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

Influence of Foreign Threats on the Cyber World

VERSION 26 November 2024

Intro

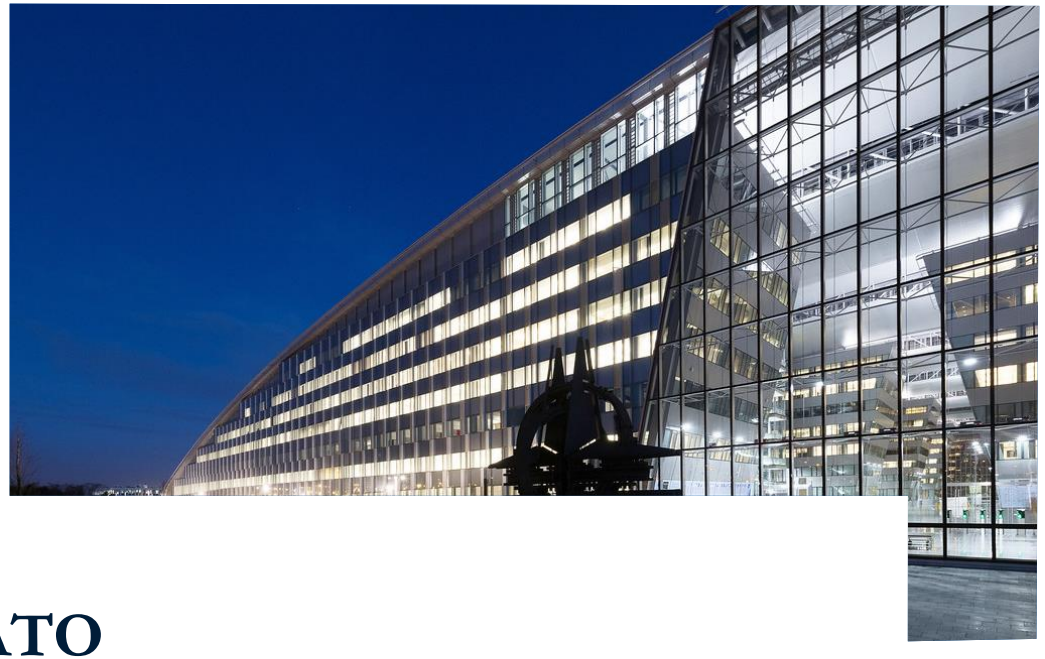
Dr. Manfred Boudreaux-Dehmer

NATO Chief Information Officer

boudreaux-dehmer.manfred@hq.nato.int

Agenda

1. NATO and Cyber
2. NATO through Time
3. Geopolitical Ecosystem
4. Dynamics of Cybersecurity
5. Growing Threats
6. NATO’s Response
7. “Self Advertising”



NATO

Washington Treaty

32 Member nations

Purpose is to safeguard 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

Cyber is a military domain

Focus on

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

NATO

NATO 1.0 – 1949 through early 2000s

NATO 2.0 – through approximately 2014

NATO 3.0 – current

NATO through Time

NATO 1.0

- Cold war
- Counterweight to Warsaw Pact

NATO 2.0

- Article 5 of Washington Treaty (for Afghanistan)
- Focus on fighting terrorism
- Major missions: Afghanistan / Iraq

NATO 3.0

- Russia's invasion into Ukraine (2014 and 2022)
- Rise of China
- Converging interests: Russia, North Korea, China

Geopolitical Ecosystem

Russia

China

North Korea

Iran

Dynamics of Cybersecurity

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

- Risk awareness / know your environment
- Invest in people
- Information hyper-triangulation
- Step-up defense through technology

Growing Threats

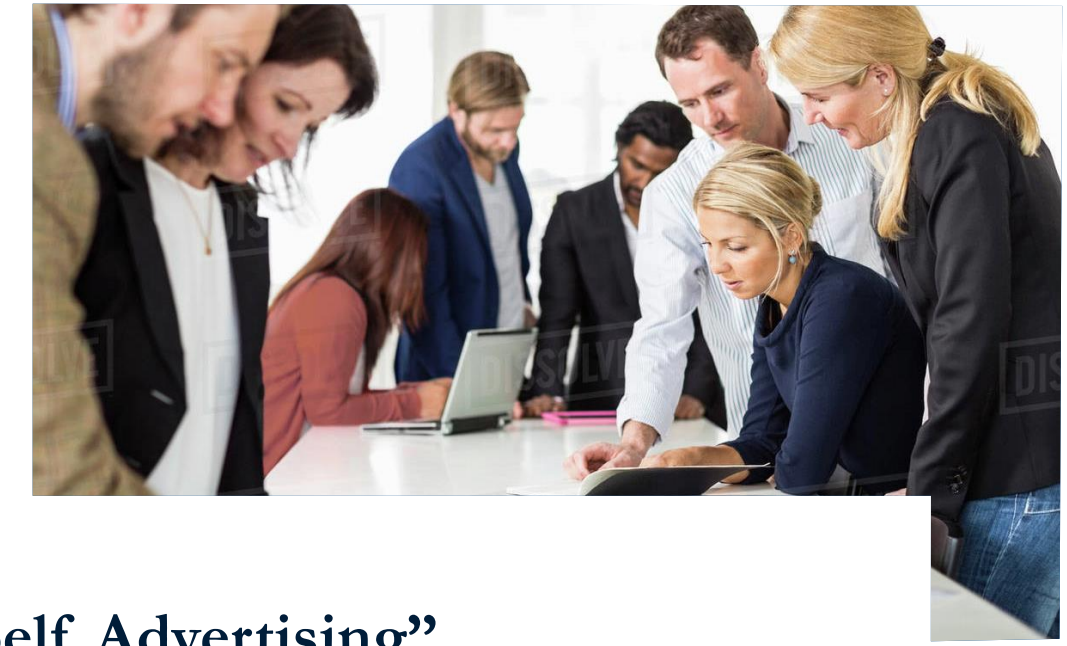
- Based on geopolitical and criminal interests
- Fueled by technological advancements (AI)
- Continue to take advantage of "the unprepared"

1. Espionage
2. Ransomware
3. Supply Chain
4. Local-to-Cloud
5. Disinformation

Responses to Threats

- No AI guilt
- Do not forget about the basics
- Threat → Risk → Action

1. Start with threats and risks
2. Know your environment
3. People first – before processes & technology
4. Hyper-triangulate data
5. Use technology smartly



“Self Advertising”

If you want to help safeguard freedom and security for one billion people…

Opportunities to Engage

Employment

- Staff positions
- Interns
- Young Professionals Program (YPP)

  www.nato.int

Business

- Defense Accelerator for the North Atlantic (DIANA)

  www.diana.nato.int

- Request for Proposals / Quotations

  www.ncia.nato.int

Q & A