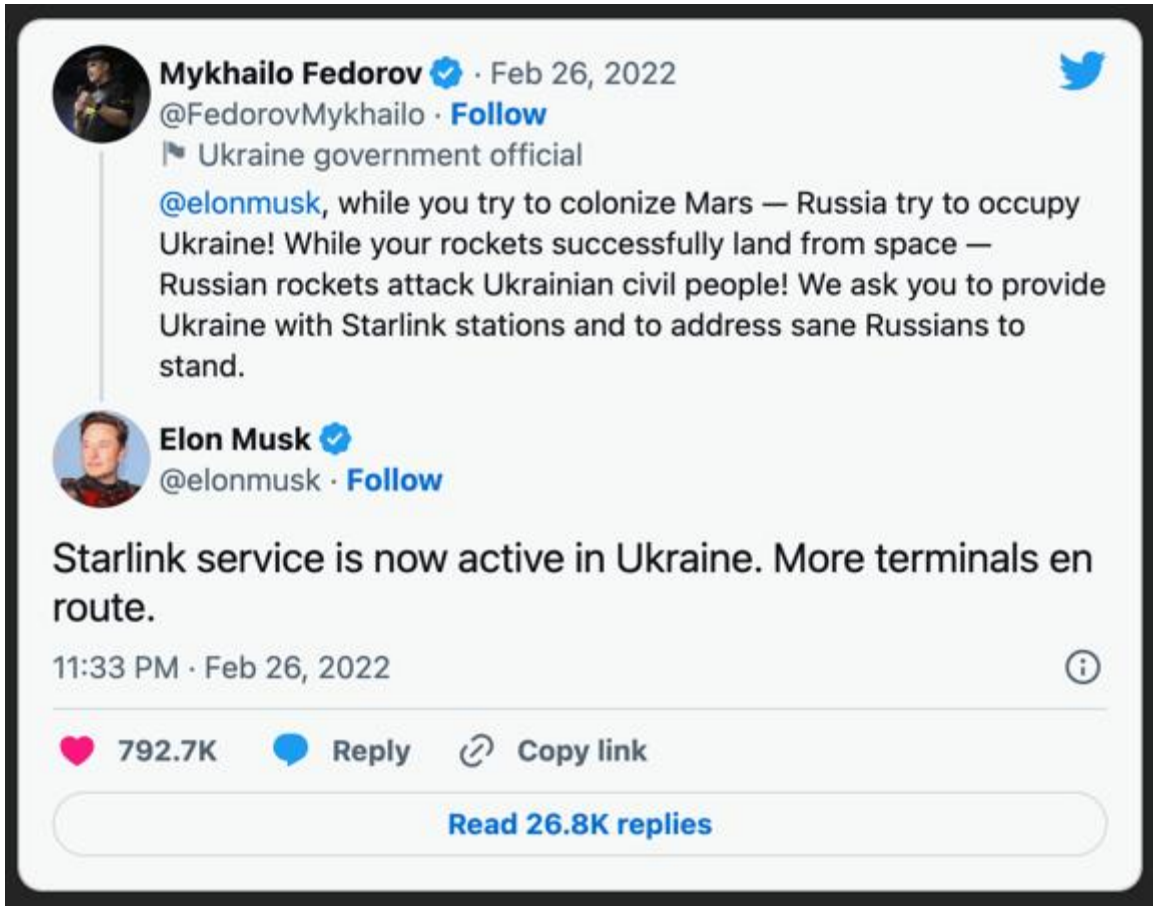
An agreement to share knowledge, information, technology assessment and capabilities

Improved contacts between NATO Enterprise relevant entities and:

- National Cyber Commands
- National Cybersecurity Agencies
- Academic and other government entities related to cyber

RUS/UKR Conflict

- Pre-conflict relevant incidents -- Black Energy (2015), NotPetya (2017), preparatory actions (2021), malware usage (2021/2022)
- Conflict implications
  - Spin-off and collateral damage
  - Role of disinformation
  - Role of Hacktivism
- Resilience of UKR's ICT infrastructure & cloud computing adoption
- ***Role of the private sector***



Observations

- Peacetime, crisis and conflict are increasingly difficult to differentiate
- The threshold of acceptable malicious activity is moving up, quickly
- Cyberspace (and AI) heavily depend on civilian infrastructure
- Effects of a kinetic conflict in a geographical area expand across Cyberspace
- Preparation and preventive measures are essential
- Cooperation with industry is a key factor

In brief

Cybersecurity is a team sport!

- → Cyberspace is heavily asymmetric (both effort and risk)
- → Skills, technology and risk management are quite complex
- → Organizations cannot stand the challenge on their own
- → Infrastructure control provides a strategic advantage
- → Role of industry is paramount

Thank you!