How to Ensure Resilient Cyber Security?

Kenneth Geers
Atlantic Council / NATO CCDCOE

Nordic-Baltic Security Summit 2024

Kes ma olen?

- 93-13: US Army, NSA, NCIS, NATO
- 13-24: Priv Sec InfoSec
- PhD: TalTech / Prof: U Kyiv
- Languages: FR, RU
- Think Tanks: AC, NATO, DSI-B, TCF
- Pubs: 3000+ citations
- Cons: DC, BH, RSA, CyCon

No military

Geostrategic link: NA-EU

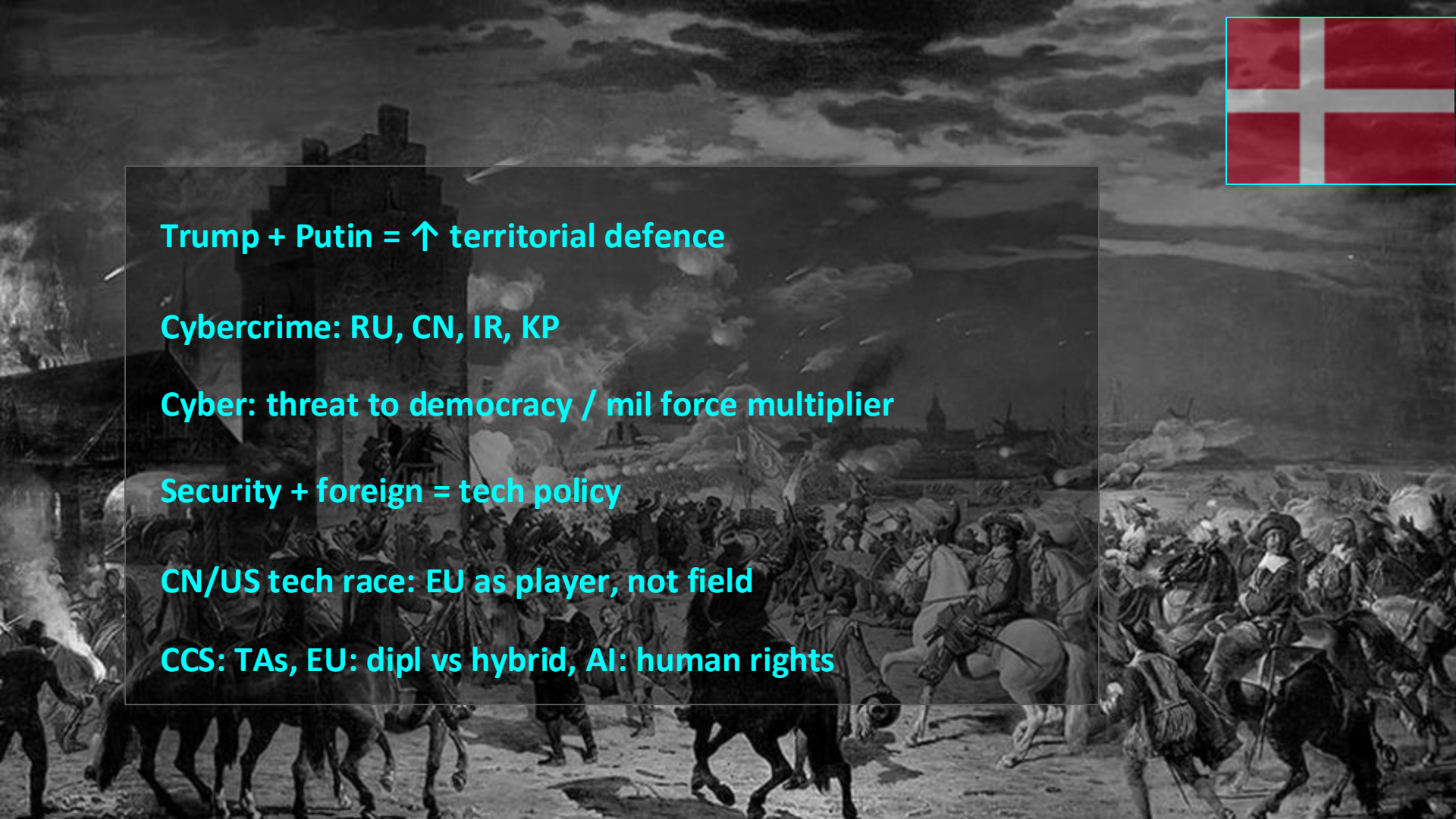
Undersea cables

“Unprecedented” cyberattacks

Security culture & public trust

InfoSec “pillar of prosperity”

Arctic Council (1996)



Trump + Putin = ↑ territorial defence

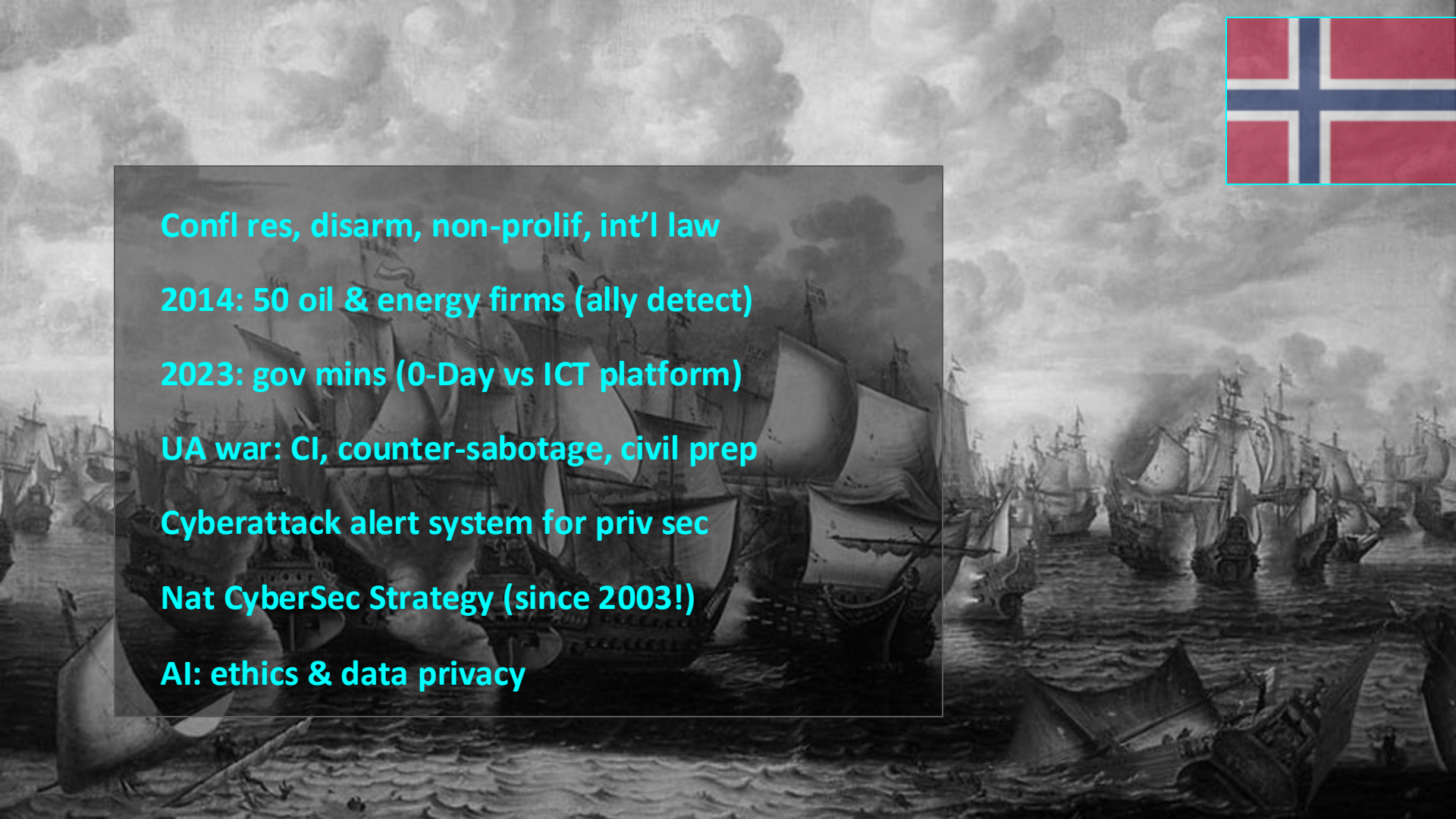
Cybercrime: RU, CN, IR, KP

Cyber: threat to democracy / mil force multiplier

Security + foreign = tech policy

CN/US tech race: EU as player, not field

CCS: TAs, EU: dipl vs hybrid, AI: human rights



Confl res, disarm, non-prolif, int'l law

2014: 50 oil & energy firms (ally detect)

2023: gov mins (0-Day vs ICT platform)

UA war: CI, counter-sabotage, civil prep

Cyberattack alert system for priv sec

Nat CyberSec Strategy (since 2003!)

AI: ethics & data privacy

Sec “fundamental” Δ, “best defended” in NATO

Public serv + priv own = unready for war

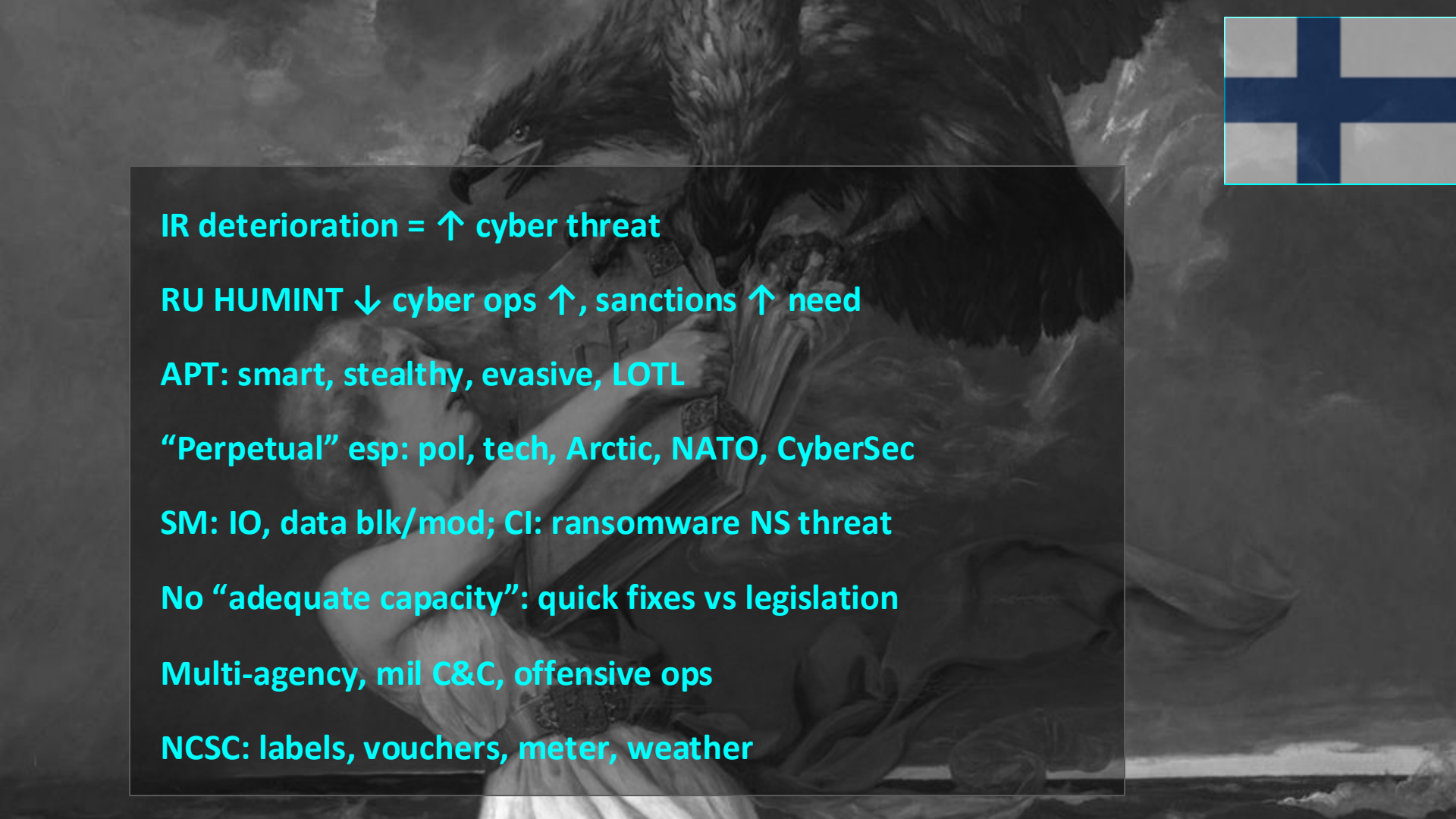
Targets: society, values / CI: kinetic impact

RU: infl ops / CN: acq/inv in dual-use tech

“Total defence”: offense, active defence, intel, attrib

Future info/cyber centre; MFA cyber envoy

IR: “like-minded” resp to attacks & consequences



IR deterioration = ↑ cyber threat

RU HUMINT ↓ cyber ops ↑, sanctions ↑ need

APT: smart, stealthy, evasive, LOTL

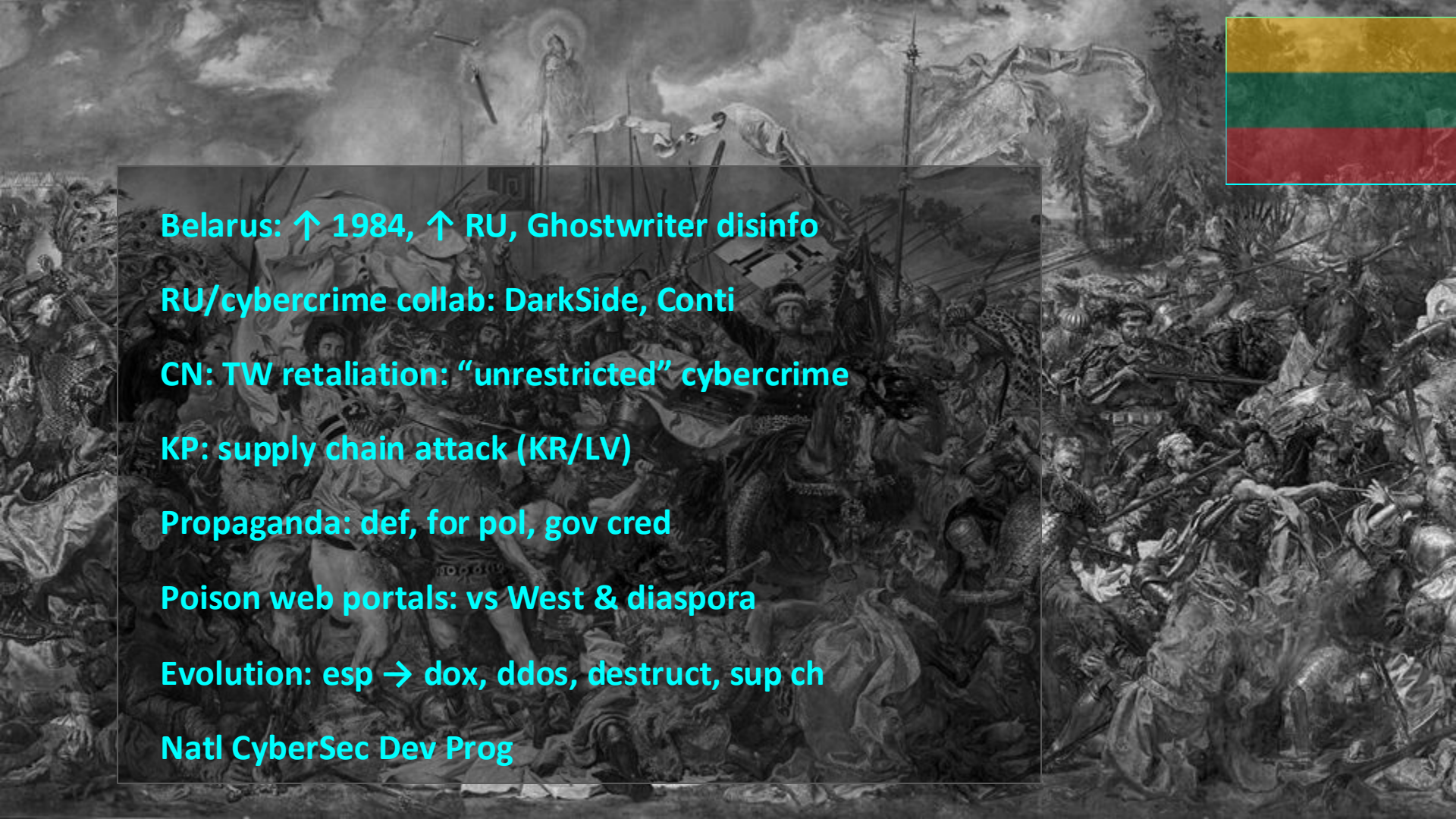
“Perpetual” esp: pol, tech, Arctic, NATO, CyberSec

SM: IO, data blk/mod; CI: ransomware NS threat

No “adequate capacity”: quick fixes vs legislation

Multi-agency, mil C&C, offensive ops

NCSC: labels, vouchers, meter, weather



Belarus: ↑ 1984, ↑ RU, Ghostwriter disinfo

RU/cybercrime collab: DarkSide, Conti

CN: TW retaliation: “unrestricted” cybercrime

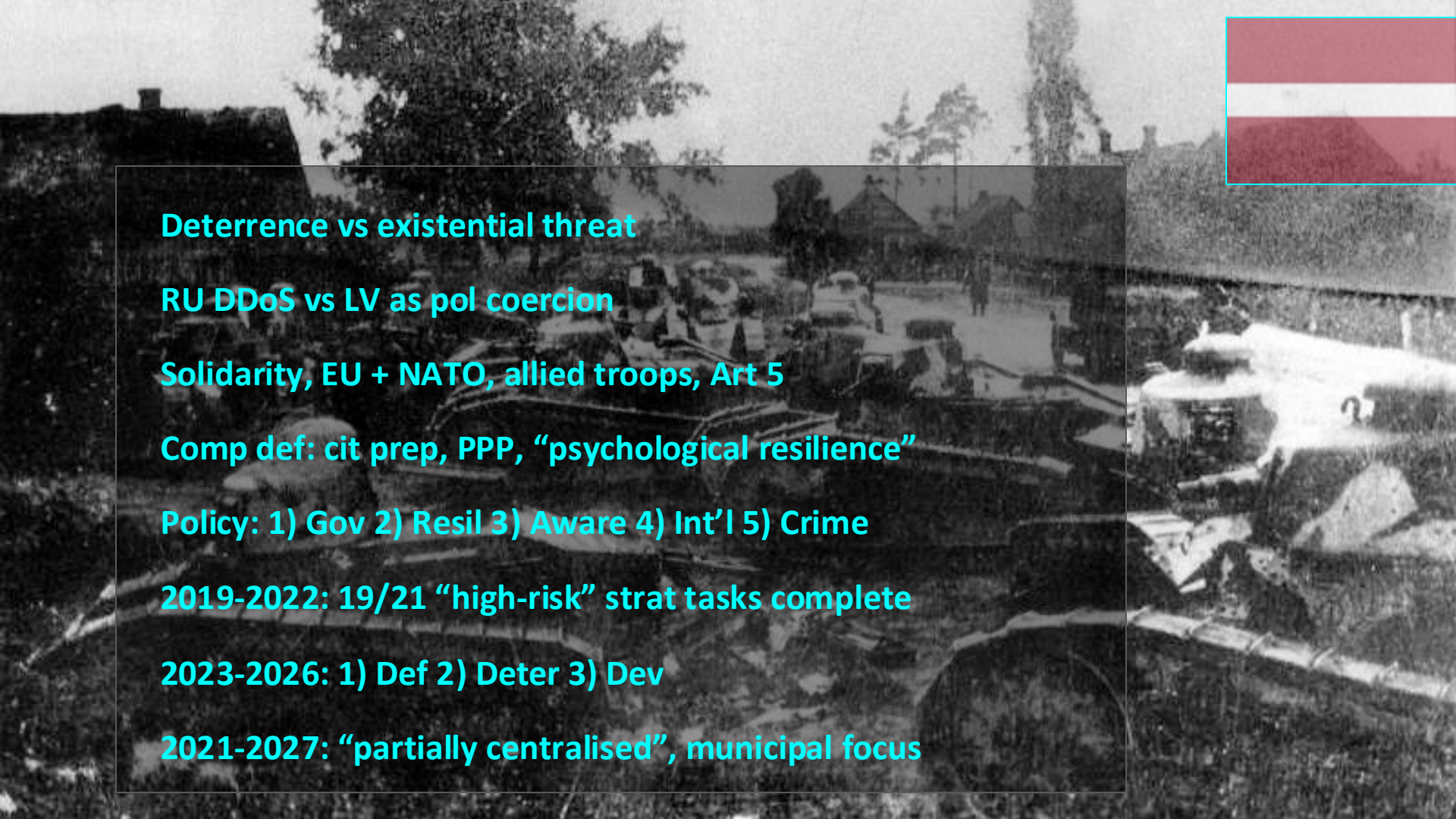
KP: supply chain attack (KR/LV)

Propaganda: def, for pol, gov cred

Poison web portals: vs West & diaspora

Evolution: esp → dox, ddos, destruct, sup ch

Natl CyberSec Dev Prog



Deterrence vs existential threat

RU DDoS vs LV as pol coercion

Solidarity, EU + NATO, allied troops, Art 5

Comp def: cit prep, PPP, “psychological resilience”

Policy: 1) Gov 2) Resil 3) Aware 4) Int’l 5) Crime

2019-2022: 19/21 “high-risk” strat tasks complete

2023-2026: 1) Def 2) Deter 3) Dev

2021-2027: “partially centralised”, municipal focus

How to Ensure Resilient Cyber Security?

Kenneth Geers
Atlantic Council / NATO CCDCOE

Nordic-Baltic Security Summit 2024