Programme

Unlocking the Future of Legal Defence in Cyberspace

CYBER SECURITY COALITION.be

WELCOME

Pieter Timmermans

CEO
VBO FEB

VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique

CYBER SECURITY A MAJOR CHALLENGE FOR COMPANIES

Pieter Timmermans

CEO FEB

14 March 2023

CYBER SECURITY
A MAJOR CHALLENGE FOR COMPANIES

Cyber threats on the rise

Objectives of cyber criminals:

- Profit
- Data sabotage
- Dark web

Significant risks at various levels, including pressure on the stability of public institutions

SITUATION FOR COMPANIES IN BELGIUM

98% OF COMPANIES FACED WITH RISKS ACCORDING TO IT SECURITY AUDIT

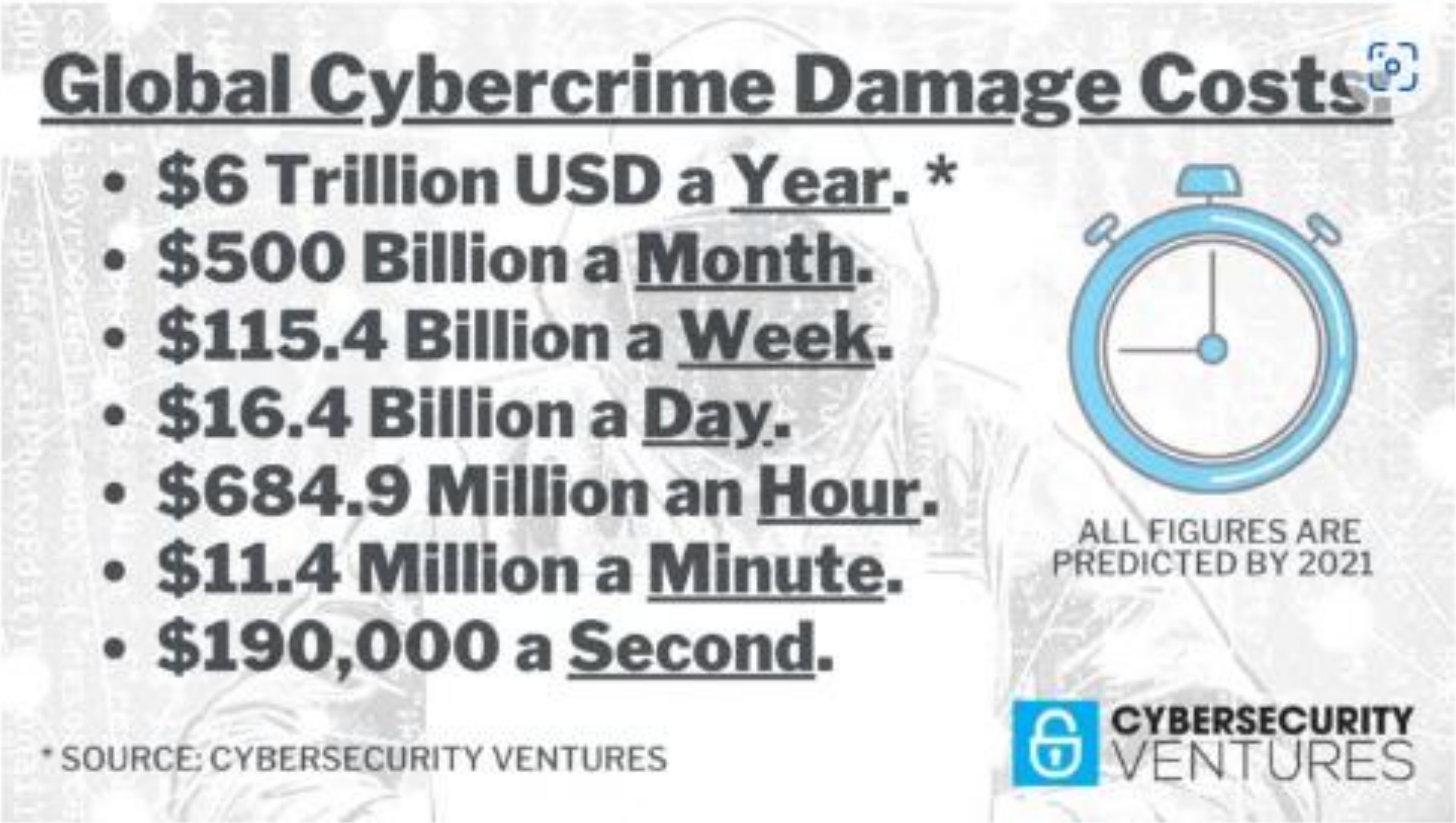
66% HAVE SUFFERED AN ATTACK IN THE LAST TWO YEARS

87% HAVE SUFFERED FINANCIAL DAMAGE OR LOSS OF REPUTATION DUE TO CYBER ATTACKS

28% OF COMPANIES EVEN FEAR THAT THE RISK LEVEL COULD DRIVE THEM INTO BANKRUPTCY

THE FIGHT AGAINST CYBER CRIME MUST BE PURSUED AT MULTIPLE LEVELS

1. Belgian level
2. European level
3. International level



Global Cybercrime Damage Costs:

- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

ALL FIGURES ARE PREDICTED BY 2021

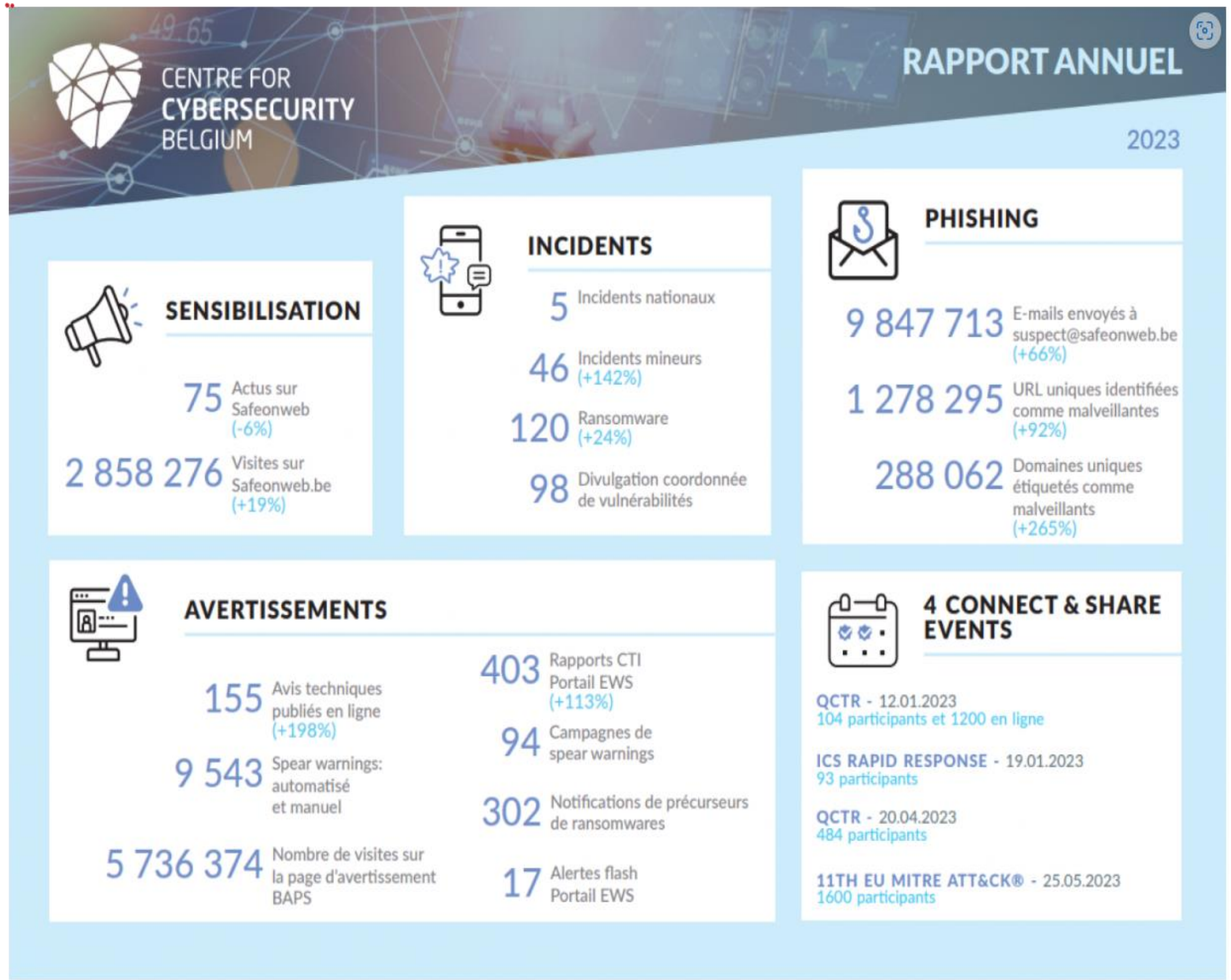
* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY VENTURES

1. BELGIAN LEVEL

CENTRE FOR CYBERSECURITY BELGIUM

- Key role of the CCB in the fight against cyber crime
- Publica Awards for the **Spear Warning** (9,543 warnings sent to organisations in 2023)
- Belgium is home to many international organisations, including NATO and the European Union institutions



CENTRE FOR CYBERSECURITY BELGIUM

RAPPORT ANNUEL

2023

SENSIBILISATION

75 Actus sur Safeonweb (-6%)

2 858 276 Visites sur Safeonweb.be (+19%)

INCIDENTS

5 Incidents nationaux

46 Incidents mineurs (+142%)

120 Ransomware (+24%)

98 Divulgation coordonnée de vulnérabilités

PHISHING

9 847 713 E-mails envoyés à suspect@safeonweb.be (+66%)

1 278 295 URL uniques identifiées comme malveillantes (+92%)

288 062 Domaines uniques étiquetés comme malveillants (+265%)

AVERTISSEMENTS

155 Avis techniques publiés en ligne (+198%)

9 543 Spear warnings: automatisé et manuel

5 736 374 Nombre de visites sur la page d'avertissement BAPS

403 Rapports CTI Portail EWS (+113%)

94 Campagnes de spear warnings

302 Notifications de précurseurs de ransomwares

17 Alertes flash Portail EWS

4 CONNECT & SHARE EVENTS

QCTR - 12.01.2023
104 participants et 1200 en ligne

ICS RAPID RESPONSE - 19.01.2023
93 participants

QCTR - 20.04.2023
484 participants

11TH EU MITRE ATT&CK® - 25.05.2023
1600 participants

2. EUROPEAN LEVEL

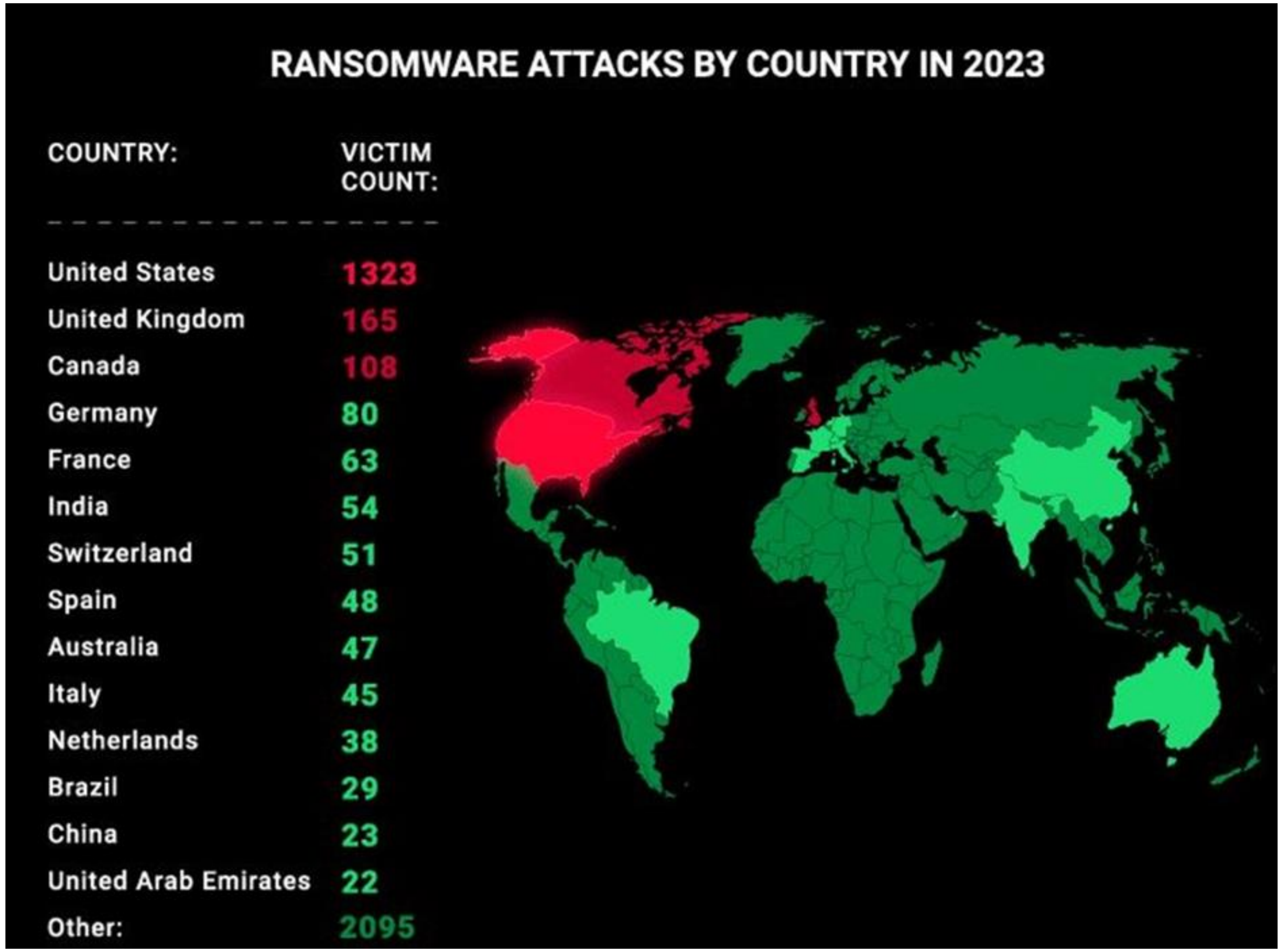
- Hacktivism ↗
- Ransomware ↗
- Public administrations especially targeted (24%)

- **Importance**
  - European legislation/regulations
  - European cooperation
  - Cyber diplomacy

3. INTERNATIONAL LEVEL

Cyber crime will cost the world $10.5 trillion annually by 2025

- ➢ Cyber threat mainly comes from China and Russia
- ➢ Sharing knowledge is necessary
- ➢ Best practices



RANSOMWARE ATTACKS BY COUNTRY IN 2023

COUNTRY:	VICTIM COUNT:
United States	1323
United Kingdom	165
Canada	108
Germany	80
France	63
India	54
Switzerland	51
Spain	48
Australia	47
Italy	45
Netherlands	38
Brazil	29
China	23
United Arab Emirates	22
Other:	2095

CONCLUSION

- ✓ New cyber standards
- ✓ Cyber security implications of advanced technologies like quantum computing
- ✓ Role of AI

VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique

Creating value for society

Verbond van Belgische Ondernemingen vzw
Fédération des Entreprises de Belgique asbl

Rue Ravensteinstraat 4, 1000 Brussel/Bruxelles
BE476 519 923 – RPR Brussel/Bruxelles
www.vbo-feb.be –

David Hickton

Founding Director
Institute for Cyber Law, Policy, and Security
University of Pittsburgh

Rule of Law in the Digital Age

David Hickton, Founding Director, Pitt Cyber

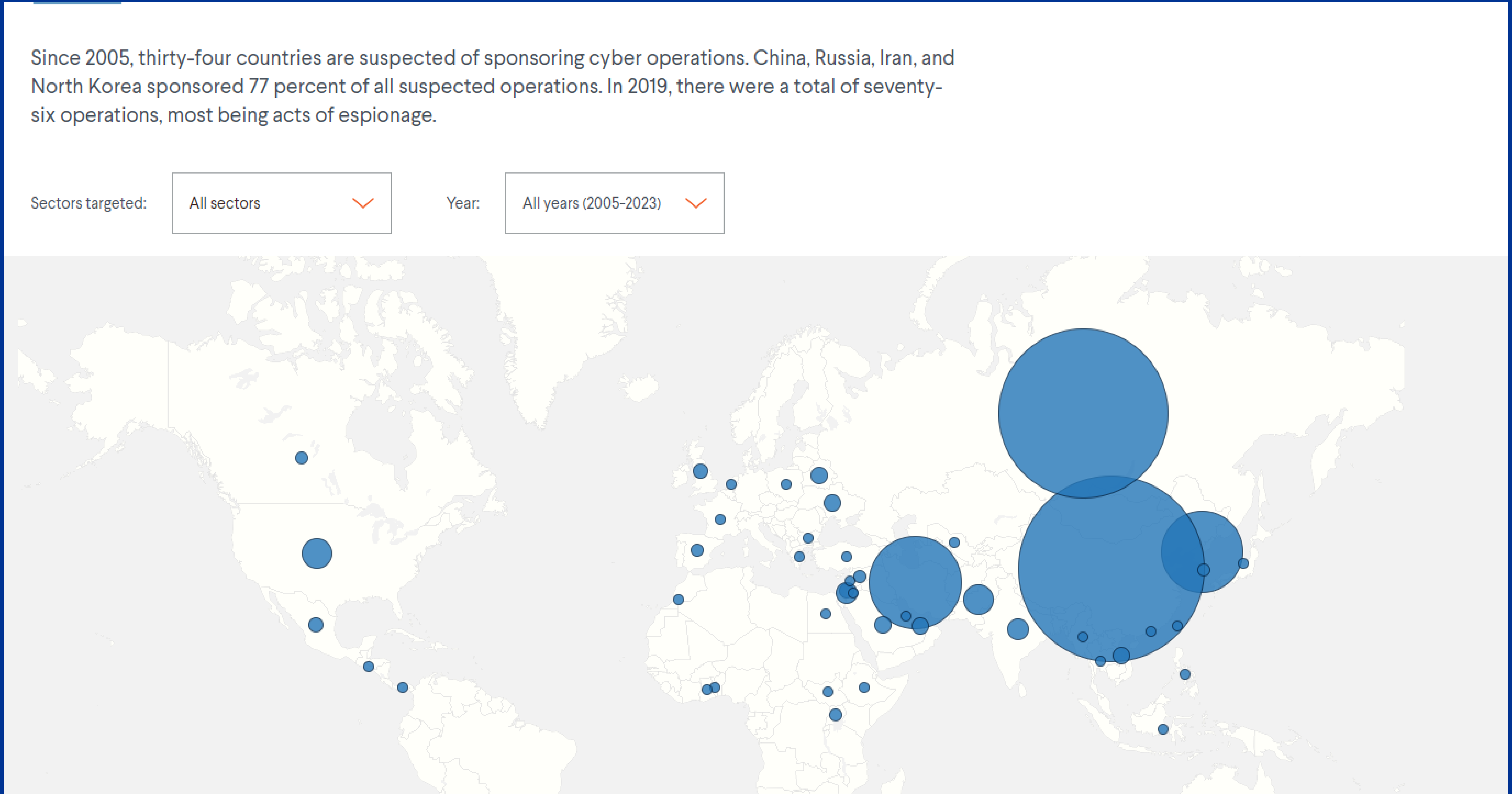
Cyber Security Coalition

March 19, 2024

University of Pittsburgh

Understanding the Threat and Legal Precedent

Scale of the Problem:
Council on Foreign Relations Cyber Operations Tracker



Since 2005, thirty-four countries are suspected of sponsoring cyber operations. China, Russia, Iran, and North Korea sponsored 77 percent of all suspected operations. In 2019, there were a total of seventy-six operations, most being acts of espionage.

Sectors targeted: All sectors

Year: All years (2005-2023)

Illustration of the China Threat/Signature

PLA Military Hacking

- First time the United States leveled cyber espionage charges against the military of a foreign country
- 31-count indictment charging five members of Chinese military with theft of technological secrets and communications

PLA Military Hacking

- PLA Unit 61398
  - Employs hundreds, perhaps thousands of personnel
  - Requires personnel trained in computer security and computer network operations
  - Requires personnel proficient in the English language
  - Has large-scale infrastructure and facilities in the “Pudong New Area” of Shanghai

Boyusec

- “An indictment was unsealed today against Wu Yingzhuo, Dong Hao and Xia Lei, all of whom are Chinese nationals and residents of China, for **computer hacking, theft of trade secrets, conspiracy and identity theft** directed at U.S. and foreign employees and computers of three corporate victims in the **financial, engineering and technology industries** between 2011 and May 2017. The three Chinese hackers work for the purported China-based Internet security firm Guangzhou Bo Yu Information Technology Company Limited (a/k/a “Boyusec”).”

- November 27, 2017

Thomas Rukovina

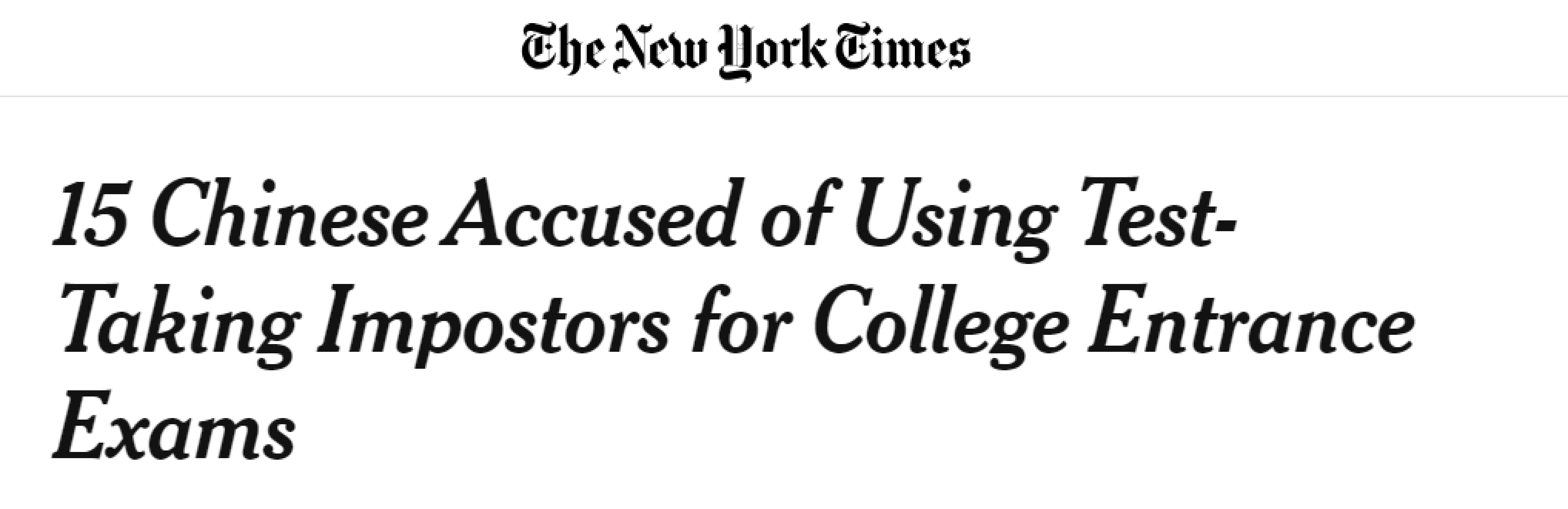
- *“Theft, whether hands-on or through cyber intrusions, diminishes our competitive edge in technology and product development and deprives our citizens of economic opportunities,” stated U.S. Attorney Hickton. “We will aggressively pursue intellectual property theft regardless of who commits the crime.”*

- The criminal complaint alleges that Rukavina retired from PPG in July of 2012. As early as June 2014, Rukavina passed proprietary and confidential information to J.T.M.G. Co., a glass company based in Jiangsu, China, that specializes in automotive and other specialty glass. The trade secret information he passed included PPG’s manufacturing specifications for windows, which are made of synthetic plastics and used for high-speed transportation, including airplanes.”

- May 8, 2015

SAT

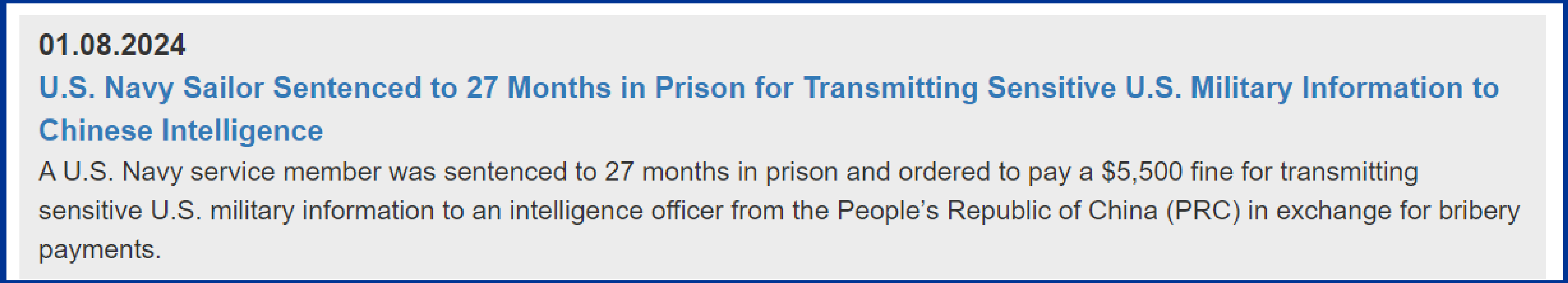
“The 35-count indictment, which was returned on May 21 in the Western District of Pennsylvania, sketches out a complex scheme in which certain individuals are accused of paying impostors using fake Chinese passports to take college entrance exams, mostly at testing sites in the Pittsburgh area, including the SAT and the Test of English as a Foreign Language, or Toefl, in the hope of using them to gain admission to American colleges.”



The New York Times

15 Chinese Accused of Using Test-Taking Impostors for College Entrance Exams

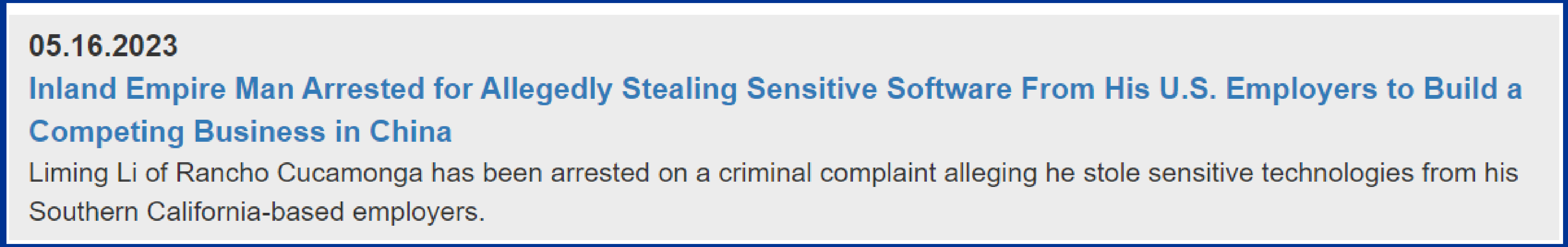
Ongoing Chinese Sponsored Attacks



01.08.2024

U.S. Navy Sailor Sentenced to 27 Months in Prison for Transmitting Sensitive U.S. Military Information to Chinese Intelligence

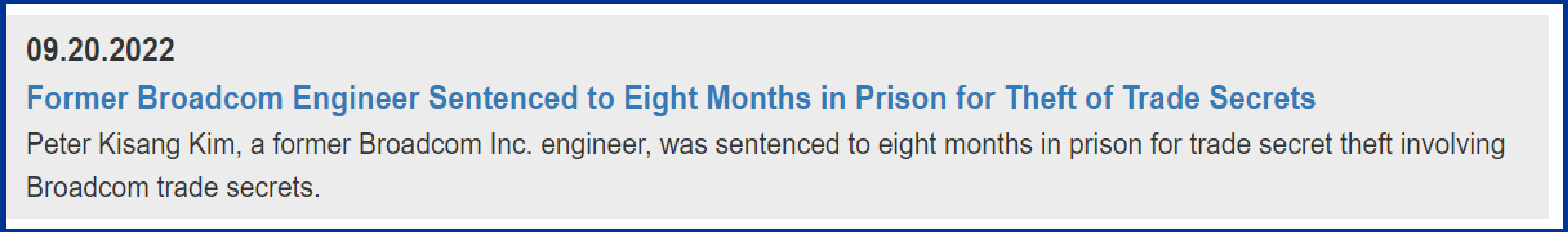
A U.S. Navy service member was sentenced to 27 months in prison and ordered to pay a $5,500 fine for transmitting sensitive U.S. military information to an intelligence officer from the People's Republic of China (PRC) in exchange for bribery payments.



05.16.2023

Inland Empire Man Arrested for Allegedly Stealing Sensitive Software From His U.S. Employers to Build a Competing Business in China

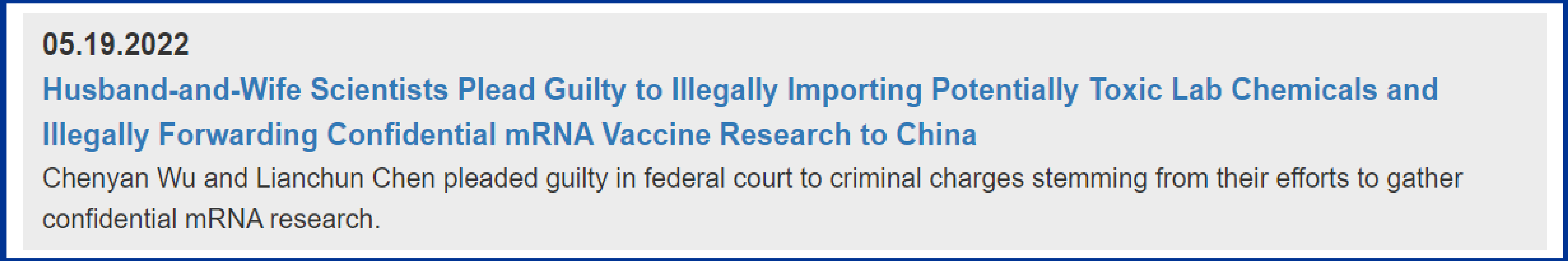
Liming Li of Rancho Cucamonga has been arrested on a criminal complaint alleging he stole sensitive technologies from his Southern California-based employers.



09.20.2022

Former Broadcom Engineer Sentenced to Eight Months in Prison for Theft of Trade Secrets

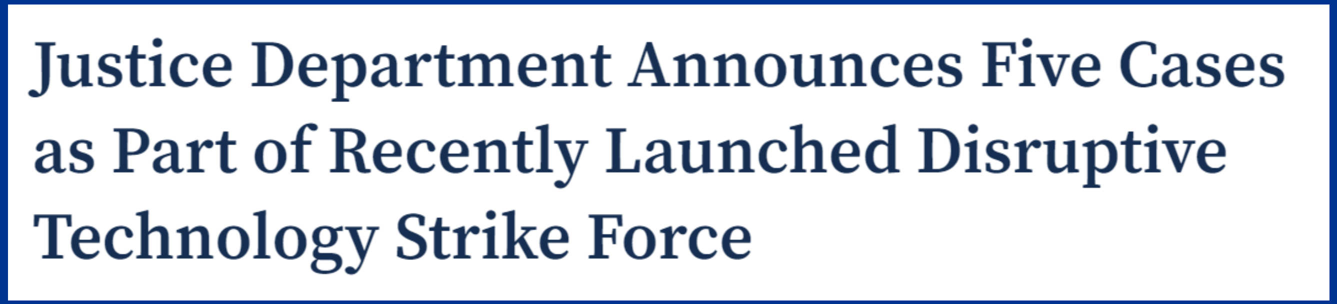
Peter Kisang Kim, a former Broadcom Inc. engineer, was sentenced to eight months in prison for trade secret theft involving Broadcom trade secrets.



05.19.2022

Husband-and-Wife Scientists Plead Guilty to Illegally Importing Potentially Toxic Lab Chemicals and Illegally Forwarding Confidential mRNA Vaccine Research to China

Chenyan Wu and Lianchun Chen pleaded guilty in federal court to criminal charges stemming from their efforts to gather confidential mRNA research.

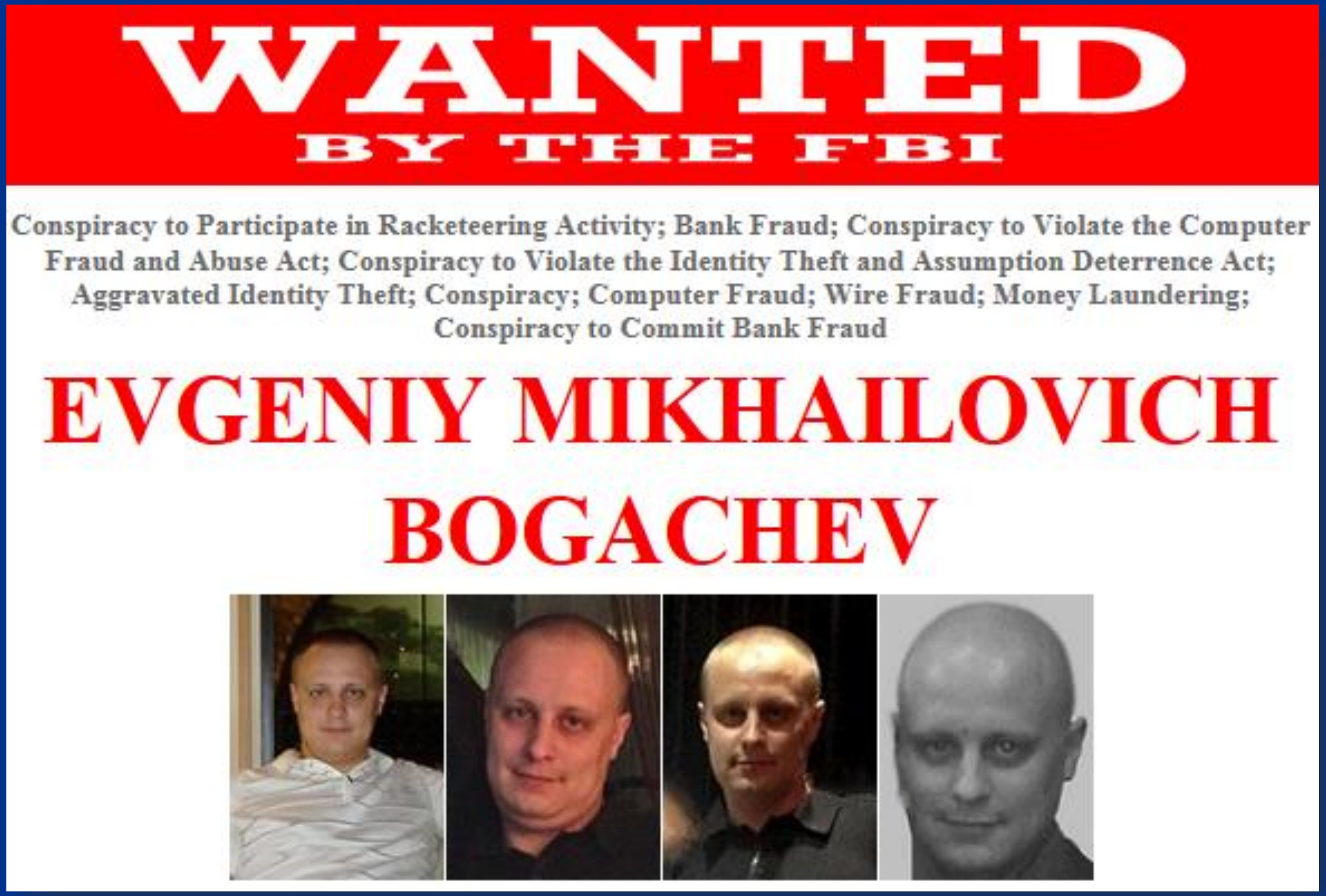


Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force

Illustration of the Russia Threat/Signature

Bogachev

- GameOver Zeus/Cryptolocker
  - One million infected computers worldwide; 25% in the United States
  - $100M+ wire transferred from compromised computers to cyber criminals overseas
  - Haysite Reinforced Plastics in Erie, Penn. bilked of $375K in October 2011



WANTED

BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Bogachev

- All tools approach:
  - Criminal Indictment
  - Civil injunction to dismantle botnet
  - International partners
  - Private business partners
  - $3M reward/ FBI Cyber Most Wanted

Bugat/Dridex/Cridex

- 2011: Zeus-based Trojan Variant
  - Widespread malware but much smaller than GameOver Zeus (GOZ)
  - While investigating GOZ, discovered Bugat

- 2017: Dridex Botnet distributed ransomware
- Aqua is the leader
- Organization known as “Evil Corp.”

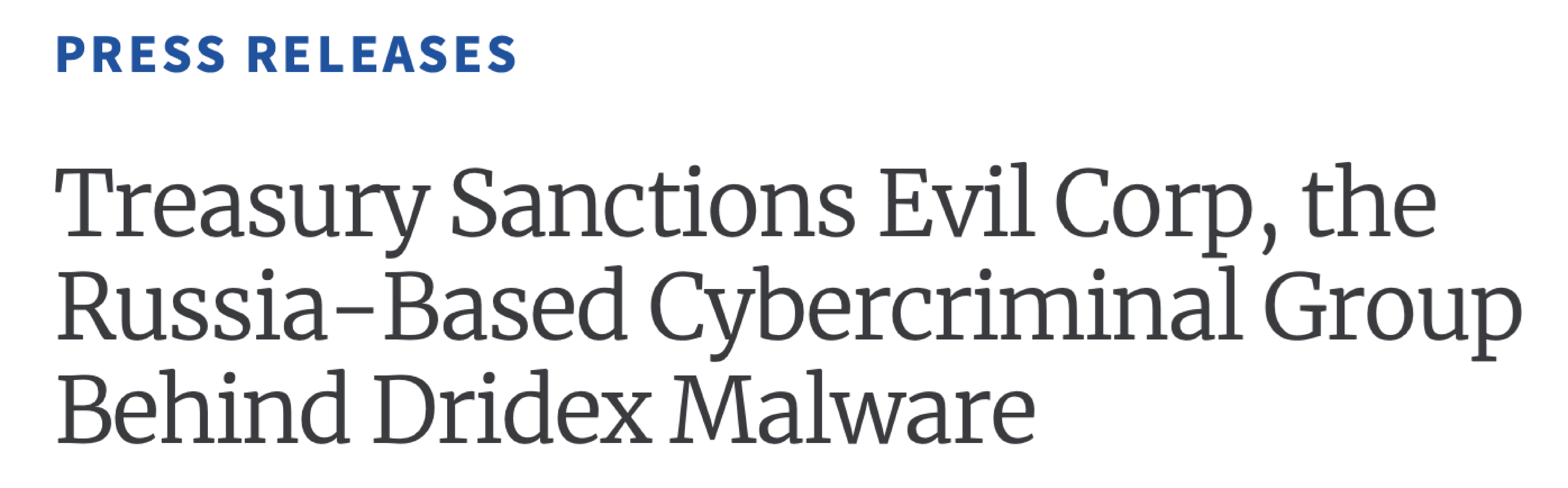
Evil Corp

“Evil Corp (AKA UNC2165) is a one of the most capable cybercriminal syndicates in the world. They are based out of Russia and have been operational since 2009. They are responsible for the development and operations **of several of the most powerful malware and ransomware variants**, and maintain strong relationships not just with other powerful cybercriminal gangs, but also the Russian government.

The U.S. federal government has indicted members of their gang and has an active bounty offered for information on their leadership. Evil Corp has been observed **modifying their activities to circumvent U.S. federal government actions to stop them**.”

- Health Sector Cybersecurity Coordination Center (HC3) threat portfolio

Evil Corp



PRESS RELEASES

Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware

Fancy Bear/Cosy Bear

- **Fancy Bear** (also known as **APT28** , **Pawn Storm**, **Sofacy Group** , **Sednit**, **Tsar Team** and **STRONTIUM)** is a Russian cyber espionage group.
- Among other things, it uses zero-day exploits, spear phishing and malware to compromise targets.
- The group promotes the political interests of the Russian government, and is known for hacking DNC emails to attempt to influence the outcome of the US 2016 presidential elections.

Recent Russian Affiliated Attacks

LONDON, Dec 13 (Reuters) – "A hacking group believed by Kyiv to be affiliated with Russian military intelligence claimed responsibility on Wednesday for a cyberattack that knocked Ukraine's biggest mobile network operator offline."

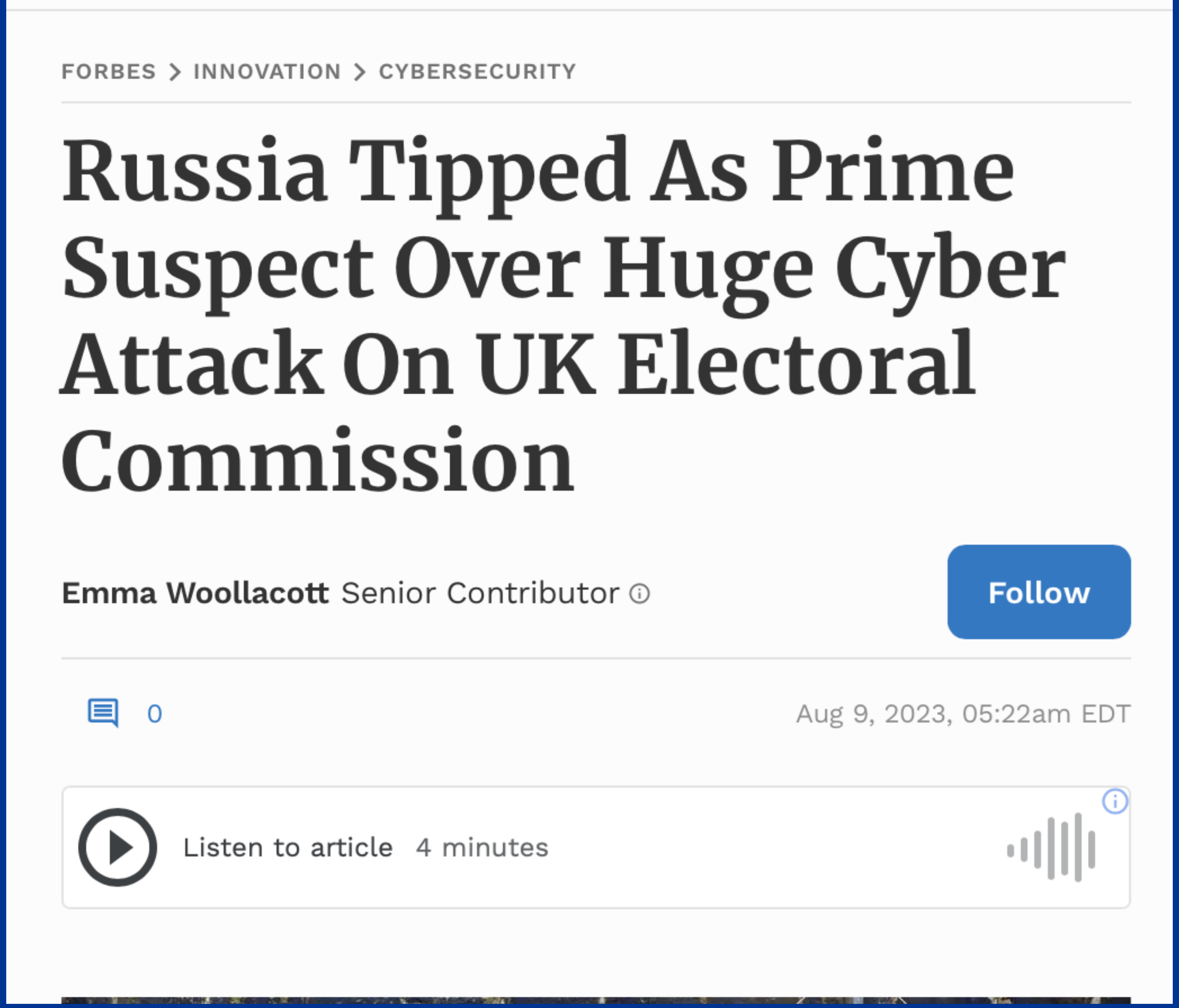
October 10, 2023 (Reuters) "Hacking groups, including some tied to Russia, are attacking Israeli government and media websites, allying themselves with the Palestinian military group Hamas that launched a series of deadly strikes on the country over the weekend."

CISA
CNMF
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
a part of GCHQ
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre
National Cyber Security Centre
PART OF THE GCSB

May 9, 2023: The National Security Agency (NSA) and several partner agencies have identified infrastructure for Snake malware—a sophisticated Russian cyberespionage tool—in over 50 countries worldwide.

Real World Impacts

Election Security

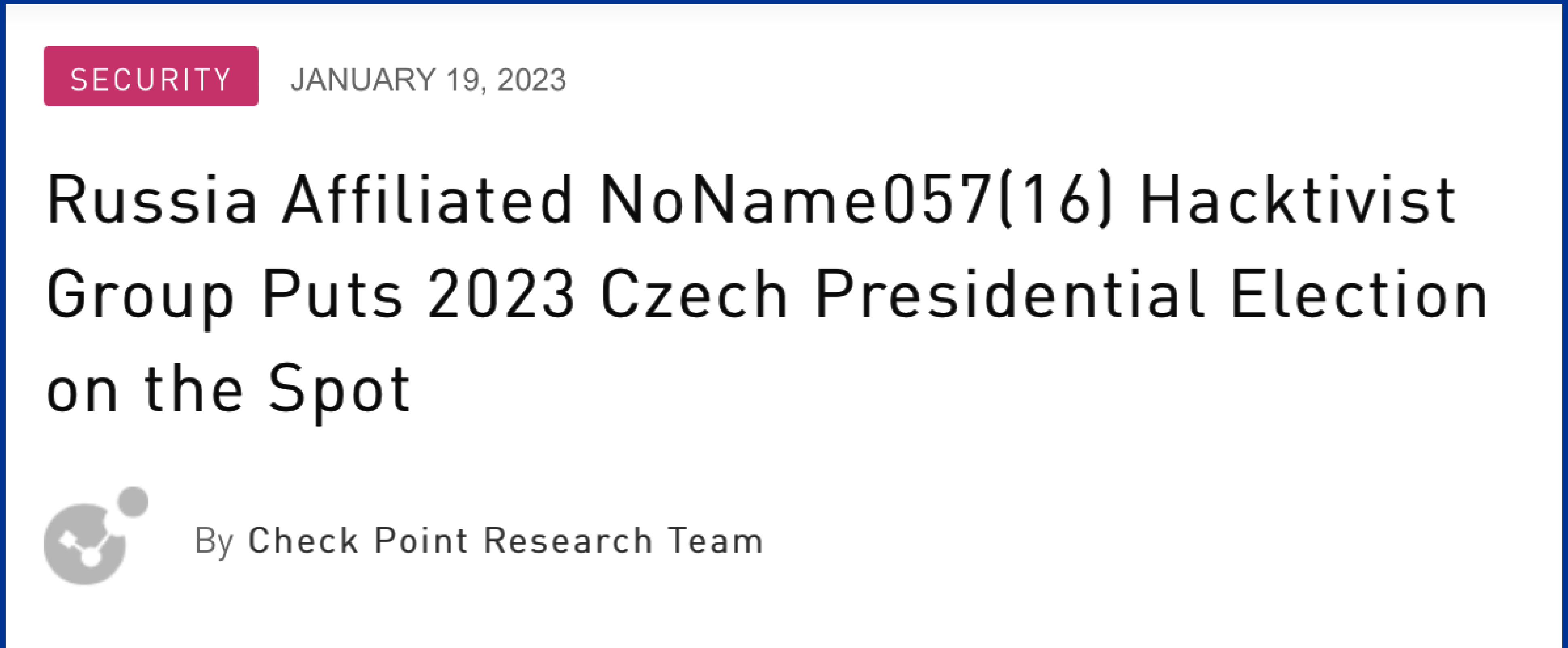


FORBES > INNOVATION > CYBERSECURITY

Russia Tipped As Prime Suspect Over Huge Cyber Attack On UK Electoral Commission

Emma Woollacott Senior Contributor ⓘ

Aug 9, 2023, 05:22am EDT



SECURITY JANUARY 19, 2023

Russia Affiliated NoName057(16) Hacktivist Group Puts 2023 Czech Presidential Election on the Spot

By Check Point Research Team

Security experts warn of foreign cyber threat to 2024 voting

National Security & Critical Infrastructure

“Lawyers, diplomats, and experts generally agree that international law applies (in principle) to cyberspace. Yet they have long and inconclusively debated how it applies and, most pointedly, when cyber attacks cross the threshold to be legitimately considered acts of war.”

-- Carnegie Endowment for International Peace, “Integration Cyber into Warfighting: Some Early Takeaways From the Ukraine Conflict”

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

APRIL 2023 | CYBER CONFLICT IN THE RUSSIA-UKRAINE WAR

Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict

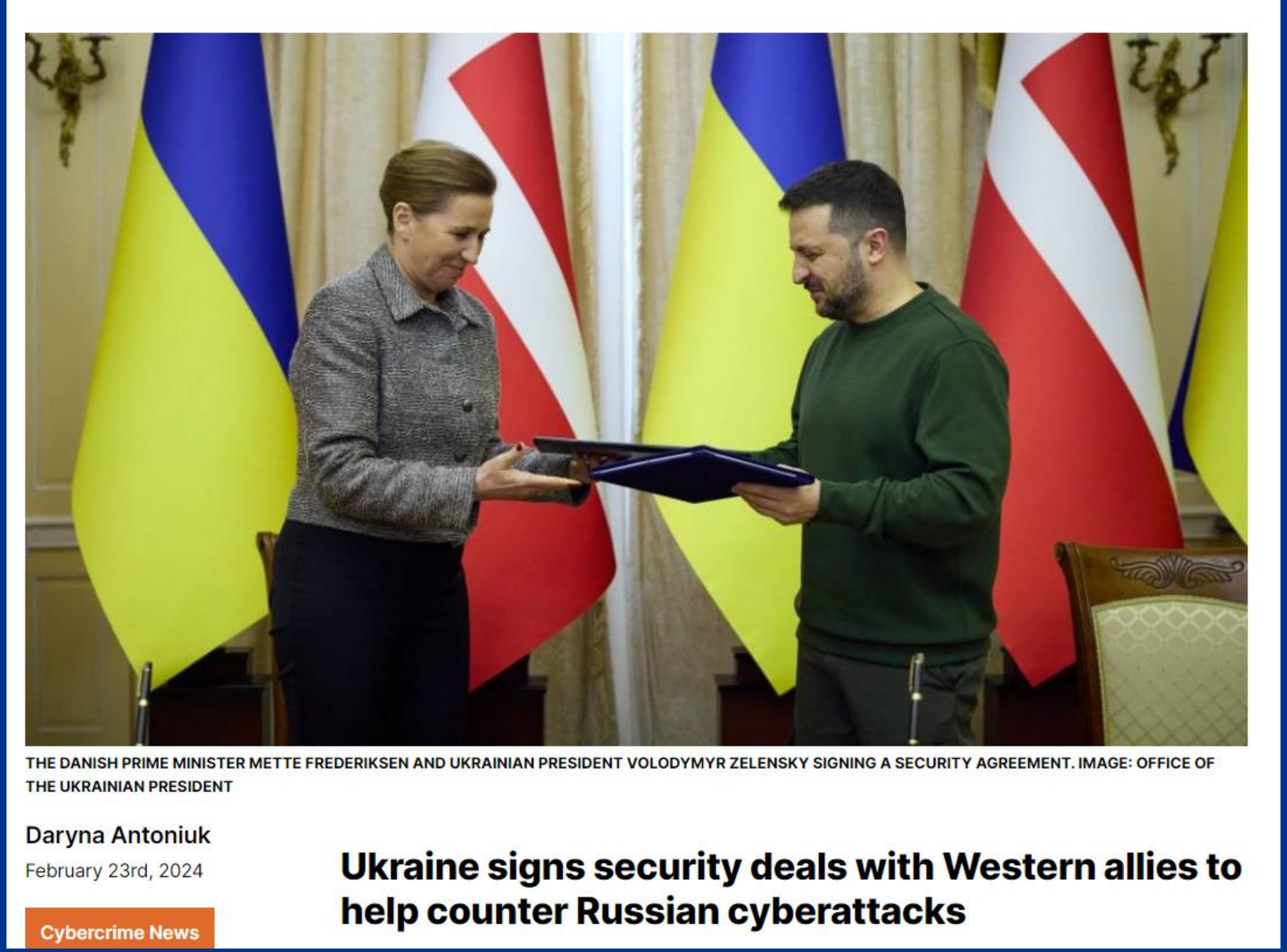
Ariel E. Levite

Warfighting Capabilities

“Russia’s cyber aggression against Ukraine over the past decade has been overwhelmingly directed toward civilian infrastructure, aimed at demoralizing political leaders and eroding popular will … it has backfired. The net outcome of Russia’s relentless cyber attacks appears to have been a digital rally-round-the-flag effect both within Ukraine and among its backers.”

- Carnegie Endowment for International Peace

--



THE DANISH PRIME MINISTER METTE FREDERIKSEN AND UKRAINIAN PRESIDENT VOLODYMYR ZELENSKY SIGNING A SECURITY AGREEMENT. IMAGE: OFFICE OF THE UKRAINIAN PRESIDENT

Daryna Antoniuk

February 23rd, 2024

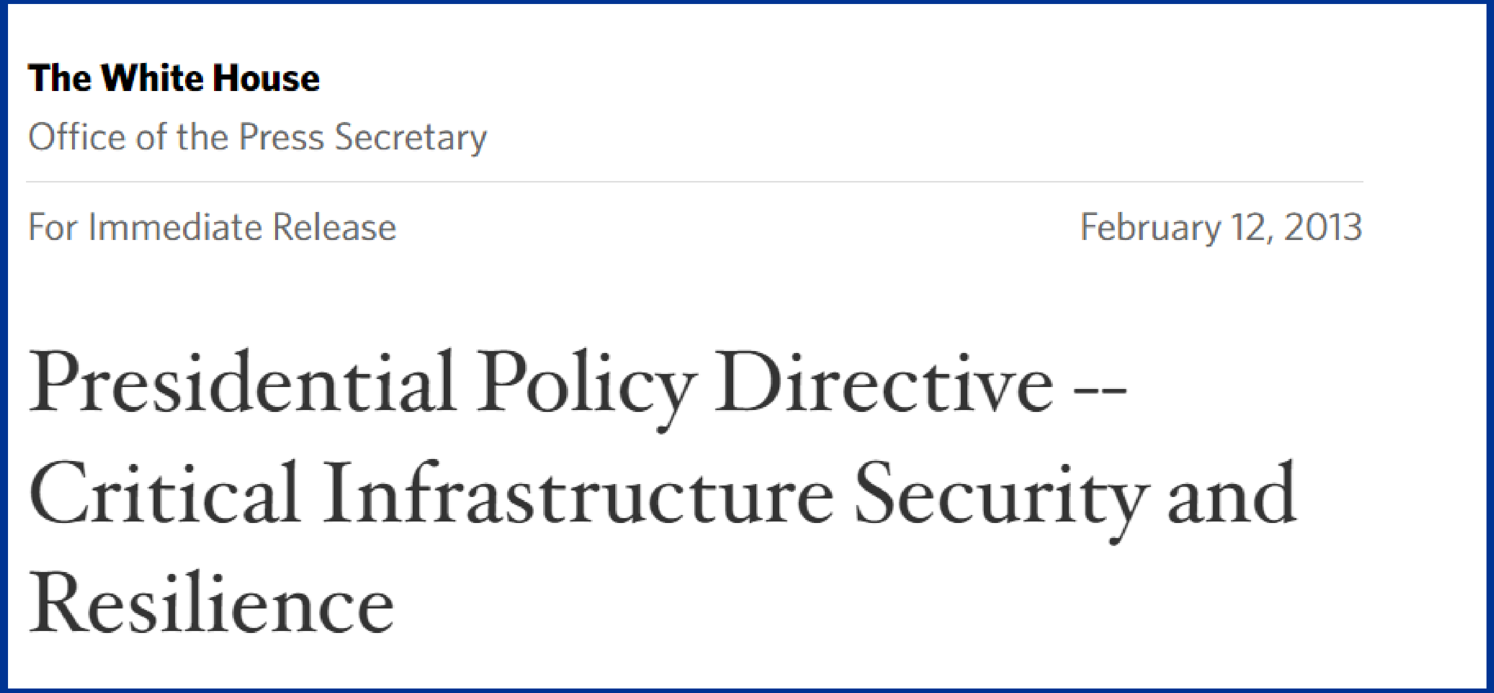
Cybercrime News

Ukraine signs security deals with Western allies to help counter Russian cyberattacks

National Security & Critical Infrastructure

"Moreover, the interconnectivity of critical infrastructure systems raises the possibility of cyber attacks that cause devastating kinetic and non-kinetic effects. As innovation, hyper-connectivity, and digital dependencies all outpace cybersecurity defenses, the warning signs are all present for a potential "cyber 9/11" on the horizon."

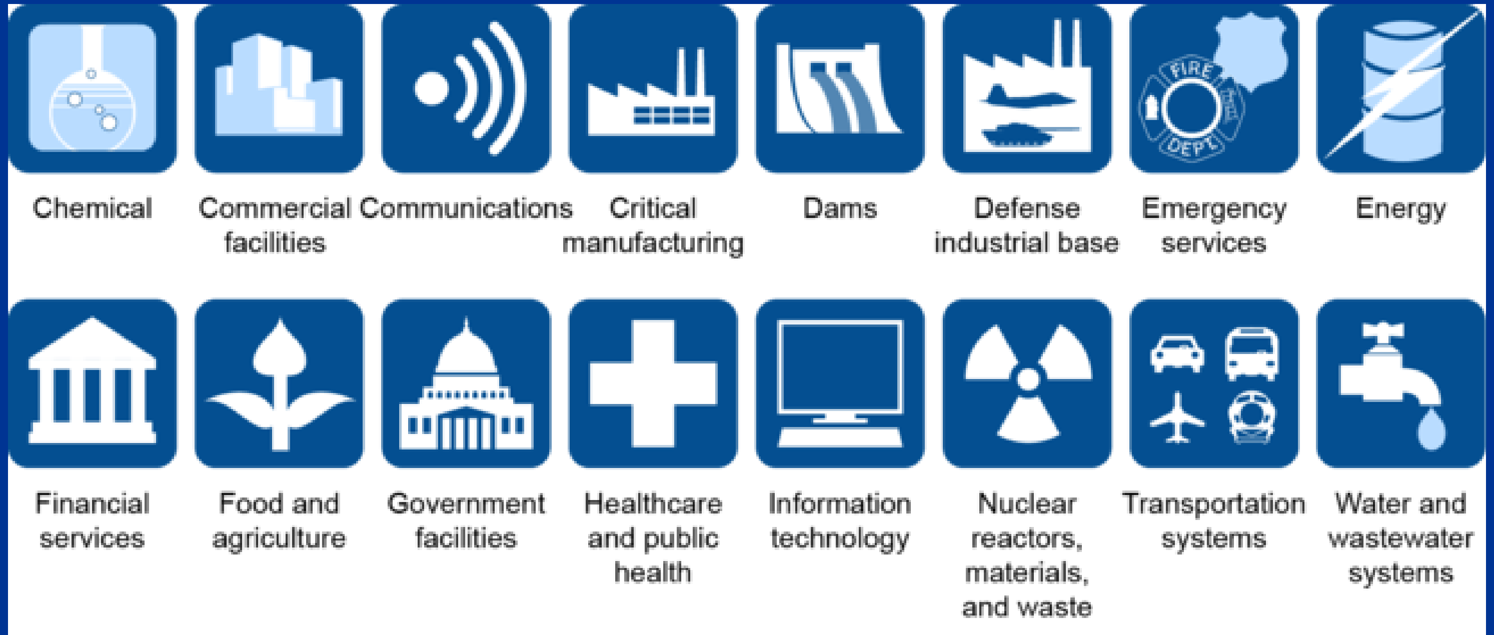
-- U.S. Department of Homeland Security



The White House
Office of the Press Secretary

For Immediate Release February 12, 2013

Presidential Policy Directive -- Critical Infrastructure Security and Resilience



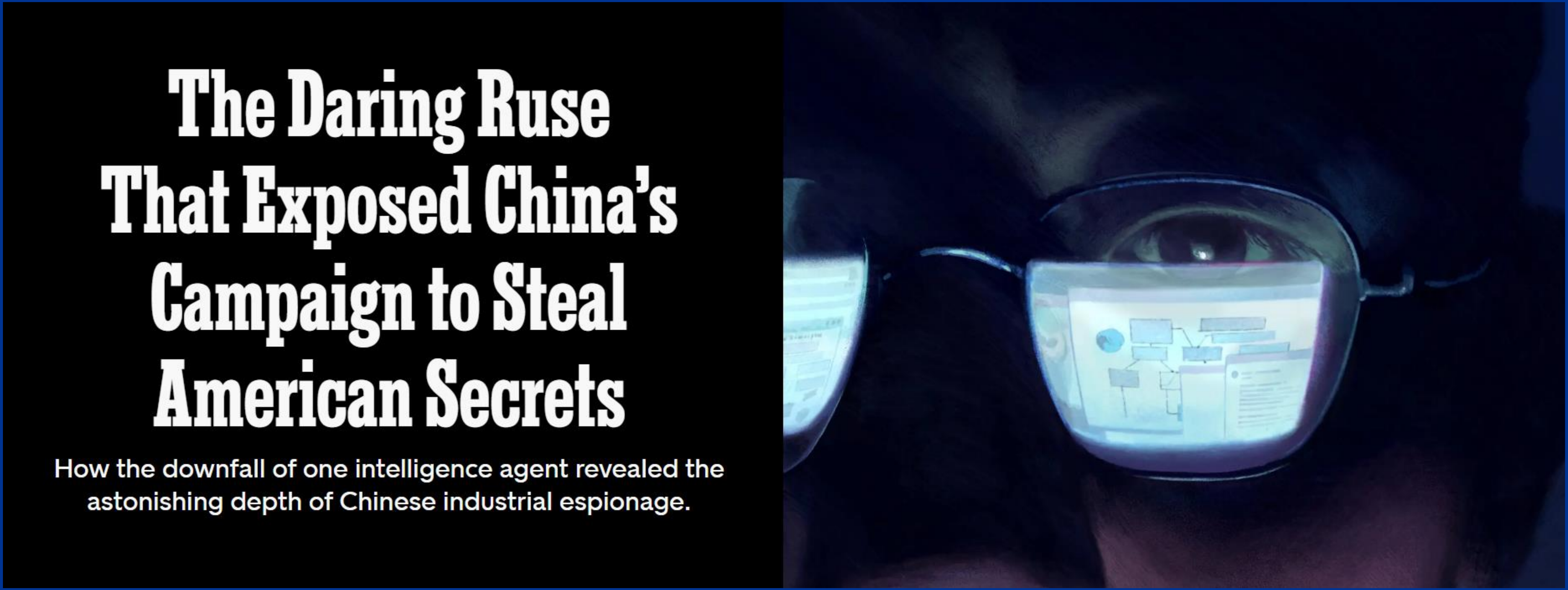
Source: GAO analysis of Presidential Policy Directive-21. | GAO-23-105806

Protect Innovations & Intellectual Property

““““The greatest long-term threat to our nation’s information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China.”

- FBI Director Chris Wray

Economic Vitality



The Daring Ruse That Exposed China's Campaign to Steal American Secrets

How the downfall of one intelligence agent revealed the astonishing depth of Chinese industrial espionage.

Is it working?

The U.S. and Western legal response & deterrence, assessing impact of our collective efforts

Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act is the primary law by which the federal government prosecutes computer hacking. Section 1030 creates an offense if a person intentionally or knowingly accesses a computer without or in excess of authorization, resulting in loss and/or harm. The loss or harm requirement varies with the type of offense charged.

The CFAA was originally enacted as a response to the growing use of computers, particularly by the federal government, and the growing threat of computer crimes.

- Analogized hacking to physical-world trespass
- Limited to certain types of criminal misconduct; mostly ones that would be subject to federal jurisdiction

The CFAA has been amended a number of times to widen its scope

- Most computers, including cell phones, come under the CFAA's jurisdiction because of the interstate nature of the internet
- Modified by the PATRIOT Act, the Identity Theft Enforcement and Restitution Act (ITERA)

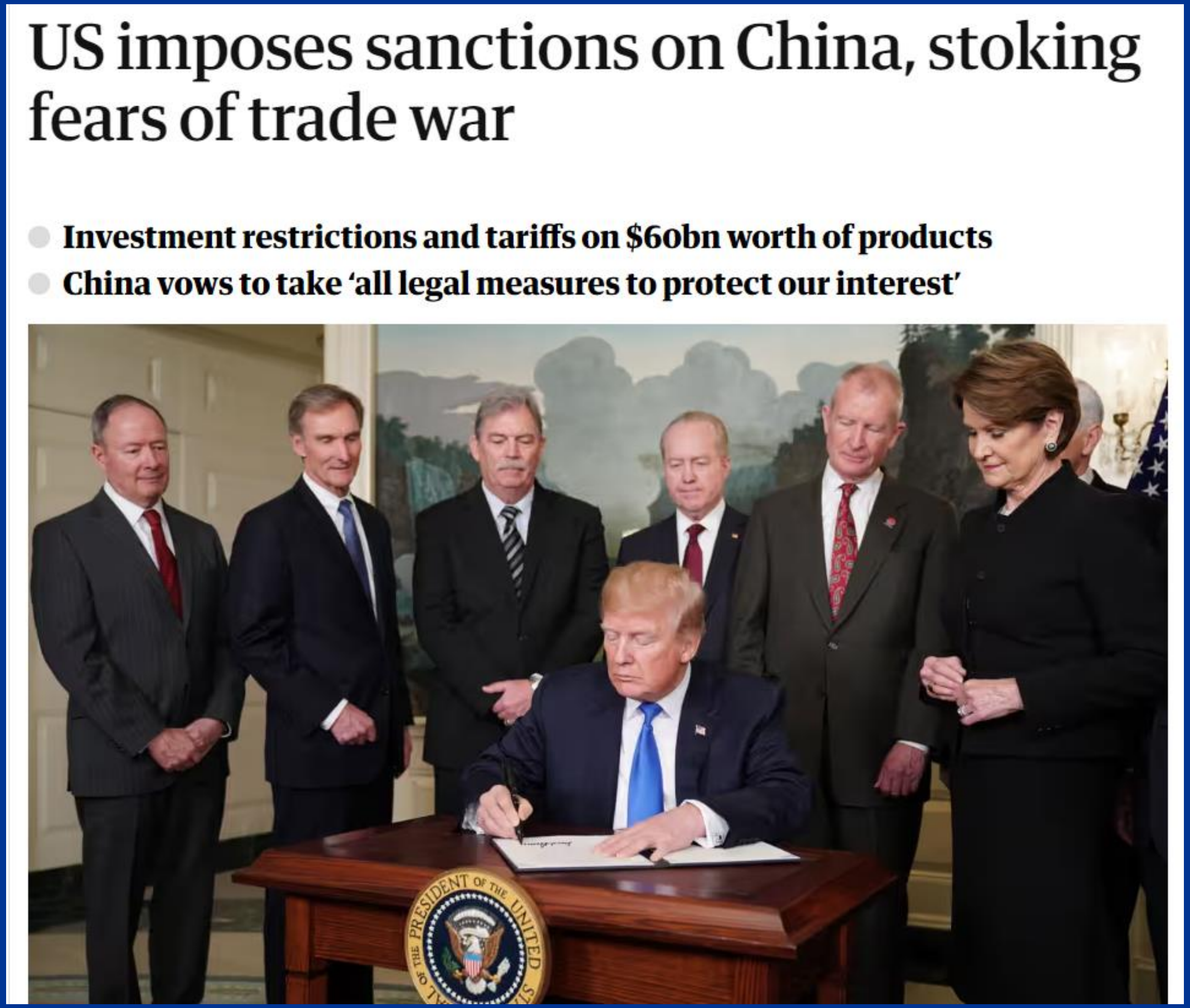
Obama-Xi 2014 Agreement

“The United States and China agree that **neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property**, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors…

Both sides are committed to making common effort to further identify and **promote appropriate norms of state behavior in cyberspace** within the international community…

The United States and China agree to establish a **high-level joint dialogue** mechanism on fighting cybercrime and related issues…”

President Trump’s China Sanctions



US imposes sanctions on China, stoking fears of trade war

- Investment restrictions and tariffs on $60bn worth of products
- China vows to take ‘all legal measures to protect our interest’

President Biden’s China Policy

The Biden Administration’s EO 14105 restricts outbound investment to China, Hong Kong, and Macau in areas deemed critical to U.S. national security. These include three main industries:

- Advanced computing chips and microelectronics
- Quantum technology
- Artificial intelligence (AI)

Aug 9, 2023

Looking Towards the Future

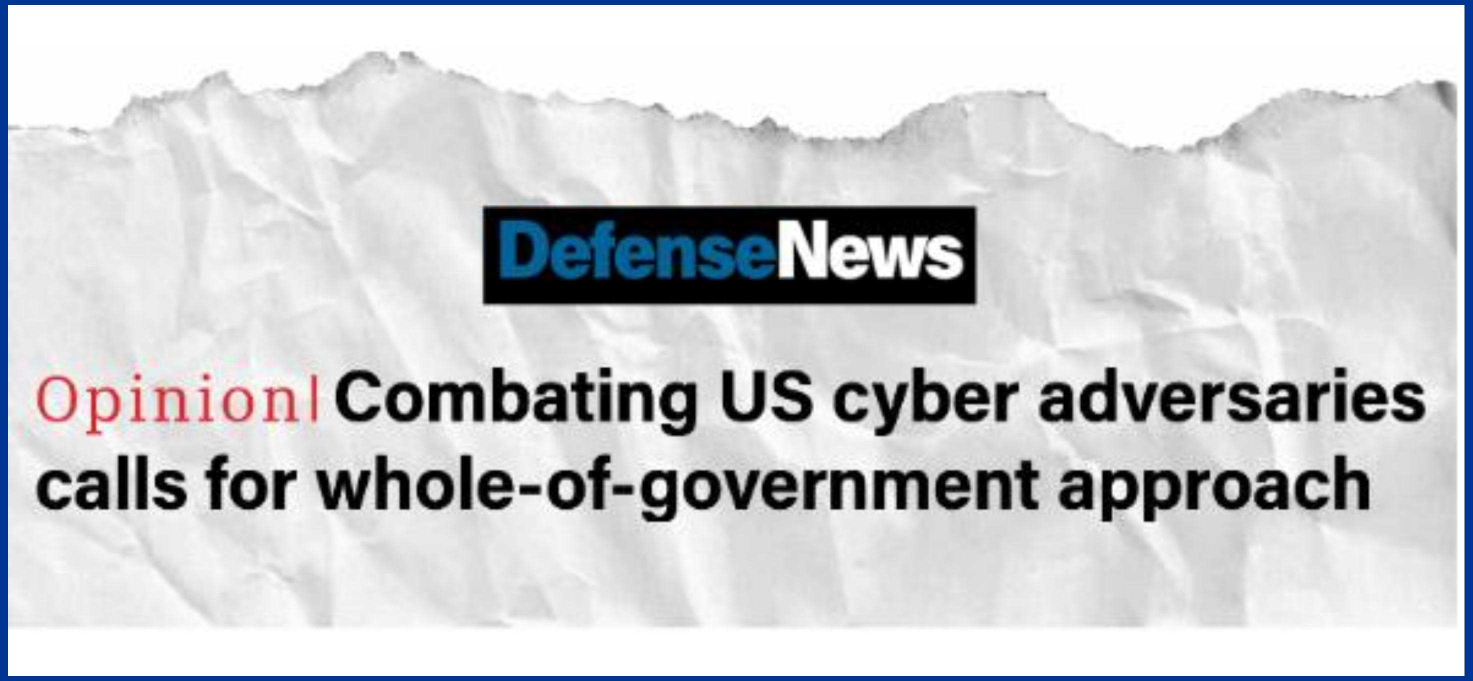
Where do we go from here?

Leveraged Engagement

- Make market access dependent on adherence to global norms/treaties
- Best laid plans vs reality:
  - "China's membership [to the WTO] commits it to comply with the principles and rules of the international trading system … Second, China's commitments are a lever its reform-oriented leadership can use to complete the transition to a more market-oriented economy."
    - – *Brookings commentary, 2001*
  - "A key part of China's technology drive involves the acquisition of foreign technologies through acts, policies, and practices of the Chinese government that are unreasonable or discriminatory and burden or restrict U.S. commerce and are part of a multifaceted strategy to advance China's industrial policy objectives … As the global economy has increased its dependence on information systems in recent years, cybertheft has become one of China's preferred methods of collecting commercial information."
    - *– 2018 USTR Report "Findings of the investigation into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under Section 301 of the Trade Act of 1974*

Use All Tools Available

- Criminal enforcement (DoJ)
- Licensing
- Debarment
- Sanctions (Commerce/Treasury)
- WTO (USTR)
- Negotiations & démarche (State)



DefenseNews

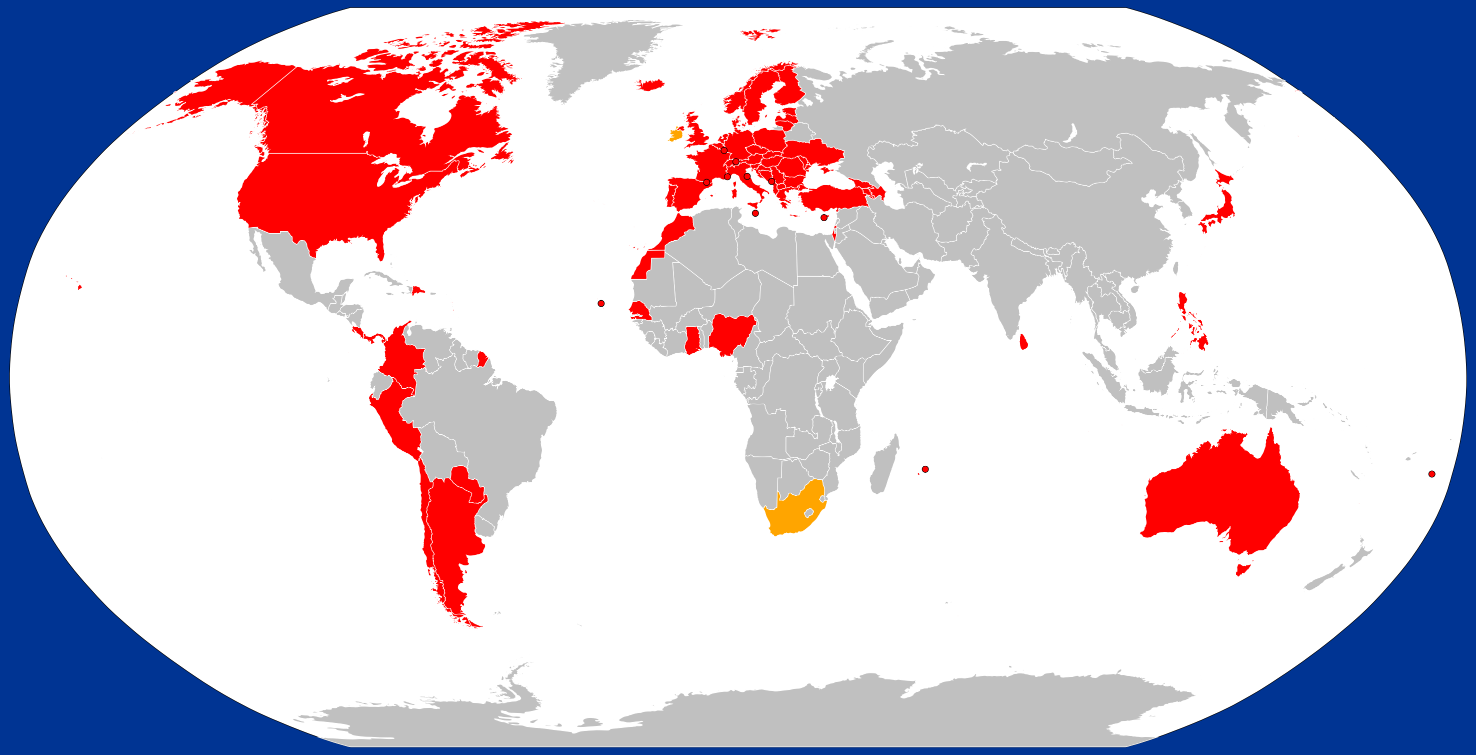
Opinion| Combating US cyber adversaries calls for whole-of-government approach

The Fight for Cyber Norms and Diplomacy

- Cyber diplomacy involves the use of diplomatic tools and initiatives to achieve objectives in the complex and continuously evolving uncharted territory of cyberspace, as described in the national strategy for cyberspace. States use the shared and accepted rules, protocols, and behaviours, to facilitate interactions between global actors of the public and the private sector.
- Functions:
  - formation of dialogue and communication between states and non-state actors
  - the collective response to cyber threats
  - non-proliferation of cyber arms
  - advancement of national interests in cyberspace through diplomacy & cybersecurity policies
  - the protection of human rights in cyberspace
  - development of international cyber laws

The Fight for Cyber Norms and Diplomacy

- Budapest Convention on Cybercrime
  - Signed 2001
  - Neither Russia nor China are party to the Treaty
  - “The Budapest Convention reconciles the vision of a free Internet, where information can freely flow and be accessed and shared, with the **need for an effective criminal justice response in cases of criminal misuse.** Restrictions are narrowly defined; only specific criminal offences are investigated and prosecuted, and specified data that is needed as evidence in specific criminal proceedings is secured subject to human rights and rule of law safeguards.”



- New, potential problematic cybercrime treaty under negotiation in the UN

“The draft treaty risks not just legitimizing the misuse of cybercrime laws to squash dissent and expand state control, but expanding this misuse to other countries. It would also make governments more likely to help abusive allies.” – [Human Rights Watch]

University of Pittsburgh

Key EU Cyber Initiatives and Legislation

- European Union Agency for Cybersecurity (ENISA)
  - Founded in 2004, ENISA “contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow”
- 2019 EU Cybersecurity Act
  - Tasks ENISA with setting up and maintaining the European cybersecurity certification framework for ICT products, services and processes
- 2020 EU Cybersecurity Strategy
  - “Aims to ensure a global and open Internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe … [by] … deploying three principal instruments … regulatory, investment and policy initiatives.”
- NIS (2016) and NIS2 (2023) directives
  - Harmonizes national cybersecurity capabilities, cross-border collaboration and the supervision of critical sectors across the EU

U.S. – EU Cyber Cooperation

- **Annual United States-European Union 9th Cyber Dialogue**
  - Enhanced cooperation between ENISA and CISA in the areas of capacity building to boost cyber resilence; knowledge sharing on the cybersecurity threat landscape; and best practices on the implementation of cyber legislation
- **EU-US Joint Cyber Safe Products Action Plan**
  - Mutual recognition on cybersecurity requirements on Internet of Things (IoT) hardware and software consumer products via the EU Cyber Resilience Act & U.S. Cyber Trust Mark program
- **International Counter Ransomware Initiative**
  - 2023 Joint Statement: “members reaffirmed our joint commitment to building our collective resilience to ransomware, cooperating to undercut the viability of ransomware and pursue the actors responsible, countering illicit finance that underpins the ransomware ecosystem, working with the private sector to defend against ransomware attacks, and continuing to cooperate internationally across all elements of the ransomware threat.”

On the Horizon: AI and Quantum

“AI is expanding the **window of vulnerability** the United States has already entered. For the first time since World War II**, America’s technological predominance—the backbone of its economic and military power—is under threat.** China possesses the might, talent, and ambition to surpass the United States as the world’s leader in AI in the next decade if current trends do not change. Simultaneously, AI is deepening the threat posed by cyber attacks and disinformation campaigns that Russia, China, and others are using to infiltrate our society, steal our data, and interfere in our democracy.”

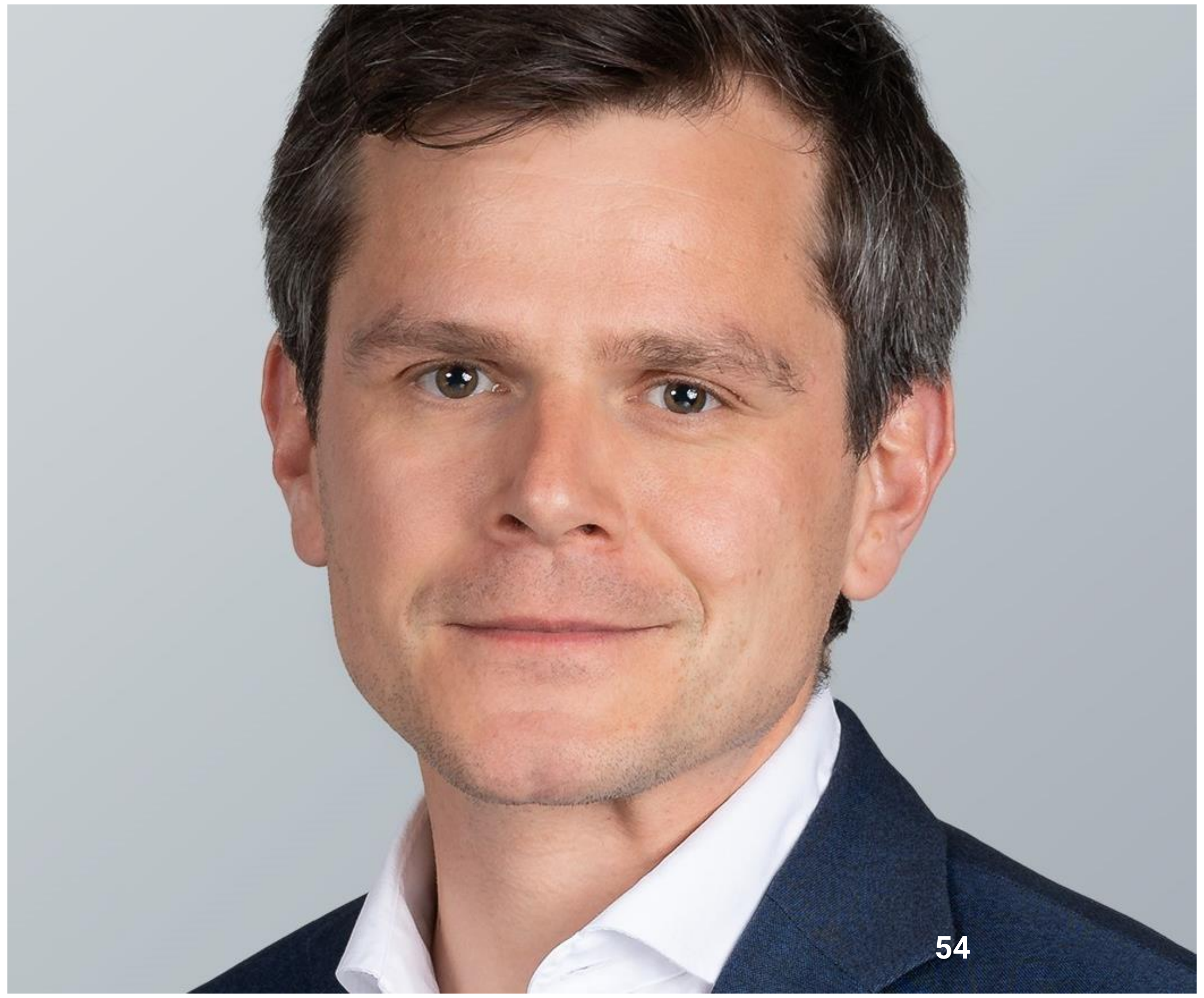
- National Security Commission on Artificial Intelligence Final Report

Discussion & Questions

Roundtable:

Cyber Law Unbound:

Exploring legal frontiers in the battle against cybercrime



Cyber Law Unbound

All crimes are cybercrimes nowadays.

There is a hotline between Washington and Brussels to fight cybercriminals.

We need a parallel criminal code for cybercrimes.

Choose your battles:

it is not worth investing in a criminal investigation, as the money from scams is most probably forever gone.

Encryption is an absolute human right that should not give way to law enforcement needs.

Lawmakers stand in the way of economic progress.

It is an open secret that in case of a ransomware attack companies and institutions pay it off.

In an era where companies become more powerful than governments, there is a way to enhance public-private cooperation.

CYBER SECURITY COALITION.be

Thank you