

Cyber Warfare

The new realities of digital geopolitics

SCION DAY 2026 · BENELUX EDITION



Don Eijndhoven, MSc

Introduction



Don Eijndhoven

- Founder and Chairman **Dutch Cyber Warfare Community**
- SME Cyber Warfare and Digital Geopolitics
- MSc Cyber Security Governance, Leiden University
- Bachelor of IT, Amsterdam University of Applied Science

And

- **Chief Executive Officer of Argent Consulting BV**
- Chief Information Security Officer (CISO), Enterprise Security Architect and Strategist
- Former Cyber Warfare Officer - Dutch Ministry of Defense
- Former Guest lecturer Nyenrode Business University
- Former board secretary **Connect2Trust Foundation**



Christmas Day 2024



Estlink-2 power cable severed — four data cables damaged — longest single-ship drag mark on the public record

EAGLE S · Cook Islands flag · Russian shadow fleet · Saint Petersburg → Port Said



Cyber as one instrument among many



Vladimir Putin and Chief of the General Staff Valery Gerasimov

Russian doctrine

Information warfare (1995)

Col. Vitaly Tsymbal: cyber attacks as substitute for nuclear deterrence

Gerasimov Doctrine (2013)

Non-military means now play decisive role; integration of all instruments

Sabotage, espionage, influence

Three threads running concurrently and reinforcing each other

Deniability is the product

Cook Islands flags, dormant Dutch NGOs, previously unknown APTs

Russia is operating at industrial scale.



Three threads, one campaign

SABOTAGE

BALTIC CABLES

Oct 2023 · Newnew Polar Bear

Nov 2024 · Yi Peng 3

Dec 2024 · Eagle S

Dec 2025 · Fitburg

Jan 2026 · Sventoji-Liepāja

Flag-of-convenience, opaque ownership, plausible deniability

ESPIONAGE

LAUNDRY BEAR



Sep 2024 · Intrusion against Dutch police

Work contact details exfiltrated

Jointly attributed to previously unknown Russian actor by AIVD & MIVD

May 2025 · Public disclosure

Russian state-sponsored, distinct from APT28

INFLUENCE

VOICE OF EUROPE



Founded NL 2016, dormant 2019

Re-emerged Prague May 2023

Funded by Medvedchuk via Marchevsky

FSB Fifth Service tasking

EU sanctions 17 May 2024 — paid MEPs in DE, FR, PL, BE, HU, NL

Information warfare with Dutch origin

“In the eighty years the AIVD has existed, there has not previously been a threat picture like the current one.”

Simone Smit, Director-General AIVD — 2025 annual report, April 2026

Salt Typhoon

“The worst telecom hack in our nation’s history”

Sen. Mark Warner, Chair, US Senate Intelligence Committee



9

US telecoms compromised

Verizon, AT&T, T-Mobile, Charter, Lumen, + others August 2025 · Netherlands included

13

countries in joint advisory

200+

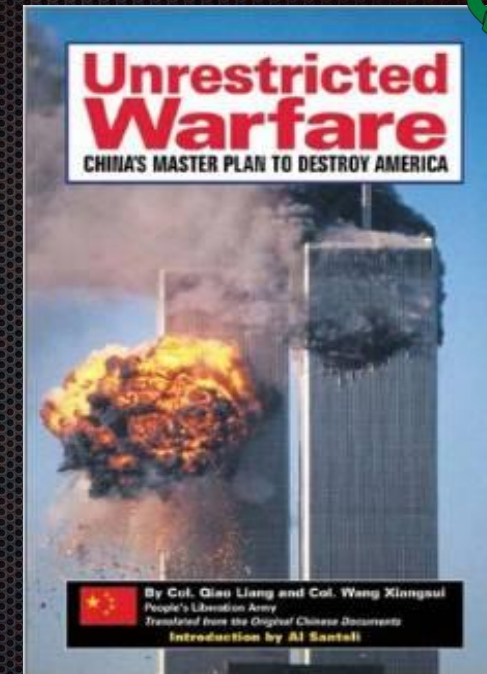
organisations breached

across more than 80 countries

2019

active since at least

and continuing through 2026



*Qiao Liang & Wang Xiangsui
People's Liberation Army (1999)*

IN THE NETHERLANDS

Smaller ISPs and hosting providers · TU Delft as a confirmed target · Sistemi Informativi / IBM Italy (April 2026, attribution tentative)



The technique — and what comes next

HOW THEY GET IN



Cisco IOS XE

CVE-2023-20198 + CVE-2023-20273

Citrix NetScaler

Edge gateway compromise, Oct 2025

Ivanti VPN

Repeated zero-day exploitation

Fortinet, Palo Alto

Same class of perimeter device

MIVD PROGNOSIS FOR 2026

Chinese cyber campaigns will continue to focus on:

Routers

Firewalls

VPN solutions

— *the perimeter devices on which most organisations still rely*

MIVD Public Annual Report 2025 — 21 April 2026

This is not happening in Microsoft 365. It is happening one layer down.



The kill switch was never hypothetical



U.S. extraterritorial reach over European digital systems

The legal instruments

CLOUD Act (2018)

Compels U.S. providers to disclose data wherever stored

FISA Section 702

Warrantless surveillance of non-U.S. persons outside the U.S.

Schrems II (2020)

CJEU strikes down Privacy Shield, identifies exposure

Executive Orders 2025-26

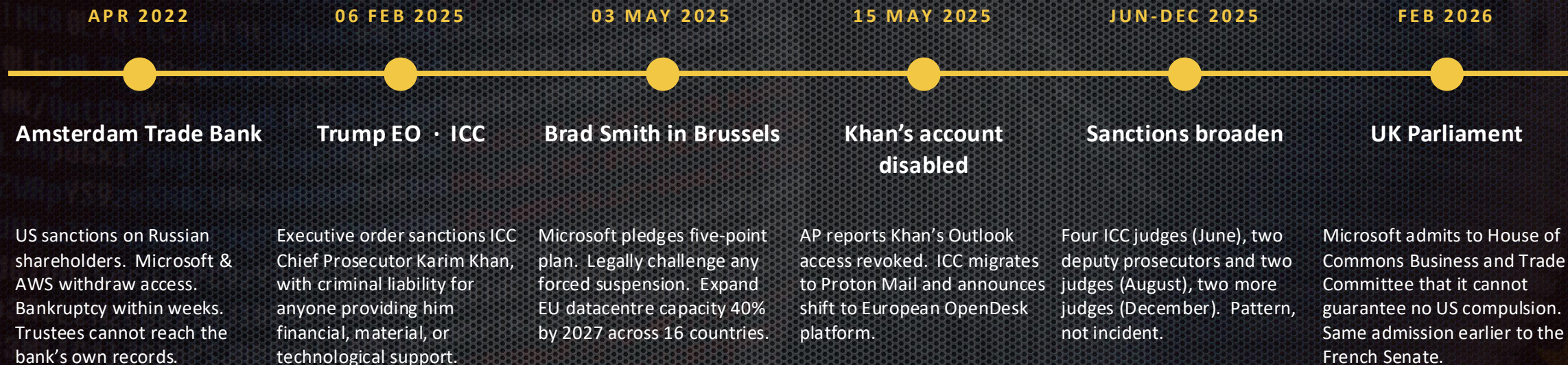
Sanctions weaponising the above against EU institutions



Until early 2025 this was largely theoretical. Then it stopped being theoretical.



Six milestones, four years



Concurrently: Hegseth pause on Russia cyber ops · CSRB disbanded · Salt Typhoon sanctions withdrawn · SignalGate



Institutional confirmation



We are moving increasingly into a world of power blocs. A world in which the European Union is regarded differently by both ally — the United States — and adversary Russia.

VICE-ADMIRAL PETER REESINK

Director, Dutch Military Intelligence and Security Service (MIVD)

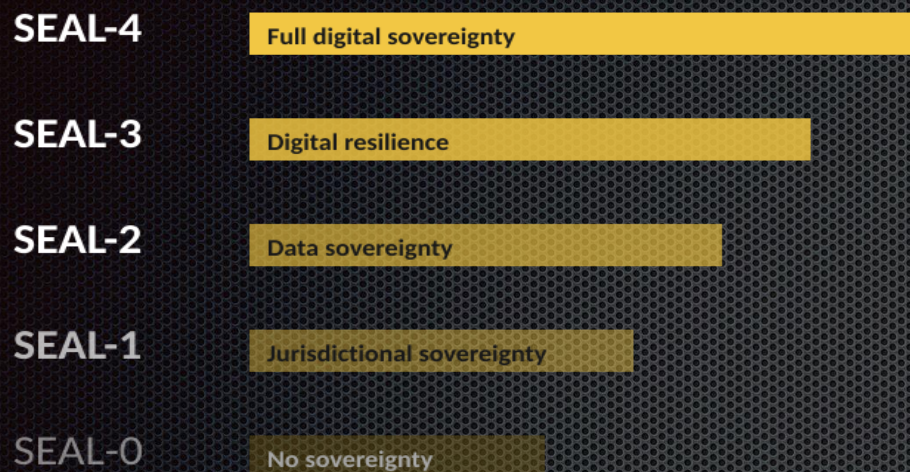
Foreword, Public Annual Report 2025 — 21 April 2026



From principle to procurement

SEAL FRAMEWORK

EU Cloud Sovereignty Framework v1.2.1, Oct 2025



THREE LAYERS OF CONTROL

Dutch Government Vision on Digital Autonomy, Dec 2025



APRIL 2026 EC awards €180M sovereign cloud tender:

STACKIT, Scaleway, Post Telecom + partners reach SEAL-3 · Proximus + S3NS reaches SEAL-2

"Sovereignty is the freedom to make choices" — Willemijn Aerdt, State Secretary for Digital Economy and Sovereignty



Europe is moving

MAY 2025

ICC, The Hague

Microsoft → Proton Mail → OpenDesk

after Khan account disabled

The marquee migration

2025

Denmark

Microsoft Office
→ LibreOffice

repeating breed

APRIL 2024 → ROLLING

Schleswig-Holstein

Windows → Linux · Office → LibreOffice

30,000 PCs across the German state administration

first full state-level migration

SEPT 2025

Swiss Army

Chief Thomas Süssli calls for
exit strategy from Microsoft cloud

National military command, on the record

2025

Lyon

Open-source migration
completed across city admin

2025

Airbus

Sovereign-cloud tender issued to replace existing Microsoft estate
across European aerospace operations

Major European industrial player

17 APRIL 2026

EC sovereign cloud tender awarded · €180 million

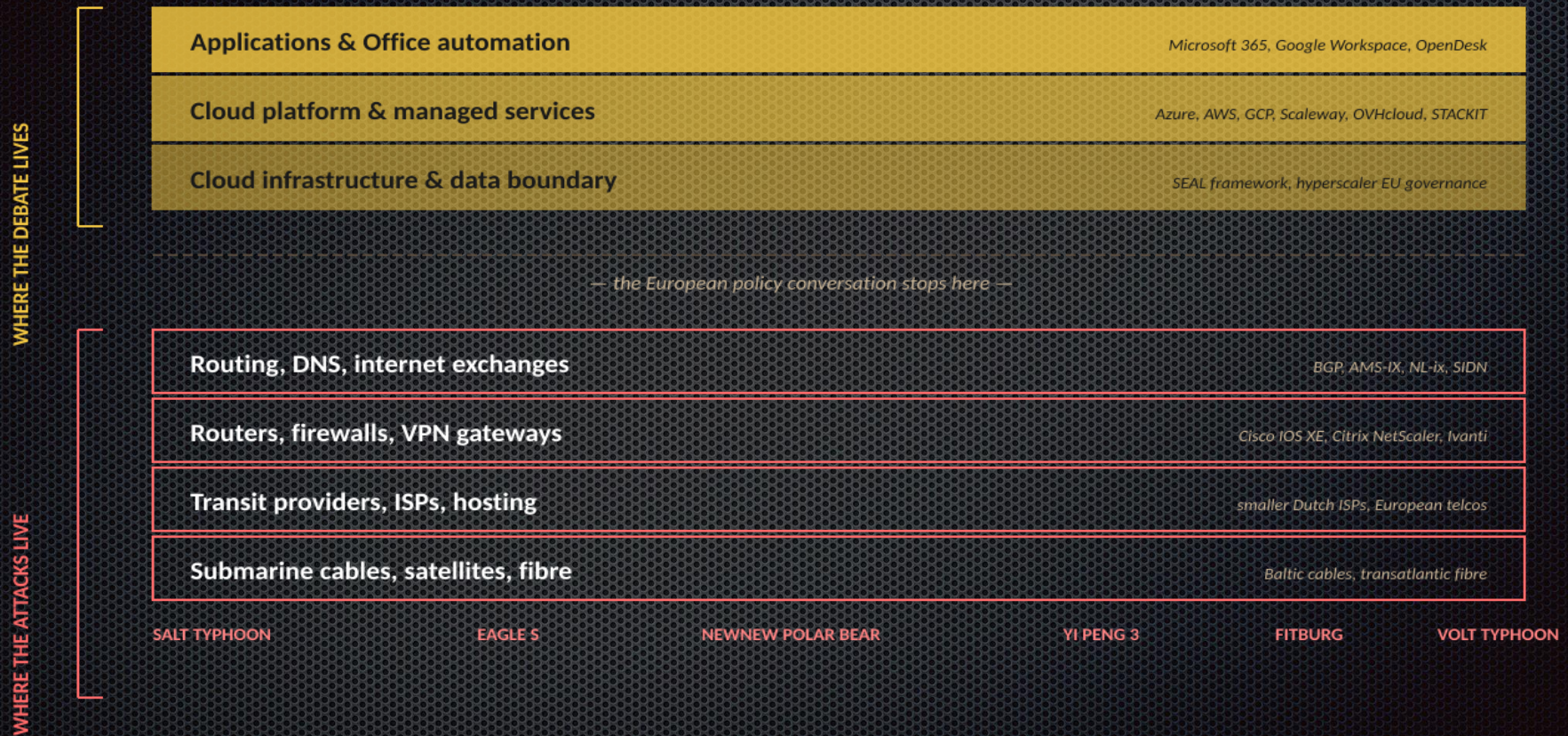
STACKIT · Scaleway · Post Telecom (with CleverCloud/OVHcloud) → SEAL-3

Proximus with S3NS / Clarence / Mistral → SEAL-2

First tender of its kind. The framework now has market evidence.



The debate has settled on the layer above where the attacks live



Digital sovereignty is not the absence of dependency but the presence of choice — at every layer of the stack, with realistic exit paths for the workloads where risk acceptance must be low, and with explicit attention to the infrastructure layer beneath the cloud.

Questions?

CONTACT INFORMATION

DON EIJNDHOVEN, MSc

Mail: d.eijndhoven@argentconsulting.nl

Mobile Phone: +31 (0)6 450 850 21

