STATE-SPONSORED CYBER ATTACKS HERE TO STAY

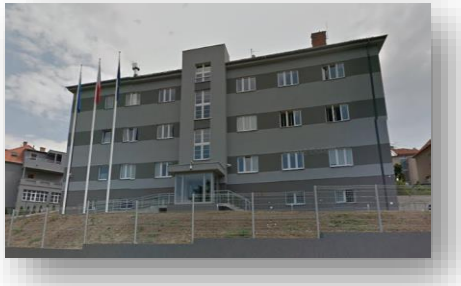
Ondřej Rojčík

o.rojcik@nukib.cz

NÚKIB

NATIONAL CYBER AND INFORMATION SECURITY AGENCY (NÚKIB)

- Czech national authority in cyber security
- Established: August 1, 2017
- Governmental CERT operates as a part of NÚKIB
- Support to public sector institutions
- Control and determine critical information infrastructure (CII) systems
- Responsible for legal and policy aspects of CS
- Monitoring and analysis of cyber threats



2024?

STATE SPONSORED CYBER ATTACKS: HERE TO STAY

Why malicious state actors can´t resist the cyberspace?

- They will not catch you **(attribution problem)**
- No punishment **(weak law enforcement)**
- Everybody can do it **(proliferation of cyber tools)**
- You can attack other states without provoking real word response **(high threshold level)**
- You can do whatever you are capable of **(permissible environment)**
- The attack surface is growing

ATTRIBUTION PROBLEM

- Very difficult to attribute attacks in cyberspace

- State actors have sufficient resources to cover their tracks

- BUT People make mistakes

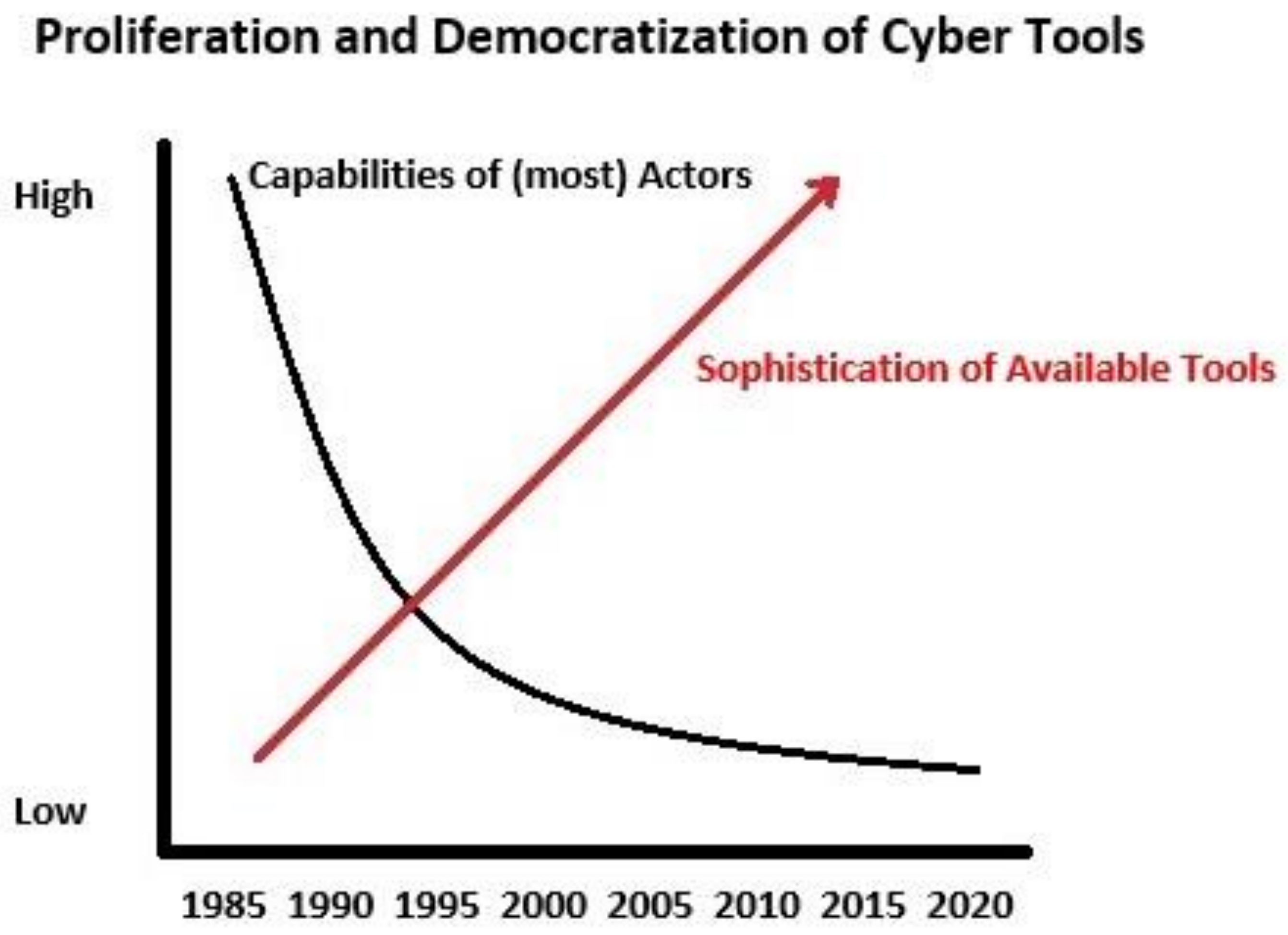
- **Not a binary problem**: Degrees of certainty

ATTRIBUTION PROBLEM

- Attribution also depends on political stakes: the higher is the damage, the more resources will government invest in investigation

- Difficult to communicate conclusions
- Room for plausible deniability

PROLIFERATION OF CYBER TOOLS



HIGH THRESHOLD LEVEL

You can attack other states **without** provoking „real word“ **response**

- Saudi Aramco
- Stuxnet
- BlackEnergy

Few exceptions

APT (ADVANCED **PERSISTENT** THREATS)

Advanced

- Skills

Persistent

- The are patient
- They have time…
- …a lot of time
- …and a lot of money

WHY IS CYBERSPACE SO ATTRACTIVE FOR STATE-SPONSORED WRONGDOERS?

- Lack of formal procedures and repercussions for perpetrators (state actors)
- Insufficient law enforcement capabilities (criminal groups)

- PERMISSIBLE ENVIRONMENT attracts all sorts of actors
- Attracted by LOW COSTS and HIGH EXPECTED UTILITY

Expected utility – costs = Attractive option

THREAT = CAPABILITY x INTENSION

- Tendency to underestimate attractiveness of the Czech Republic as a target of cyber threat actors

- Both political and economic reasons to be a target
- EU and NATO membership
- Specific economic and political interests of the attackers
- Advanced industrial and R&D capabilities

NÚKIB

Report on the state of cyber security in the Czech Republic in 2018

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

*„From the perspective of the state, the most important cyber threat actors… are **state actors**.*

*…In the case of the Czech Republic, according to the information available to the NÚKIB, this specifically means operations of **actors linked to** the **Russia**n Federation and the People’s Republic of **China**.“*

Available on: https://www.nukib.cz/cs/informacni-servis/publikace/

WHAT CAN WE DO ABOUT IT?

- Intensions and motivation of attackers will likely remain the same
- We can expect a high level of persistence

- Resilience = do your homeworks
- Detection capabilities
- Attribution
- Cyber defence

→ Possibly cyber deterrence

- **Cyberspace will remain an attractive option for state actors**
- **Attribution is difficult, but not impossible**
- **It is a manageable threat, but we need to be diligent**

Ondřej Rojčík
o.rojcik@nukib.cz

NÚKIB