



Oppeja Ukrainasta, kybersota kriittistä infraa vastaan

Juha Karppinen
National Technology Officer
Microsoft
Juha.Karppinen@microsoft.com

Sisältö

- Taustaa Microsoftin kybertoiminnoista
- Kokemuksia Hybridistä Sodasta
- Hybridisodan opetukset



Microsoft Threat Analysis Center

Tavoite – *Havainnoida, arvioida ja torjua* digitaliisia uhkia, jotka kohvistuvat Microsoftiin, asiakkaisiin tai demokratioille (valtioille)

What is MTAC?

Team of expert analysts

- Detection of and response to foreign influence operations
- Cyber threat context analysis
- Coverage spanning languages, geographies, & online environments

Intersection of influence & cyber threats

- **Cyber-enabled influence**
 - Proprietary data fuels expert analysis
 - **Focus:** Nation state-aligned actors
- **Report:** Deliver analysis to enable response & build resilience



Lopputulema

Kyky lieventää ja häiritä erilaisia vaikutus- ja kyberoperaatioita

How MTAC Operates

Assessment & Proprietary Collection



Proprietary telemetry & automation

Intelligence Analysis & AI-Based Applications



Global "hubs"
>14 languages

Actionable Intelligence



Intelligence reports & threat briefs

Microsoftin hyperskaalautuva kyber resilienssi suojaustoimet digitaaliseen ekosysteemiin



Maailman suurin tietoturvapalvelujen tarjoaja

1500+

kyberrikollisryhmää
(300+ v. 2023)

- 600+ valtiollista
(160+ v. 2023)
- 300+ kyberrikollista
(50+ v. 2023)
- 200+ vaikuttaja ryhmää

78T

signaalia / päivä
(65T v. 2023)

4 500

Ddos hyökkäystä / päivä
(1 700 v. 2023)

600M

identiteetti
hyökkäystä/
päivää

7 000

Salasana
hyökkäystä
/sekunti
(4000 v. 2023)

34 000

Microsoft
tietoturvaosaajaa
(10.000+ 2023)

Strateginen ja taktinen hyöty kyberoperaatioista

Vaikuttaa

Kohteita häiritsemällä ja vaikuttamalla ohjata tekemään vapaaehtoisesti turvallisuuden kannalta haitallisia päätöksiä, käyttämällä virheellistä tietoa.

Vahingoittaa

Aggressiivisten ja näkyvien hyökkäysten suorittaminen tavoitteena polarisointiin, demoralisointiin ja/tai pirstoutumiseen.

Kiristää

Usein yhdistettynä kineettiseen hyökkäykseen, hallituksen tai siviiliinfrastruktuurin pakottaminen hyökkääjän tavoitteisiin tai jopa tuhoaminen



Kokemuksia Hybridistä Sodasta

Tuhoiset kyberhyökkäykset

Venäjän hallituksen tahot (Blizzard), jotka ovat vastuussa kyberhyökkäyksistä



GRU



STRONTIUM (*Forest Blizzard*)
Data theft, phishing (military targets)

IRIDIUM (*Seashell Blizzard*)
Destruction: FoxBlade wiper;
CaddyWiper, Industroyer2

DEV-0586 (*Cadet Blizzard*)
Destruction: WhisperGate wiper,
data theft, influence operations

SVR



NOBELIUM (*Midnight Blizzard*)
Password spray, phishing
(Ukrainian and NATO member diplomatic targets)

FSB



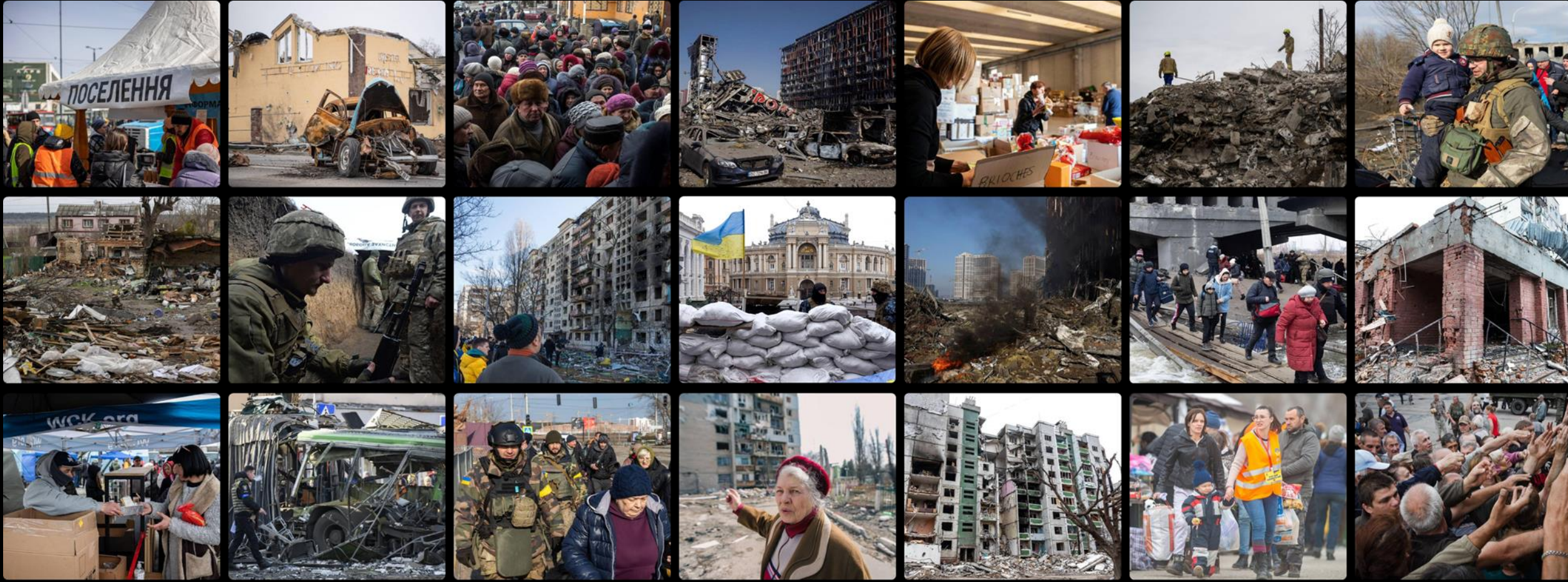
ACTINIUM (*Aqua Blizzard*)
Phishing, data theft

BROMINE (*Ghost Blizzard*)
Data theft

KRYPTON (*Secret Blizzard*)
Reconnaissance, phishing

Ensimmäisen **neljän kuukauden** aikana tapahtui enemmän kuin edellisten **kahdeksan vuoden**.

Ensimmäiset "laukaukset" käytiin cyberavaruudessa



23rd Feb 2022: The cyberwar started 10 hours before the physical invasion

Venäjän kybertoimet

Käyttää kyberoperaatioita se tukeakseen kineettistä sotaan mutta pyrkii myöskin videoväärennyksillä ja huijaussisällöllä vaikuttamaan omiin kansalaisiin, että myös Ukrainalaisiin ja erityisesti muihin NATO- maihin

Venäjän koordinoitua kyber- ja sotilasoperaatioita Ukrainassa



April 19

IRIDIUM launches destructive attack on Lviv-based logistics provider



April 29

IRIDIUM conducts reconnaissance against transportation sector network in Lviv



May 3

Russian missiles strike railway substations, disrupting transport service



March 4

STRONTIUM targets government network in Vinnytsia



March 6

Russian forces launch eight missiles at Vinnytsia airport³



March 16

Russian rockets strike TV tower in Vinnytsia



February 14

Odessa-based critical infrastructure compromised by likely Russian actors



April 3

Russian airstrikes hit fuel depots and processing plants around Odessa



February 28

Threat actor compromises a Kyiv-based media company



March 1

Missile strikes Kyiv TV tower



March 1

Kyiv-based media companies face destructive attacks and data exfiltration.



March 11

Dnipro government agency targeted with destructive implant



March 11

First direct Russian strikes hit Dnipro government buildings, among others



March 2

Russian group moves laterally on network of Ukrainian nuclear power company



March 3

Russia's military occupies Ukraine's largest nuclear power station



LEGEND



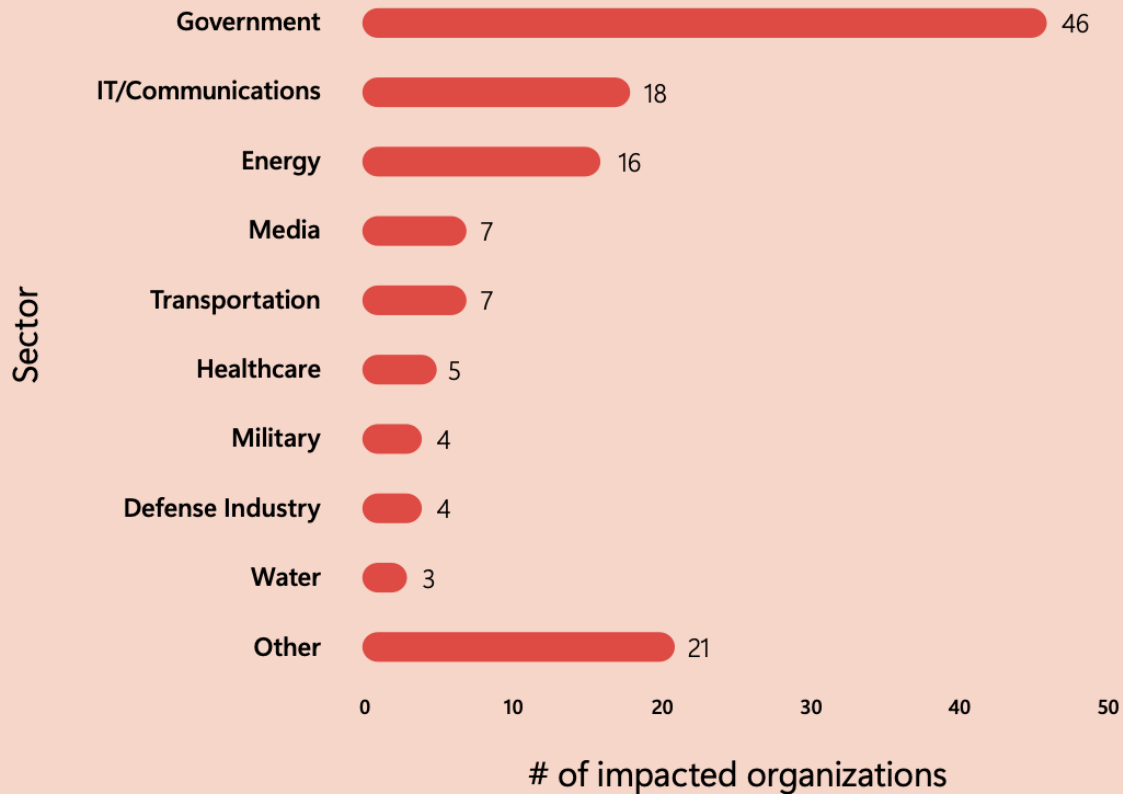
Cyber



Kinetic

Hybridin sodankäynnin kohteet toimialoittain Ukrainassa

Sample of Ukraine targets since Feb 2022

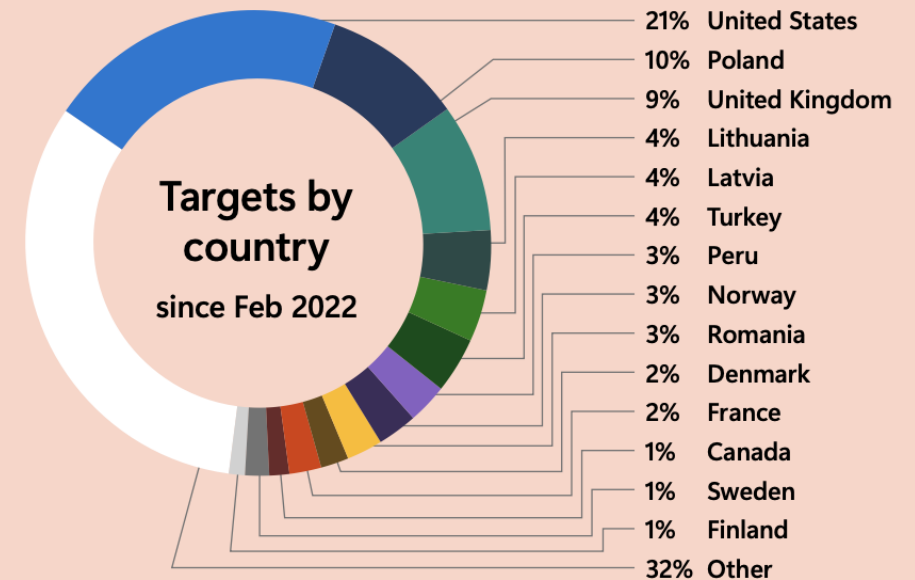
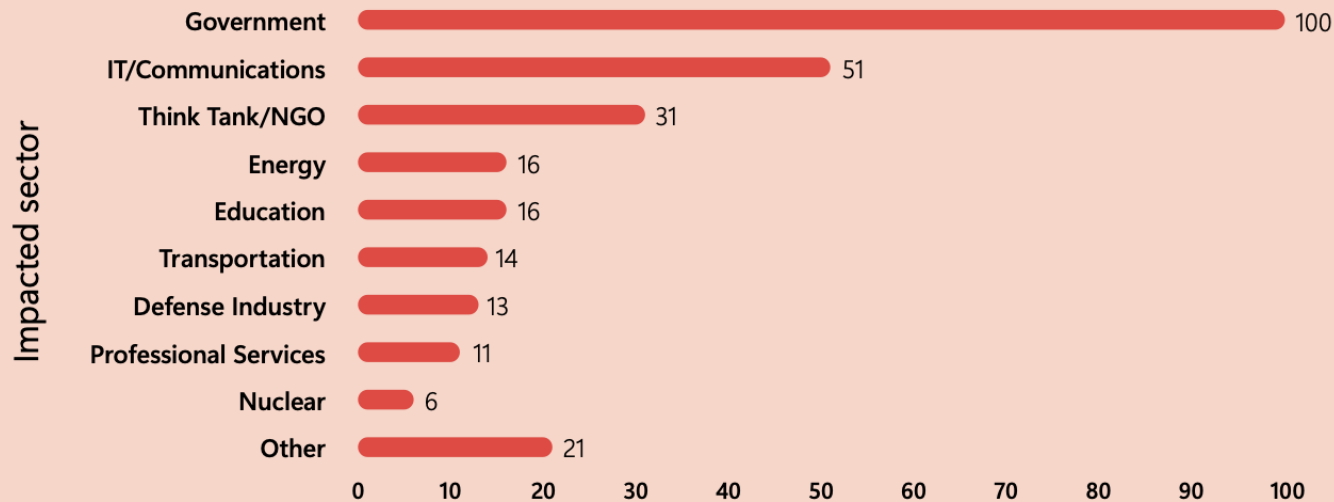


This chart provides a sample of Ukrainian sectors impacted by known or suspected Russian state-affiliated network intrusions or destructive attacks, as reflected in Microsoft data between February 2022 and January 2023.



Tarketoituit toimialat muissa maissa (ei Ukraina)

Targeted sectors outside Ukraine since Feb 2022



of observed events

- *Activities range from reconnaissance to data exfiltration.*
- *Russian threat actors most interested in government and IT sectors. Several actors compromise IT firms to exploit trusted technical relationships and gain access to those firms' clients in government, policy, and other sensitive organizations.*

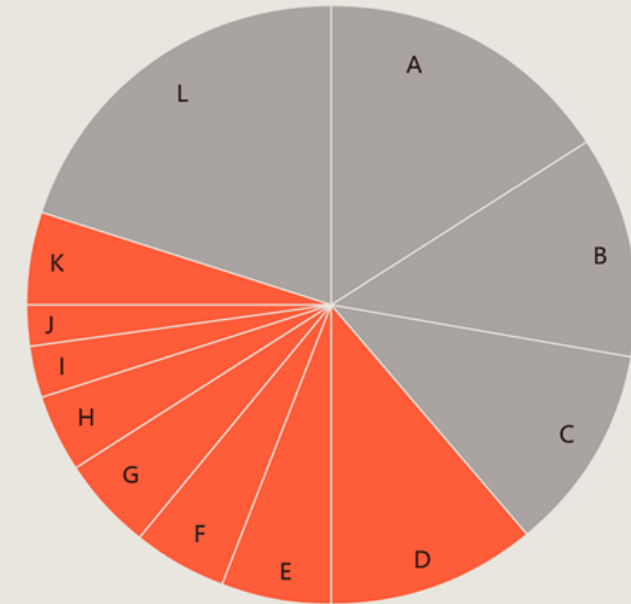
Kremlin kasvava focus kriittiseen infrastruktuuriin

- > Critical infrastructure targeting increased in the last year
- > Using techniques to establish persistence and evade detection

Most targeted sectors globally

State-sponsored threat groups target broadly as part of their intelligence collection.

Critical infrastructure sectors (highlighted) comprised 41% of the NSNs sent in FY2023.



Source: Microsoft Threat Intelligence NSN data.

Kreml hyökkää Ukrainan maataloussektoriin

KEY: ▲ Cyber activity ● Kinetic activity ■ Propaganda messages

JULY 17
Moscow withdraws from grain deal

JULY 22-23 ●
10 cruise missiles fired against key agricultural sites in Odesa

JULY 25-26 ▲
Seashell Blizzard lateral movement on a Ukrainian agricultural equipment organization's network

JULY 31 ▲
Seashell Blizzard conducts wiper attacks against 2 agriculture targets

AUGUST 2 ▲
Seashell Blizzard conducts reconnaissance on an agricultural organization's network

AUGUST 24 ●
Russian missiles target a civilian cargo ship in the Black Sea

SEPTEMBER 11 ▲
Suspected Russian military actor lateral movement at an agricultural support organization

JULY

AUGUST

SEPTEMBER

JULY 23 ■
Military equipment, rather than grain, was stored in Ukrainian hangars that were attacked

JULY 25 ■
Ukraine, US, and NATO abuse grain corridor for terrorist purposes rather than for humanitarian aid

JULY 26 ■
The grain deal was a disguise for supplying weapons to Ukraine

JULY 27 ■
The EU asked Russia to reduce their grain prices for "fair competition"

JULY 28 ■
Ukraine used the grain deal to export drugs

SEPT 5 ■
Moscow did not extend the grain deal because only the West benefited

SEPT 25 ■
Zelensky gave Poland an ultimatum about the grain embargo

Hybridisodan opetukset

Taistelut kriittisestä infrastruktuurista



The importance of moving fast
The need to move data across borders

Vuoden 2022 loppu

Arviolta 10 miljoonaa gigatavua Ukrainan hallituksen dataa on tallennettu pilvipohjaisille alustoille.

Yli 100 valtion tietokantaa on siirretty pilvialustoille ympäri Eurooppaa. Ukraina on varonut paljastamasta, missä palvelimet sijaitsevat.



Myös pankit siirtyivät pilvipalveluihin :

- Kesti 45 päivää siirtää kaikki kriittiset sovellukset pilvipalveluihin
- Tiedot siirrettiin 3 500 palvelimelta
- 4 petatavua dataa ja tapahtumia
- 270 tärkeää sovellusta
- Projektin teki 460 PrivatBankin IT-asiantuntijaa ja konsulttia

NV THE NEW VOICE OF UKRAINE

NATION BUSINESS LIFE OPINION

BUSINESS

Prova gratis beroende-frankallande.

PrivatBank moves all databases to the Cloud

29 April, 06:54 PM 261

[f](#) [t](#) [p](#) [e](#)



PrivatBank (Photo:Reuters)

Ensimmäiset opit tulevaisuudessa puolustukseen

Microsoft on oppinut useita strategisia oppeja osallistumisestamme Ukrainan puolustamiseen

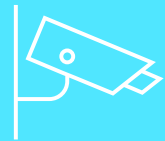
1. "Ei niin perusasioiden" merkitys
2. Jokainen sotaresurssi on kohde
3. Ihmisten ja luottamuksen kriittinen rooli
4. Tietojen jakamisella sekä julkisen ja yksityisen sektorin kumppanuuksilla on myönteinen vaikutus.

Sota-ajan painopisteet ja rauhan ajan valmius



Manufacturing companies

- Disrupt war production



CCTV cameras

- Tactical view of the battlefield



Personal protective services

- Gain intelligence on VIPs



Natural resources

- Disrupt upstream war production

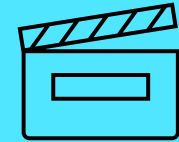


Industrial Controls

- Attacks against ICS systems

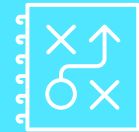
Electronic billboards

- Commandeered for news control



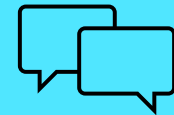
Logistics companies

- Gain picture/ disrupt support.



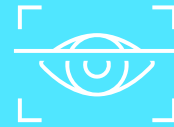
Communications & ISPs

- Disrupt comms. and info.



Local govts. along front lines

- Intel. gathering for occupation



Resiliency planning

- Migrate data outside borders



Keskeiset kyberuhkien sietokykyyn vaikuttavat asiat

How resilient is my organization?

80%

of incidents can be stopped by basic Security approaches (including Zero Trust, timely patching, MFA, and identity hygiene)

Microsoft studied victims of cyberattacks and found these factors to be the top 6 contributors to their vulnerability

Insufficient privilege access and lateral movement controls 92%

Insecure configuration of identity provider 86%

Limited adoption of modern security frameworks 85%

Lack of multi-factor authentication 74%

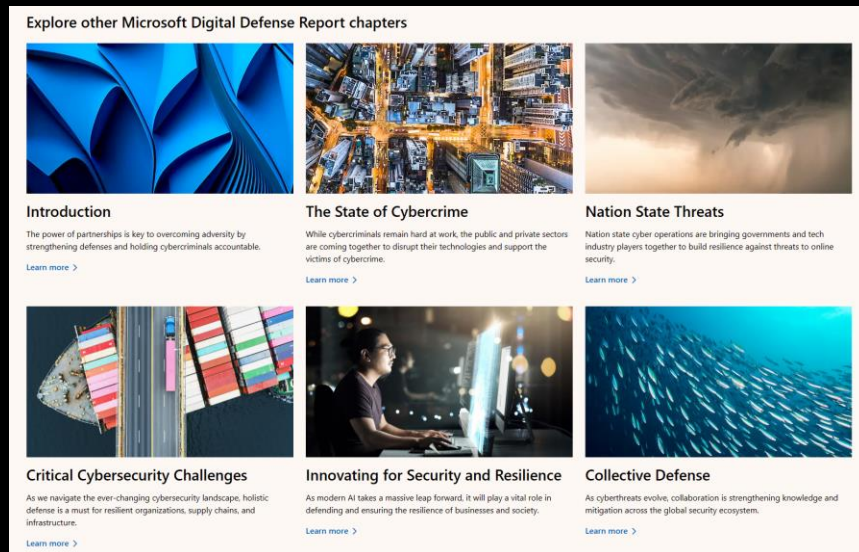
Lack of information protection controls 64%

Low maturity of security operations 58%

Microsoft Defense Report <https://microsoft.com/mddr>

Viimeisin ilmestyi lokakuussa 2024

Explore other Microsoft Digital Defense Report chapters



- Introduction**
The power of partnerships is key to overcoming adversity by strengthening defenses and holding cybercriminals accountable.
[Learn more >](#)
- The State of Cybercrime**
While cybercriminals remain hard at work, the public and private sectors are coming together to disrupt their technologies and support the victims of cybercrime.
[Learn more >](#)
- Nation State Threats**
Nation state cyber operations are bringing governments and tech industry players together to build resilience against threats to online security.
[Learn more >](#)
- Critical Cybersecurity Challenges**
As we navigate the ever-changing cybersecurity landscape, holistic defense is a must for resilient organizations, supply chains, and infrastructure.
[Learn more >](#)
- Innovating for Security and Resilience**
As modern AI takes a massive leap forward, it will play a vital role in defending and ensuring the resilience of businesses and society.
[Learn more >](#)
- Collective Defense**
As cyberthreats evolve, collaboration is strengthening knowledge and mitigation across the global security ecosystem.
[Learn more >](#)



Muita raportteja:

Cyber Signals: [Cyber signals Archives | Security Insider \(microsoft.com\)](#)

Nation State reports: [Reports | Security Insider \(microsoft.com\)](#)

Kiitos

