

Cyber Threat Landscape

Bjørn Rasmussen
CTO Norway

Our research on
Cy-X / Ransomware
and **Hacktivism**



Cyberdefense

Today's itinerary (travel time ~50 mins)

1 Introduction
Speaker bio
Our research & intelligence org

3 Hacktivism
Geopolitics in
cyberspace

2 Cy-X
Cyber extortion
(ransomware)

4 Crossover
Cy-X and Hacktivism
commonalities





1

Introductions

Speaker bio

Our research and intelligence
organisation

\$whoami

- CTO for Orange Cyberdefense Norway
- GIAC certified CTI analyst
- 12+ years police & military service
 - NATO military operations
 - Afghanistan & Balkans
 - Combat engineer
 - Norwegian NCIS investigator
 - National Cybercrime Centre
 - Investigating organized crime and cyberattacks



Threat research and intelligence are part of our DNA.

Our cybersecurity experts, researchers and analysts monitor the latest threats and vulnerabilities, allowing you to stay ahead of threats and focus efforts where it matters.



250+

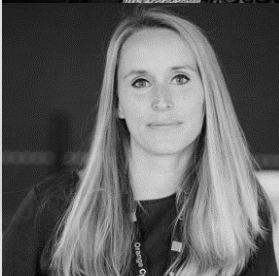
experts dedicated to R&D and threat research.

20%

of pentesters' time is dedicated to research.

50

days in advance our intel entries can be seen versus other sources.



80+

published papers and presentations at cyber conferences last year.

2.500

unique threat intelligence entries not known to any other source.

30

CVEs assigned to us by MITRE.



2

Cy-X

**Cyber extortion
(ransomware)**



A word on terminology

Cyber extortion (Cy-X)

Ransomware

Software family: many variants

Tools: who's responsible?

Technical focus: "how"

VS.

Cyber extortion

Criminal act

Legal framework: Victim, offender, rights

Human focus: "who", "why"

"Hack & leak" attacks:
extortion without
ransomware?

BLUF: The nature of the problem

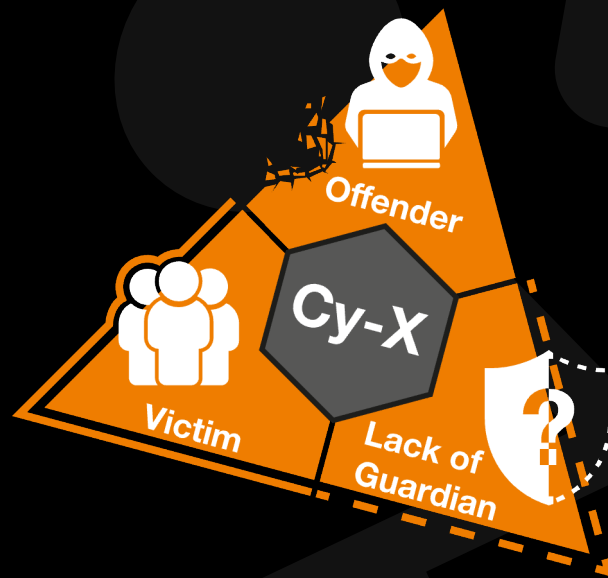
Cyber extortion as Routine Activity Theory¹

Cybercrime as a service

- **Evolution:** 7-8 years from “shotgun” to “big game hunting”
- **Politization:** Victimology, recruitment

Target-rich environment

- **Value:** Ransom payments record high
- **Inertia:** Speed of digitization
- **Visibility:** Attack surface management
- **Access:** Internet is the new LAN, identity is the new perimeter



Deterrence

- **Law enforcement action** takes time
- Security standards not enforced
- Private cybersecurity is costly (SMBs)

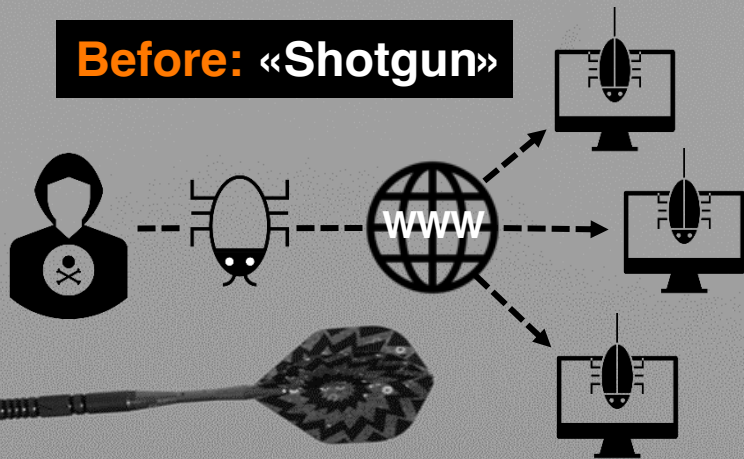
1. <https://doi.org/10.2307/2094589>

Criminal evolution

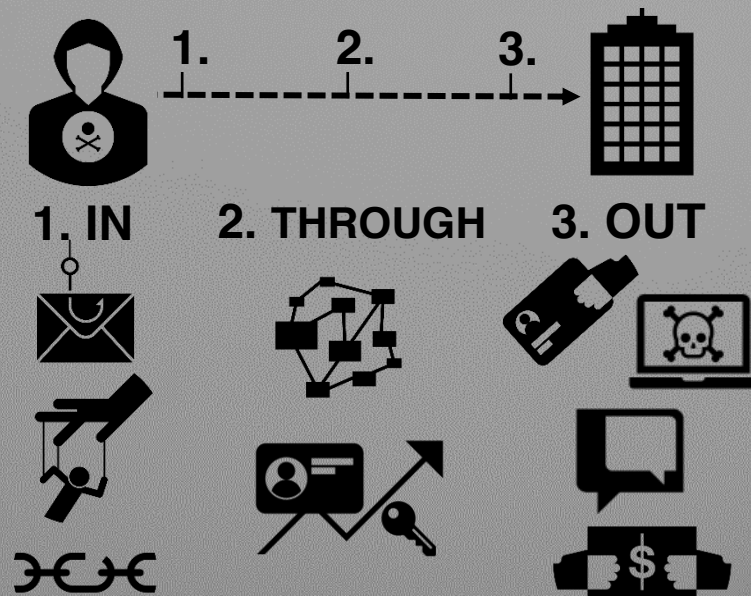
From “shotgun” to “big game hunting”



Before: «Shotgun»



Now: «Big-game hunting»



Target-rich environment

Ransom payment statistics



Victim

go.chainalysis.com/crypto-crime-2024.html

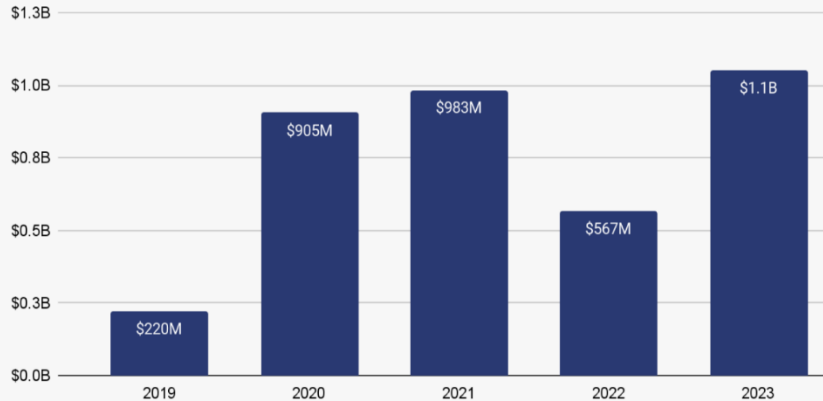
Chainalysis

FEBRUARY 2024

The 2024 Crypto Crime Report

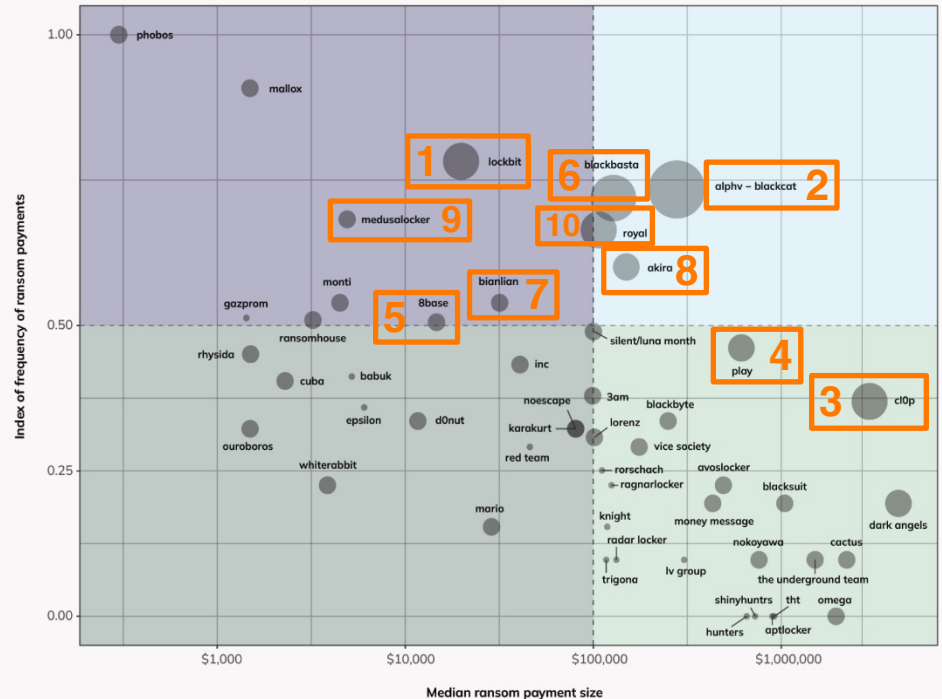
The latest trends in ransomware, scams, hacking, and more

Total value received by ransomware attackers
2019 - 2023



Top 50 ransomware strains by median payment size and payment frequency

Note: Bubble size denotes total 2023 ransom inflows

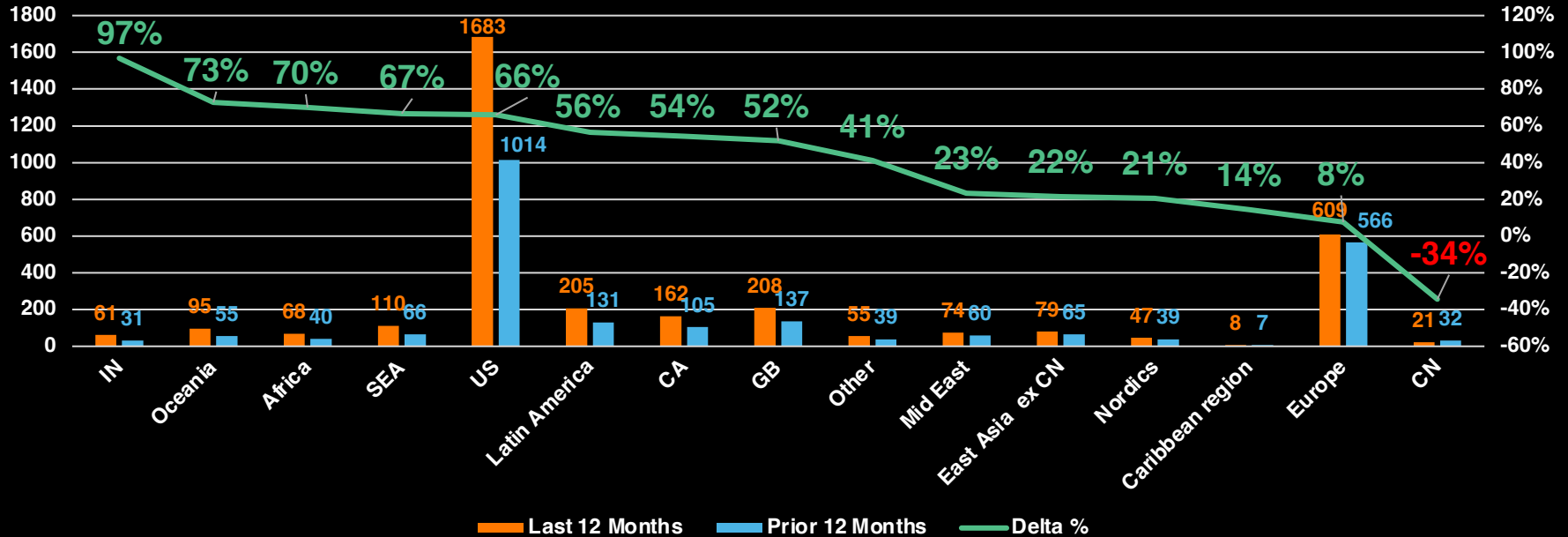


Target-rich environment

Distinct victims per country 2022 vs. 2023 comparison



Regional shift in the past 24 month

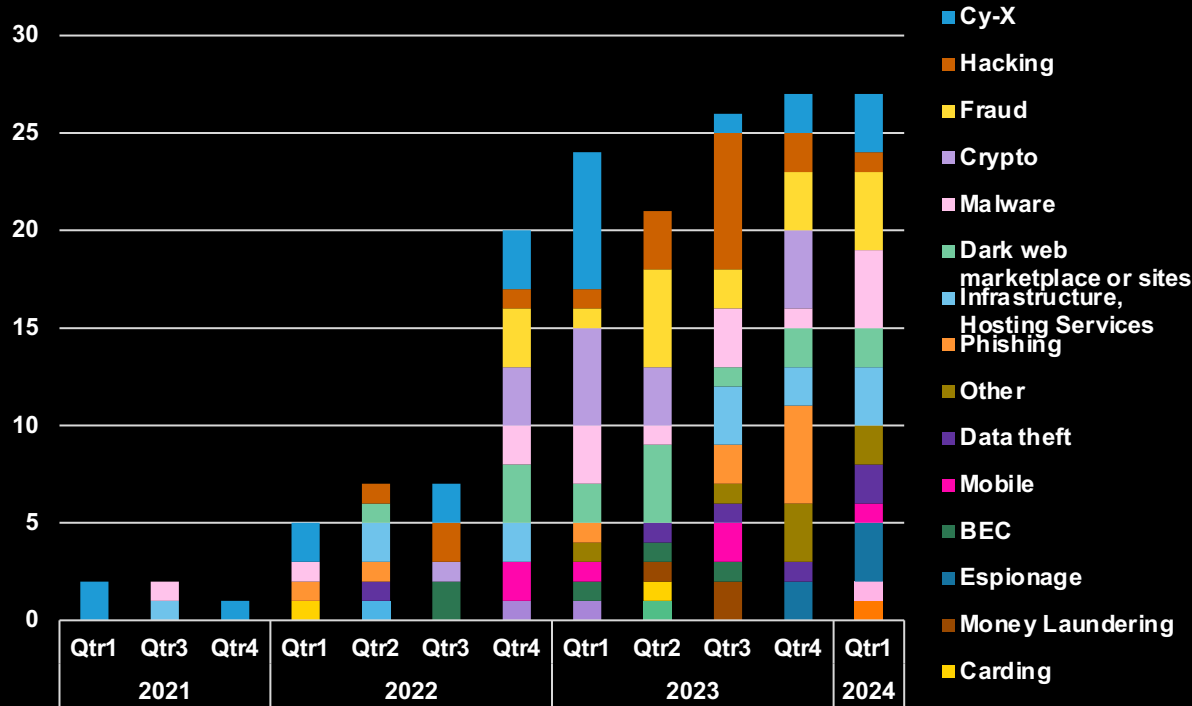


Deterrence

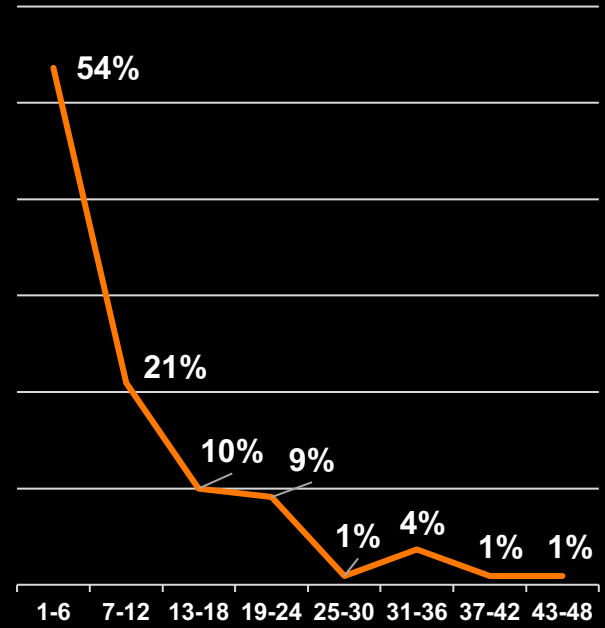
Why is disruption of Cy-X ecosystem so difficult?



Law Enforcement Activities

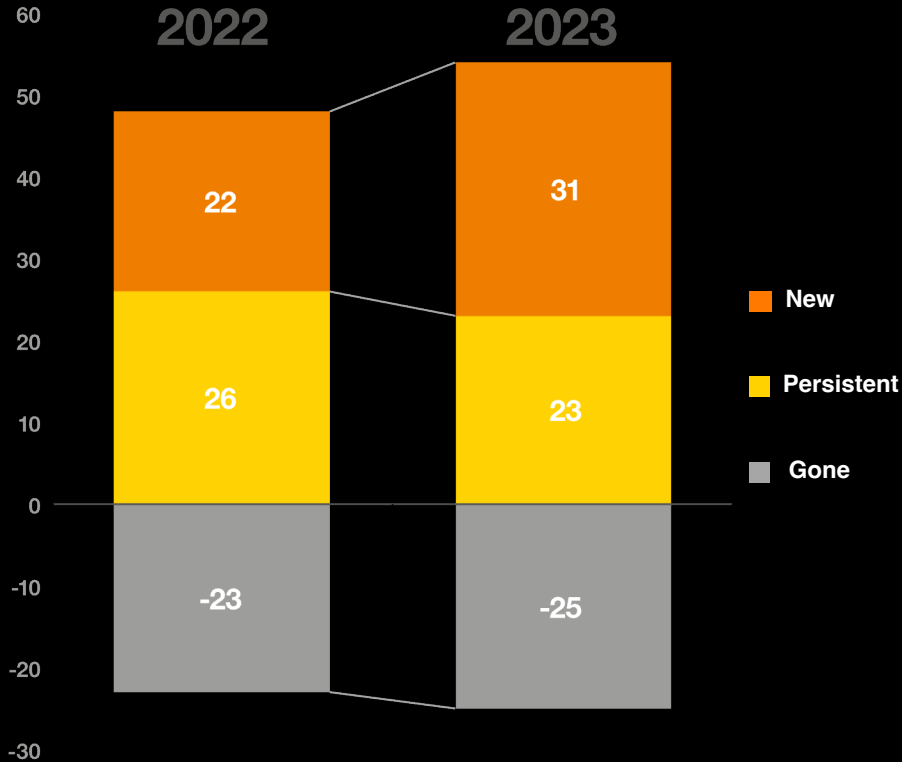


Threat actor lifespan

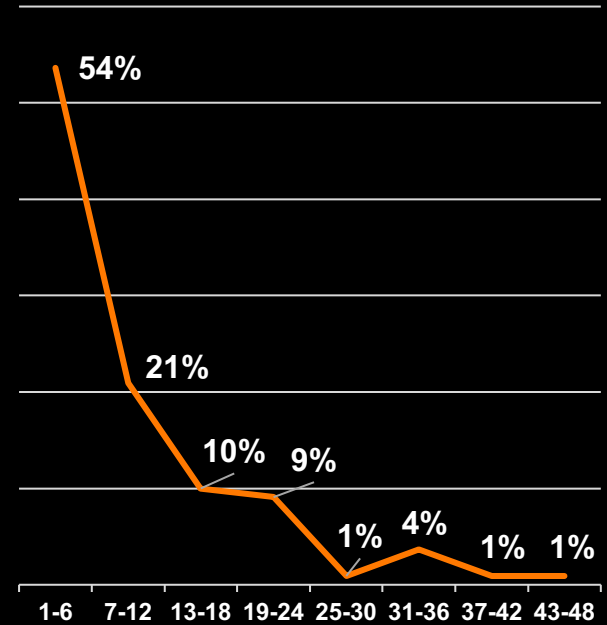


Deterrence

Why is disruption of Cy-X ecosystem so difficult?



Threat actor lifespan

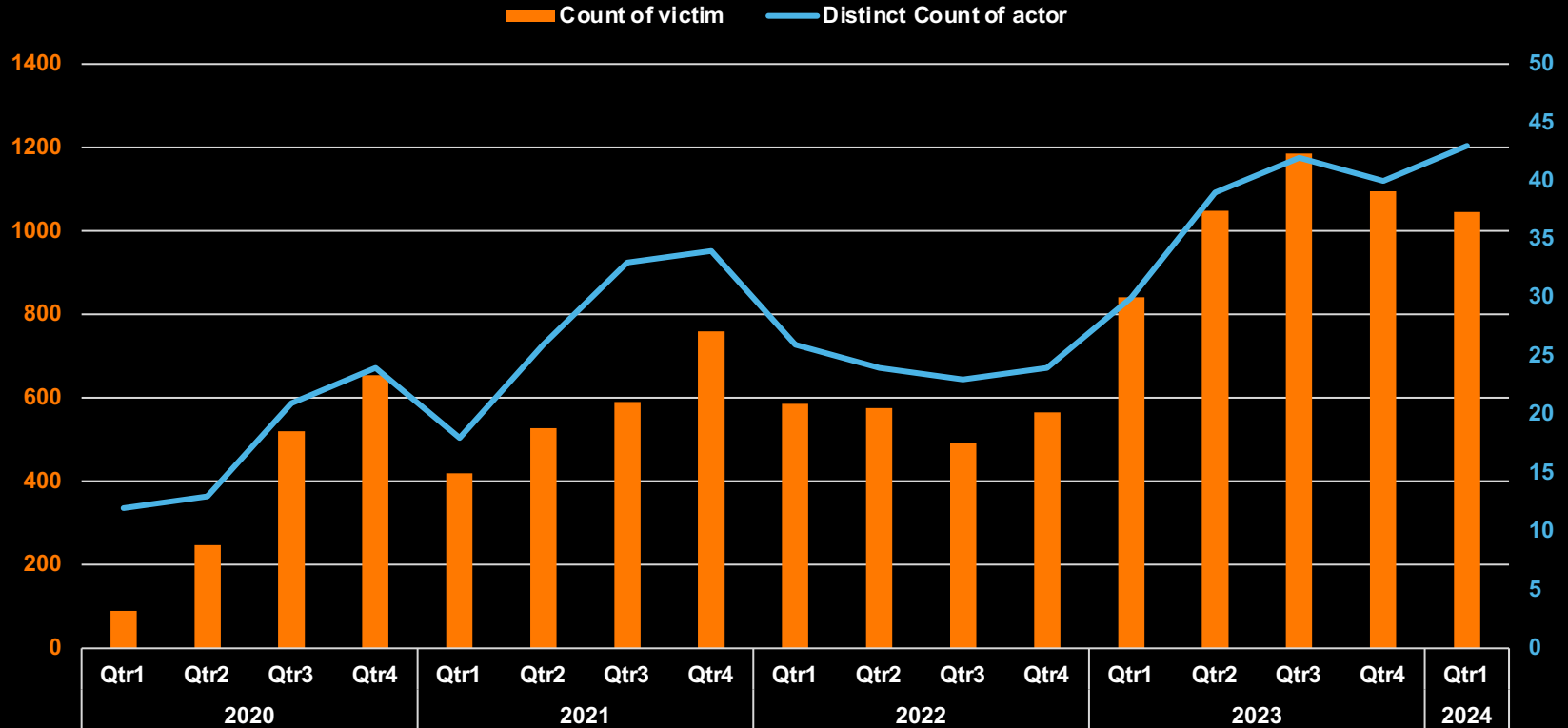


Cyber Extortion Development

Global victims and offenders over time

n=11,244

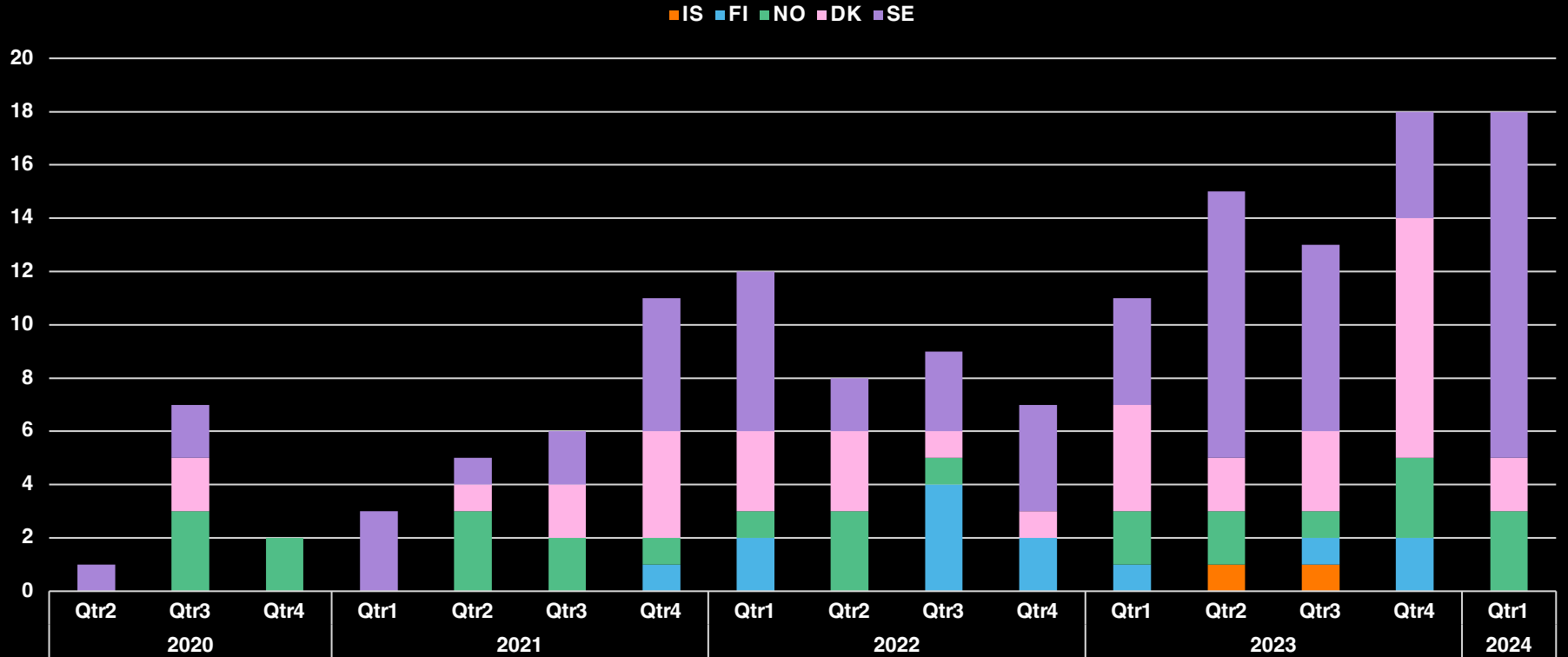
n=123



Cyber Extortion Development

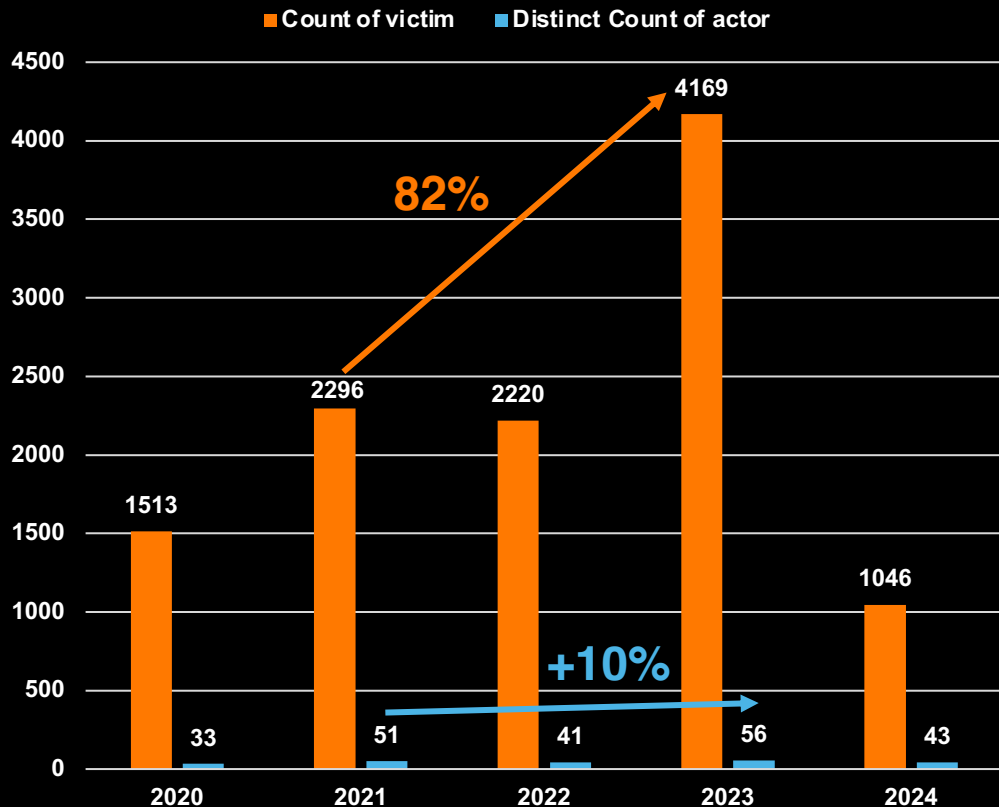
Impact to the Nordic countries

n=146

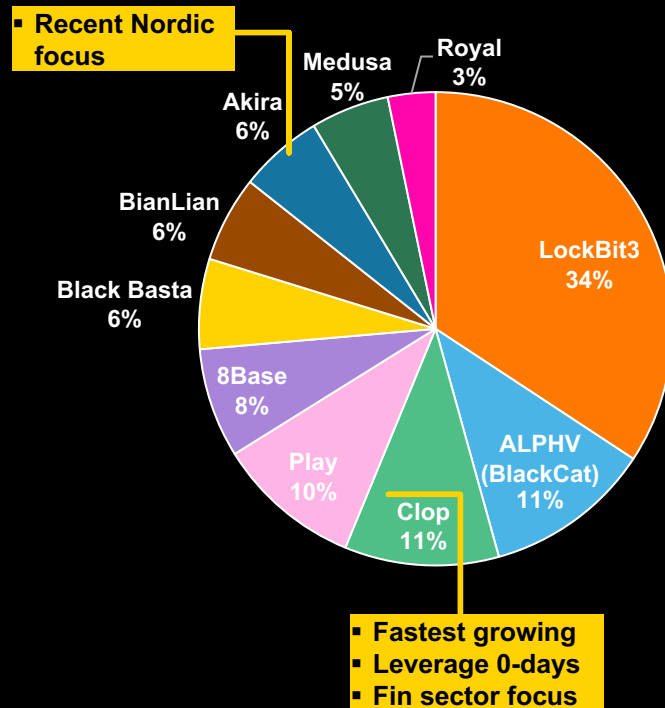


Cyber Extortion Development

Global year by year comparison



Top 10 Cy-X groups



Cyber Extortion Ecosystem

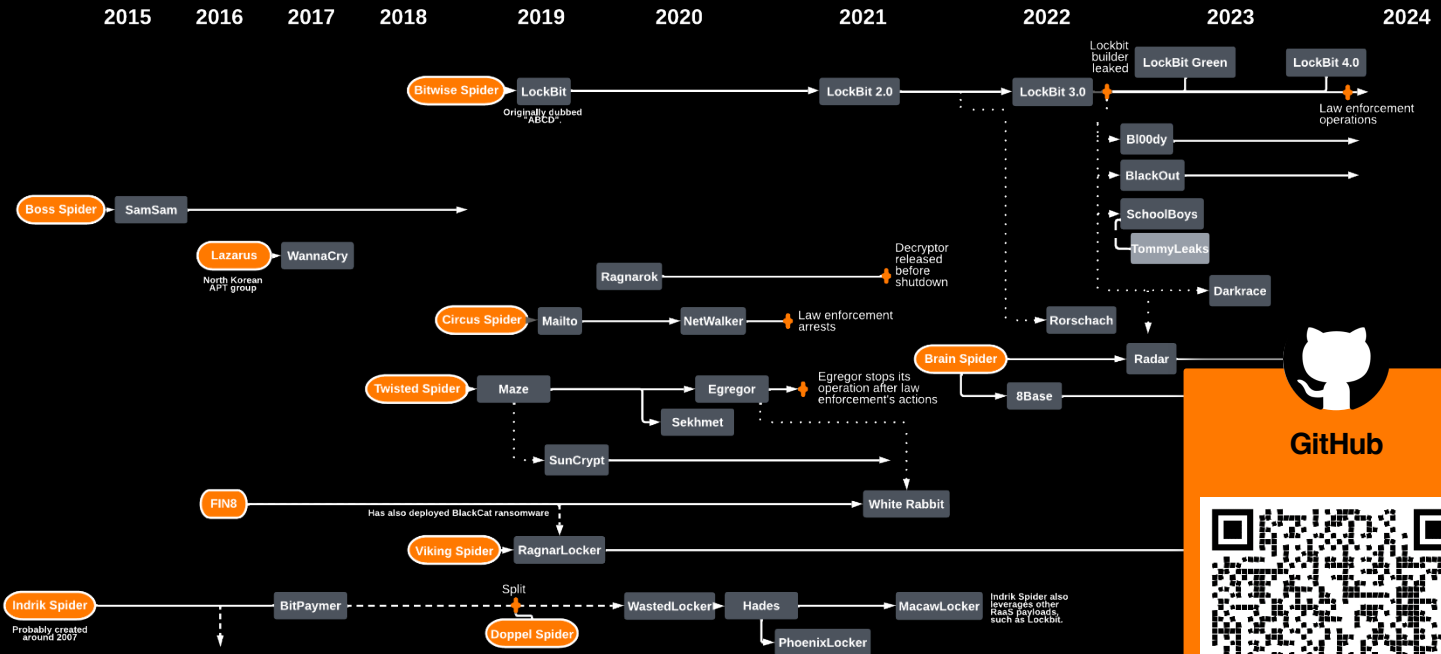
Our CERT “Ransomware map”

Cyberdefense



Ransomware cartography (2014-2024)
 © MIT Center for Cyber Operations

Legend:
 - Ransomware groups
 - Ransomware variants
 - Ransomware attacks
 - Ransomware victims

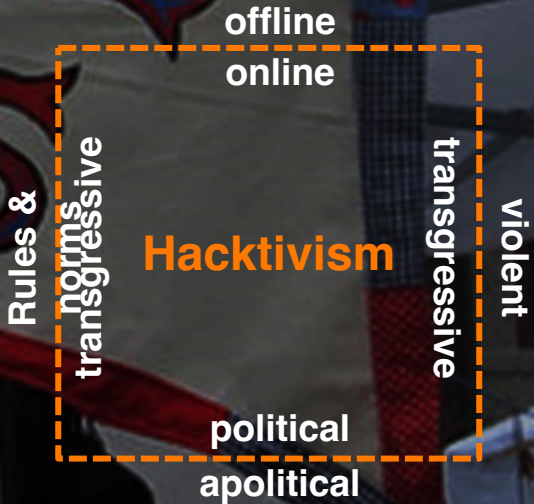


GitHub

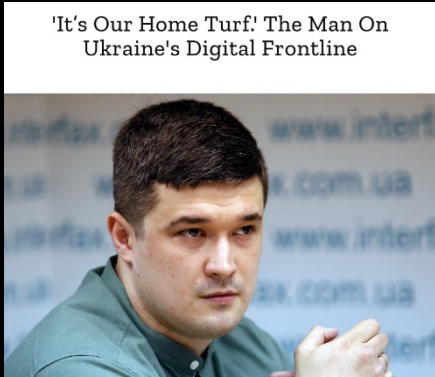


3

Hacktivism



Hacktivism | A state-sponsored activity



Source: Time magazine (2022)

“Ukraine’s cyber response plan was carefully crafted by its Minister of Digital Transformation – Mykhailo Albertovych Fedorov – **who coordinated one of the most successful, multifaceted information operations campaigns ever witnessed in history.**”

Source: [Darkowl.com](https://darkowl.com)

Mykhailo Fedorov @FedorovMykhailo

We are creating an IT army. We need digital talents. All operational tasks will be given here: t.me/itarmyofurraine. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.

[t.me](https://t.me/itarmyofurraine)
Telegram: Contact @itarmyofurraine

7:38 PM · Feb 26, 2022

9,076 Reposts 1,305 Quotes 20.9K Likes 852 Bookmarks

Hactivism | Pro-Russian Hactivism in DK

Hvis danske myndigheder tror, at vi vil stoppe vores cyberangreb, så tager de fejl. Så længe de støtter Zelenskyjs kriminelle regime, vil vi fortsætte med at teste deres internetinfrastruktur til det yderste.

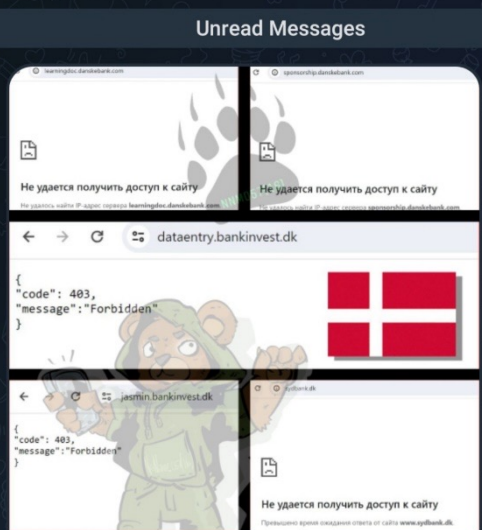
NoName057(16)

Pro-russisk hackergruppe

NoName057(16) har taget ansvaret for en række af de DDoS-angreb, der bl.a. ramte Forsvarsministeriets, Københavns lufthavns, Movias, DOT's, Trafikstyrelsens og en række kommuners hjemmesider i slutningen af februar 2024. Angrebene kommer i kølvandet på regeringens udmelding om, at Danmark garanterer økonomisk støtte til Ukraine de næste 10 år.

February 23

Unread Messages

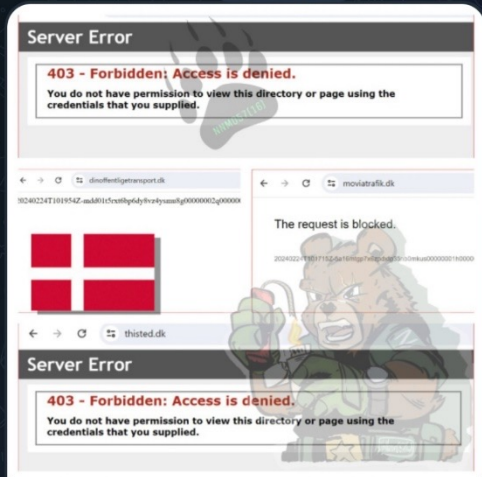


Denmark has guaranteed aid to Ukraine for the next ten years.

Denmark and Ukraine have signed an agreement on long-term support for Kiev. Copenhagen promised that Ukraine could receive F-16 fighter jets as early as summer.

At the moment Denmark can't help itself and "lift" its websites after our cyberattack 🐾:

February 24



We **continue** to cause material damage in Denmark and this time the logistics industry 🐾 has fallen under our spite:

✗ Movia is Denmark's largest transportation company
<https://check-host.net/check-report/15e66aedka47>

✗ DOT service that provides customer service, coordinated traffic information, coordinated schedules and ticketing
<https://check-host.net/check-report/15e66c4ckb0f>

Hactivism | Ongoing geopolitical conflicts

- GhostSec – Hack/DDoS
- SecJuice - OSINT
- Belarusian Cyber-Partisans - Ransomware
- BeeHive Cybersecurity – Hack/Sec
- HackenClub - Hack
- studentcyberarmy - DDoS
- CyberPalyanitsa - DDoS
- Cybercossacks - DDoS
- NAFO - Psyops
- Anonsec Italia – Hack/DDoS
- Saint Javelin - Psyops
- Ukrainian Cyber Alliance - Hack
- HimarsDDoS - DDoS
- IT Army of Ukraine – DDoS/Hack
- Cyber Legions – Hack
- Ukrainian Hackers Group – Hack/DDoS
- KT “special CIA Operation – OSINT
- Cyber Anarchy Squad – DDoS/Hack
- FRC Army UA – DDoS
- Cyber Resistance – Hack
- Cybersecs – DDoS
- CyberPolk - Hack
- AltroAnon - DDoS/Hack
- Hack Your Mom - Hack
- International Intelligence Legion - OSINT
- cyber-Regiment - DDoS/Hack
- Twelve - DDoS/Hack
- YourAnonUKRIR - DDoS
- Windef - Hack
- HGH - Hack
- AltroX – DDoS
- Ghostclan – DDoS/Hack
- AnonGhost – DDoS/Hack
- Anonymous Romania – DDoS
- Kromsec – Hack

NEW ADDITIONS

- Clawritsec – DDoS
- HDR0 – Deface/Hack
- InformNapalm – Infoops
- Blackwolves Team – DDoS
- Kobrig – Infoops/Hack
- Anon Koryos – DDoS
- Ukraine GUR - Hack

21 FEB2024 Russia Ukraine War CyberTracker #26 – 125 Total Groups

Pro-Ukraine - 44 Groups

Pro-Russia – 81 Groups

- RaHDit - Hack
- Bear IT Army - Hack
- DDoS/Infoops
- ZOV cyber army - Hack
- Cyber Front Z - Pysops/Dox
- Info Front VoZzdie – Psyops/Dox
- Cyber Army Russia - DDoS/Hack/Deface
- Legion - DDoS
- Beredini - Hack/DDoS
- NoName057(16) - DDoS
- FHWLteam - Ransomware
- RedHackersAlliance – Hack/DDoS
- Anonymous Russia - DDoS
- Phoenix – DDoS/Deface
- JokerDPR – Hack/Psyops
- DDoSia Project - DDoS
- GhostWriter - Hack
- SandWorm - Hack
- Gamaredon - Hack
- Cadet Blizzard - Hack
- FancyBear/APT28 - Hack
- Turlia APT - Hack
- SaintBear/TA471 - Hack
- Calisto Group - Hack
- Russian Hackers Team - DDoS
- Infinity Hackers By – DDoS/Hack
- Anonymous Sudan - DDoS
- Usersec – DDoS
- Zarya legion – DDoS
- 62IX - DDoS
- Net-Worker - DDoS
- Solntsepyok - Hack
- Combatosint - OSINT
- Ember Bear - Hack
- UAC-0099 – Hack
- UAC-0050 – Hack
- Storm-0978 (RomCom) – Hack
- akur.group – DDoS
- Krypton Botnet - DDoS
- Patriot Black Matrix – DDoS
- Zulik Group - DDoS
- Nethunters – DDoS
- Anonymous Central Russia – DDoS/Hack
- Voshod – DDoS
- Sila_ikc – DDoS
- Darkseek – DDoS
- Rubit - DDoS
- Ruddos – DDoS
- Jar2 Zov - DDoS
- Russianbirdsec - DDoS
- Onfpower – DDoS
- Bear Spaw – DDoS
- Server Killers – DDoS
- RussiaV2022 – Infoops
- InfoCentre - Infoops
- NEW ADDITIONS
- Fr13nds - DDoS
- Mrakoborecniev - Infoops
- Darkstorm - DDoS
- Pravdanf - Infoops
- Skynet_Botnet (GodZilla) - Botnet
- Istocni_front - DDoS
- Cyber Dragon - DDoS
- We are Legion - DDoS
- Just Evil (Killmilk) – DDoS/Hack
- R00TK1T - Hack
- Kingofversus - DDoS
- Darknet Joker – DDoS/Deface
- Russian Cult Group - DDoS
- Kanehill – DDoS/Deface
- Anonymous Legion - DDoS
- Grafnetworks – DDoS/Hack
- CoupTeam - DDoS
- Killnet 2.0 - DDoS
- Phanonas Cyber Army (PCA) – DDoS/Hack
- Federal Legion - DDoS
- Mistnet (botnet) - Botnet
- CortadorZ - DDoS
- WolfframiumZ - Infoops
- Xhinetsha - DDoS
- Angel_anoncent - Infoops
- Robin Hood Cyber – DDoS/Deface
- Skillnet - DDoS
- ClowmsNet - DDoS
- Blooder V2 – DDoS
- 22C – DDoS/Deface

Orange = Capability

Hactivism | Ongoing geopolitical conflicts

02 NOV2023 Israel-Palestine CyberTracker #5 – 137 Groups

Pro-Israel - 19 Groups

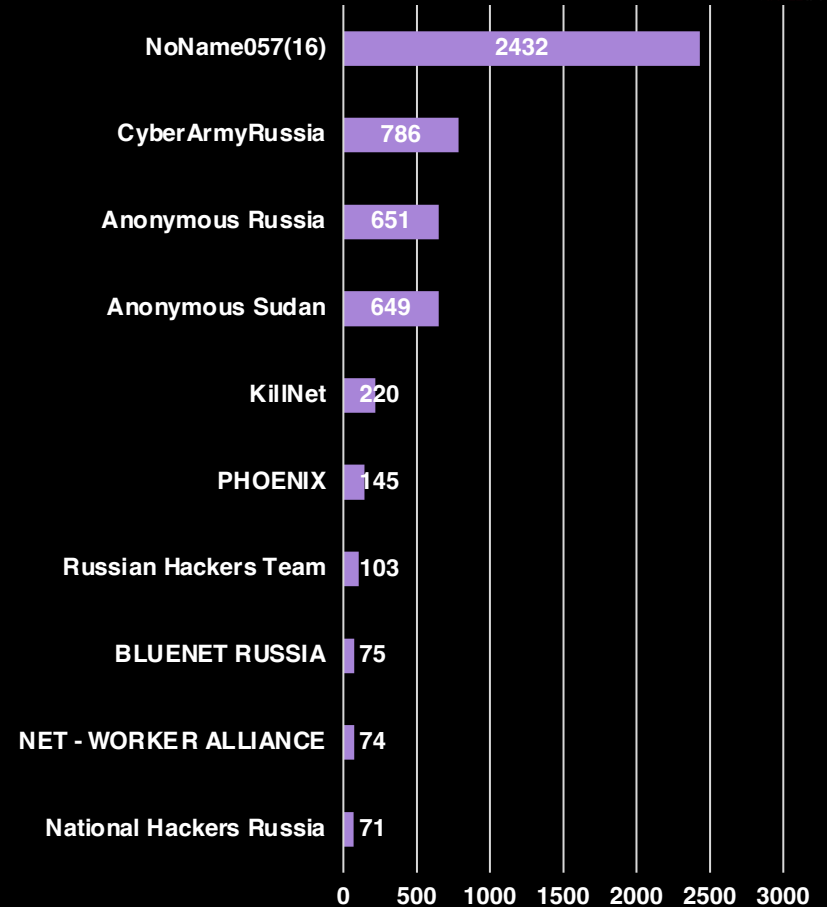
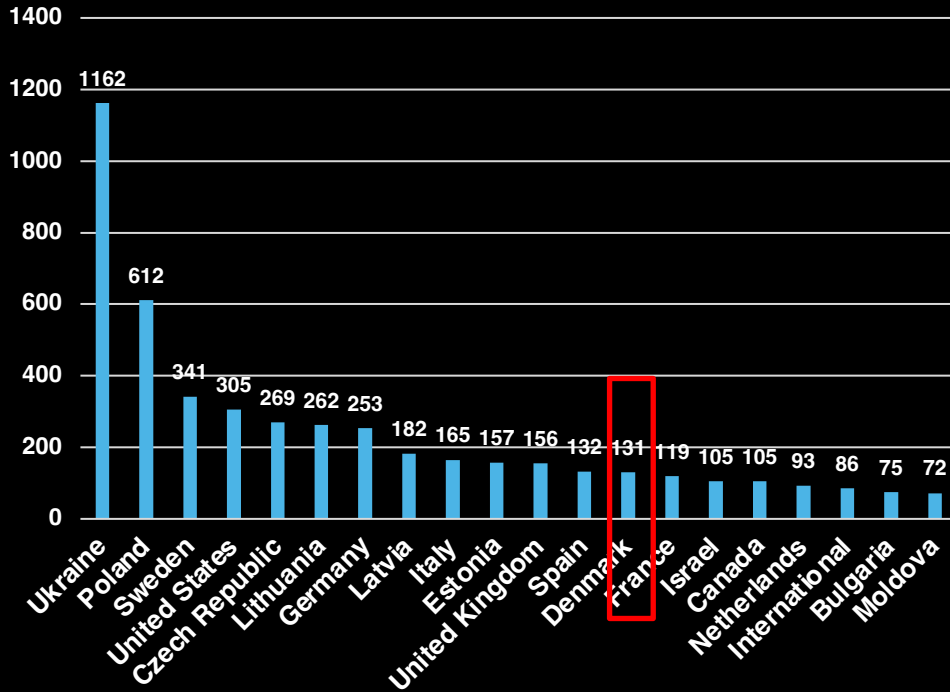
- Team UCC Operations – DDoS
- Garuna Ops – DDoS
- Indian Cyber Force – Hack/DDoS
- SilentOne – DDoS
- Kerala Cyber Xtractors – DDoS
- Gaza Parking Lot Crew – Hack
- AnonymMiss – DDoS
- Termux Israel – DDoS/Hack
- Silencers of Evil – Hack
- Israel Cyber Defence – DDoS
- **Predatory Sparrow – Hack**
- Glorysec – Hack
- Dark Cyber Warrior – DDoS
- Anonymous India – DDoS
- Red Evils – DDoS/Hack
- Ares – Data Leak
- Op Iran – DDoS/Hack
- NEW ADDITIONS**
- Kerala Cyber Thunders – DDoS/Deface
- Black Dragon Sec – DDoS/Deface

Pro-Palestine/Anti-Israel – 118 Groups

- **Mysterious Team Bangladesh – DDoS**
- Team HeroX – DDoS
- Ghosts of Palestine – DDoS
- AnonGhost – DDoS
- Blackshieldcrew MY – DDoS
- GhostClan – DDoS
- **Anonymous Sudan – DDoS – Pro Russian**
- Team insane Pakistan – DDoS
- GanoSec team – DDoS
- Team Azrael Angel of Death – DDoS
- Garnesia Team – DDoS
- Moroccan Black Cyber Army – DDoS
- Hactivist Indonesia – DDoS
- 4 Exploitation – DDoS
- Gb Anon 17 – DDoS
- Team r70 – DDoS
- Electronic Tigers Unit – DDoS
- YourAnonTBX – DDoS
- StuxTeam – DDoS
- Hizbullah Cyb3r Team – DDoS
- StarsX Team – DDoS
- Cscrow – DDoS
- SynixCyberCrimeMY – DDoS
- TYG Team – DDoS
- Eagle Cyber Crew – DDoS
- Ghost Clan Malaysia – DDoS
- 1015 Team – DDoS
- **Killnet – DDoS – Pro Russian**
- Panoc team – DDoS
- Sylhet Gang-SG – DDoS
- Muslim Cyber Army – DDoS
- Anonymous Morocco – DDoS
- Pakistani Leaf Hackers – DDoS
- **Cyber Avengers – Hack**
- GhoStSec – Hack/Ransomware
- Weedsec – Hack
- Dragonforce Malaysia – DDoS/Deface
- Storm-1133 – Hack
- Cyb3r Drag0nz – DDoS
- End Sodoma – DDoS/Hack
- Usersec – DDoS/Deface – Pro Russian
- Tengkorakcyber – DDoS
- Khalifah Cyber Crew – DDoS/Deface
- Skynet – DDoS
- ACEH – DDoS/Hack
- Boom Security – DDoS
- DevilAttacks – DDoS
- Moses Staff – Hack
- PMOI – DDoS/Hack
- Kep Team – DDoS
- Islamic Hacker Army – DDoS/Deface
- Arab Anonymous Team – DDoS
- Garuda Security – DDoS
- Anonymous BD – DDoS
- Stuxc Team – DDoS/Box
- Mysterious Silent Force – DDoS
- Ghost Princess of Palestine – DDoS
- Moroccan Ghosts – DDoS
- R4gn4r0k Gh0st – DDoS
- karawang cyber team – DDoS
- Komandan Hansip – DDoS
- Black Security Team – DDoS
- Tunisian Cyber Army – DDoS
- Cyber System Error – DDoS
- Ox Web Moroccan – DDoS/Deface
- Night Raid Cyber – DDoS/Hack
- ThreatMilitiy – DDoS
- Cyber Army Palestine – DDoS
- C.O.A Agency – DDoS
- Esteem Restoration Eagle – DDoS
- Ketapang Grey Hat Team – DDoS
- Lulz Security Agency – DDoS
- 313 team – DDoS
- HostKillCrew – DDoS
- cyber sederhana team – DDoS
- kuningan Exploiter – DDoS
- Xecatsha – Hack
- Infinite Insight.ID – DDoS/Hack
- Anony_M0us – DDoS
- Vulzsec – DDoS/Hack
- Haghjoyan – DDoS
- Ben M'Hidi 54 – DDoS/Hack
- Anonghost Indonesian – DDoS
- US Nexus Networks – DDoS/Hack
- Soldiers of Solomon – Ransomware
- RuBit – DDoS – Pro Russian
- The Returnees – DDoS/Deface
- The Cyber Watchers – DDoS/Hack
- Xv888 – DDoS
- Blacksec – DDoS/ Hack – Pro Russian
- iRoX Team – DDoS/Hack
- Darkseek Hacking Group – DDoS/Deface – Pro Russian
- Fallaga Team – DDoS
- Dark Strom Team – DDoS/Hack
- NEW ADDITIONS**
- Anonymous X – DDoS
- iEthesia – Hack
- Dark Olympuzt Crew – DDoS/Hack
- Kuwait Hackers – Deface
- 5ul4wes1 teng4h bl4ckhat – DDoS
- H4xor Umbarella Corp – DDoS/Deface
- The Camp 22 – DDoS/Deface
- Deadline – DDoS/Hack
- 1 teng4h bl4ckhat – DDoS
- IXP686secteam – DDoS/Deface
- /JRes As7 – DDoS
- The Ddoser Garuda – DDoS
- Padang System Error – DDoS/Hack
- Agen Massive – Deface
- Esteem Restoration Evil – DDoS/Deface
- Team 1956 – DDoS/Deface
- Nixon Cyber Team – DDoS/Deface
- Brave Redstorm Eagle – DDoS/Deface
- Indonesia Anonymous – DDoS/Deface
- FR13nds – DDoS
- 177 Members Team – Deface/DDoS
- Nothwh0me – Deface/DDoS
- Anonymous Collective – DDoS
- Malaysia Cyber Defacer – Deface

cyberknow.substack.com/p/israel-palestine-cybertracker-2nov

Hacktivism | Pro-Russian activity



Hactivism | Who attacks the Nordics and why

Ukraine support tracker

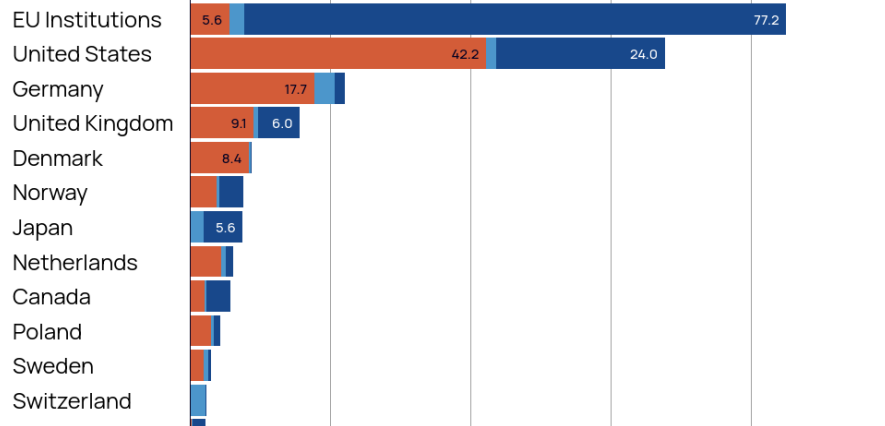
Government support to Ukraine: Type of assistance, € billion



Commitments Jan. 24, 2022 to Jan. 15, 2024. Data on 42 donors ; scroll to see more donors

■ Military ■ Humanitarian ■ Financial

Select the type of aid ▼



Source: Trebesch et al. (2023) "The Ukraine Support Tracker" Kiel WP

ifw-kiel.de/ukrainetracker

Disclaimer



For Media | EN / DE

Topics ▾ Experts Publications Institute ▾

Search

Kiel Institute

Data Set

Ukraine Support Tracker Data

Download

Facebook Twitter LinkedIn Email

Total bilateral aid to Ukraine separated in Type of aid, in \$Bln:

Country	Military	Humanitarian	Financial
United States	3.88930723	0.00000000	24.00000000
EU Institutions	0.00000000	0.00000000	77.20000000
United Kingdom	2.09127963	0.00000000	6.00000000
Germany	1.77000000	1.70000000	0.00000000
Poland	0.50000000	0.00000000	0.50000000
Canada	0.50000000	0.00000000	0.50000000
France	0.00000000	0.00000000	0.50000000
Japan	0.00000000	0.00000000	5.60000000
Norway	0.00000000	0.00000000	0.50000000
Italy	0.00000000	0.00000000	0.50000000
Sweden	0.00000000	0.00000000	0.50000000
Czech Republic	0.00000000	0.00000000	0.50000000
Portugal	0.00000000	0.00000000	0.50000000
Estonia	0.00000000	0.00000000	0.50000000
Greece	0.00000000	0.00000000	0.50000000
Australia	0.00000000	0.00000000	0.50000000
LTU	0.00000000	0.00000000	0.50000000
Ukraine	0.00000000	0.00000000	0.00000000
Sri Lanka	0.00000000	0.00000000	0.00000000
Finland	0.00000000	0.00000000	0.00000000

Open Ukraine Support Tracker
Related Working Paper

Authors

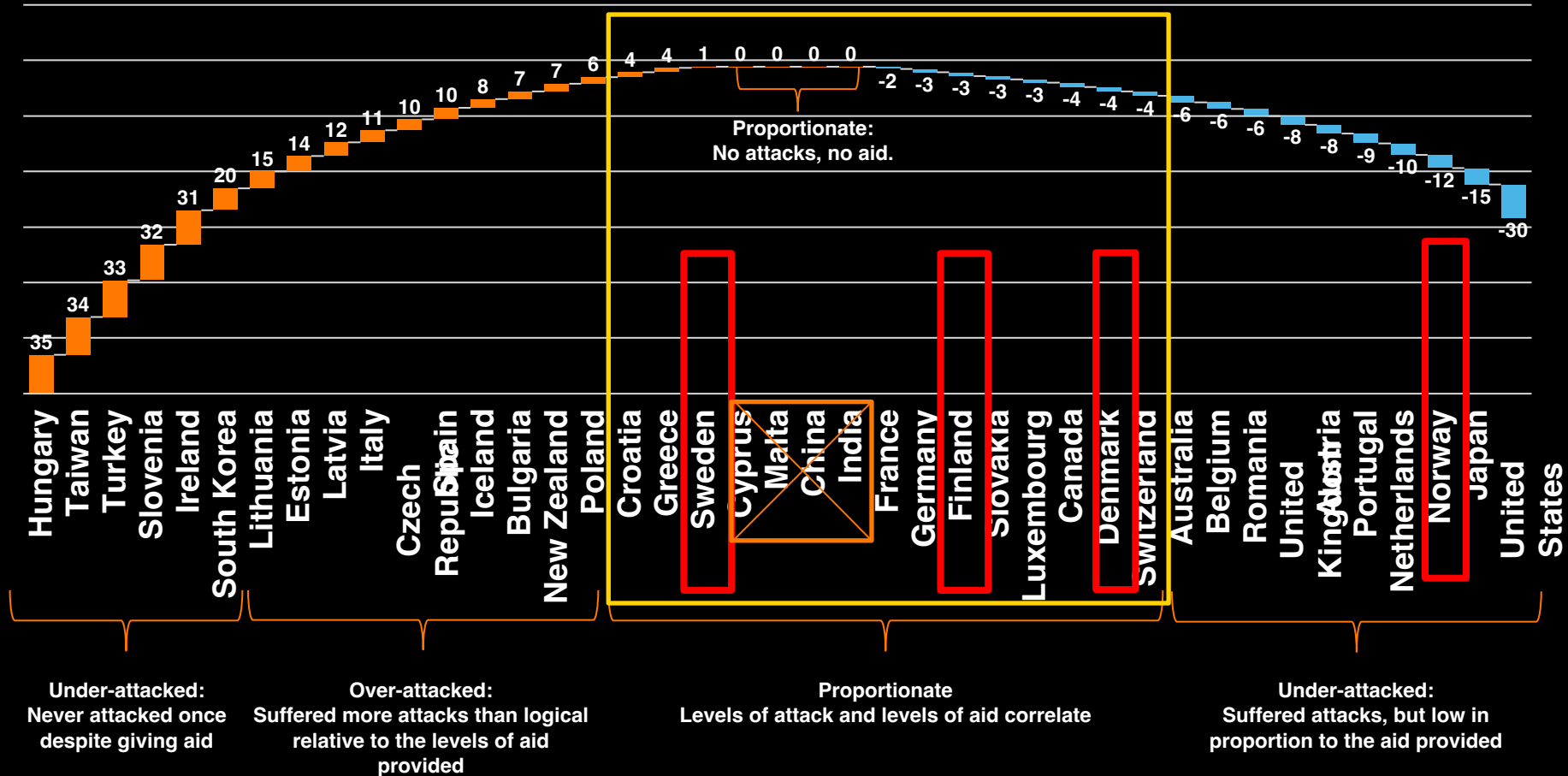
Arianna Antezza, Katelyn Bushnell, Andre Frank, Pascal Frank, Lukas Franz, Ivan Kharitonov, Bharath Kumar, Ekaterina Rebinskaya, Christoph Trebesch, Stefan Schramm, Leon Weiser, Christopher Schade

Publication Date

09/2023

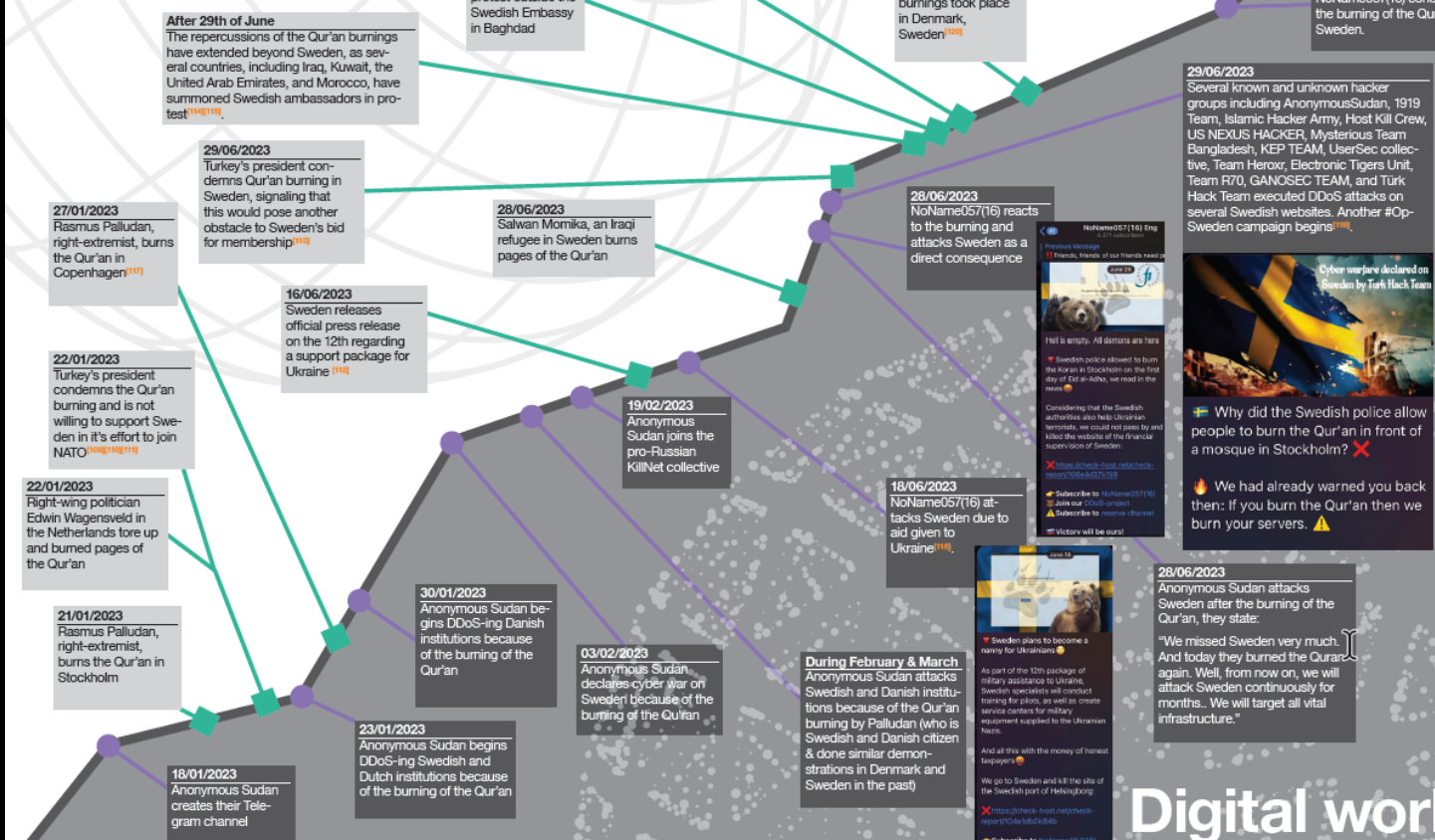
This database lists and quantifies military, financial and humanitarian aid transferred by governments to Ukraine since the end of diplomatic relations between Russia and Ukraine on January 24, 2022. It will be updated regularly. We focus on commitments from Western governments, namely by G7 and European Union member countries. We quantify government-to-government commitments, and provide preliminary (non-exhaustive) data on non-bilateral aid. To value in-kind support like military equipment or weapons, we use market prices and consider upper bounds to avoid underestimating the true extent of bilateral assistance.

We focus on bilateral donors. The largest group are the 27 EU member countries. Besides, we include the (remaining) G7 countries plus Australia, New Zealand, Norway, South Korea, Switzerland, Turkey, India, China, Taiwan, and Iceland. Moreover, we include assistance provided by the EU in the core database under EU (Commission and Council), European Peace Facility, European Investment Bank



A timeline of recent geopolitical events, showing pro-Russian hacktivist activity impacting the Nordics between January and August 2023

Physical world



27/01/2023
Rasmus Palludan, right-extremist, burns the Qur'an in Copenhagen^[17]

22/01/2023
Turkey's president condemns the Qur'an burning and is not willing to support Sweden in its effort to join NATO^{[18][19][11]}

21/01/2023
Rasmus Palludan, right-extremist, burns the Qur'an in Stockholm

After 29th of June
The repercussions of the Qur'an burnings have extended beyond Sweden, as several countries, including Iraq, Kuwait, the United Arab Emirates, and Morocco, have summoned Swedish ambassadors in protest^{[14][15]}

29/06/2023
Turkey's president condemns Qur'an burning in Sweden, signaling that this would pose another obstacle to Sweden's bid for membership^[11]

16/06/2023
Sweden releases official press release on the 12th regarding a support package for Ukraine^[11]

30/01/2023
Anonymous Sudan begins DDoS-ing Danish institutions because of the burning of the Qur'an

23/01/2023
Anonymous Sudan begins DDoS-ing Swedish and Dutch institutions because of the burning of the Qur'an

18/01/2023
Anonymous Sudan creates their Telegram channel

19/07/2023
Iraqi police officers trying to disperse a protest outside the Swedish Embassy in Baghdad

20/07/2023
Iraq expelled the Swedish ambassador in response to another planned Qur'an burning in Stockholm^[14]

28/06/2023
Salwan Morrika, an Iraqi refugee in Sweden burns pages of the Qur'an

19/02/2023
Anonymous Sudan joins the pro-Russian KillNet collective

03/02/2023
Anonymous Sudan declares cyber war on Sweden because of the burning of the Qur'an

During February & March
Anonymous Sudan attacks Swedish and Danish institutions because of the Qur'an burning by Palludan (who is Swedish and Danish citizen & done similar demonstrations in Denmark and Sweden in the past)

21/08/2023
Swedish Security Services raises terror threat level

22/07/2023
Several Qur'an burnings took place in Denmark, Sweden^[14]

28/06/2023
NoName057(16) reacts to the burning and attacks Sweden as a direct consequence

18/06/2023
NoName057(16) attacks Sweden due to aid given to Ukraine^[10]

25/08/2023
Denmark presents bill banning the burnings of scriptures^[14]

Events don't stop here - but this is meant as an excerpt of the chain of events.

14/08/2023
NoName057(16) condemns the burning of the Qur'an in Sweden.

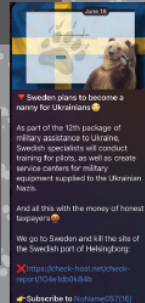
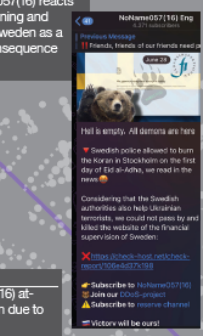
29/06/2023
Several known and unknown hacker groups including AnonymousSudan, 1919 Team, Islamic Hacker Army, Host Kill Crew, US NEXUS HACKER, Mysterious Team Bangladesh, KEP TEAM, UserSec collective, Team Heroxr, Electronic Tigers Unit, Team R70, GANOSEC TEAM, and Turk Hack Team executed DDoS attacks on several Swedish websites. Another #Op-Sweden campaign begins^[10].



Why did the Swedish police allow people to burn the Qur'an in front of a mosque in Stockholm? ❌

We had already warned you back then: If you burn the Qur'an then we burn your servers. ⚠️

28/06/2023
Anonymous Sudan attacks Sweden after the burning of the Qur'an, they state:
"We missed Sweden very much. And today they burned the Qur'an again. Well, from now on, we will attack Sweden continuously for months.. We will target all vital infrastructure."



Digital world



4

Crossover

What do Cy-X and
Hacktivism have in
common?

Cy-X politization



Offender

2021 RaaS affiliate ad

(RaaS) (80/20)

Introducing the Affiliate Program

Soft:

- C++
- The software is written without any dependencies
- ESXI/WIN/NAS
- Strong full encryption

Forbidden:

- Work in the CIS

- Draining builds and panel/blog addresses

- Any communication only TOX

- We take into work interesting targets for us to work

- When submitting an application, be prepared to answer a number of questions

- We do not work with English speakers (except if there is a Russian speaking partner)

- Work starts from 70% in your direction, the conditions are revised from the reputation, the volume of targets

Source: [linkedin.com/in/ilana-t-851889198/](https://www.linkedin.com/in/ilana-t-851889198/)

Commonwealth of Independent States (CIS)



Ransomware w/ hardwired geofencing...

2023 RaaS affiliate ad

Evidence of cooperation with other RaaS group (including, but not limited to, screenshots)
The best and quickest way to join is to pay a deposit (Returned to you after first getting paid)

Rules

We are not allowed to attack CIS as well as Cuba, North Korea, China and Romania.

Accounts that add false targets or have no activity for a certain period of time will be banned
Repeated attacks on paid targets are not allowed, encryption of non-profit hospitals is not allowed
After the target pays, you must fulfill all the terms and agreements promised in the negotiation

Source: x.com/azalsecurity/status/1755300909087707334

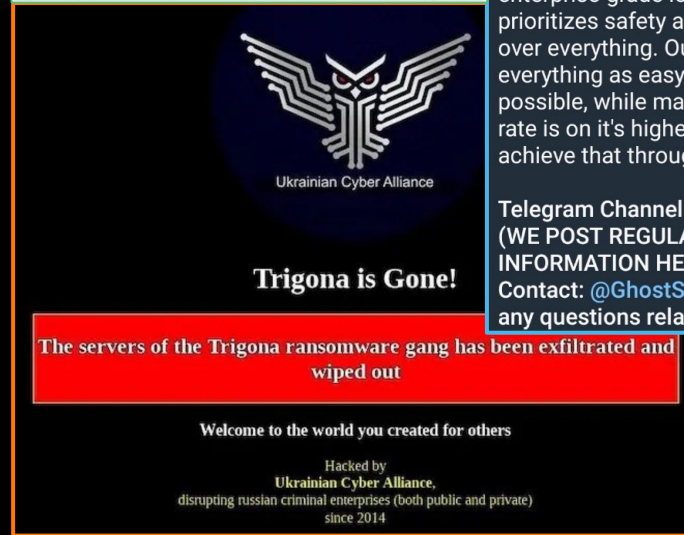
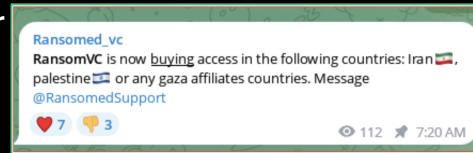
Hacktivism crossover to Cy-X

Strategy similarities

- **Recruitment:** Whether Cy-X affiliates on Darkweb forums, or political followers on Telegram
- **Success rate:** The success of their operations rely on how visible they are – to the victim and/or to the general public

Becoming very messy

- **Ukraine Cyber Alliance** targeted down Russian RaaS **Trigona**
- **RansomVC** looking to buy access in Iran or Palestine
- **Anonymous Sudan** has demanded ransom from DDoS victims (i.e. SAS in May 2023)
- **GhostSec** entering the RaaS ecosystem with their **GhostLocker** RaaS



Conclusion

The overall Cy-X and Hacktivism threat landscape has undergone **massive growth** in recent years

Evolution is **rapid** and **difficult to predict**

We see **direct & indirect geopolitical influence**, with clear political implications in the public messaging, victimology and recruitment

We see a **entanglement of cyber & physical** events in the targeting countries & governments

Organised cyberime play much more of an active role in information campaigns & **cognitive attacks**

- Spread Fear, Uncertainty & Doubt (FUD)
- Reputation as target

Offenders are getting better at **crowdsourcing capabilities**, **sharing resources** (such as infrastructure), adopting **new tactics rapidly** when the old ones fail

WHY AREN'T WE?

Orange
Cyberdefense

Thank you



[orangecyberdefense.com](https://www.orange-cyberdefense.com)

