Microsoft Security

Cybersecurity Operations & Influence: A Journey From Cyber-Crime to Cyber-war

Mihai George Forlafu
Senior Cybersecurity Architect

February 2025

Agenda

Introduction

Typical Cybersecurity Criminals

A Cybercrime That Changed the World

The Rise of Cybercrime Empires

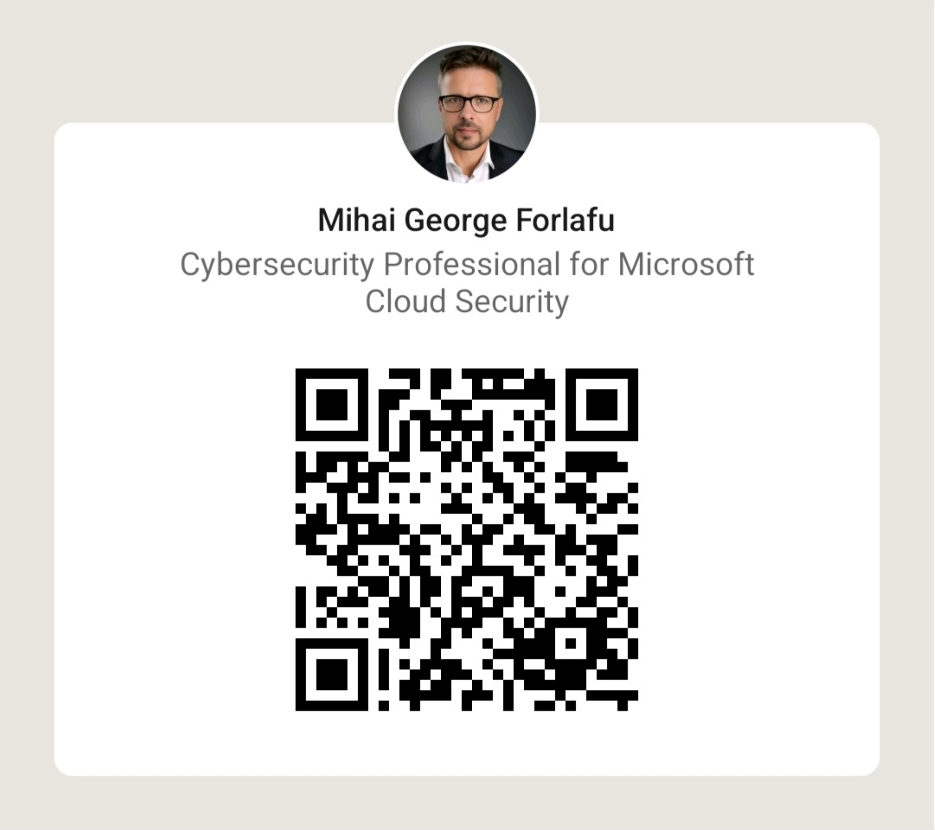
Cybercrime Meets Geopolitics

Cyberwarfare in Action

Key Take Aways

Q&A + Something Extra

Intro

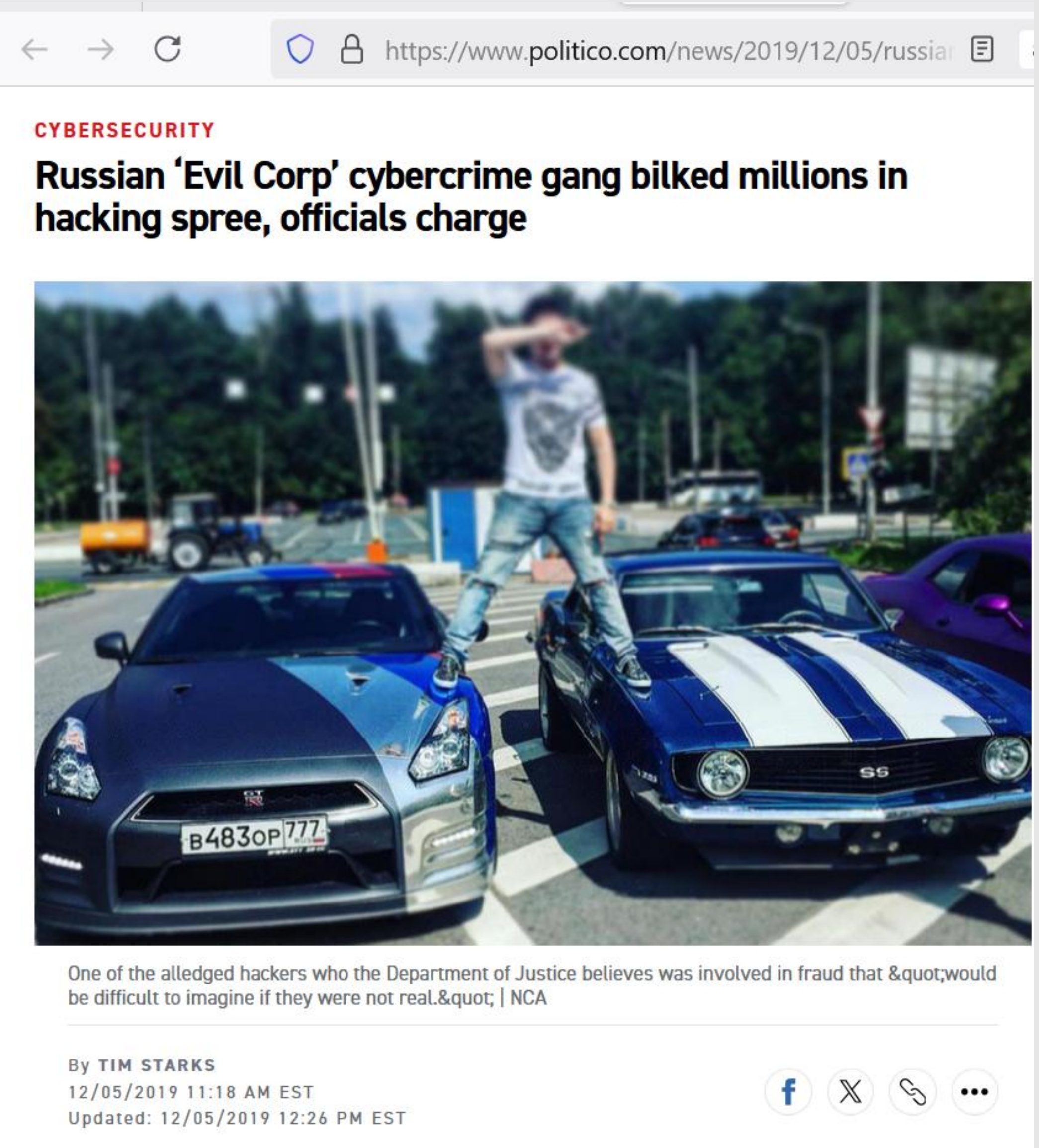


Mihai George Forlafu

Cybersecurity Professional for Microsoft Cloud Security

- Cybersecurity architect
- 11+ years in IT&C
- 6+ years in cybersecurity
- Former Microsoft, former Entrust / ICY Security / Columbus, ...and now Microsoft again.

Typical Cybersecurity Criminals



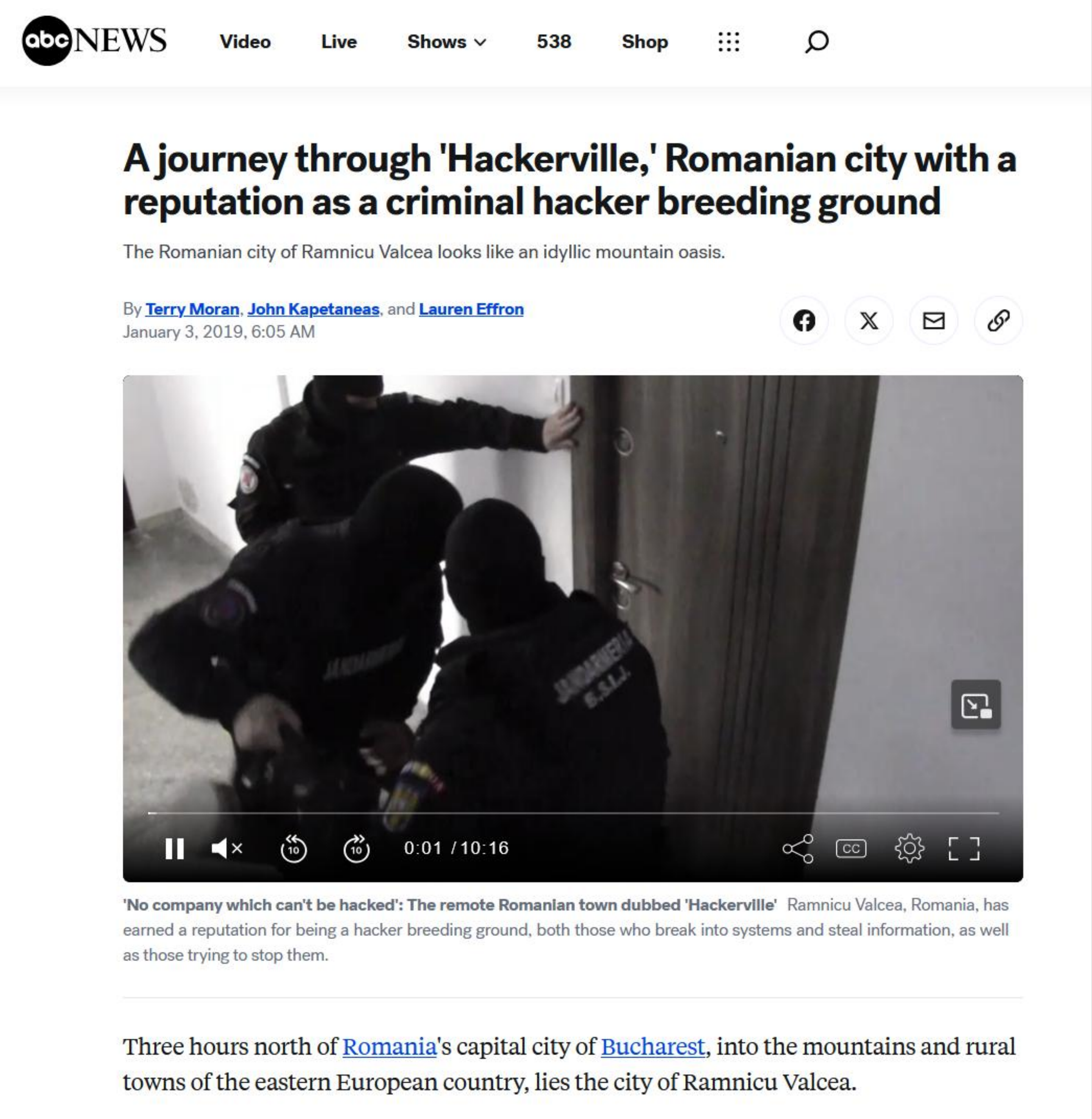
https://www.politico.com/news/2019/12/05/russiar

CYBERSECURITY

Russian ‘Evil Corp’ cybercrime gang bilked millions in hacking spree, officials charge

One of the alledged hackers who the Department of Justice believes was involved in fraud that &quot;would be difficult to imagine if they were not real.&quot; | NCA

By TIM STARKS
12/05/2019 11:18 AM EST
Updated: 12/05/2019 12:26 PM EST



A journey through 'Hackerville,' Romanian city with a reputation as a criminal hacker breeding ground

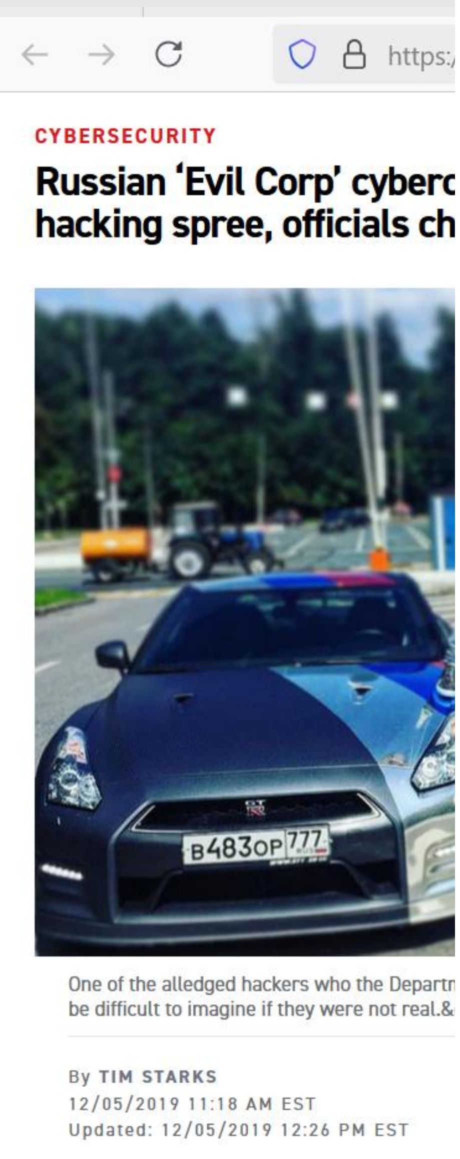
The Romanian city of Ramnicu Valcea looks like an idyllic mountain oasis.

By Terry Moran, John Kapetaneas, and Lauren Effron
January 3, 2019, 6:05 AM

'No company which can't be hacked': The remote Romanian town dubbed 'Hackerville' Ramnicu Valcea, Romania, has earned a reputation for being a hacker breeding ground, both those who break into systems and steal information, as well as those trying to stop them.

Three hours north of Romania's capital city of Bucharest, into the mountains and rural towns of the eastern European country, lies the city of Ramnicu Valcea.

Typical Cybe

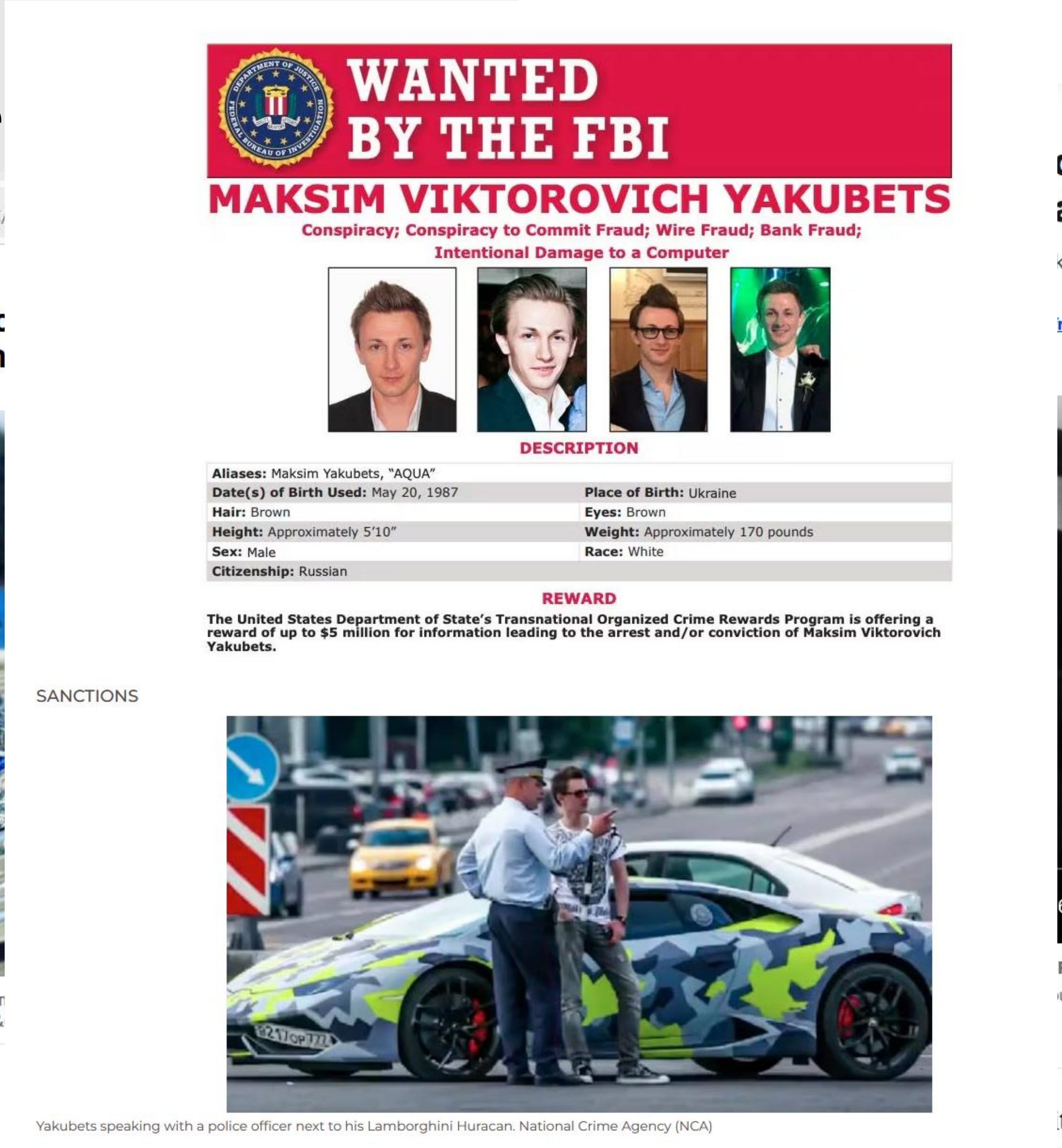


CYBERSECURITY

Russian ‘Evil Corp’ cyberc hacking spree, officials ch

One of the alledged hackers who the Departm be difficult to imagine if they were not real.&

By TIM STARKS
12/05/2019 11:18 AM EST
Updated: 12/05/2019 12:26 PM EST



WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

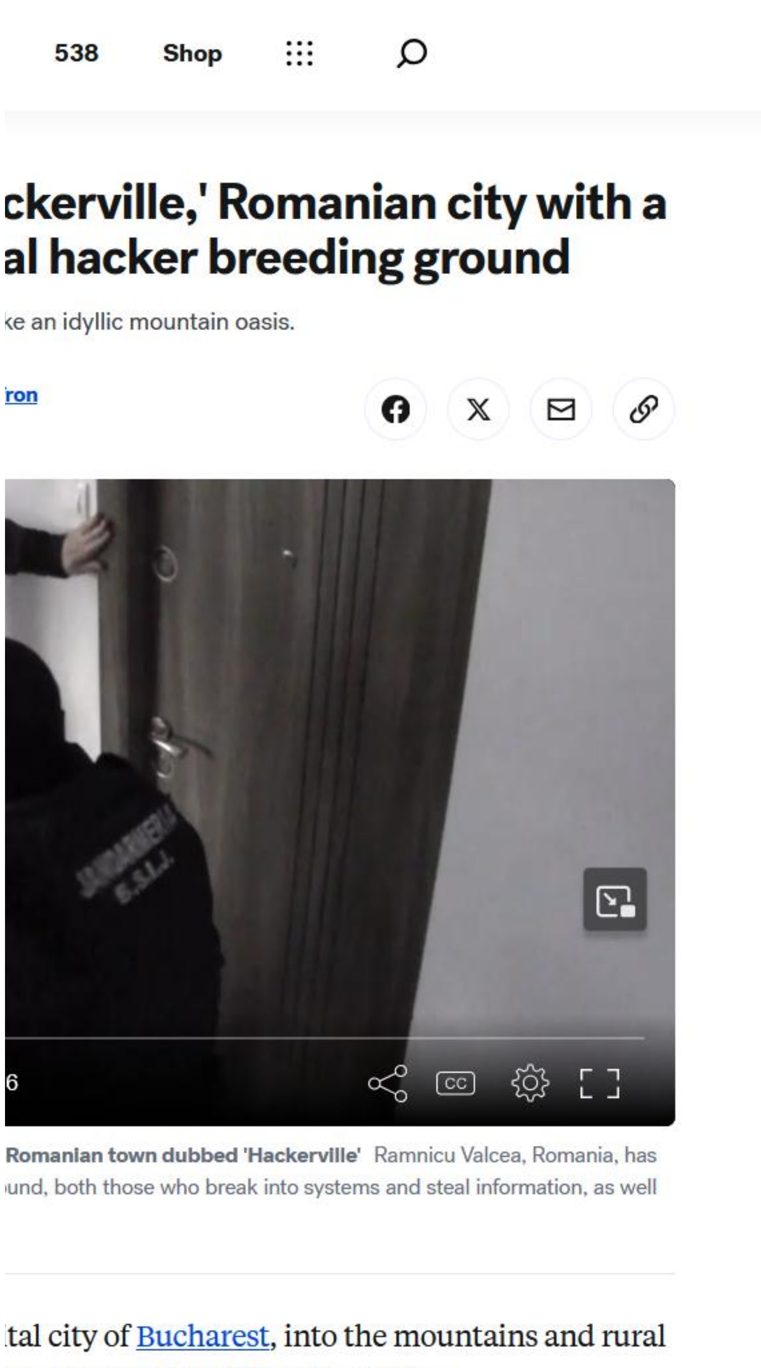
Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

SANCTIONS

Yakubets speaking with a police officer next to his Lamborghini Huracan. National Crime Agency (NCA)



ckerville,' Romanian city with a al hacker breeding ground

ke an idyllic mountain oasis.

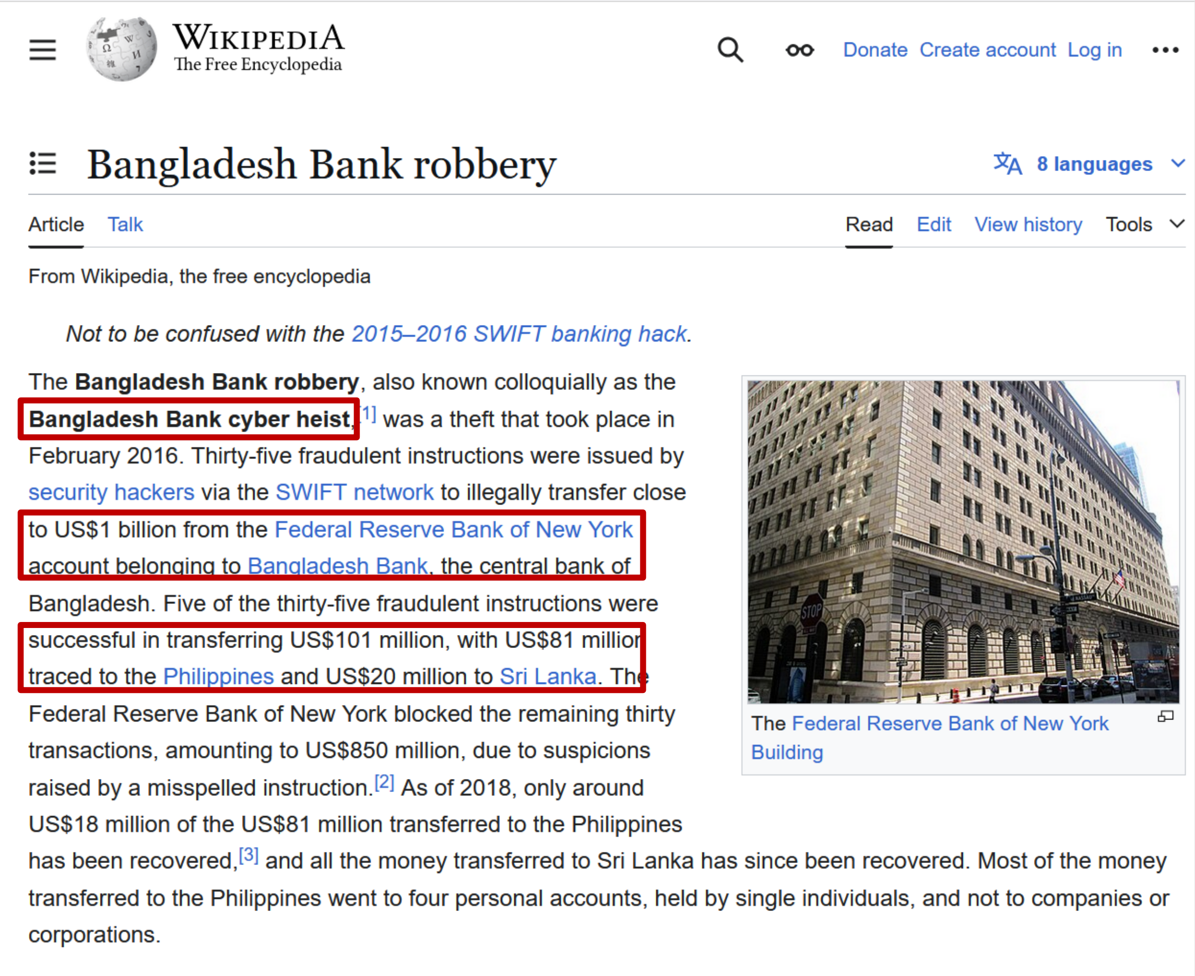
Romanian town dubbed 'Hackerville' Ramnicu Valcea, Romania, has und, both those who break into systems and steal information, as well

tal city of Bucharest, into the mountains and rural towns of the eastern European country, lies the city of Ramnicu Valcea.

A Cybercrime That Changed the World

It started with a simple bank heist.

But cybercriminals accidentally laid the foundation for cyberwarfare



Bangladesh Bank robbery

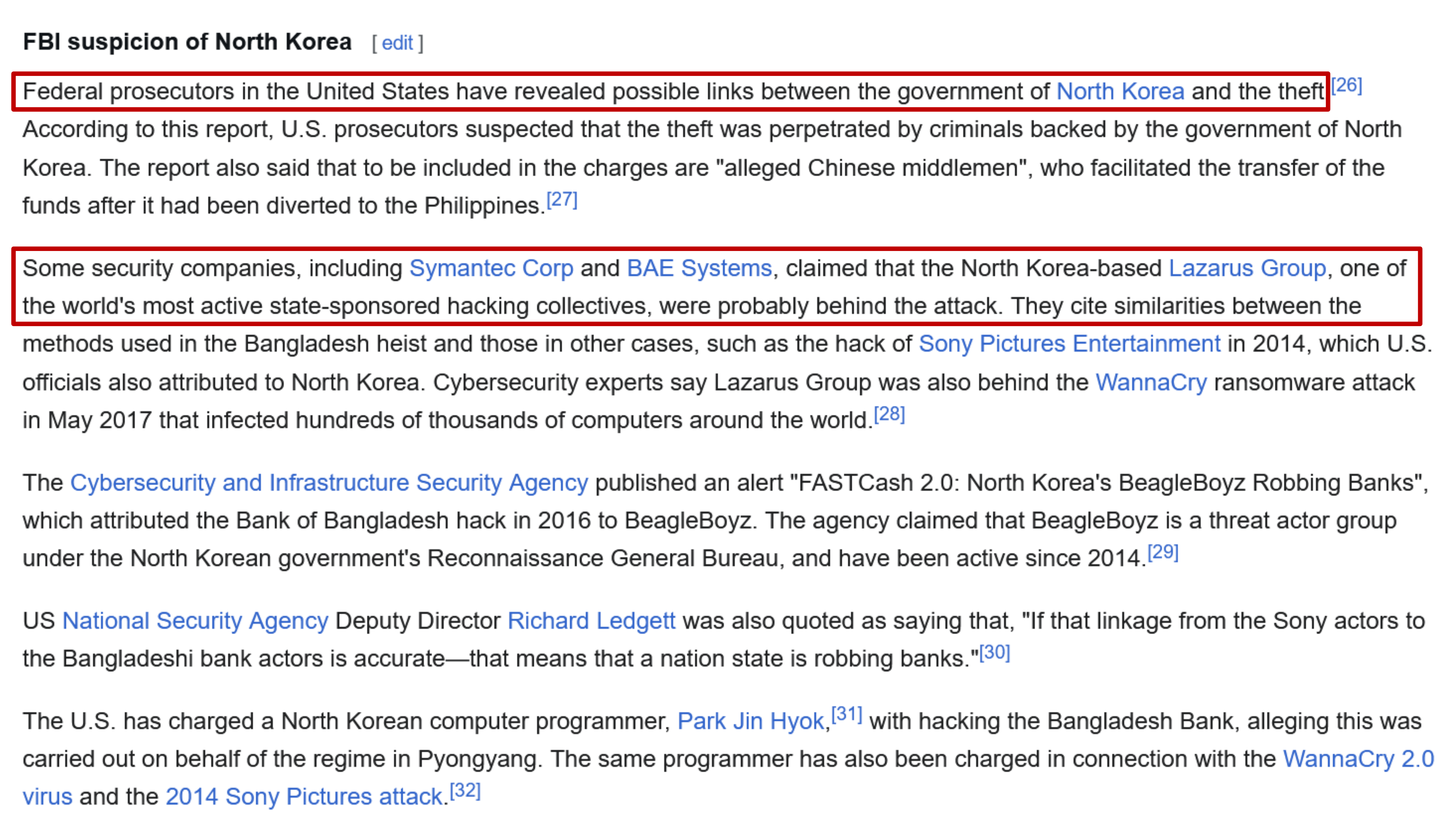
From Wikipedia, the free encyclopedia

Not to be confused with the 2015–2016 SWIFT banking hack.

The **Bangladesh Bank robbery**, also known colloquially as the **Bangladesh Bank cyber heist**,[1] was a theft that took place in February 2016. Thirty-five fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer close to US$1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank, the central bank of Bangladesh. Five of the thirty-five fraudulent instructions were successful in transferring US$101 million, with US$81 million traced to the Philippines and US$20 million to Sri Lanka. The Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to US$850 million, due to suspicions raised by a misspelled instruction.[2] As of 2018, only around US$18 million of the US$81 million transferred to the Philippines has been recovered,[3] and all the money transferred to Sri Lanka has since been recovered. Most of the money transferred to the Philippines went to four personal accounts, held by single individuals, and not to companies or corporations.

The Federal Reserve Bank of New York Building

A Cybercrime That Changed the World



FBI suspicion of North Korea

Federal prosecutors in the United States have revealed possible links between the government of North Korea and the theft[26] According to this report, U.S. prosecutors suspected that the theft was perpetrated by criminals backed by the government of North Korea. The report also said that to be included in the charges are "alleged Chinese middlemen", who facilitated the transfer of the funds after it had been diverted to the Philippines.[27]

Some security companies, including Symantec Corp and BAE Systems, claimed that the North Korea-based Lazarus Group, one of the world's most active state-sponsored hacking collectives, were probably behind the attack. They cite similarities between the methods used in the Bangladesh heist and those in other cases, such as the hack of Sony Pictures Entertainment in 2014, which U.S. officials also attributed to North Korea. Cybersecurity experts say Lazarus Group was also behind the WannaCry ransomware attack in May 2017 that infected hundreds of thousands of computers around the world.[28]

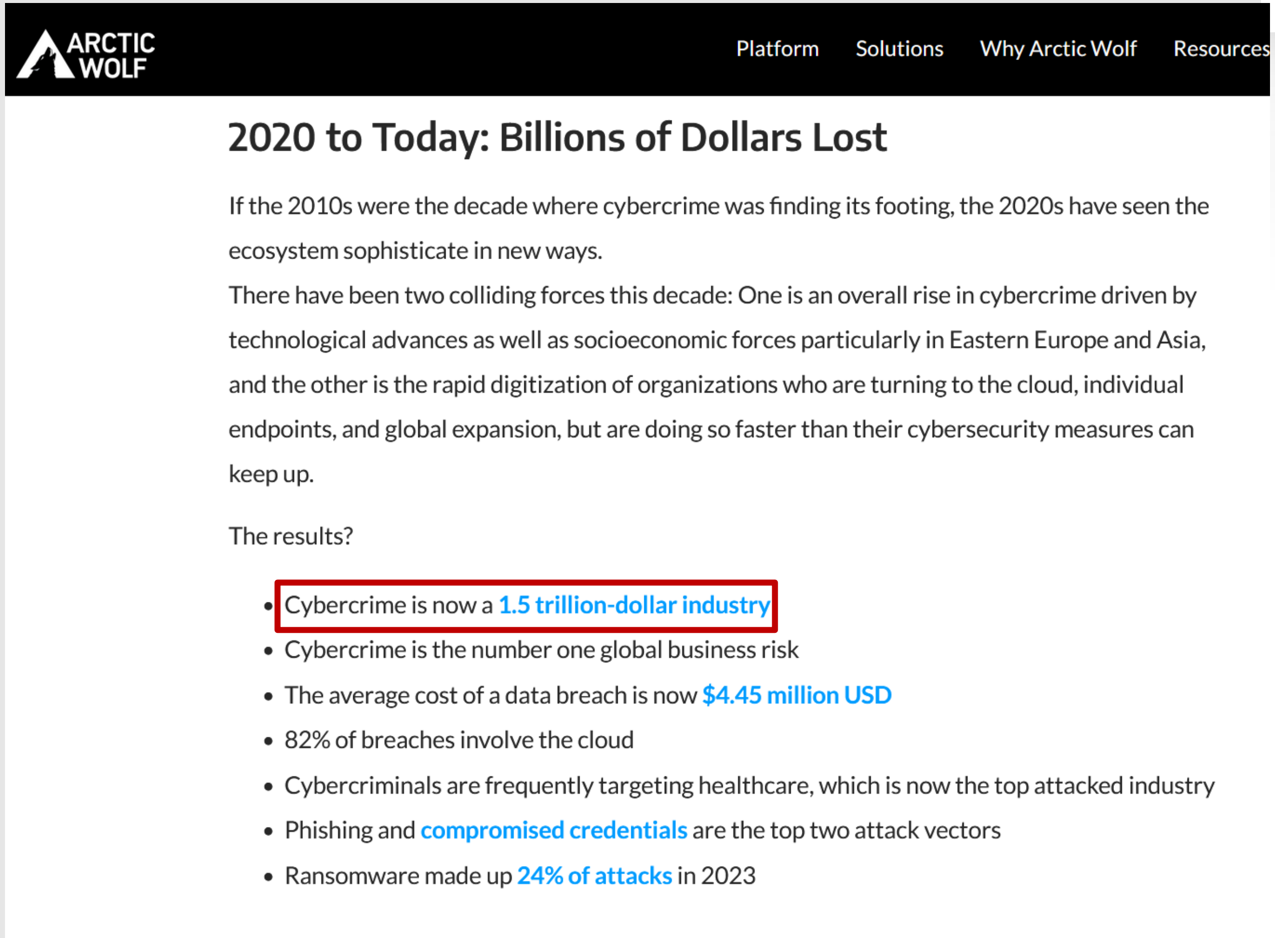
The Cybersecurity and Infrastructure Security Agency published an alert "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks", which attributed the Bank of Bangladesh hack in 2016 to BeagleBoyz. The agency claimed that BeagleBoyz is a threat actor group under the North Korean government's Reconnaissance General Bureau, and have been active since 2014.[29]

US National Security Agency Deputy Director Richard Ledgett was also quoted as saying that, "If that linkage from the Sony actors to the Bangladeshi bank actors is accurate—that means that a nation state is robbing banks."[30]

The U.S. has charged a North Korean computer programmer, Park Jin Hyok,[31] with hacking the Bangladesh Bank, alleging this was carried out on behalf of the regime in Pyongyang. The same programmer has also been charged in connection with the WannaCry 2.0 virus and the 2014 Sony Pictures attack.[32]

The Rise of Cybercrime Empires

Cybercriminals evolve into billion-dollar operations



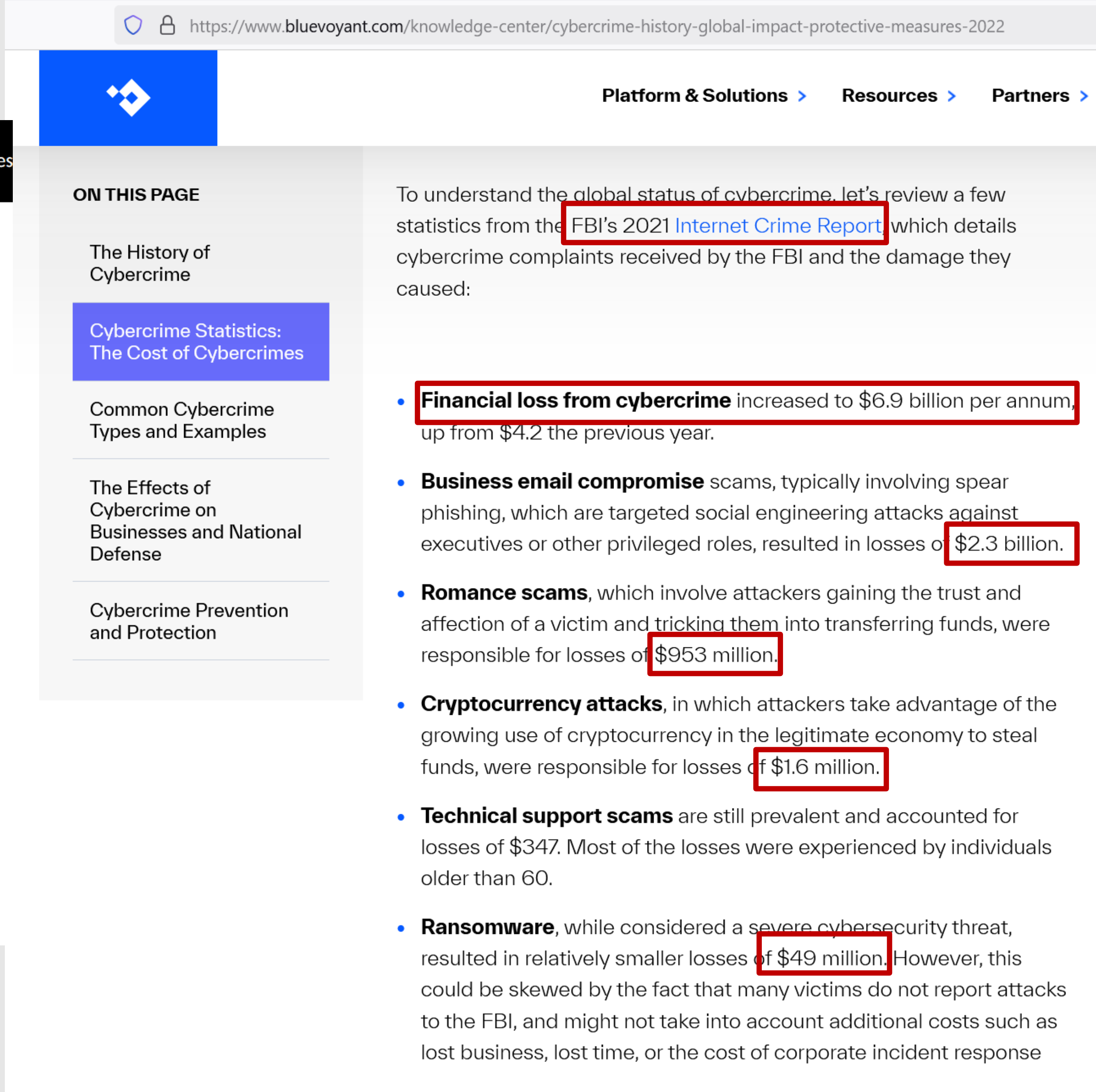
2020 to Today: Billions of Dollars Lost

If the 2010s were the decade where cybercrime was finding its footing, the 2020s have seen the ecosystem sophisticate in new ways.

There have been two colliding forces this decade: One is an overall rise in cybercrime driven by technological advances as well as socioeconomic forces particularly in Eastern Europe and Asia, and the other is the rapid digitization of organizations who are turning to the cloud, individual endpoints, and global expansion, but are doing so faster than their cybersecurity measures can keep up.

The results?

- Cybercrime is now a 1.5 trillion-dollar industry
- Cybercrime is the number one global business risk
- The average cost of a data breach is now $4.45 million USD
- 82% of breaches involve the cloud
- Cybercriminals are frequently targeting healthcare, which is now the top attacked industry
- Phishing and compromised credentials are the top two attack vectors
- Ransomware made up 24% of attacks in 2023


https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022
Platform & Solutions
Resources
Partners
ON THIS PAGE
The History of Cybercrime
Cybercrime Statistics: The Cost of Cybercrimes
Common Cybercrime Types and Examples
The Effects of Cybercrime on Businesses and National Defense
Cybercrime Prevention and Protection

To understand the global status of cybercrime, let's review a few statistics from the FBI's 2021 Internet Crime Report which details cybercrime complaints received by the FBI and the damage they caused:

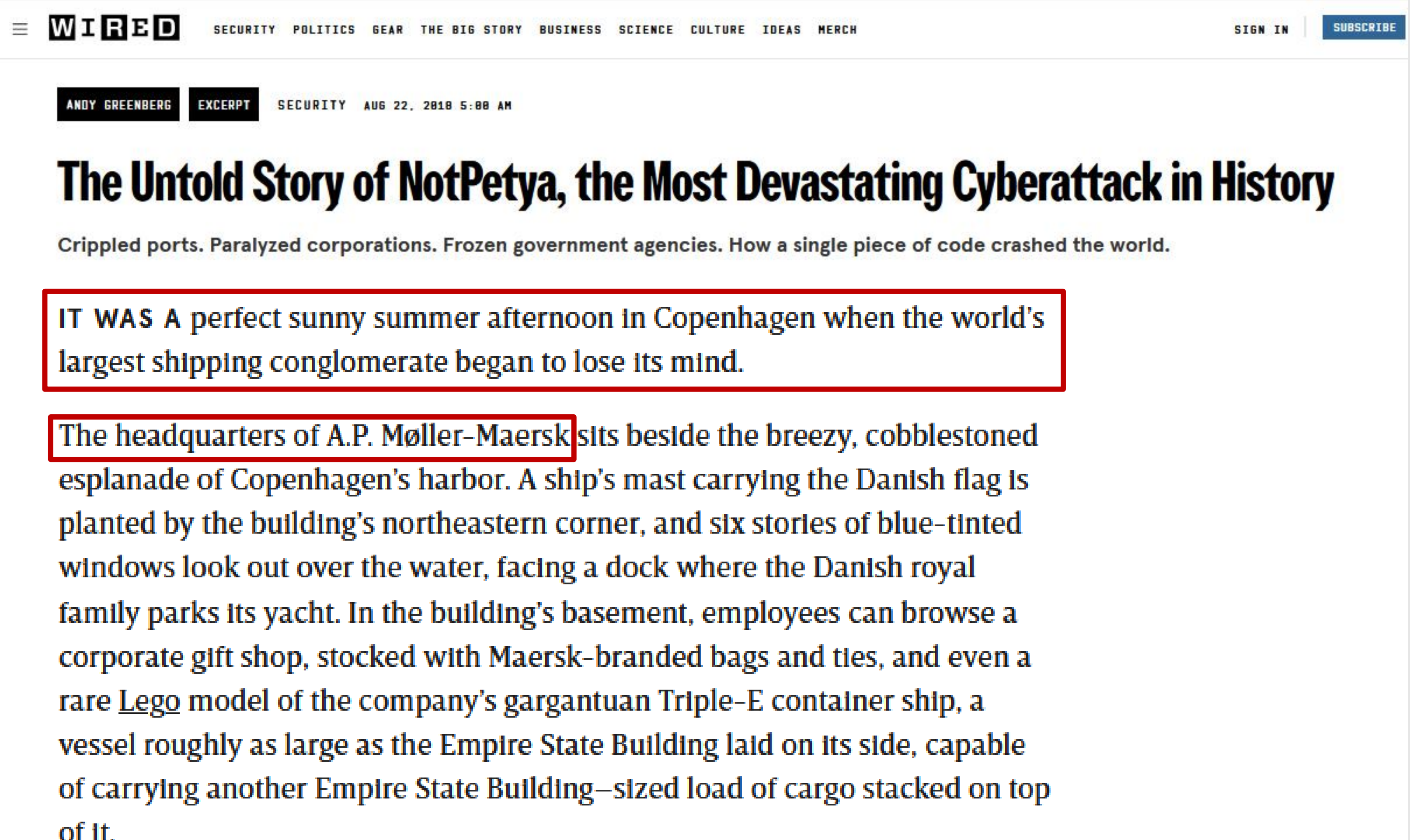
- **Financial loss from cybercrime** increased to $6.9 billion per annum, up from $4.2 the previous year.
- **Business email compromise** scams, typically involving spear phishing, which are targeted social engineering attacks against executives or other privileged roles, resulted in losses of $2.3 billion.
- **Romance scams**, which involve attackers gaining the trust and affection of a victim and tricking them into transferring funds, were responsible for losses of $953 million.
- **Cryptocurrency attacks**, in which attackers take advantage of the growing use of cryptocurrency in the legitimate economy to steal funds, were responsible for losses of $1.6 million.
- **Technical support scams** are still prevalent and accounted for losses of $347. Most of the losses were experienced by individuals older than 60.
- **Ransomware**, while considered a severe cybersecurity threat, resulted in relatively smaller losses of $49 million. However, this could be skewed by the fact that many victims do not report attacks to the FBI, and might not take into account additional costs such as lost business, lost time, or the cost of corporate incident response

Cybercrime Meets Geopolitics

Nation-states weaponizing cyber gangs

The line between cybercrime and cyberwarfare blurs

NotPetya (2017): Disguised as ransomware but actually cyberwar


WIRED
SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH
SIGN IN
SUBSCRIBE

ANDY GREENBERG EXCERPT SECURITY AUG 22, 2018 5:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen's harbor. A ship's mast carrying the Danish flag is planted by the building's northeastern corner, and six stories of blue-tinted windows look out over the water, facing a dock where the Danish royal family parks its yacht. In the building's basement, employees can browse a corporate gift shop, stocked with Maersk-branded bags and ties, and even a rare Lego model of the company's gargantuan Triple-E container ship, a vessel roughly as large as the Empire State Building laid on its side, capable of carrying another Empire State Building–sized load of cargo stacked on top of it.

Cybercrime Meets Geopolitics

In June 2017, the NotPetya cyberattack, initially targeting Ukraine, rapidly spread worldwide, severely impacting numerous organizations, including the Danish shipping giant Maersk.

The malware infiltrated systems through a compromised update of the Ukrainian tax software M.E.Doc, which was widely used by businesses operating in Ukraine.

Once inside a network, NotPetya propagated swiftly, encrypting data and rendering systems inoperable. Maersk, having operations in Ukraine and utilizing the M.E.Doc software, became one of the most prominent international victims.

The attack forced Maersk to halt operations temporarily, leading to significant disruptions in global shipping logistics.

The company had to reinstall thousands of servers and workstations, a massive undertaking that **highlighted the far-reaching consequences of cyberattacks originating from localized geopolitical conflicts.**

Cyberwarfare in Action

Microsoft

Iran surges cyber-enabled influence operations in support of Hamas

February 7, 2024

Microsoft Threat Intelligence

Cyberwarfare in Action

Iran’s Influence Objectives in the Israel-Hamas War

Iran’s operations worked toward four broad objectives: destabilization, retaliation, intimidation, and undermining international support for Israel. All four of these objectives also seek to undermine Israel and its supporters’ information environments to create general confusion and lack of trust.

Destabilization through polarization

Iran’s targeting of Israel during the Israel-Hamas war has increasingly focused on stoking domestic conflict over the Israeli government’s approach to the war. Multiple Iranian influence operations have masqueraded as Israeli activist groups to plant inflammatory messaging that criticizes the government’s approach to those kidnapped and taken hostage on October 7.[17] Netanyahu has been a primary target of such messaging, and calls for his removal were a common theme in Iran’s influence operations.[18]

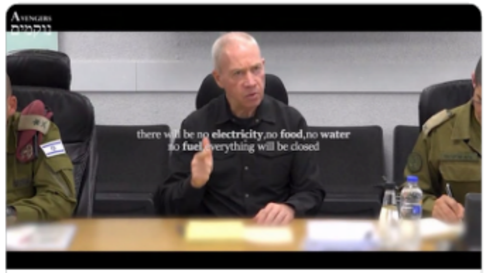

Avengers
נוקמים
there will be no electricity,no food,no water
no fuel everything will be closed

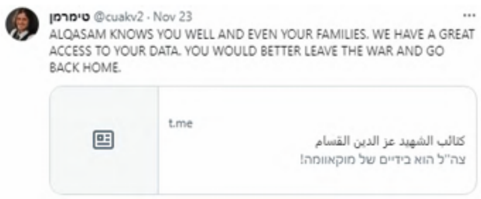
Figure 9: Cyber Avengers re-posted the video of Israel’s Defense Minister announcing Israel would blockade Gaza.

Retaliation

Much of Iran's messaging and choice of targets emphasizes its operations' retaliatory nature. For example, the duly named persona Cyber Avengers released a video showing Israel's Defense Minister stating that Israel would cut off electricity, food, water, and fuel to Gaza City (see Figure 9), followed by a series of claimed Cyber Avengers attacks targeting Israeli electricity, water and fuel infrastructure.[19] Their previous claims of attacks on Israel's national water systems days earlier included the message "An eye for an eye" and the IRGC-affiliated Tasnim News Agency reported that the group said the attacks on water systems were retaliation for the siege on Gaza.[20] An MOIS-linked group we track as Pink Sandstorm (a.k.a. Agrius) conducted a hack and leak against an Israeli hospital in late November that appeared to be retaliation for Israel's days-long siege of al-Shifa Hospital in Gaza two weeks earlier.[21]

Intimidation

Iran's operations also serve to undermine Israeli security and intimidate the citizens of Israel and its supporters by delivering threatening messaging and convincing target audiences that their state's infrastructure and government systems are insecure. Some of Iran's intimidation appears aimed at undermining Israel willingness to continue the war, like messaging attempting to convince IDF soldiers that they should “leave the war and go back home” (Figure 10).[22] One Iranian cyber persona, which may be masquerading as Hamas, claimed to send threatening text messages to the families of Israeli soldiers, adding “The IDF [Israel Defense Forces] soldiers should be aware that till our families are not secure, then their families won't be either."[23] Sockpuppets amplifying the Hamas persona spread messaging on X that the IDF “does not have any power to protect its own soldiers" and pointed viewers to a series of messages allegedly sent from IDF soldiers asking Hamas to spare their families.[24]


טימרמן @cuakv2 · Nov 23

ALQASAM KNOWS YOU WELL AND EVEN YOUR FAMILIES. WE HAVE A GREAT ACCESS TO YOUR DATA. YOU WOULD BETTER LEAVE THE WAR AND GO BACK HOME.

t.me

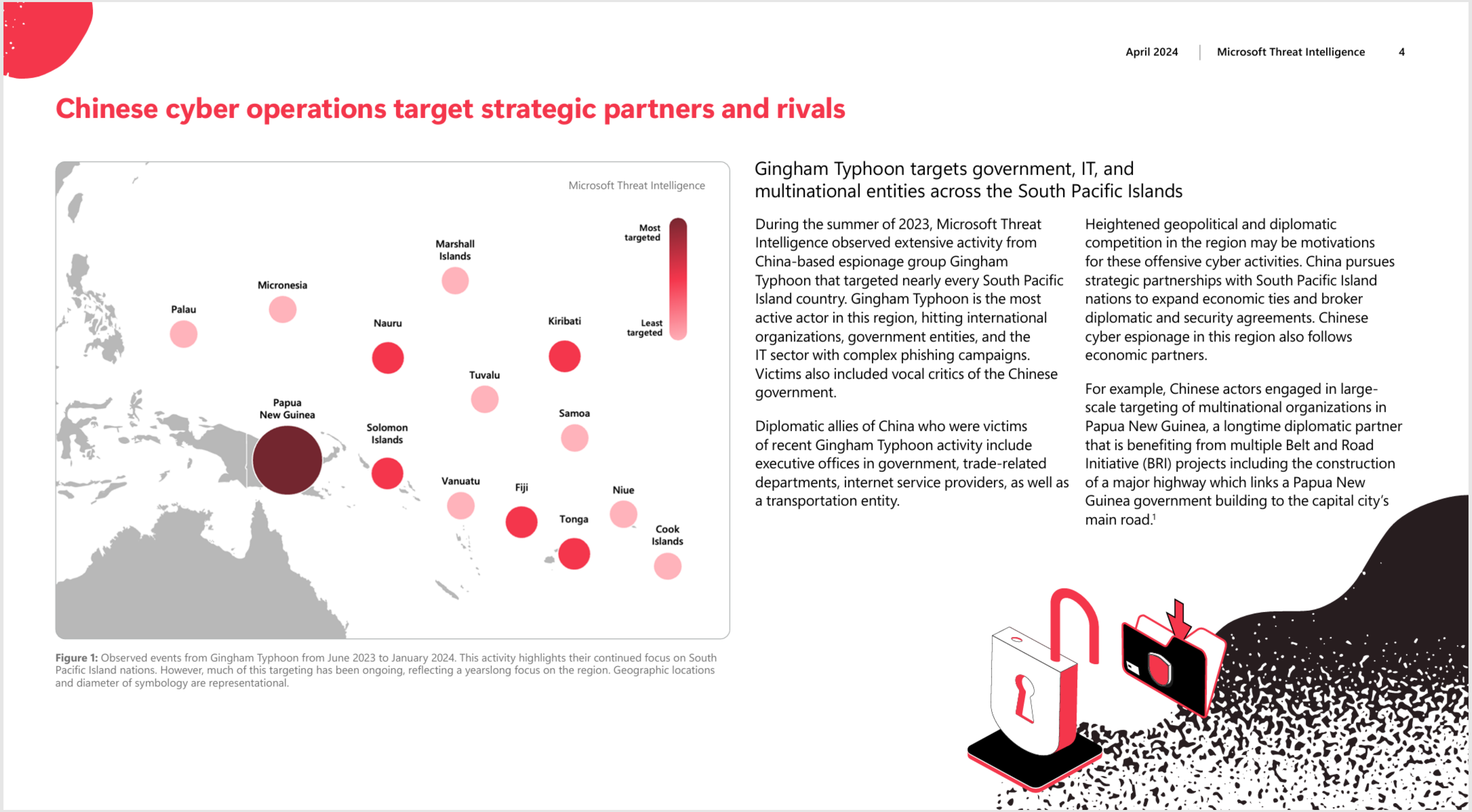
كتائب الشهيد عز الدين القسام
צה"ל הוא בידיים של מוקאוומה!

Figure 10: A Cotton Sandstorm-run sockpuppet posting threatening messages in response to Israelis' posts on X. The message is accompanied by a link to a Cotton Sandstorm-run Telegram channel that contains a series of emails allegedly sent from IDF soldiers asking Hamas to spare their families.

Undermining international support for Israel

Iran’s influence operations targeting international audiences often included messaging that seeks to weaken international support for Israel by highlighting the damage caused by Israel's attacks on Gaza. A persona masquerading as a pro-Palestinian group referred to Israel's actions in Gaza as “genocide.”[25] In December, Cotton Sandstorm ran multiple influence operations—under the names "For Palestinians" and “For Humanity”—that called on the international community to condemn Israel's attacks on Gaza.[26]

Cyberwarfare in Action



Chinese cyber operations target strategic partners and rivals

Figure 1: Observed events from Gingham Typhoon from June 2023 to January 2024. This activity highlights their continued focus on South Pacific Island nations. However, much of this targeting has been ongoing, reflecting a yearslong focus on the region. Geographic locations and diameter of symbology are representational.

Gingham Typhoon targets government, IT, and multinational entities across the South Pacific Islands

During the summer of 2023, Microsoft Threat Intelligence observed extensive activity from China-based espionage group Gingham Typhoon that targeted nearly every South Pacific Island country. Gingham Typhoon is the most active actor in this region, hitting international organizations, government entities, and the IT sector with complex phishing campaigns. Victims also included vocal critics of the Chinese government.

Diplomatic allies of China who were victims of recent Gingham Typhoon activity include executive offices in government, trade-related departments, internet service providers, as well as a transportation entity.

Heightened geopolitical and diplomatic competition in the region may be motivations for these offensive cyber activities. China pursues strategic partnerships with South Pacific Island nations to expand economic ties and broker diplomatic and security agreements. Chinese cyber espionage in this region also follows economic partners.

For example, Chinese actors engaged in large-scale targeting of multinational organizations in Papua New Guinea, a longtime diplomatic partner that is benefiting from multiple Belt and Road Initiative (BRI) projects including the construction of a major highway which links a Papua New Guinea government building to the capital city's main road.[1]

Cyberwarfare in Action

Chinese threat actors retain focus on South China Sea amid Western military exercises

China-based threat actors continued to target entities related to China's economic and military interests in and around the South China Sea. These actors opportunistically compromised government and telecommunications victims in the Association of Southeast Asian Nations (ASEAN). Chinese state-affiliated cyber actors appeared particularly interested in targets related to the numerous US military drills conducted in the region. In June 2023, Raspberry Typhoon, a nation-state activity group based out of China, successfully targeted military and executive entities in Indonesia and a Malaysian maritime system in the weeks prior to a rare multilateral naval exercise involving Indonesia, China, and the United States.

Similarly, entities related to US-Philippines military exercises were targeted by another Chinese cyber actor, Flax Typhoon. Meanwhile, Granite Typhoon, yet another China-based threat actor, primarily compromised telecommunication entities in the region during this period, with victims in Indonesia, Malaysia, the Philippines, Cambodia, and Taiwan.

Since the publication of Microsoft's blog on Flax Typhoon, Microsoft has observed new Flax Typhoon targets in the Philippines, Hong Kong, India, and the United States in the early fall and winter of 2023.[2] This actor also frequently attacks the telecommunications sector, often leading to many downstream effects.

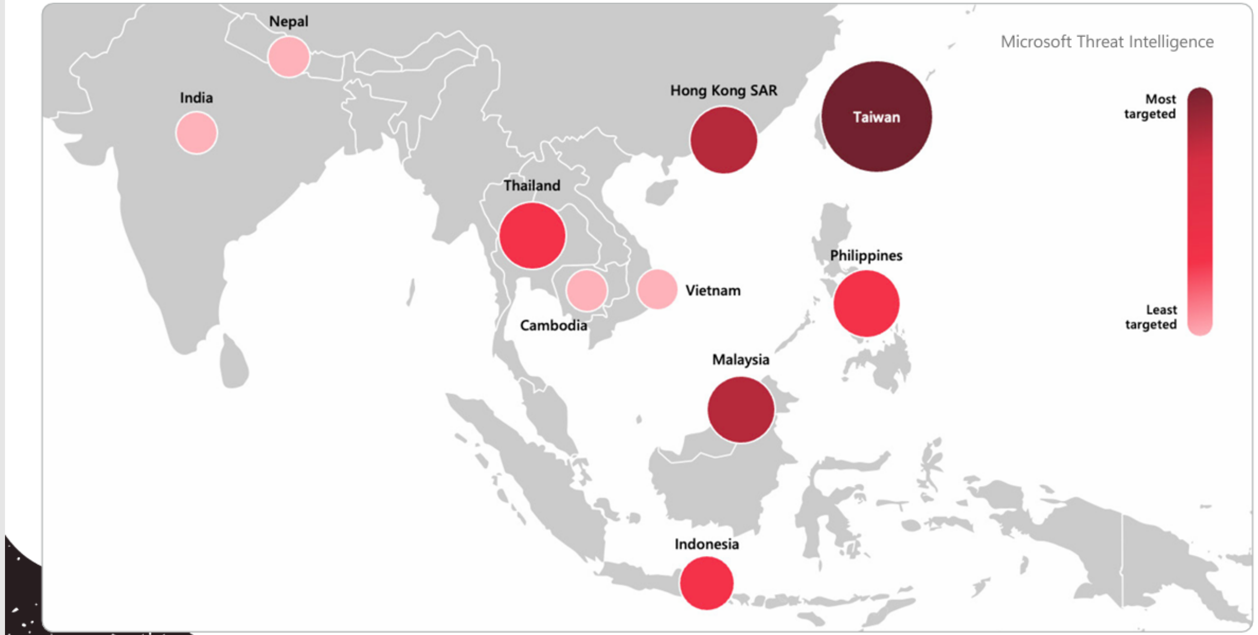


Figure 2: Observed events targeting countries in or around the South China Sea by Flax Typhoon, Granite Typhoon, or Raspberry Typhoon. Geographic locations and diameter of symbology are representational.

Nylon Typhoon compromises foreign affair entities worldwide

China-based threat actor Nylon Typhoon has continued its long-running practice of targeting foreign affairs entities in countries around the world. Between June and December of 2023, Microsoft observed Nylon Typhoon at government entities in South America including in Brazil, Guatemala, Costa Rica, and Peru. The threat actor was also observed in Europe, compromising government entities in Portugal, France, Spain, Italy, and the United Kingdom. While most of the European targets were government entities, some IT companies were also compromised. The purpose of this targeting is intelligence collection.

Cyberwarfare in Action

North Korea cyber operations

North Korean cyber threat actors stole hundreds of millions of dollars in cryptocurrency, conducted software supply chain attacks, and targeted their perceived national security adversaries in 2023. Their operations generate revenue for the North Korean government—particularly its weapons program—and collect intelligence on the United States, South Korea, and Japan.[16]

Microsoft Threat Intelligence

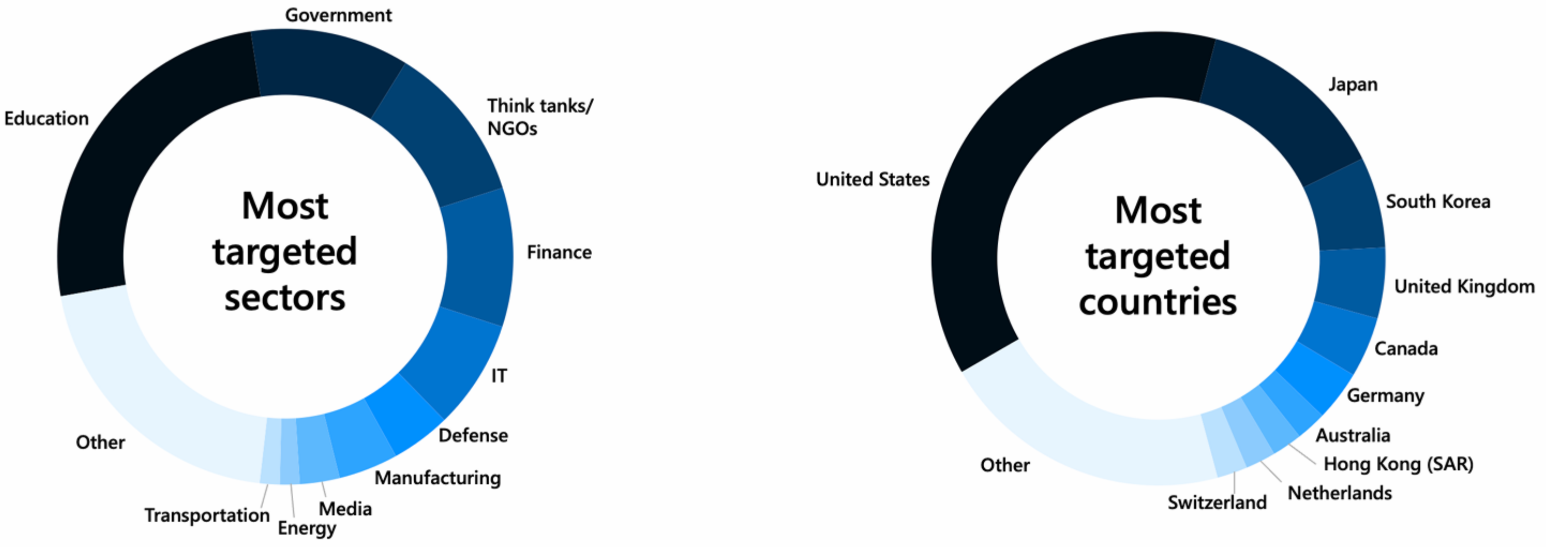


Figure 13: North Korea's most targeted sectors and countries from June 2023 to January 2024 based on Microsoft Threat Intelligence nation-state notification data.

North Korean cyber actors loot a record-setting amount of cryptocurrency to generate revenue for state

The United Nations estimates that North Korean cyber actors have stolen over $3 billion in cryptocurrency since 2017.[17] Heists totaling between $600 million and $1 billion occurred in 2023 alone. These stolen funds reportedly finance over half of the country's nuclear and missile program, enabling North Korea's weapons proliferation and testing despite sanctions.[18] North Korea conducted numerous missile tests and military drills over the past year and even successfully launched a military reconnaissance satellite into space on November 21, 2023.[19]

Cyberwarfare in Action

Microsoft Threat Intelligence

```
01000001 00100000 01111001
01100101 01100001 01110010
00100000 01101111 01100110
00100000 01010010 01110101
01110011 01110011 01101001
01100001 01101110 00100000
00001010 01101000 01111001
01100010 01110010 01101001
01100100 00100000 01110111
01100001 01110010 01100110
01100001 01110010 01100101
00100000 01101001 01101110
00100000 01010101 01101011
01110010 01100001 01101001
01101110 01100101
```

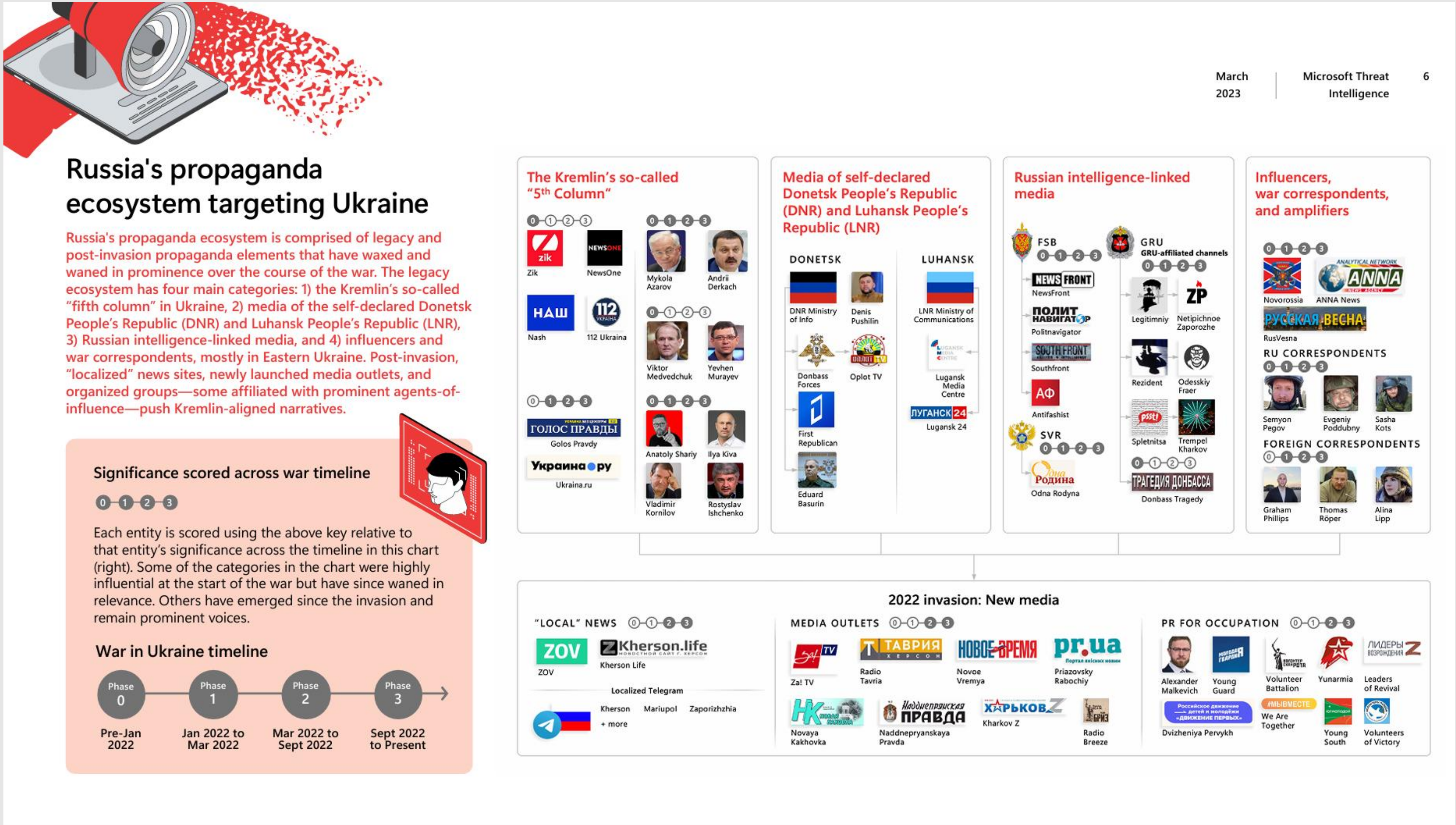
A year of Russian hybrid warfare in Ukraine

What we have learned about nation state tactics so far and what may be on the horizon

March 15, 2023

Microsoft

Cyberwarfare in Action



March 2023 | Microsoft Threat Intelligence 6

Russia's propaganda ecosystem targeting Ukraine

Russia's propaganda ecosystem is comprised of legacy and post-invasion propaganda elements that have waxed and waned in prominence over the course of the war. The legacy ecosystem has four main categories: 1) the Kremlin's so-called "fifth column" in Ukraine, 2) media of the self-declared Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR), 3) Russian intelligence-linked media, and 4) influencers and war correspondents, mostly in Eastern Ukraine. Post-invasion, "localized" news sites, newly launched media outlets, and organized groups—some affiliated with prominent agents-of-influence—push Kremlin-aligned narratives.

Significance scored across war timeline

⓿❶❷❸

Each entity is scored using the above key relative to that entity's significance across the timeline in this chart (right). Some of the categories in the chart were highly influential at the start of the war but have since waned in relevance. Others have emerged since the invasion and remain prominent voices.

War in Ukraine timeline

Phase 0 — Pre-Jan 2022

Phase 1 — Jan 2022 to Mar 2022

Phase 2 — Mar 2022 to Sept 2022

Phase 3 — Sept 2022 to Present

The Kremlin's so-called "5th Column"

⓿①②③ Zik, NewsOne, Nash, 112 Ukraina

⓪❶❷❸ Golos Pravdy, Ukraina.ru

⓿❶❷❸ Mykola Azarov, Andrii Derkach

⓿①②③ Viktor Medvedchuk, Yevhen Murayev

⓿❶❷❸ Anatoly Shariy, Ilya Kiva, Vladimir Kornilov, Rostyslav Ishchenko

Media of self-declared Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR)

DONETSK

DNR Ministry of Info, Denis Pushilin, Donbass Forces, Oplot TV, First Republican, Eduard Basurin

LUHANSK

LNR Ministry of Communications, Lugansk Media Centre, Lugansk 24

Russian intelligence-linked media

FSB ⓿❶❷❸

NewsFront, Politnavigator, Southfront, Antifashist

SVR ⓿❶❷❸

Odna Rodyna

GRU

GRU-affiliated channels ⓿❶❷❸

Legitimniy, Netipichnoe Zaporozhe, Rezident, Odesskiy Fraer, Spletnitsa, Trempel Kharkov

⓿①②③ Donbass Tragedy

Influencers, war correspondents, and amplifiers

⓿❶❷❸ Novorossia, ANNA News, RusVesna

RU CORRESPONDENTS ⓿❶❷❸

Semyon Pegov, Evgeniy Poddubny, Sasha Kots

FOREIGN CORRESPONDENTS ⓪❶❷❸

Graham Phillips, Thomas Röper, Alina Lipp

2022 invasion: New media

"LOCAL" NEWS ⓪①❷❸

ZOV, Kherson Life

Localized Telegram

Kherson, Mariupol, Zaporizhzhia + more

MEDIA OUTLETS ⓪①❷❸

Za! TV, Radio Tavria, Novoe Vremya, Priazovsky Rabochiy, Novaya Kakhovka, Naddnepryanskaya Pravda, Kharkov Z, Radio Breeze

PR FOR OCCUPATION ⓪①❷❸

Alexander Malkevich, Young Guard, Volunteer Battalion, Yunarmia, Leaders of Revival, Dvizheniya Pervykh, We Are Together, Young South, Volunteers of Victory

Cyberwarfare in Action

Phase 2: Cyber and influence focus turns to undermining Kyiv's foreign and domestic support

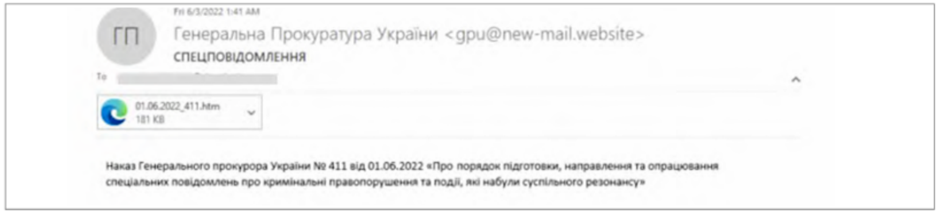
Late March 2022 – September 2022

From late March to April 2022, Russian forces withdrew from their axes of advance toward Kyiv from the north and east to focus on Donbas and other then-occupied regions.[29] At this time, Microsoft observed a cyber and influence operational pivot to target material and political support to Ukraine. Microsoft telemetry showed Russian threat actors directing their destructive cyberattacks toward the logistics and transportation sector inside Ukraine possibly to disrupt weapons or humanitarian flow to the frontlines. As reported in June, Microsoft observed GRU-affiliated threat actor IRIDIUM launch destructive wiper attacks and intelligence collection intrusions against Ukraine's transportation sector in the spring.[30] Russian forces launched numerous missile strikes against Ukrainian transportation infrastructure during this same time, suggesting a disruption of the flow of goods and people across Ukraine as a common objective.[31]

Cyber threat actors also conduced robust cyberespionage operations against organizations providing military or humanitarian assistance to Ukraine. ACTINIUM, also known as Gamaredon, conducted multiple phishing campaigns targeting humanitarian aid and resettlement organizations active in Ukraine, and entities involved in war crimes investigations from April through June 2022.[32] In April, ACTINIUM attempted to gain access to networks of entities sympathetic to Ukraine by sending phishing emails masquerading as Ukrainian military officials asking for additional humanitarian and military assistance. From late May to June, the group sent targeted phishing emails to multiple relief organizations based in Ukraine and the Baltics, as well as intergovernmental agencies assisting victims of war and documenting war crimes.

Since at least May, SEABORGIUM, also known as ColdRiver, has sent phishing messages to compromise organizations that produce or transport weapons, drones, protective equipment, and other military supplies for US and European military customers. Many of the targeted organizations provide services in support of Ukraine.[33]

Moscow also remobilized its propaganda efforts to target populations within occupied Ukrainian territory and abroad, pivoting to focus on fighting that hit the Zaporizhzhia Nuclear Power Plant in southern Ukraine, with Russia's propagandists fearmongering about nuclear attacks.[34] Aiming to garner Kremlin-aligned coverage in international press, the Russian government sponsored a PR tour of Donbas in the spring—with press members visiting from France, Germany, India, and Turkey, among others—as well as tours to the Zaporizhzhia Nuclear Power Plant.[35] Kremlin-affiliated occupation authorities even appeared to take control of much smaller radio stations and local print outlets in many occupied cities.[36]



Fri 6/3/2022 1:41 AM

Генеральна Прокуратура України <gpu@new-mail.website>

СПЕЦПОВІДОМЛЕННЯ

To [redacted]

01.06.2022_411.htm
181 KB

Наказ Генерального прокурора України № 411 від 01.06.2022 «Про порядок підготовки, направлення та опрацювання спеціальних повідомлень про кримінальні правопорушення та події, які набули суспільного резонансу»

Screenshot of one of the phishing messages ACTINIUM sent to accounts at Ukraine- based humanitarian organizations between April and June. The themes ranged from purported official communications on decrees and requests for additional humanitarian assistance. The lure above, masquerading as a communication from Ukraine's General Prosecutor's Office, concerns procedures for reports on high-profile criminal cases, according to machine translation.

[29] https://www.reuters.com/world/europe/russia-says-first-phase-ukraine-operation-mostly-complete-focus-now-donbass-2022-03-25/; https://www.businessinsider.com/russian-forces-withdraw-kyiv-failure-capture-ukraine-capital-city-war-2022-4; https://thehill.com/policy/defense/3260613-pentagon-russian-forces-outside-kyiv-chernihiv-have-completely-withdrawn/

[30] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[31] https://www.cnn.com/2022/05/04/europe/ukraine-russia-railways-intl/index.html

[32] For past reporting on the technical details of ACTINIUM's phishing campaigns see https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

[33] Our statement about support to Ukraine is based on information posted on the impacted organizations' public websites.

[34] https://euvsdisinfo.eu/report/ukraines-attack-on-zaporizhzhia-plant-is-nuclear-terrorism

[35] https://t.co/gY6zJ2TDCQ

[36] https://t.me/Kharkov_Z_news/10666

Cyberwarfare in Action

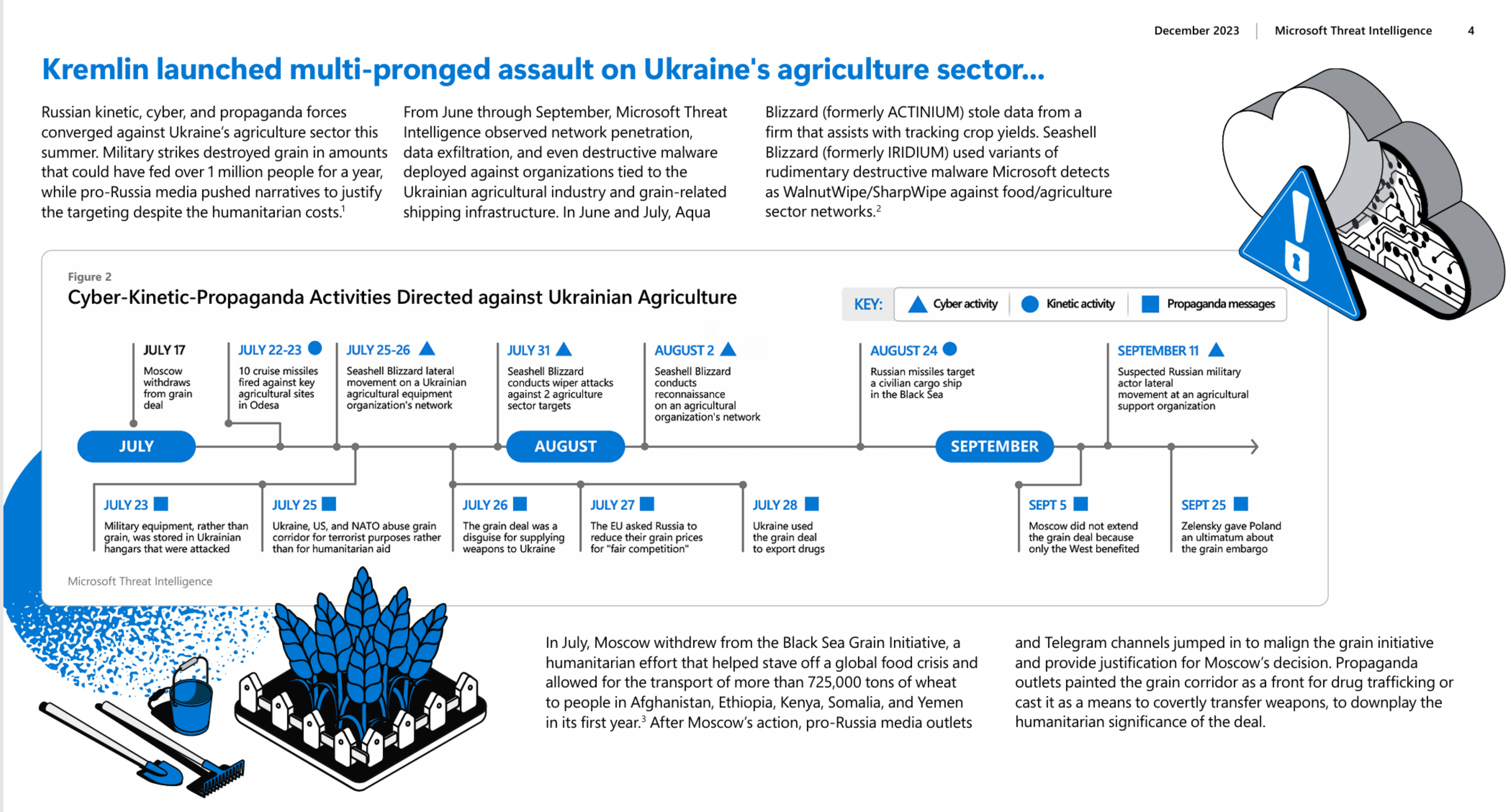
Microsoft

Russian threat actors dig in, prepare to seize on war fatigue

December 8, 2023

Microsoft Threat Intelligence

Cyberwarfare in Action



Kremlin launched multi-pronged assault on Ukraine's agriculture sector...

Russian kinetic, cyber, and propaganda forces converged against Ukraine's agriculture sector this summer. Military strikes destroyed grain in amounts that could have fed over 1 million people for a year, while pro-Russia media pushed narratives to justify the targeting despite the humanitarian costs.[1] From June through September, Microsoft Threat Intelligence observed network penetration, data exfiltration, and even destructive malware deployed against organizations tied to the Ukrainian agricultural industry and grain-related shipping infrastructure. In June and July, Aqua Blizzard (formerly ACTINIUM) stole data from a firm that assists with tracking crop yields. Seashell Blizzard (formerly IRIDIUM) used variants of rudimentary destructive malware Microsoft detects as WalnutWipe/SharpWipe against food/agriculture sector networks.[2]

Figure 2

Cyber-Kinetic-Propaganda Activities Directed against Ukrainian Agriculture

KEY: ▲ Cyber activity ● Kinetic activity ■ Propaganda messages

JULY

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 sector targets

AUGUST

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

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

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

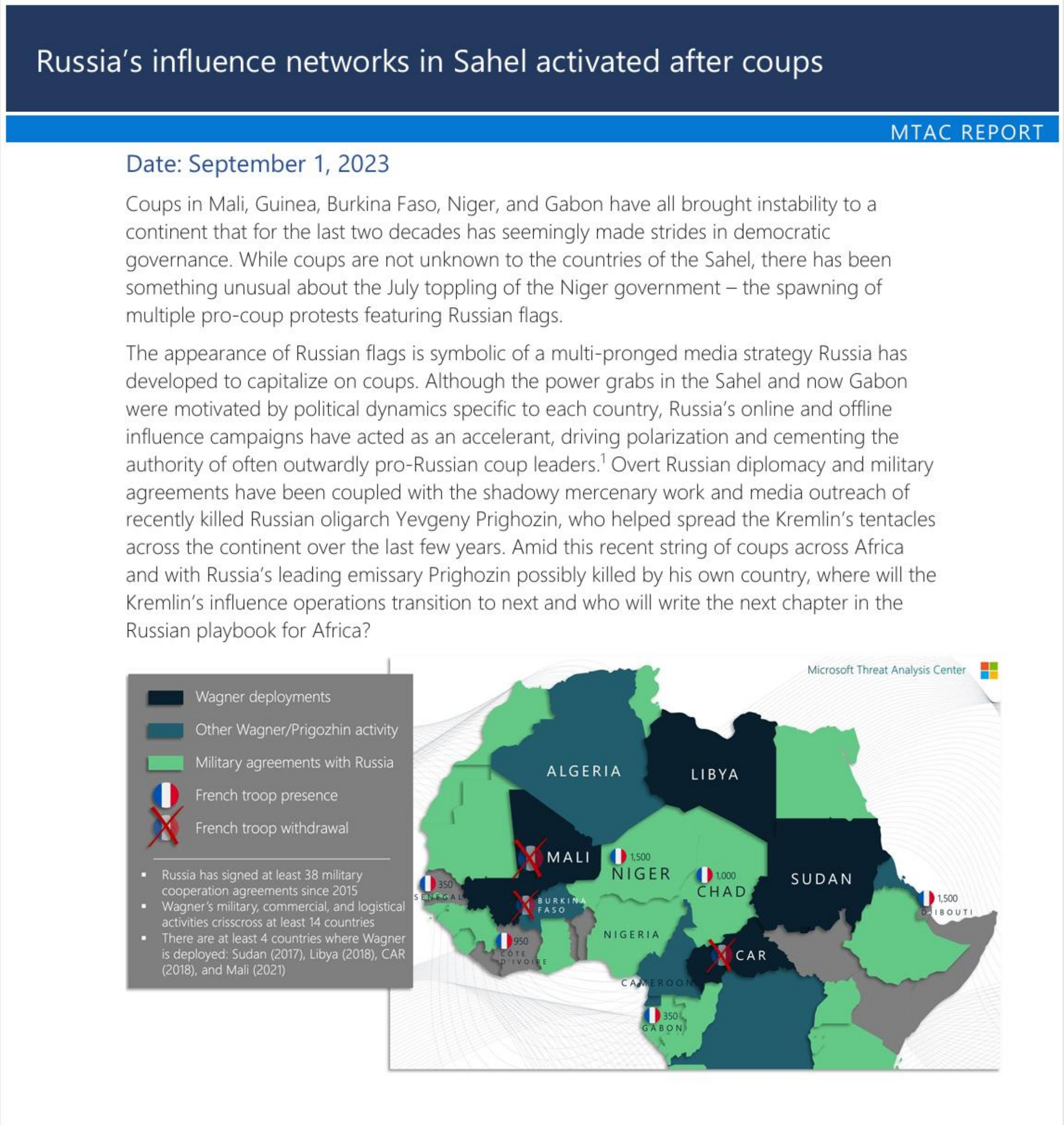
SEPT 5 ■ — Moscow did not extend the grain deal because only the West benefited

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

Microsoft Threat Intelligence

In July, Moscow withdrew from the Black Sea Grain Initiative, a humanitarian effort that helped stave off a global food crisis and allowed for the transport of more than 725,000 tons of wheat to people in Afghanistan, Ethiopia, Kenya, Somalia, and Yemen in its first year.[3] After Moscow's action, pro-Russia media outlets and Telegram channels jumped in to malign the grain initiative and provide justification for Moscow's decision. Propaganda outlets painted the grain corridor as a front for drug trafficking or cast it as a means to covertly transfer weapons, to downplay the humanitarian significance of the deal.

Cyberwarfare in Action



Russia’s influence networks in Sahel activated after coups

MTAC REPORT

Date: September 1, 2023

Coups in Mali, Guinea, Burkina Faso, Niger, and Gabon have all brought instability to a continent that for the last two decades has seemingly made strides in democratic governance. While coups are not unknown to the countries of the Sahel, there has been something unusual about the July toppling of the Niger government – the spawning of multiple pro-coup protests featuring Russian flags.

The appearance of Russian flags is symbolic of a multi-pronged media strategy Russia has developed to capitalize on coups. Although the power grabs in the Sahel and now Gabon were motivated by political dynamics specific to each country, Russia’s online and offline influence campaigns have acted as an accelerant, driving polarization and cementing the authority of often outwardly pro-Russian coup leaders.[1] Overt Russian diplomacy and military agreements have been coupled with the shadowy mercenary work and media outreach of recently killed Russian oligarch Yevgeny Prighozin, who helped spread the Kremlin’s tentacles across the continent over the last few years. Amid this recent string of coups across Africa and with Russia’s leading emissary Prighozin possibly killed by his own country, where will the Kremlin’s influence operations transition to next and who will write the next chapter in the Russian playbook for Africa?

- ■ Wagner deployments
- ■ Other Wagner/Prigozhin activity
- 🟩 Military agreements with Russia
- ● French troop presence
- ☒ French troop withdrawal

- Russia has signed at least 38 military cooperation agreements since 2015
- Wagner’s military, commercial, and logistical activities crisscross at least 14 countries
- There are at least 4 countries where Wagner is deployed: Sudan (2017), Libya (2018), CAR (2018), and Mali (2021)

Microsoft Threat Analysis Center

Cyberwarfare in Action

Russia's influence networks i

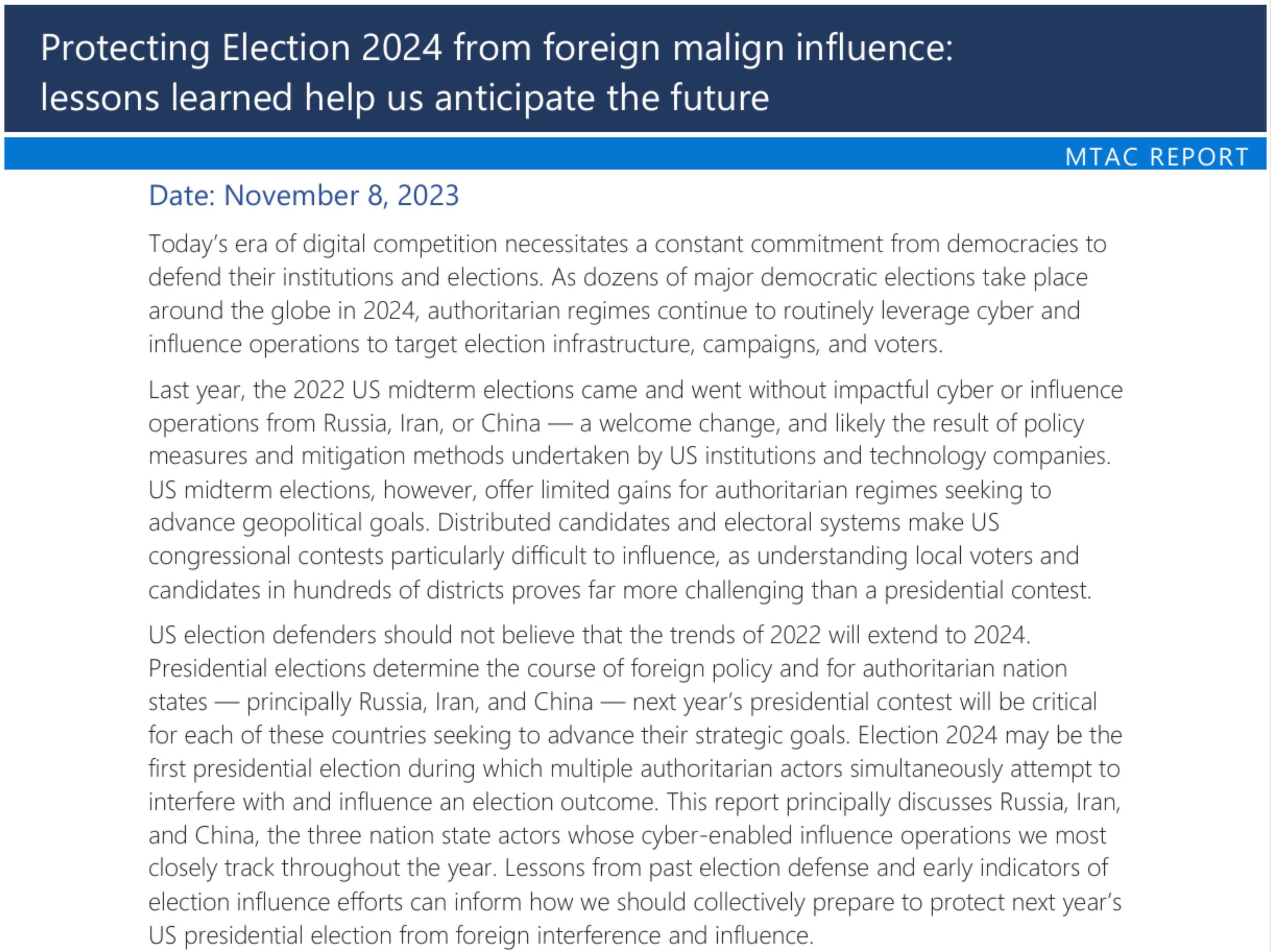
Date: September 1, 2023

Coups in Mali, Guinea, Burkina Faso
continent that for the last two deca
governance. While coups are not u
something unusual about the July t
multiple pro-coup protests featurin

The appearance of Russian flags is
developed to capitalize on coups. A
were motivated by political dynami
influence campaigns have acted as
authority of often outwardly pro-Ru
agreements have been coupled wit
recently killed Russian oligarch Yevg
across the continent over the last fe
and with Russia's leading emissary P
Kremlin's influence operations trans
Russian playbook for Africa?

■ Wagner deployments
■ Other Wagner/Prigozhin activity
🟩 Military agreements with Russia
French troop presence
French troop withdrawal

- Russia has signed at least 38 military cooperation agreements since 2015
- Wagner's military, commercial, and logistical activities crisscross at least 14 countries
- There are at least 4 countries where Wagner is deployed: Sudan (2017), Libya (2018), CAR (2018), and Mali (2021)



Protecting Election 2024 from foreign malign influence: lessons learned help us anticipate the future

MTAC REPORT

Date: November 8, 2023

Today's era of digital competition necessitates a constant commitment from democracies to defend their institutions and elections. As dozens of major democratic elections take place around the globe in 2024, authoritarian regimes continue to routinely leverage cyber and influence operations to target election infrastructure, campaigns, and voters.

Last year, the 2022 US midterm elections came and went without impactful cyber or influence operations from Russia, Iran, or China — a welcome change, and likely the result of policy measures and mitigation methods undertaken by US institutions and technology companies. US midterm elections, however, offer limited gains for authoritarian regimes seeking to advance geopolitical goals. Distributed candidates and electoral systems make US congressional contests particularly difficult to influence, as understanding local voters and candidates in hundreds of districts proves far more challenging than a presidential contest.

US election defenders should not believe that the trends of 2022 will extend to 2024. Presidential elections determine the course of foreign policy and for authoritarian nation states — principally Russia, Iran, and China — next year's presidential contest will be critical for each of these countries seeking to advance their strategic goals. Election 2024 may be the first presidential election during which multiple authoritarian actors simultaneously attempt to interfere with and influence an election outcome. This report principally discusses Russia, Iran, and China, the three nation state actors whose cyber-enabled influence operations we most closely track throughout the year. Lessons from past election defense and early indicators of election influence efforts can inform how we should collectively prepare to protect next year's US presidential election from foreign interference and influence.

Cyberwarfare in Action

Russia's influence networks i

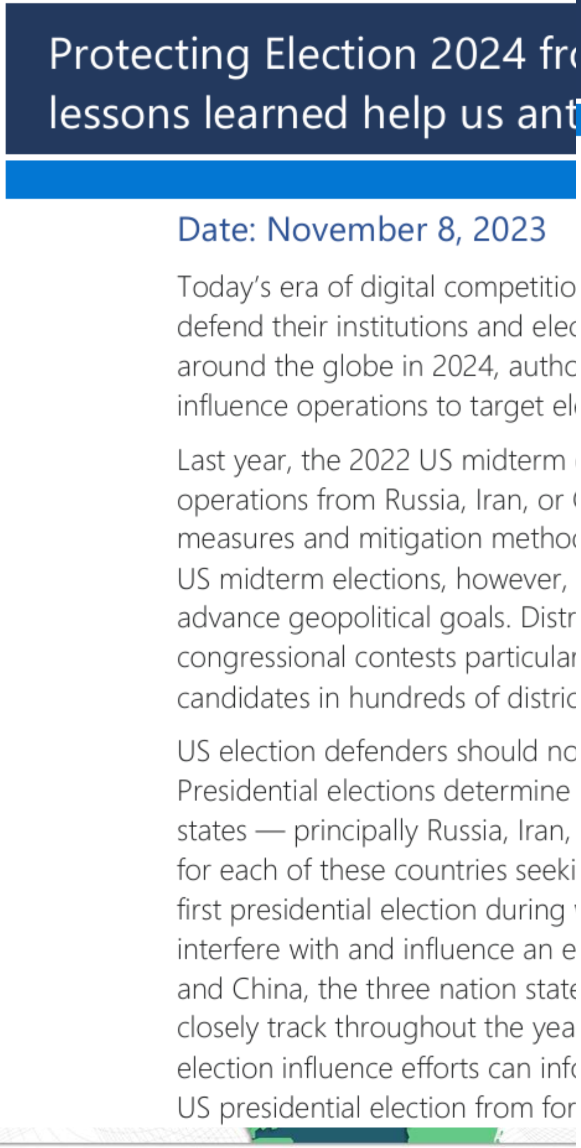
Date: September 1, 2023

Coups in Mali, Guinea, Burkina Fasc
continent that for the last two deca
governance. While coups are not u
something unusual about the July t
multiple pro-coup protests featurin

The appearance of Russian flags is
developed to capitalize on coups. A
were motivated by political dynami
influence campaigns have acted as
authority of often outwardly pro-Ru
agreements have been coupled wit
recently killed Russian oligarch Yevg
across the continent over the last fe
and with Russia's leading emissary P
Kremlin's influence operations trans
Russian playbook for Africa?

■ Wagner deployments
■ Other Wagner/Prigozhin activity
■ Military agreements with Russia
French troop presence
French troop withdrawal

- Russia has signed at least 38 military cooperation agreements since 2015
- Wagner's military, commercial, and logistical activities crisscross at least 14 countries
- There are at least 4 countries where Wagner is deployed: Sudan (2017), Libya (2018), CAR (2018), and Mali (2021)



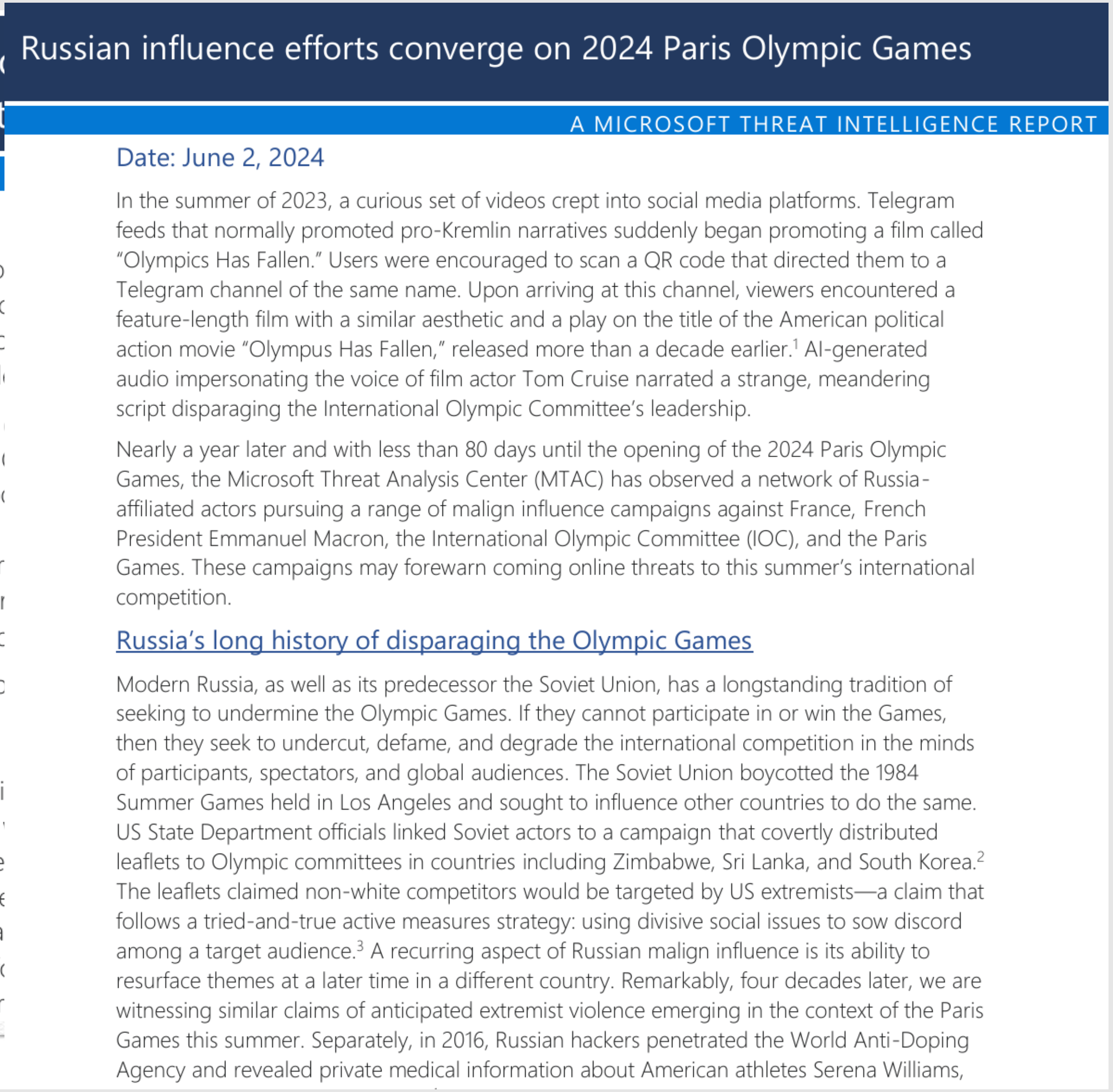
Protecting Election 2024 fr
lessons learned help us ant

Date: November 8, 2023

Today's era of digital competitio
defend their institutions and elec
around the globe in 2024, authc
influence operations to target el

Last year, the 2022 US midterm
operations from Russia, Iran, or
measures and mitigation metho
US midterm elections, however,
advance geopolitical goals. Distr
congressional contests particular
candidates in hundreds of distric

US election defenders should nc
Presidential elections determine
states — principally Russia, Iran,
for each of these countries seeki
first presidential election during
interfere with and influence an e
and China, the three nation state
closely track throughout the yea
election influence efforts can infc
US presidential election from for



Russian influence efforts converge on 2024 Paris Olympic Games

A MICROSOFT THREAT INTELLIGENCE REPORT

Date: June 2, 2024

In the summer of 2023, a curious set of videos crept into social media platforms. Telegram feeds that normally promoted pro-Kremlin narratives suddenly began promoting a film called "Olympics Has Fallen." Users were encouraged to scan a QR code that directed them to a Telegram channel of the same name. Upon arriving at this channel, viewers encountered a feature-length film with a similar aesthetic and a play on the title of the American political action movie "Olympus Has Fallen," released more than a decade earlier.[1] AI-generated audio impersonating the voice of film actor Tom Cruise narrated a strange, meandering script disparaging the International Olympic Committee's leadership.

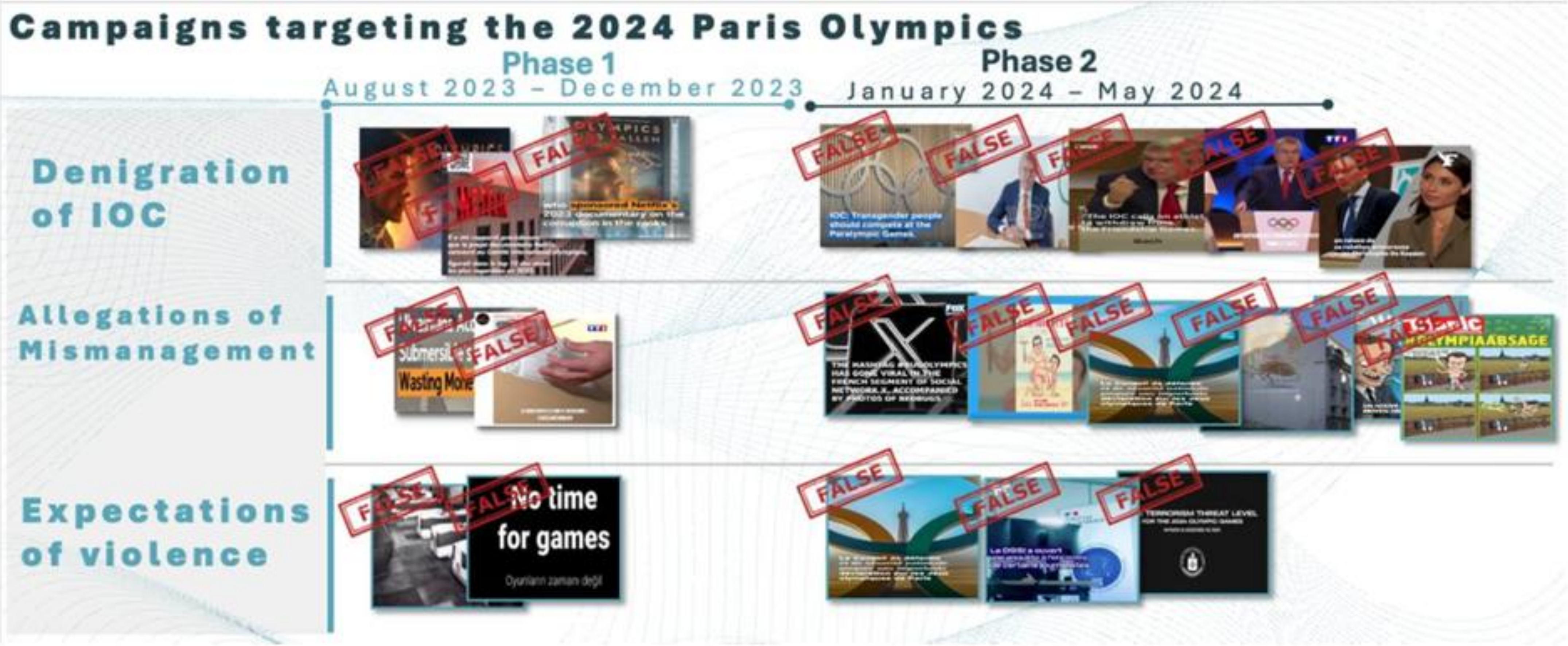
Nearly a year later and with less than 80 days until the opening of the 2024 Paris Olympic Games, the Microsoft Threat Analysis Center (MTAC) has observed a network of Russia-affiliated actors pursuing a range of malign influence campaigns against France, French President Emmanuel Macron, the International Olympic Committee (IOC), and the Paris Games. These campaigns may forewarn coming online threats to this summer's international competition.

Russia's long history of disparaging the Olympic Games

Modern Russia, as well as its predecessor the Soviet Union, has a longstanding tradition of seeking to undermine the Olympic Games. If they cannot participate in or win the Games, then they seek to undercut, defame, and degrade the international competition in the minds of participants, spectators, and global audiences. The Soviet Union boycotted the 1984 Summer Games held in Los Angeles and sought to influence other countries to do the same. US State Department officials linked Soviet actors to a campaign that covertly distributed leaflets to Olympic committees in countries including Zimbabwe, Sri Lanka, and South Korea.[2] The leaflets claimed non-white competitors would be targeted by US extremists—a claim that follows a tried-and-true active measures strategy: using divisive social issues to sow discord among a target audience.[3] A recurring aspect of Russian malign influence is its ability to resurface themes at a later time in a different country. Remarkably, four decades later, we are witnessing similar claims of anticipated extremist violence emerging in the context of the Paris Games this summer. Separately, in 2016, Russian hackers penetrated the World Anti-Doping Agency and revealed private medical information about American athletes Serena Williams,

Cyberwarfare in Action

Russian influence efforts converge on 2024 Paris Olympic Games



Campaigns targeting the 2024 Paris Olympics

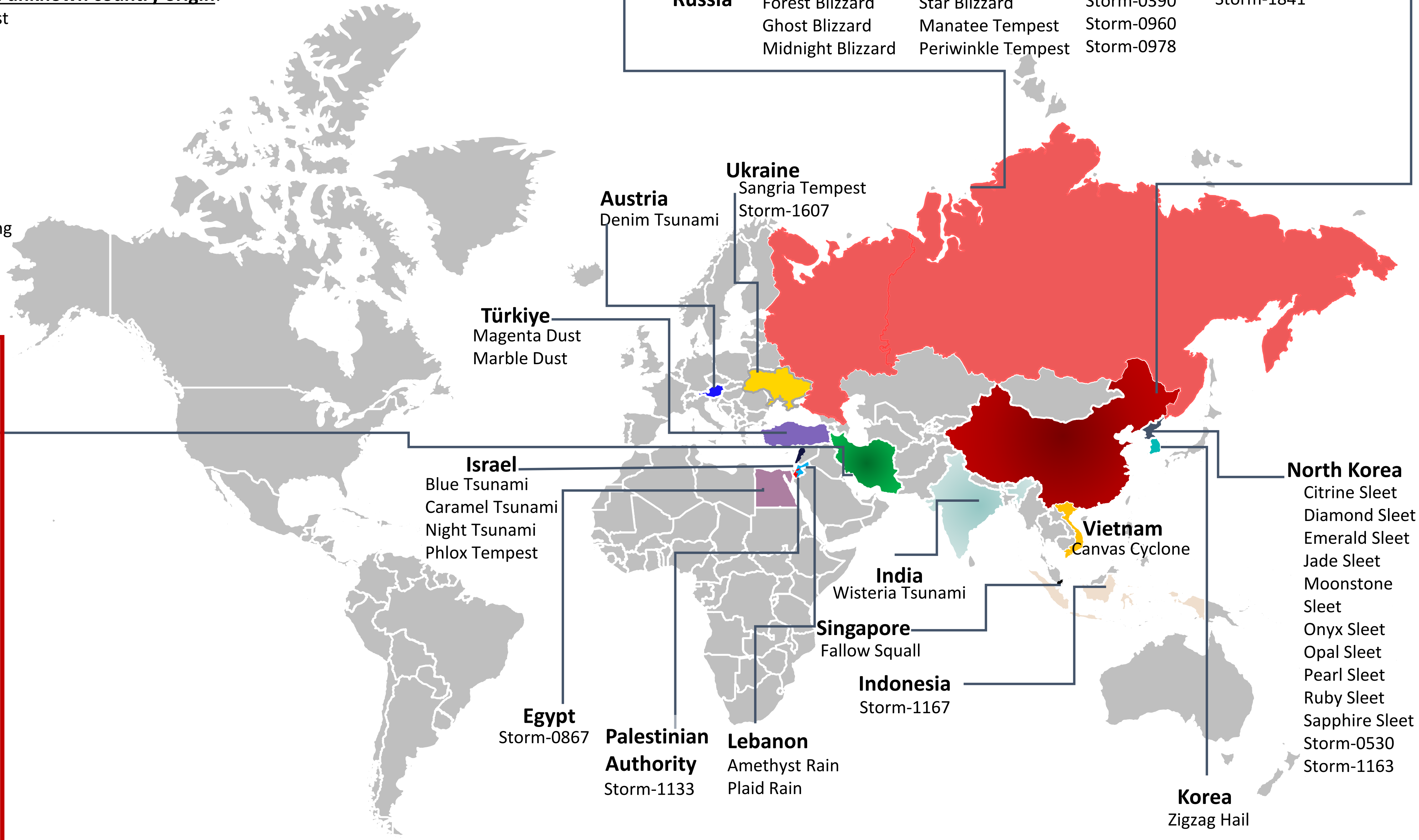
Phase 1
August 2023 – December 2023

Phase 2
January 2024 – May 2024

Denigration of IOC

Allegations of Mismanagement

Expectations of violence



Threat actors with unknown country origin:

- Pistachio Tempest
- Storm-0257
- Storm-0300
- Storm-0302
- Storm-0609
- Storm-1339
- Storm-1957

N/A

- Pinstripe Lightning

Iran

Burgundy Sandstorm
Cotton Sandstorm
Crimson Sandstorm
Cuboid Sandstorm
Gray Sandstorm
Hazel Sandstorm
Lemon Sandstorm
Mango Sandstorm
Marigold Sandstorm
Mint Sandstorm
Peach Sandstorm
Pink Sandstorm
Pumpkin Sandstorm
Sefid Flood
Smoke Sandstorm
Storm-0133
Storm-0166
Storm-0270
Storm-0589
Storm-0699
Storm-0755
Storm-0784
Storm-0842
Storm-0861
Storm-1084
Storm-2035

Russia

Aqua Blizzard
Cadet Blizzard
Forest Blizzard
Ghost Blizzard
Midnight Blizzard
Seashell Blizzard
Secret Blizzard
Star Blizzard
Manatee Tempest
Periwinkle Tempest
Ruza Flood
Storm-0165
Storm-0390
Storm-0960
Storm-0978
Storm-1010
Storm-1516
Storm-1841

Ukraine

Sangria Tempest
Storm-1607

Austria

Denim Tsunami

Türkiye

Magenta Dust
Marble Dust

Israel

Blue Tsunami
Caramel Tsunami
Night Tsunami
Phlox Tempest

Egypt

Storm-0867

Palestinian Authority

Storm-1133

Lebanon

Amethyst Rain
Plaid Rain

India

Wisteria Tsunami

Singapore

Fallow Squall

Indonesia

Storm-1167

Vietnam

Canvas Cyclone

Korea

Zigzag Hail

North Korea

Citrine Sleet
Diamond Sleet
Emerald Sleet
Jade Sleet
Moonstone Sleet
Onyx Sleet
Opal Sleet
Pearl Sleet
Ruby Sleet
Sapphire Sleet
Storm-0530
Storm-1163

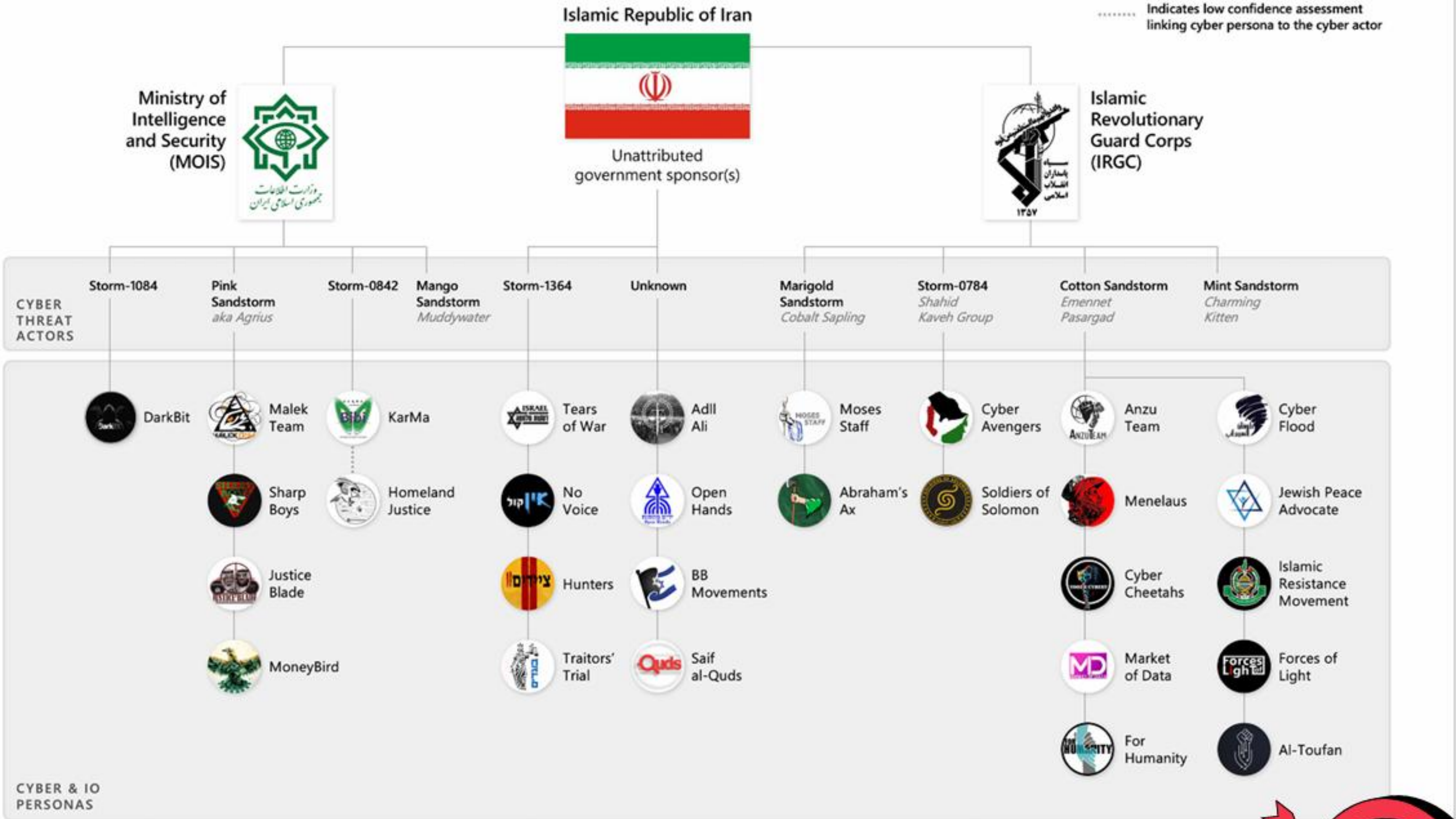
China

Antique Typhoon
Brass Typhoon
Brocade Typhoon
Canary Typhoon
Charcoal Typhoon
Checkered Typhoon
Cinnamon Typhoon
Circle Typhoon
Crescent Typhoon
Flax Typhoon
Gingham Typhoon
Granite Typhoon
Heart Typhoon
Hexagon Typhoon
Houndstooth Typhoon
Leopard Typhoon
Lilac Typhoon
Linen Typhoon
Mulberry Typhoon
Nylon Typhoon
Purple Typhoon
Raspberry Typhoon
Salmon Typhoon
Salt Typhoon
Satin Typhoon
Shadow Typhoon
Silk Typhoon
Swirl Typhoon
Taffeta Typhoon
Tumbleweed Typhoon
Twill Typhoon
Violet Typhoon
Volt Typhoon
Taizi Flood
Storm-0147
Storm-0219
Storm-0247
Storm-0337
Storm-0391
Storm-0601
Storm-0705
Storm-0848
Storm-0866
Storm-0940
Storm-1175
Storm-1197
Storm-1849
Storm-2077

Figure 3

Microsoft Threat Intelligence

Iran at the crossroads of cyber and influence



Islamic Republic of Iran

Indicates low confidence assessment linking cyber persona to the cyber actor

Ministry of Intelligence and Security (MOIS)

Unattributed government sponsor(s)

Islamic Revolutionary Guard Corps (IRGC)

CYBER THREAT ACTORS

Storm-1084

Pink Sandstorm *aka Agrius*

Storm-0842

Mango Sandstorm *Muddywater*

Storm-1364

Unknown

Marigold Sandstorm *Cobalt Sapling*

Storm-0784 *Shahid Kaveh Group*

Cotton Sandstorm *Emennet Pasargad*

Mint Sandstorm *Charming Kitten*

CYBER & IO PERSONAS

DarkBit

Malek Team

Sharp Boys

Justice Blade

MoneyBird

KarMa

Homeland Justice

Tears of War

No Voice

Hunters

Traitors' Trial

Adll Ali

Open Hands

BB Movements

Saif al-Quds

Moses Staff

Abraham's Ax

Cyber Avengers

Soldiers of Solomon

Anzu Team

Menelaus

Cyber Cheetahs

Market of Data

For Humanity

Cyber Flood

Jewish Peace Advocate

Islamic Resistance Movement

Forces of Light

Al-Toufan

This chart shows a sampling of assessed Iran state-run personas that we track at Microsoft Threat Intelligence. The IRGC's Cotton Sandstorm remains Iran's most prolific influence operator, regularly standing up new cyber-enabled influence operations. We have tracked double the number of personas operated by Cotton Sandstorm than represented here.

Live Maps of Cybersecurity Attacks

https://attackmap.sonicwall.com/live-attack-map/

https://livethreatmap.radware.com/

https://threatmap.checkpoint.com/

https://threatmap.bitdefender.com/

Key Take Aways

Cyberwarfare is not science fiction—it’s happening now. The question is: Are we ready?"

Governments and organizations must take cybersecurity seriously.

Emerging Threats and Considerations

AI-Powered Cyberattacks: The integration of artificial intelligence into cyber operations could lead to more sophisticated and adaptive threats.

Quantum Computing and Cybersecurity: Advancements in quantum computing pose potential risks to current encryption standards, necessitating the development of quantum-resistant algorithms.

Q&A + Something Extra

Link to download the investigation document:
https://lnkd.in/d8_UNGHC

The Foreign Policy Centre

Networks of Influence: Decoding foreign meddling in Romania's elections

Article by Andra-Lucia Martinescu, Sorina Stallard, Alina Balatchi-Lupascu, Mihai George Forlafu and the Osavul Data Team

December 20, 2024

A collaborative investigation into disinformation campaigns and influence operations.