

Cyber Risk GmbH  
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341  
Dammstrasse 16, 8810 Horgen, Switzerland  
Tel: +41 79 505 89 60 Web: <https://www.cyber-risk-gmbh.com>



*May 2023, top cyber risk and compliance related  
local news stories and world events*

Dear readers,

Following the Digital Services Act (DSA), the European Commission *designated* 17 Very Large Online Platforms (VLOPs) and 2 Very Large Online Search Engines (VLOSEs) that reach at least 45 million monthly active users. Quiz: How many entities are not European?



Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, Bing, Google Search, **the clock is ticking**. Following the designation, you have to comply, within four months, with the full set of new obligations under the Digital Services Act (DSA).

Platforms and search engines need to take measures to address risks linked to the *dissemination of illegal content online* and to negative effects on freedom of expression and information.

Users will get clear information on why they are recommended certain information, and will have the right to opt-out from recommendation systems based on profiling;

Platforms will have to identify, analyse and mitigate a wide array of systemic risks ranging from how illegal content and disinformation can be amplified on their services, to the impact on the freedom of expression and media freedom.

Similarly, specific risks around gender-based violence online and the protection of minors online and their mental health must be assessed and mitigated.

The risk mitigation plans of designated platforms and search engines will be subject to an independent audit and oversight by the Commission.

Read more at number 19 below.

---

Lucius Annaeus Seneca has said: “It is not because things are difficult that we do not dare, it is because we do not dare that they are difficult.”

Dear Lucius, even if we dare, things are becoming very difficult for the healthcare industry, and the regulatory landscape becomes way more complex. Healthcare compliance officers may need some medical assistance in the near future, but at least they work in the right place for that.

It is very difficult to achieve a balance between the need for patient access to affordable medicinal products and the need to stimulate innovation.

The European Commission has just introduced *two* legislative proposals, a directive and a regulation for medicinal products. *Why should we choose between a directive and a regulation, when we can have both?*

The *proposal for a Regulation* “laying down Union procedures for the authorisation and supervision of medicinal products for human use and establishing rules governing the European Medicines Agency”, is *182 pages long*. It covers the authorisation, supervision and pharmacovigilance of medicinal products for human use at Union level, and establishes rules and procedures at Union and at Member State level relating to the *security of supply* of medicinal products.

The Regulation will not affect the powers of Member States' authorities as regards *setting the prices* of medicinal products, or their *inclusion in the scope* of the national health system or social security schemes on the basis

of health, economic and social conditions.

The *proposal for a Directive* “on the Union code relating to medicinal products for human use” is *184 pages long*. It covers rules for the *placing on the market, manufacturing, import, export, supply, distribution, pharmacovigilance, control and use of medicinal products for human use*.

These two legal acts are on top of the *proposed European Health Data Space (EHDS)*, a key pillar of the *European Health Union* that builds further on the General Data Protection Regulation (GDPR) and the NIS 2 Directive. Yes, it is becoming very complex and difficult to understand.

The European Health Union covers how EU countries prepare and respond to health crises, have available, affordable, innovative and adequate medical supplies, and work together to improve prevention, treatment and aftercare for diseases.

*The proposed EHDS regulation applies to:*

(a) manufacturers and suppliers of electronic health record (HER) systems and wellness applications placed on the market and put into service in the Union and the users of such products;

(b) controllers and processors [established in the Union](#) processing electronic health data of Union citizens and third-country nationals legally residing in the territories of Member States;

(c) controllers and processors [established in a third country](#) that has been connected to or are interoperable with MyHealth@EU;

There are interesting *security related* definitions too. In the proposed EHDS regulation we read:

‘[Serious incident](#)’ means [any](#) malfunction or deterioration in the characteristics or performance of an EHR system made available on the market that [directly or indirectly leads, might have led or might lead](#) to any of the following:

(i) the death of a natural person or serious damage to a natural person’s health;

(ii) a serious disruption of the management and operation of critical infrastructure in the health sector;

Marcus Tullius Cicero has said that “It is the peculiar quality of a fool to perceive the faults of others and to forget his own”. There are no fools in

the European Commission, and they definitely do not want to forger their own mistakes in the past, so they try to make no mistakes now. How can you forget something in a legal act if you call “serious incident” something that **might** have led or **might** lead to problems?

The list of the ‘serious incidents’ is probably very long. If we combine it with the “all-hazards approach” in the NIS 2 Directive, risk and compliance officers in the future will have to spend way more time learning and understanding the legal aspects, in a very complex environment.

Read more at number 7 and 8 below.

---

Sophocles believed that people should rather fail with honor than succeed by fraud. There are many that believe exactly the opposite.

The European Banking Authority (EBA) published the new Consumer Trends Report (CTR), and there are some very interesting observations.

*1. Fraud in retail payments* – Fraudsters have started to deploy different methods to defraud consumers. For example, they are increasingly exploiting the increased digitalisation of retail payments, through methods such as ‘phishing’, ‘vishing’, ‘subscriber identity module’ (SIM) swapping, ‘ID spoofing’, ‘manipulation’, ‘spyware’, and ‘smishing’, and perpetrate their fraud particularly on credit card transactions and credit transfers.

Furthermore, several NCAs and other stakeholders reported an increase in fraudulent payments executed to purchase crypto-assets. In response, NCAs took measures focused on assessing financial institutions’ compliance with applicable security requirements, raising consumer awareness, and financial institutions enhancing their IT systems.

*2. Over-indebtedness and arrears* – the more recent changes in the economic environment with persistently increasing inflation where central banks across the EU are normalising interest rates to pre-crisis levels have resulted in more expensive borrowing costs for consumers, a general increase in the cost of living and of consumers’ demand to access credit facilities.

Several Member States have already implemented measures to support consumers in repayment difficulties and/or financial distress. The aforementioned effects exacerbate already existing issues arising from the impact of poor creditworthiness assessment procedures applied by some financial institutions.

Relatedly, new business models and credit products have become

increasingly popular, all of which are often exclusively available through digital channels and many of which currently fall outside of the regulatory perimeter (buy-now-pay-later, peer-to-peer lending).

Read more at number 9 below.

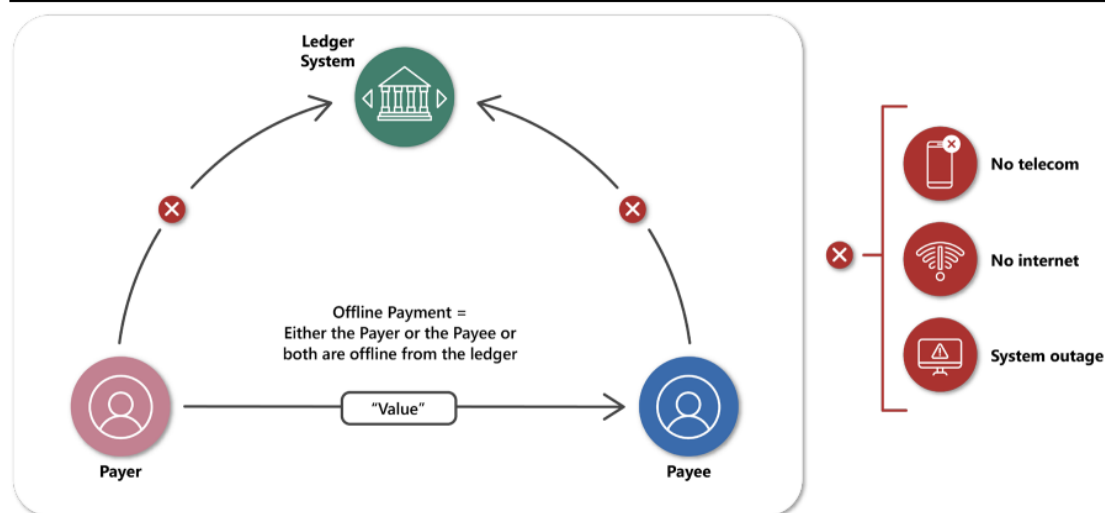
An *offline* payment with CBDC is a transfer of value between devices, that does not require connection to any ledger system, often in the absence of internet or telecoms connectivity. A user device may be online (connected to the internet), but still disconnected from a ledger system.

This is an interesting definition, in the new paper with title “Project Polaris: Offline payments with CBDC” from the Bank for International Settlements (BIS). The paper is intended to help central banks to:

- understand the available technologies and *security* measures;
- understand the main *threats, risks and risk management* measures;
- understand the *privacy* issues, inclusion needs and resilience options;
- understand the design and architecture principles involved; and
- gain perspective on potential *operational and change management* issues.

#### Offline payments and ledger systems

Figure 1



In CBDC systems, *risk management by design* is key. This is particularly important for CBDC systems that provide offline payments functionality, as offline payment solutions are exposed to *different threats and vulnerabilities*, and therefore different risks, than online solutions.

We have a new paper, and some interesting definitions in this context:



- A *risk* refers to the potential for destruction, damage or loss of business assets and data resulting from a threat.
- A *threat* is an event that unintentionally or intentionally exploits a vulnerability to damage, destroy or obtain an asset.
- A *vulnerability* is a weakness in networks, hardware, software or processes which a threat actor exploits to damage, destroy or obtain an asset.

Risk types can be categorised as:

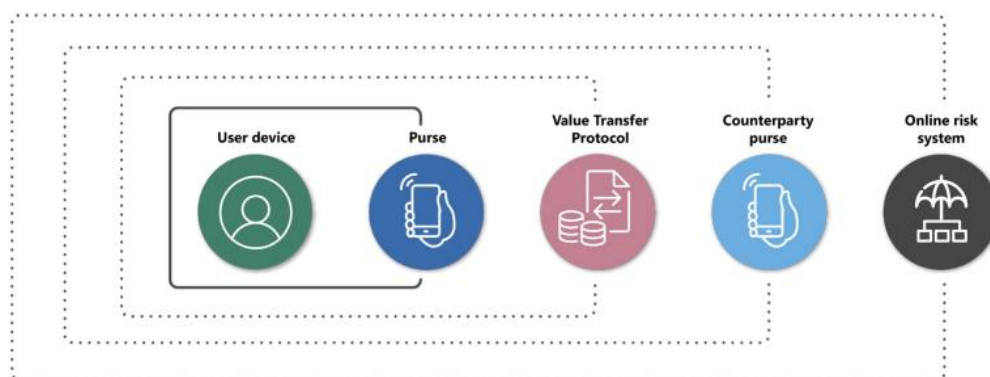
- *Technology risks* – the risk that any technology failure will disrupt an entity’s business or operations.
- *Operational risks* – the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
- *Reputational risks* – the risk of reputational damage to an entity when it fails to meet the expectations of its stakeholders and this is negatively perceived.

Risks can belong to one or more of the categories above. Each would need to be carefully assessed and mitigated through either technical or non-technical risk management measures or a combination of both, with some element of residual risk that would have to be deemed acceptable to the organisation.

There are surprises in the paper too: “There may be other kinds of risk in connection with offline payments, for example *legal risks*, that are out of scope of the handbook. The degree of risk each presents may vary by country, capabilities, infrastructure and solution used.”

A simplified view of the layers of risk management components

Figure 8



Read more at number 12 below.

---

I liked this question: *What is corruption?*

According to the new “Joint Communication to the European Parliament, the Council, and the European Economic and Social Committee on the fight against corruption”, corruption is commonly referred to as *the abuse of entrusted power for private gain*.

While the nature and scope of corruption may differ from one country to another, no country can call itself corruption-free. As a global problem with major cross-border implications, it is the subject of a dedicated United Nations Convention, the United Nations Convention against Corruption (UNCAC).

The Convention is a universal anti-corruption instrument, and gives definitions of different manifestations of corruption, embracing crimes from petty bribery to major political scandals.

The Organisation for Economic Cooperation and Development (OECD) also works on measures to prevent corruption, and has established legally binding provisions to criminalise the bribery of foreign public officials in international business transactions.

What is new? The European Commission has just adopted *two* targeted proposals to strengthen EU law in this area.

First, the Commission is proposing *a directive* to update and harmonise EU rules, to ensure high standards against the full range of corruption offences.

Second, the High Representative of the Union for Foreign Affairs and Security Policy, with the Commission’s support, is proposing to complement the Common Foreign and Security Policy (CFSP) toolbox of restrictive measures (sanctions) with a dedicated *CFSP sanctions regime* to fight corruption.

I remember what Alan Greenspan has said: “Corruption, embezzlement, fraud, these are all characteristics which exist everywhere. It is regrettably the way human nature functions, whether we like it or not. What successful economies do, is keep it to a minimum. No one has ever eliminated any of that stuff.” This is very clear, and I feel uncomfortable, as Alan Greenspan has also said: “If I turn out to be particularly clear, you've probably misunderstood what I've said”

Read more at number 23 below.

---

We have some great developments in Switzerland. At its meeting on 24 May, the Swiss Federal Council appointed Mr. Florian Schütz, currently the Federal Cyber Security Delegate and head of the National Cyber Security Centre (NCSC), as director of the new Federal Office for Cyber Security as of 1 January 2024.



According to the Swiss National Cyber Security Centre (NCSC), Florian Schütz, who is 41, studied at ETH Zurich and graduated with an MSc in Computer Science in 2007.

During his studies, he gained initial professional experience as a software developer and risk analyst at Siemens Schweiz AG and as an information security laboratory technician at ETH Zurich.

Between 2008 and November 2016, he worked at RUAG Schweiz AG as an IT security architect and business consultant, as head of cyber security, and as a business developer for cyber & intelligence in Israel.

During that time, he also completed a Master of Advanced Studies in Security Policy and Crisis Management.

From December 2016 to July 2019, he was head of IT Risk & Security at Zalando SE Germany. He assumed his role as Federal Cyber Security Delegate in August 2019.

In view of his qualifications and his many years of experience in IT security in the private sector and as the Federal Cyber Security Delegate, Florian Schütz is the ideal candidate for the position.

In his role as director, Florian Schütz will have the opportunity to shape and develop the new federal office within the DDPS.



The next step, this summer, will be for the DDPS to submit amendments to the ordinance regulating the NCSC's transition to a federal office within the DDPS to the Federal Council.

---

According to the Swiss National Cyber Security Centre (NCSC), phishers are constantly trying new ways to trick victims into providing their access details. In doing so, they also do not shy away from telling the victim that *intimate pictures* have supposedly been published.

### *Phishing with threat*

Never divulge personal data such as passwords or credit card details on a website that you have accessed by clicking on a link in an email or text message. This simple basic rule will already prevent many phishing attempts.

Thanks to internet users being ever more aware, many now react sensitively to classic phishing emails that threaten to block an account or offer the prospect of a refund, for example.

The attackers therefore try to catch the recipients off guard with a stream of new stories and exploit the brief moment when the victims are unsettled, do not pause to think about the plausibility of the story and therefore do not suspect anything.

A particularly perfidious case was reported to the NCSC last week. In the name of a person who was "friends" with the victim, the victim was told via a Facebook message that someone had posted nude photos of them on the internet.

In order to see the photos for themselves, they were told to click on the link provided. The page that then opened mimicked Facebook and contained numerous comments which did indeed suggest that the content contained compromising images.

These comments and the indication that the content had already been shared 947 times were intended to put the victim under pressure. However, in order to view the images, they first had to confirm their age, as it involved adult content. To do this, they had to provide their Facebook login details. In this case, of course, this information did not go to Facebook, but directly to the attackers.

The whole page was a bluff to make the victim feel insecure. After the login details had been entered, a page appeared saying that the photos had already been removed.

As mentioned above, the victim was tipped off about the page with the alleged nude photos by a Facebook acquaintance, giving the message even more credibility. The NCSC assumes that the purported sender had also been previously phished and that the contact details are being used to send more targeted phishing messages.

### *Oops! – Phishing email addressed to the wrong person*

Phishing attempts with real names are still rare. In many cases, the fraudsters use an impersonal "Hello" or "Hi customer", or use the information from the email address to display a more or less appropriate form of address.

Last week, a new variant of the well-known SBB phishing attempt appeared, luring people with an alleged ticket refund or threatening to block their Swisspass account.

In the current variant, the victim was addressed personally. At first, it had to be assumed that the fraudsters were using data from a data leak, which makes a very targeted attack possible. However, after the initial reports received by the NCSC, it quickly became clear that the same surname was always used as the form of address, regardless of the name of the recipient.

This error by the attackers is an example of how they operate. They hack into email accounts and search the inbox for useful material. Emails from companies, in this case a ticket refund from the SBB, are of course of interest to the fraudsters and are subsequently customised and a phishing link is added. In this way, the fraudsters do not have to worry about the accuracy of the language.

These emails are written in perfect German, French or Italian, *except* of course for the sections that have been adapted by the fraudsters. In this case, the attackers used "Mr Hammer" everywhere and forgot to personalise it.

Advice from the National Cyber Security Centre (NCSC):

- Never divulge personal data such as passwords or credit card details on a website that you have accessed by clicking on a link in an email or text message.
- Wherever possible, use two-factor authentication. This offers an additional layer of protection to prevent your account from being hacked.
- No bank or credit card company will ever send you an email

requesting that you change your password or verify your credit card details.

- Bear in mind that email sender IDs can easily be spoofed.
- Be sceptical if you receive emails that require action from you and otherwise threaten with consequences (loss of money, criminal charges or legal proceedings, account or card blocking, missed opportunity, misfortune).

Welcome to our monthly newsletter.

Best regards,

*George Lekatis*

George Lekatis  
 General Manager, Cyber Risk GmbH  
 Dammstrasse 16, 8810 Horgen  
 Phone: +41 79 505 89 60  
 Email: [george.lekatis@cyber-risk-gmbh.com](mailto:george.lekatis@cyber-risk-gmbh.com)  
 Web: [www.cyber-risk-gmbh.com](http://www.cyber-risk-gmbh.com)

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer:  
 CHE-244.099.341

Visit our reading room at:

[https://www.cyber-risk-gmbh.com/Reading\\_Room.html](https://www.cyber-risk-gmbh.com/Reading_Room.html)

[https://www.cyber-risk-gmbh.com/Reading\\_Room.html](https://www.cyber-risk-gmbh.com/Reading_Room.html)



[ABOUT](#) [TRAINING](#) [FOR THE BOARD](#) [ASSESSMENT](#) [READING ROOM](#) [CONTACT](#) [CYBER RISK LINKS](#) [IMPRESSUM](#)

#### 1. Black Hat Asia 2023. Christina Lekati and Samuel Lolagar lead the class: "Fundamentals of Cyber Investigations and Human Intelligence" at Marina Bay Sands, Singapore.

In this class, participants learn a comprehensive methodology for gathering in-depth information on a human target, following three intelligence disciplines:

- Open-source intelligence (OSINT),
- Social media intelligence (SOCMINT), a sub-branch of OSINT,
- Human intelligence (HUMINT), and particularly, virtual HUMINT.

<https://www.blackhat.com/asia-23/training/schedule/#fundamentals-of-cyber-investigations--human-intelligence-29747>



*Number 1 (Page 17)***National Cybersecurity Centre's (NCSC), second semi-annual report**

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Federal Department of Finance FDF  
National Cyber Security Centre NCSC

*Number 2 (Page 19)***Recommendations to Achieve Greater Convergence in Cyber Incident Reporting, Final Report**

FINANCIAL  
STABILITY  
BOARD

*Number 3 (Page 24)***Supercharging security with generative AI**  
Sunil Potti, VP/GM, Google Cloud Security*Number 4 (Page 26)***Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI***Number 5 (Page 28)***Active Cyber Defence (ACD) program - The Sixth Year**  
Key findings from the 6th year of the ACD program

National Cyber  
Security Centre

*Number 6 (Page 30)***If you have people, you have an Insider Risk:  
A David Smith case study**

National Protective  
Security Authority

*Number 7 (Page 34)***Proposal for a Regulation**

laying down Union procedures for the authorisation and supervision of **medicinal** products for human use and establishing rules governing the European Medicines Agency.

*Number 8 (Page 36)***Proposal for a Directive,**

on the Union code relating to **medicinal** products for human use,

*Number 9 (Page 38)*

**EBA identifies fraud in retail payments and over indebtedness as key issues affecting consumers**

*Number 10 (Page 40)***2023 State of Homeland Security Remarks: Tackling an Evolving Threat Landscape – Homeland Security in 2023**

Secretary Mayorkas delivered the State of Homeland Security address at the Council on Foreign Relations

*Number 11 (Page 48)***Awareness campaigns**



*Number 12 (Page 50)*

Project Polaris: secure and resilient CBDC systems, offline and online



*Number 13 (Page 55)*

European Court of Justice (CJEU), requirements under which data subjects affected by a breach of the GDPR can claim for compensation of non-material damages under Art. 82 GDPR



*Number 14 (Page 59)*

Responsible Cyber Power in Practice



*Number 15 (Page 61)*

Meta's Q1 2023 Security Reports: Protecting People and Businesses

Guy Rosen, Chief Information Security Officer



*Number 16 (Page 65)*

Quarterly Adversarial Threat Report



*Number 17 (Page 70)*

Using math to map social connections



*Number 18 (Page 73)***Sweep Targets Darknet Markets**

**Operation SpecTor** spanned three continents, seized millions of dollars, and removed tens of thousands of potentially lethal drugs from circulation

*Number 19 (Page 75)*

The European Commission adopted the first designation decisions under the Digital Services Act (DSA).

*Number 20 (Page 78)***Developing Agile, Reliable Sensing Systems with Microbes**

DARPA's Tellus program seeks to advance remote environmental sense-and-respond platforms with enhanced breadth, resolution

*Number 21 (Page 80)*

Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service

*Number 22 (Page 85)***Hunting Russian Intelligence "Snake" Malware**

*Number 23 (Page 88)***Joint Communication to the European Parliament, the Council, and the European Economic and Social Committee on the fight against corruption**

HIGH REPRESENTATIVE  
OF THE UNION FOR  
FOREIGN AFFAIRS AND  
SECURITY POLICY

*Number 24 (Page 91)***Proposal for a Directive on combating corruption***Number 25 (Page 93)*

From CNIL, the French Data Protection Agency  
**Artificial intelligence: the action plan of the CNIL**

*Number 26 (Page 96)***Pre-Infected - Over 8.9 Million Android Phones Worldwide**

Fyodor Yarochkin, Zhengyu Dong, Paul Pajares

*Number 27 (Page 97)***Why more transparency around cyber attacks is a good thing for everyone**

Eleanor Fairford, Deputy Director of Incident Management at the NCSC, and Mihaela Jembei, Director of Regulatory Cyber at the Information Commissioner's Office (ICO).



## *Number 1*

# National Cybersecurity Centre's (NCSC), second semi-annual report



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Federal Department of Finance FDF  
National Cyber Security Centre NCSC

The National Cybersecurity Centre's (NCSC) second semi-annual report deals with the most important cyberincidents of the second half of 2022 in Switzerland and internationally. It focuses on the most important issues surrounding cybersecurity in SMEs.

Digitalisation is progressing in small and medium-sized enterprises. Numerous computers are connected to each other via network interfaces. Processes such as order processing, planning, production and logistics are increasingly interlinked and digitally managed. This increases the number of systems that are accessible from the internet and therefore need the best possible protection. However, SMEs in particular often pay too little attention to cybersecurity.

For this reason, the current semi-annual report focuses on cybersecurity in SMEs and highlights the most important aspects of protection against cyberthreats. In addition, a business and a police authority provide insight into how specific cyberincidents unfold.

### *Most frequently reported: fraud*

In the second half of 2022, the number of reports received by the NCSC remained very high at 17,341, which was practically identical to the first half of the year.

In total, the NCSC received 34,527 reports last year. Of these, 85% came from the public and the remaining 15% from businesses, associations and authorities.

The reports concerned various forms of fraud, with fake extortion emails, i.e. threatening emails in the name of prosecution authorities, accounting for almost one third of the reports. Other frequently reported forms of fraud included CEO fraud and invoice manipulation scams.

### *Unchanged amount of ransomware*

Ransomware reports remained constant and accounted for almost half of all reports in the malware category. About one third of the 76 reports concerned private individuals, two thirds involved businesses. The LockBit ransomware is often used in attacks targeting businesses.

This malware is known for the fact that not only is data encrypted, but it is also stolen and posted on the internet if the ransom is not paid. Such double extortion approaches are being observed more and more frequently.

Since many businesses have recognised the threat of ransomware and now have backups, pure encryption is no longer lucrative enough for attackers. The initial infection in ransomware incidents is often due to a vulnerability or poor configuration, as well as emails with malicious attachments and links.

### *Hacking reports continued to rise sharply*

Compared to the previous half-year period, the number of reports regarding hacking almost doubled in the second half of the year, with 276 reports.

In particular, social media accounts are a popular target for hackers, for example to blackmail users or to use the hacked accounts to distribute advertising for investment fraud.

11 May 2023 | National Cyber Security Centre NCSC



Semi-annual report 2022/II (July – December)

## Information assurance

Situation in Switzerland and internationally

The report:

<https://www.news.admin.ch/newsd/message/attachments/78230.pdf>



## *Number 2*

# Recommendations to Achieve Greater Convergence in Cyber Incident Reporting, Final Report



### *Executive summary*

Cyber incidents are rapidly growing in frequency and sophistication. At the same time, the cyber threat landscape is expanding amid digital transformation, increased dependencies on third party service providers and geopolitical tensions.

The interconnectedness of the global financial system makes it possible that a cyber incident at one financial institution (FI) (or an incident at one of its third-party service providers) could have spill-over effects across borders and sectors.

Recognising that timely and accurate information on cyber incidents is crucial for effective incident response and recovery and promoting financial stability, the G20 asked the FSB to deliver a report on achieving greater convergence in cyber incident reporting (CIR).

To meet this call, the FSB conducted work to promote greater convergence in CIR in three ways:

- (i) setting out recommendations to address the issues identified as impediments to achieving greater harmonisation in incident reporting;
- (ii) enhancing the Cyber Lexicon<sup>1</sup> to include additional terms related to CIR as a 'common language' is necessary for increased convergence; and
- (iii) identifying common types of information that are submitted by FIs to authorities for CIR purposes, which culminated in a concept for a common format for incident reporting exchange (FIRE) to collect incident information from FIs and use between themselves.

FIRE would be flexible to allow a range of adoption choices and include the most relevant data elements for financial authorities.

Drawing from the FSB's body of work on cyber, including engagement with external stakeholders, this report sets out recommendations that aim to promote convergence among CIR frameworks, while recognising that a one-size-fits-all approach is not feasible or preferable.

Financial authorities and FIs can choose to adopt these recommendations as appropriate and relevant, consistent with their legal and regulatory framework.

## Table of Contents

Executive summary .....	1
1. Introduction .....	3
2. Practical issues and challenges to achieving greater convergence in CIR .....	3
2.1. Operational challenges .....	4
2.2. Setting reporting criteria .....	8
2.3. Culture of timely reporting .....	8
2.4. Early assessment challenges .....	10
2.5. Secure communications .....	10
2.6. Cross-border and cross-sectoral issues .....	11
3. Recommendations .....	11
3.1. Design of approach to CIR .....	11
3.2. Supervisory activities and collaboration between authorities .....	18
3.3. Industry engagement .....	20
3.4. Capability development (individual and shared) .....	21
Annex A: 2022 Survey findings .....	24
Annex B: Recommendations mapped to identified issues and challenges .....	32
Annex C: Initial reporting trigger reference material .....	33

### *Recommendations:*

**1. Establish and maintain objectives for CIR.** Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

**2. Explore greater convergence of CIR frameworks.** Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability.

**3. Adopt common data requirements and reporting formats.** Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.

**4. Implement phased and incremental reporting requirements.** Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of

bringing the incident under control.

- 5. Select appropriate incident reporting triggers.** Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.
- 6. Calibrate initial reporting windows.** Financial authorities should consider potential outcomes associated with window design or calibration used for initial reporting.
- 7. Provide sufficient details to minimise interpretation risk.** Financial authorities should promote consistent understanding and minimise interpretation risk by providing an appropriate level of detail in setting reporting thresholds, using common terminologies and supplementing CIR guidance with examples.
- 8. Promote timely reporting under materiality-based triggers.** Financial authorities that use materiality thresholds should consider finetuning threshold language, or explore other suitable approaches, to encourage prompt reporting by FIs for material incidents.
- 9. Review the effectiveness of CIR and cyber incident response and recovery (CIRR) processes.** Financial authorities should explore ways to review the effectiveness of FIs' CIR and CIRR processes and procedures as part of their existing supervisory or regulatory engagement.
- 10. Conduct ad-hoc data collection.** Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.
- 11. Address impediments to cross-border information sharing.** Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.
- 12. Foster mutual understanding of benefits of reporting.** Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.
- 13. Provide guidance on effective CIR communication.** Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

**14. Maintain response capabilities which support CIR.** FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

**15. Pool knowledge to identify related cyber events and cyber incidents.** Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defence of the financial sector.

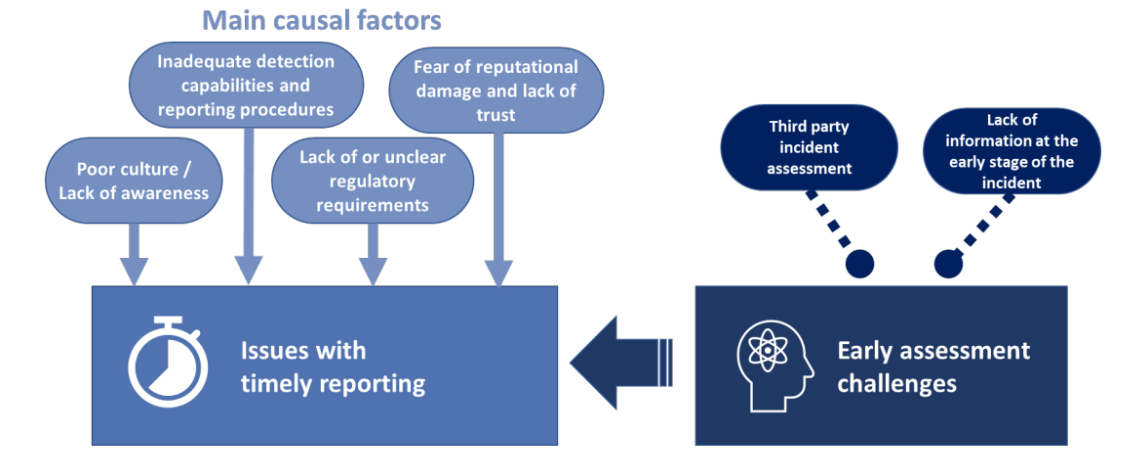
**16. Protect sensitive information.** Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.



## Recommendations to Achieve Greater Convergence in Cyber Incident Reporting

Final Report



**Possible causal factors to issues with timely reporting****Figure 3**

The report: <https://www.fsb.org/wp-content/uploads/P130423-1.pdf>



## *Number 3*

### Supercharging security with generative AI

Sunil Potti, VP/GM, Google Cloud Security



At Google Cloud, we continue to invest in key technologies to progress towards our true north star on invisible security: making strong security pervasive and simple for everyone.

Our investments are based on insights from our world-class threat intelligence teams and experience helping customers respond to the most sophisticated cyberattacks.

Customers can tap into these capabilities to gain perspective and visibility on the most dangerous threat actors that no one else has.

Recent advances in artificial intelligence (AI), particularly large language models (LLMs), accelerate our ability to help the people who are responsible for keeping their organizations safe.

These new models not only give people a more natural and creative way to understand and manage security, they give people access to AI-powered expertise to go beyond what they could do alone.

At the RSA Conference 2023, we are excited to announce Google Cloud Security AI Workbench, an industry-first extensible platform powered by a specialized, security LLM, Sec-PaLM.

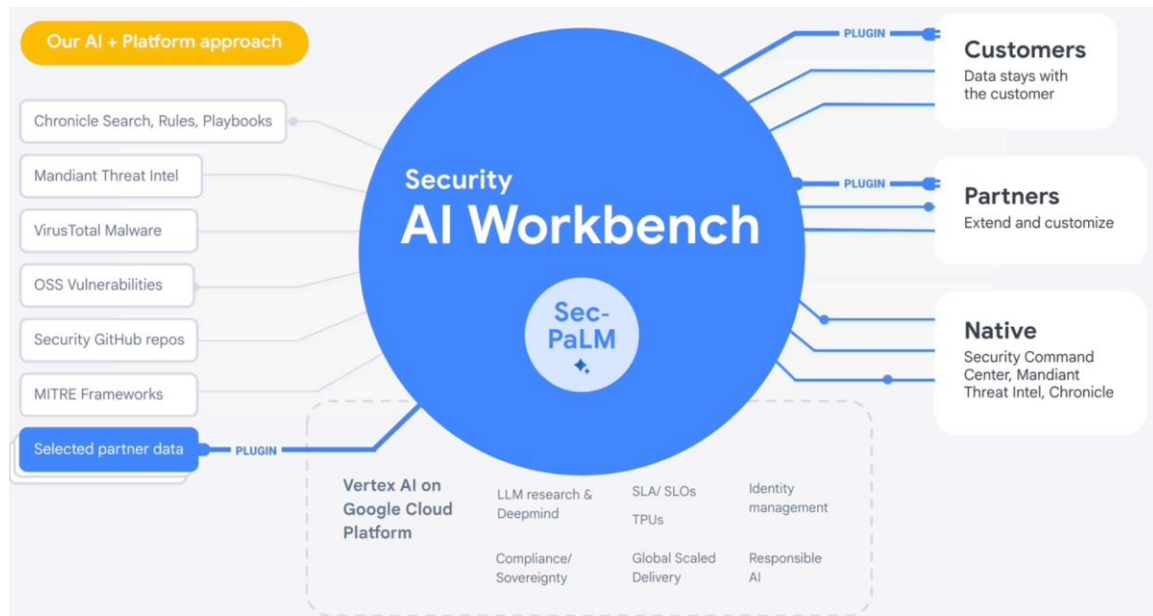
This new security model is fine-tuned for security use cases, incorporating our unsurpassed security intelligence such as Google's visibility into the threat landscape and Mandiant's frontline intelligence on vulnerabilities, malware, threat indicators, and behavioral threat actor profiles.

Google Cloud Security AI Workbench powers new offerings that can now uniquely address three top security challenges: threat overload, toilsome tools, and the talent gap.

It will also feature partner plug-in integrations to bring threat intelligence, workflow, and other critical security functionality to customers, with Accenture being the first partner to utilize Security AI Workbench.

The platform will also let customers make their private data available to the platform at inference time; ensuring we honor all our data privacy commitments to customers.

Because Security AI Workbench is built on Google Cloud's Vertex AI infrastructure, customers control their data with enterprise-grade capabilities such as data isolation, data protection, sovereignty, and compliance support.



To read more: <https://cloud.google.com/blog/products/identity-security/rsa-google-cloud-security-ai-workbench-generative-ai>

## *Number 4*

### Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI



Today the odds remain stacked against cybersecurity professionals. Too often, they fight an asymmetric battle against prolific, relentless and sophisticated attackers.

To protect their organizations, defenders must respond to threats that are often hidden among noise.

Compounding this challenge is a global shortage of skilled security professionals, leading to an estimated 3.4 million openings in the field.

The volume and velocity of attacks requires us to continually create new technologies that can tip the scales in favor of defenders.

Security professionals are scarce, and we must empower them to disrupt attackers' traditional advantages and drive innovation for their organizations.

In the last few months, the world has witnessed a wave of innovation as organizations apply advanced AI to new technologies and use cases.

We are ready for a paradigm shift and taking a massive leap forward by combining Microsoft's leading security technologies with the latest advancements in AI.

#### *Security Copilot — end-to-end defense at machine speed and scale*

Microsoft Security Copilot is the first security product to enable defenders to move at the speed and scale of AI. Security Copilot combines this advanced large language model (LLM) with a security-specific model from Microsoft.

This security-specific model in turn incorporates a growing set of security-specific skills and is informed by Microsoft's unique global threat intelligence and more than 65 trillion daily signals.

Security Copilot also delivers an enterprise-grade security and privacy-compliant experience as it runs on Azure's hyperscale infrastructure. When Security Copilot receives a prompt from a security professional, it uses the full power of the security-specific model to deploy skills and

queries that maximize the value of the latest large language model capabilities. And this is unique to a security use-case.

Our cyber-trained model adds a learning system to create and tune new skills. Security Copilot then can help catch what other approaches might miss and augment an analyst's work. In a typical incident, this boost translates into gains in the quality of detection, speed of response and ability to strengthen security posture. Security Copilot doesn't always get everything right. AI-generated content can contain mistakes.

But Security Copilot is a closed-loop learning system, which means it's continually learning from users and giving them the opportunity to give explicit feedback with the feedback feature that is built directly into the tool.

As we continue to learn from these interactions, we are adjusting its responses to create more coherent, relevant and useful answers.

Security Copilot also integrates with the end-to-end Microsoft Security products, and over time it will expand to a growing ecosystem of third-party products. So, in short, Security Copilot is not only a large language model, but rather a system that learns, to enable organizations to truly defend at machine speed.

We absolutely believe that security is a team sport, and security should be built with privacy at the core. We've built Security Copilot with security teams in mind— your data is always your data and stays within your control.

It is not used to train the foundation AI models, and in fact, it is protected by the most comprehensive enterprise compliance and security controls. While remaining private, each user interaction can be easily shared with other team members to accelerate incident response, collaborate more effectively on complex problems and develop collective skills.

To read more: <https://news.microsoft.com/ai-security-2023/>

## *Number 5*

### Active Cyber Defence (ACD) program - The Sixth Year

Key findings from the 6th year of the ACD program



The aim of Active Cyber Defence (ACD) is to “Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time.”

It was launched in 2017 and continues to protect the UK, in a relatively automated way, from a significant proportion of commodity cyber attacks.



## **Active Cyber Defence**

### **The 6th Year: Summary of Key Findings**

#### *Web shells*

Web shells are created by attackers using malicious scripts to install control panels on compromised servers.

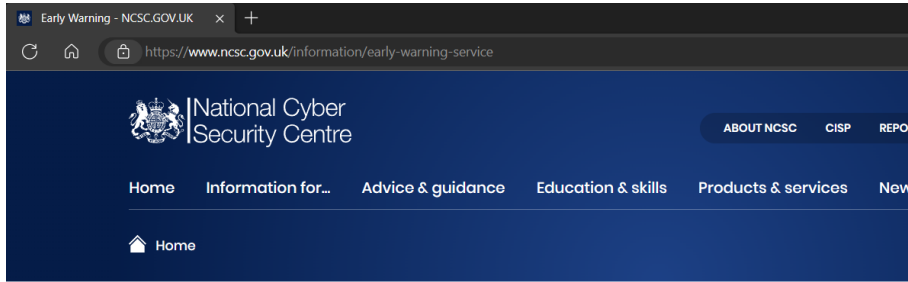
These servers can then be used as a launch pad for malicious activity such as hosting phishing sites. The number of web shells we have discovered and acted against increased in 2022 by around 15%.

The most prevalent hosting providers of web shells were Newfold Digital, Cloudflare and GoDaddy.



## Early Warning

[www.ncsc.gov.uk/information/early-warning-service](https://www.ncsc.gov.uk/information/early-warning-service)



### INFORMATION

## Early Warning

Early Warning helps organisations investigate cyber attacks on their network by notifying them of malicious activity that has been detected in information feeds.

Early Warning is a free NCSC service designed to automatically inform an organisation of potential cyber attacks on their network, as soon as possible.

The service uses a variety of information feeds from the NCSC, and trusted public, commercial and closed sources (which [includes several privileged feeds which are not available elsewhere](#)).

Early Warning filters millions of events that the NCSC receives every day and - using the IP and domain names provided by our users - correlates those which are relevant to their organisation into daily notifications for their nominated contacts.

### Contents

<b>What is Active Cyber Defence?</b> .....	<b>3</b>
<b>Takedown Service</b> .....	<b>4</b>
<b>Suspicious Email Reporting Service (SERS)</b> .....	<b>7</b>
<b>Mail Check</b> .....	<b>8</b>
<b>Vulnerability Checking</b> .....	<b>9</b>
<b>Protective Domain Name Service (PDNS)</b> .....	<b>10</b>
<b>Exercise in a Box</b> .....	<b>11</b>
<b>Early Warning</b> .....	<b>12</b>

To read more: <https://www.ncsc.gov.uk/section/active-cyber-defence/introduction>

<https://www.ncsc.gov.uk/files/acd6-summary.pdf>

## Number 6

### If you have people, you have an Insider Risk: A David Smith case study



National Protective  
Security Authority

You probably will have heard in the media about the recent case of David Smith, a former Security Guard at the British Embassy in Berlin, sentenced to over 13 years in prison for spying on behalf of a foreign intelligence agency. In this blog we will discuss how Smith was able to conduct insider activity on behalf of Russian State Actors and outline key actions that your business can take to reduce insider risk.

The facts of Smith's insider activity are outlined in Figure 1. However, the timeline in isolation only provides part of the story. As is often the case, there were numerous moving parts that collided to culminate in a significant, damaging insider act.

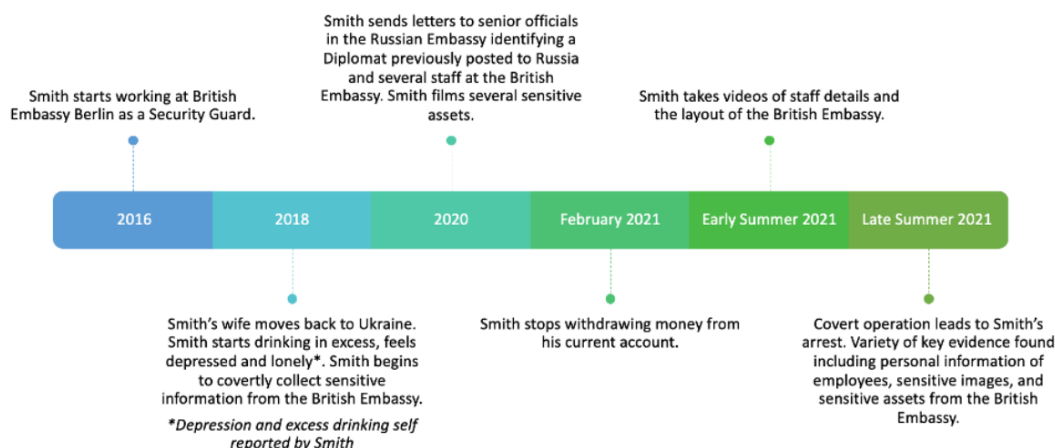


Figure 1: Timeline of Smith's Insider Activity

### Life Before

Smith worked in various roles in the military and aviation sector prior to his role as a Security Guard at the British Embassy in Berlin in 2016.

Smith's move to Germany circa 2002 was reported to have been prompted by financial struggles, but finance does not appear to be the primary motivation for his act, although did later feature as a secondary motivation.

### The Build Up to Becoming a Spy

Smith experienced significant stressors in his life in the period leading up to, and during, 2018. His Ukrainian wife moved back to her country of birth, which may have contributed to his self-reported depression and excessive drinking. Previous research into insider risk by NPSA (formerly CPNI) shows these to be issues of concern when they have an impact in the workplace.

### *The Perfect Storm*

Motivations are often complex and intertwined, and indeed, this appears to be the case here. We cannot say for certain when Smith's hostility towards the UK began but it was referenced in the Judge's sentencing remarks as a motivating factor.

His self-reported depression and excessive drinking may have been exacerbated by the COVID-19 pandemic, when Smith was not only living alone but also working at the Embassy when onsite staff numbers were greatly reduced.

Smith declared interest in conspiracy theories, his sympathies towards the Russian State and his feelings of ill will towards his employers and the British Government, all of which are also concerning factors.

The culmination of these factors, according to the Judge's sentencing remarks, influenced Smith's decision to progress down the pathway of undertaking an insider act.

Motivations are, in part, influenced by the difficulty of the task – the more difficult something is, the greater the motivation required to act.

So, the responses to the pandemic meant that Smith could access sensitive materials with much greater ease, due to fewer Embassy employees being onsite and significant changes to his operating environment.

If we view motivational factors alone, we fail to see the whole picture. But, by viewing motivations alongside the contextual factors, we can begin to understand how Smith's behaviour manifested and concluded in an insider act.

Smith also appears to have been paid by Russian State Actors for his actions. In cases of espionage, financial motivation is often not an initial factor, but it can become a significant motivator to continue to act.

This is because, while the individual might not initially need money, they become accustomed to the additional income and those benefits, and this

can motivate them to continue to act after the initial motivational factors (such as disgruntlement or ideology) have waned.

If Smith was indeed receiving enough money to sustain his daily living costs, this may have made it more difficult for Smith to stop his actions had his disgruntlement reduced.

A key element of this case study is that Smith had some legitimate access, albeit low level. Crucially, he exploited this low-level clearance to obtain sensitive information that he had no justifiable reason to access and caused significant damage by sharing this information with Russian State Actors.

Smith's actions highlight that insider risk does not only apply to vetted personnel. Individuals with low level clearance, who identify methods to exploit this access, can also cause harm. This case highlights that those with perceived low level access can also be of interest to State Actors.

### *The Consequences*

Smith is currently serving 13 years 2 months in prison after being convicted of spying for Russian State Actors. Although we cannot go into detail about the extent of the damage caused by Smith, it was certainly significant.

Though the exact financial impact cannot be determined, the British Embassy in Berlin spent in excess of £800,000 updating their security protocols.

The Judge's sentencing remarks also highlighted the impact his actions could have had on our relationships with our allies.

Finally, and critically, Smith put his ex-colleagues at risk by sharing their identities, including names, dates of birth and home addresses, with Russian State Actors. His actions caused irreversible hurt and damaged trust across the Embassy community.

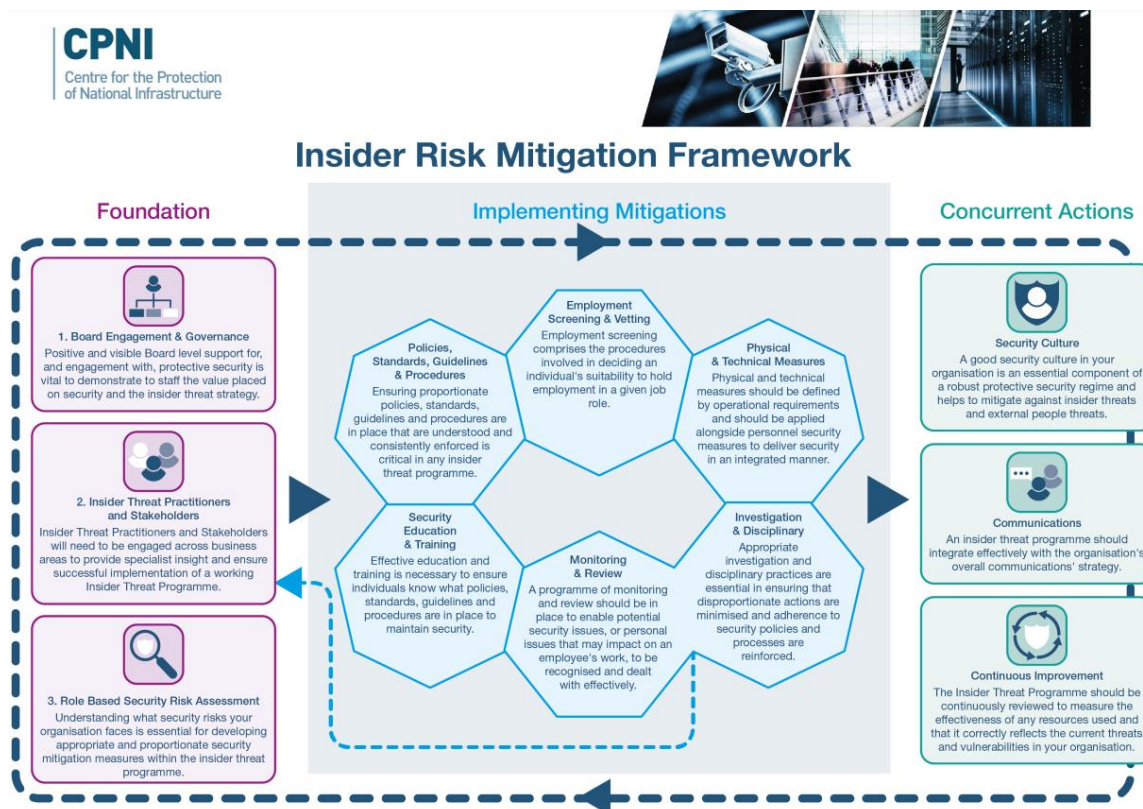
### *Lesson Learnt*

As well as being a fascinating example of modern-day espionage, there are some clear messages for any organisation to consider when assessing and seeking to reduce insider risk across your business.

1. If you have people, you have insider risk.
2. Insider Risk Mitigation needs to be an ongoing programme for it to be effective. Your programme must start with well understood Leadership and Governance structures which feed into your

organisation's wider protective security risk management. You may visit: <https://www.npsa.gov.uk/leadership-and-governance>

3. Your business must have in place effective welfare mechanisms enabling staff to share and address issues before they escalate; this may include access to professional support channels for changes in life circumstances or regular communications through periods of significant disruption to help reduce the risk of potential staff disaffection. You may visit: <https://www.npsa.gov.uk/security-campaigns/its-ok-say>
4. Consider how your business prepares for insider acts. Are you prepared to deal with such an incident occurring?
5. NPSA provide a range of information and guidance on assessing and mitigating insider risk. See the NPSA Insider Risk Mitigation Framework for more information. You may visit: <https://www.npsa.gov.uk/insider-risks/insider-risk-mitigation-framework>



To read more: <https://www.npsa.gov.uk/blog/personnel-security/if-you-have-people-you-have-insider-risk-david-smith-case-study-0>

*Number 7***Proposal for a Regulation,**

laying down Union procedures for the authorisation and supervision of **medicinal** products for human use and establishing rules governing the European Medicines Agency.

*Reasons for and objectives of the proposal*

EU pharmaceutical legislation has enabled the authorisation of safe, efficacious and high-quality medicinal products. However, patient access to medicinal products across the EU and security of supply are growing concerns, mirrored by recent Council conclusions and resolutions of the European Parliament. (Note: European Parliament resolution of 2 March 2017 on EU options for improving access to medicine (2016/2057(INI)), European Parliament resolution of 17 September 2020 on the shortage of medicines (2020/2071(INI)).

There is also a **growing problem** of shortages of medicinal products for many EU/EEA countries. Consequences of such shortages include decreased quality of treatment received by patients and increased burden on health systems and on healthcare professionals, who need to identify and provide alternative treatments.

While the pharmaceutical legislation creates regulatory incentives for innovation and regulatory tools to support timely authorisation of innovative and promising therapies, these products do not always reach the patient, and patients in the EU have differing levels of access.

Moreover, innovation is not always focused on unmet medical needs, and there are market failures, especially in the development of priority antimicrobials that can help address antimicrobial resistance.

Scientific and technological developments and digitalisation are not fully exploited, while the environmental impact of medicinal products needs attention. In addition, the authorisation system could be simplified to keep up with global regulatory competition.

The pharmaceutical strategy for Europe is a holistic answer to the current challenges of the pharmaceutical policy with legislative and non-legislative actions interacting together to achieve its overall goal of ensuring EU's supply of safe and affordable medicinal products and supporting the EU pharmaceutical industry's innovation efforts.



Reviewing the pharmaceutical legislation is key to achieving these objectives. However, innovation, access and affordability are also influenced by factors outside the scope of this legislation, such as global research and innovation activities or national pricing and reimbursement decisions.

Hence, not all problems can be addressed by the revision of the legislation alone. Despite this, EU pharmaceutical legislation can be an enabling and connecting factor for innovation, access, affordability and environmental protection.

The proposed revision of the EU pharmaceutical legislation builds on the high level of public health protection and harmonisation already achieved for the authorisation of medicinal products. The overarching aim of the reform is to ensure that patients across the EU have timely and equitable access to medicines.

Another objective of the proposal is to enhance security of supply and address shortages through specific measures, including stronger obligations on marketing authorisation holders to notify potential or actual shortages and marketing withdrawals, cessations and suspensions in advance of a foreseen interruption to continued supply of a medicinal product to the market.

To support the sector's global competitiveness and innovative power, right balance needs to be struck between giving incentives for innovation, with more focus on unmet medical needs, and measures on access and affordability. The framework needs to be simplified, adapted to scientific and technological changes, and contribute to reducing the environmental impact of medicinal products.

This proposed reform is comprehensive but targeted and focuses on provisions relevant to achieving its specific objectives; therefore it covers all provisions apart from those concerning advertising, falsified medicinal products, and homeopathic and traditional herbal medicinal products.

To read more: [https://health.ec.europa.eu/system/files/2023-04/com\\_2023\\_193\\_1\\_act\\_en.pdf](https://health.ec.europa.eu/system/files/2023-04/com_2023_193_1_act_en.pdf)

## *Number 8*

**Proposal for a Directive,**  
on the Union code relating to **medicinal** products for human use,



The Union general pharmaceutical legislation was established in 1965 with the dual objective of safeguarding public health and harmonising the internal market for medicines.

It has developed considerably since then, but these overarching objectives have guided all revisions. The legislation governs the granting of marketing authorisations for all medicines for human use by defining conditions and procedures to enter and remain on the market.

A fundamental principle is that a marketing authorisation is granted only to medicines with a positive benefit-risk balance after assessment of their quality, safety and efficacy.

The most recent comprehensive revision took place between 2001 and 2004 while targeted revisions on post-authorisation monitoring (pharmacovigilance) and on falsified medicines were adopted subsequently.

In the almost 20 years since the last comprehensive revision, the pharmaceutical sector has changed and has become more globalised, both in terms of development and manufacture.

Moreover, science and technology have evolved at a rapid pace. However, there continues to be unmet medical needs, i.e. diseases without or only with suboptimal treatments.

Moreover, some patients may not benefit from innovation because medicines may be unaffordable or not placed on the market in the Member State concerned.

There is also a greater awareness of the environmental impact of medicines. More recently, the COVID-19 pandemic has stress tested the framework.

This revision is part of the implementation of the **Pharmaceutical strategy** for Europe and aims to promote innovation, in particular for unmet medical needs, while reducing regulatory burden and the environmental impact of medicines; ensure access to innovative and established medicines for patients, with special attention to enhancing security of

supply and addressing risks of shortages, taking into account the challenges of the smaller markets of the Union; and create a balanced and competitive system that keeps medicines affordable for health systems while rewarding innovation.

This revision focuses on provisions relevant to achieve its specific objectives; therefore it covers all but provisions concerning falsified medicines, homeopathic and traditional herbal medicines.

Nevertheless, for the sake of clarity, it is necessary to replace Directive 2001/83/EC of the European Parliament and of the Council with a new Directive.

The provisions on falsified medicines, homeopathic medicines and traditional herbal medicines are therefore maintained in this Directive without changing their substance compared to previous harmonisations. However, in view of the changes in the governance of the Agency, the Herbal Committee is replaced by a working group.

The essential aim of any rules governing the authorisation, manufacturing, supervision, distribution and use of medicinal products must be to safeguard public health. Such rules should also ensure the free movement of medicinal products and the elimination of obstacles to trade in medicinal products to all patients in the Union.

The regulatory framework for medicinal products use should also take into account the needs of the undertakings in the pharmaceutical sector and trade in medicinal products within the Union, without jeopardising the quality, safety and efficacy of medicinal products.

To read more: [https://health.ec.europa.eu/system/files/2023-04/com\\_2023\\_192\\_1\\_act\\_en.pdf](https://health.ec.europa.eu/system/files/2023-04/com_2023_192_1_act_en.pdf)

*Number 9***EBA identifies fraud in retail payments and over indebtedness as key issues affecting consumers**

The European Banking Authority (EBA) published the 8th edition of its Consumer Trends Report for 2022/23, which summarises trends observed for the products and services under the EBA’s consumer protection mandate.

The Report has also identified two issues facing consumers in the EU: fraud in retail payments and over-indebtedness and arrears. These issues will shape the EBA’s consumer protection priorities over the next two years.

<b><u>Figures</u></b>	<b><u>2</u></b>
<b><u>Tables</u></b>	<b><u>3</u></b>
<b><u>Box</u></b>	<b><u>4</u></b>
<b><u>Abbreviations</u></b>	<b><u>5</u></b>
<b><u>Executive Summary</u></b>	<b><u>6</u></b>
<b><u>Background</u></b>	<b><u>9</u></b>
<b><u>Chapter 1: Retail banking products and services</u></b>	<b><u>11</u></b>
Residential mortgages	11
Consumer credit	17
Payment services	22
Electronic money	27
Payment accounts	28
Deposits	31
<b><u>Chapter 2: Topical issues</u></b>	<b><u>35</u></b>
Fraud in retail payments	35
Over-indebtedness and arrears	42
<b><u>Chapter 3: Measures adopted by the EBA and NCAs to address the topical issues identified in the CTR 2020/21</u></b>	<b><u>49</u></b>
Topical issues in the CTR 2020/21	49
EBA’s measures to address the topical issues	50
Regulatory and supervisory measures adopted by NCAs to address the topical issues identified in the previous CTR 2020/21	55
<b><u>List of References</u></b>	<b><u>59</u></b>

The Report presents quantitative data for the retail banking products which covers mortgage credit, consumer credit, payment accounts, payment services, electronic money and deposits.

The Report observes that mortgage credit was affected by rising inflation and the normalisation of interest rates, while credit products were impacted by poor creditworthiness assessments and the rise of new and unregulated credit products.

All these issues have been identified as key drivers for consumers' repayment difficulties and, ultimately, over-indebtedness.

Fraud in retail payments, mainly perpetrated by new and different techniques implemented by fraudsters, was the other identified issue as experienced by consumers, based, inter alia, on fraud data collected from the year 2021 when financial institutions in several EU Member States had not complied yet with the requirements sets out in Payment Services Directive (PSD2) and the EBA's technical standards on strong customer authentication.

The Report is based on information provided by the national authorities of the 27 EU Member States, national and EU consumer associations, the members of the 'Financial Dispute Resolution Network', and EU industry associations, and quantitative data from a variety of different sources.

The report:

[https://www.eba.europa.eu/sites/default/documents/files/document\\_library/Publications/Reports/2023/1054879/Consumer%20Trends%20Report%202022-2023.pdf](https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1054879/Consumer%20Trends%20Report%202022-2023.pdf)

*Number 10*

## 2023 State of Homeland Security Remarks: Tackling an Evolving Threat Landscape – Homeland Security in 2023

Secretary Mayorkas delivered the State of Homeland Security address at the Council on Foreign Relations



Good morning, everybody. Margaret, thank you for the introduction and for the discussion we are going to have in just a few minutes. My thanks to the Council on Foreign Relations for hosting us and thanks to all of you for being here. I would like to recognize two individuals, if I may, who have special meaning to our department. Our second Secretary of Homeland Security, Michael Chertoff. And former United States Congresswoman Jane Harman.

Reflecting on the state of our homeland security in 2023, it seemed fitting to pose a fundamental question to a generative AI model: “in one sentence, describe how the homeland security threat environment has evolved over the past 20 years.”

We are, after all, confronting a dramatically changed environment compared to the one we faced in March 2003. One that could change even more dramatically, as AI grips our imaginations and accelerates into our lives in uncharted and basically unmanaged fashion.

Deeply fascinated by generative AI’s promise of new advances and discoveries, greatly concerned for its capacity for error and its impact on our humanity, and keenly alert to its potential for harm in the hands of an adversary, I waited only seconds for the AI model’s answer:

“The homeland security threat environment has evolved from a primarily focused counterterrorism posture to a complex and diverse landscape of challenges that include cyberattacks, domestic extremism, and the COVID-19 pandemic, among others.”

A straightforward answer to an important question that addresses the evolved threat landscape that our Department of Homeland Security must now confront. Its evolution is about to accelerate.

Only about six months ago, engaging with an AI chatbot was reserved for a few in Silicon Valley and universities. Today about 100 million users per month are asking an AI chatbot just about anything, from recipe recommendations to requests for scientific analyses.

The exponential growth of internet technology and the change it has driven has been extraordinary. As we reflect on the state of our homeland security today, that explosive growth compels the question: what will this growth mean for our safety and security over the next 20 years?

We stand at the outset of what President Biden has aptly described as a “decisive decade” for our world. It is the same for our homeland security. Revolutionizing technological innovations, growing political and economic instability, widening wealth inequality, a rapidly changing climate, increasingly aggressive nation states, emerging infectious diseases, and other forces are transforming the global landscape, challenging and sometimes rendering moot a nation’s borders, and bringing national and international threats to any community’s doorstep.

Our Department was founded to protect us in the wake of the tragedy and devastation inflicted by the terrorist attacks of 9/11, bringing together 22 agencies from across the Federal Government charged with the mission of securing our homeland.

Back then, our country was focused on the threat of foreign terrorists who sought to enter the United States and do us harm. Over the next ten years emerged the threat of the homegrown violent extremist, the individual already resident here who was radicalized to violence by a foreign terrorist ideology.

While those threats certainly persist, today lone offenders and small cells of individuals motivated by a wide range of grievances and violent extremist ideologies – from white supremacy and anti-Semitism to anti-government attitudes – pose the most persistent and lethal terrorism-related threat in the United States.

The effects of climate change have intensified. Wildfire season is no longer confined to the summer months but is now year-round. Tornadoes and named hurricanes in the United States are more frequent and more destructive.

Just a few weeks ago in Mississippi, I surveyed the devastation wrought by a tornado that, in 20 seconds and at speeds up to 200 miles per hour, ripped through a small town, destroying multiple communities and taking the lives of more than 20 people.



Not for a century have we confronted the calamity of an infectious disease as we have over the past three years. COVID-19 took more than one million lives here in the United States, impacted every aspect of our daily life, and forced on us a new understanding of the threat pandemic diseases can pose as they spread through paths of international trade and travel.

Globally, the impacts of disasters coupled with the rise of authoritarianism, corruption, conflict, violence, and persecution have resulted in an historic displacement and migration of people around the world and a consequent strain on immigration systems ill-equipped to address it.

According to the United Nations High Commissioner for Refugees, at the end of 2021, 89.3 million people worldwide had fled their homes due to conflict, violence, fear of persecution and human rights violations. This is the most since World War II and more than double the number of people who remained forcibly displaced a decade ago.

Criminal organizations have capitalized on this surge. The reach and growing ruthlessness of smuggling organizations have changed how people migrate. Drug trafficking organizations have grown in sophistication and power, creating new means of manufacturing and selling death and destruction.

From late 1989 through early 2001, I prosecuted federal drug trafficking crimes, from the trafficking of cocaine to methamphetamine to black tar heroin and more. Nothing I saw then matches the scourge of fentanyl that we have confronted for over the past five years. 46,802 overdose deaths in 2018; 57,834 in 2020, and 71,238 in 2021.

Over that same time, those seeking to exploit the most vulnerable have taken their depravity to an unimaginable level. The National Center for Missing and Exploited Children, the nation's clearinghouse for child sexual abuse material, received over 32 million cyber tips in 2022, corresponding to more than 88 million images and videos of child sexual abuse, a roughly 75 percent increase in the last five years.

88 million images and videos of child sexual abuse.

As threats of the past have changed in form, complexity, and magnitude, so too have new threats emerged. This is perhaps nowhere more acute than in cyberspace.

Some estimate that roughly 14.4 billion devices are connected as part of the Internet of Things, everything from our home thermostats and doorbells to our electric grid and fuel pipelines. This has brought significant advances

in capabilities and conveniences, but it also has exponentially increased the ways our interconnected, digital world can be exploited to do us harm.

Today, malicious cyber actors are capable of disrupting gasoline supplies across an entire region of the country, preventing hospitals from delivering critical care, and causing disruption in some of the school systems around our country.

Nation states like the People's Republic of China and Russia upend our rules-based international order and threaten our security at home, whether through cyberattacks, abuse of our trade and travel systems, or through disinformation campaigns that seek to undermine our democratic institutions. Our homeland security has converged with our broader national security.

The profound evolution in the homeland security threat environment, changing at a pace faster than ever before, has required our Department of Homeland Security to evolve along with it.

We have built new institutions, modernized our approach and processes, developed new capabilities, and are harnessing innovation as we deliver critical services that are more in demand than ever before.

Our overarching strategy is one of partnership. Homeland security cannot be accomplished by government alone; it requires collective action.

To meet the threat of domestic violent extremism, we created the Center for Prevention Programs and Partnerships to share with local communities the best practice models of identification and intervention when an individual is exhibiting signs of moving towards violence.

Through our grant programs we are helping communities build threat prevention capabilities where previously they did not exist, responding to the reality that major metropolitan areas are no longer our adversaries' only targets.

Across the Federal Government, we are working with communities impacted by unprecedented extreme weather events to strengthen their long-term recovery.

We have developed for the first time Department-wide incident management teams to lead all-of-government responses to emergent challenges, from vaccinating millions of Americans against COVID-19 and resettling Afghan nationals in Operation Allies Welcome, to providing protection for fleeing Ukrainians in Uniting for Ukraine.

We are coordinating and sharing intelligence with our partner nations and executing whole of government disruption and dismantlement campaigns to attack cartels.

In collaboration with diaspora communities here in the United States, we are building lawful pathways, so that migrants fleeing persecution can access safe and orderly avenues to obtain the humanitarian relief that our laws provide.

We are working collaboratively with our partners across government, at home and abroad, and with industry and academia, to manage and reduce risk to the cyber and physical infrastructure Americans rely on every day.

We are partnering across the U.S. government to protect the most vulnerable from exploitation, whether they are migrants being trafficked by unscrupulous employers or children who are being abused online.  
Exploitation of the vulnerable.

In fact, yesterday we released the Third Quadrennial Homeland Security Review, our new vision for securing the homeland, and in it we included this work of combatting crimes of exploitation – such as human trafficking, child exploitation, and labor exploitation – as a dedicated homeland security mission alongside our work countering terrorism, securing our borders, administering our immigration system, securing cyberspace and critical infrastructure, and building resilience and responding to disasters. This reflects the overriding importance of supporting victims and stopping the perpetrators of these abhorrent crimes.

But, what of the threats as they could materialize tomorrow? I want to highlight new initiatives in two key areas that cut across all the Department's missions.

The People's Republic of China poses an especially grave threat to the homeland, one that indeed does touch all of our Department's missions.

Beijing has the capability and the intent to undermine our interests at home and abroad and is leveraging every instrument of its national power to do so, from its increasingly aggressive presence in the South China Sea to the overseas police stations used to harass and intimidate dissenters.

A PRC invasion of Taiwan would have profound reverberations in the homeland, putting our civilian critical infrastructure at risk of a disruptive cyberattack. We must ensure we are poised to guard against this threat today and into the future.

I have directed a 90-day Department-wide sprint to assess how the threats posed by the PRC will evolve and how we can be best positioned to guard against future manifestations of this threat:

One critical area we will assess, for example, involves the defense of our critical infrastructure against PRC or PRC-sponsored attacks designed to disrupt or degrade provision of national critical functions, sow discord and panic, and prevent mobilization of U.S. military capabilities.

Another area of assessment will involve how we can bolster our screening and vetting to identify illicit travelers from the PRC who exploit our lawful immigration and travel systems to collect intelligence, steal intellectual property, and harass dissidents, while still we must facilitate lawful travel.

Informed by engagements with subject matter experts and our stakeholders, we will take immediate action to drive down risk, lay the foundation for ongoing public-private collaboration, and work with Congress to ensure we continue to invest in these vital capabilities.

Next, and returning to where I began, we must address the many ways in which artificial intelligence will drastically alter the threat landscape and augment the arsenal of tools we possess to succeed in the face of these threats.

Our Department will lead in the responsible use of AI to secure the homeland and in defending against the malicious use of this transformational technology. As we do this, we will ensure that our use of AI is rigorously tested to avoid bias and disparate impact, and is clearly explainable to the people we serve.

I recently asked our Homeland Security Advisory Council, co-chair Jamie Gorelick is here, to study the intersection of AI and homeland security and deliver findings that will help guide our use of it and defense against it. The rapid pace of technological change – the pivotal moment we are now in – requires that we also act today.

To that end, I am directing the creation of our Department's first Artificial Intelligence Task Force that will drive specific applications of AI to advance our critical homeland security missions. The Task Force will, for example:

Integrate AI into our efforts to enhance the integrity of our supply chains and the broader trade environment. We will seek to deploy AI to more ably screen cargo, identify the importation of goods produced with forced labor, and manage risk.

The Task Force will also, among other charged, leverage AI to counter the flow of fentanyl into the United States.

We will explore using this technology to better detect fentanyl shipments, identify and interdict the flow of precursor chemicals around the world, and target for disruption key nodes in the criminal networks.

Countering the multi-faceted threat posed by the PRC, learning from major cyber incidents, and harnessing the power of AI to advance our security will draw on the entirety of the capabilities and expertise the 260,000 personnel of DHS bring to bear every single day.

It will require continued investment in our operational cohesion, our ability to work together in ways our founders never imagined.

We must never allow ourselves to be susceptible to ‘failures of imagination,’ which, as the 9/11 Commission concluded nearly 20 years ago, held us back from connecting the dots and preparing for the destruction that was being planned on that tragic day.

We must instead look to the future and imagine the otherwise unimaginable, to ensure that whatever threats we face, our Department – our country – will be positioned to meet the moment.

It is an especially challenging imperative to fulfill at a time not only of rapid change, but also of acute political divisiveness; when issues of homeland security that traditionally were unifying no longer are so, and when our adversaries continue to exploit innovations designed to bring us closer together, like social media, to push us apart.

We must imagine a world where even more potent and lethal synthetic opioids or infectious diseases plague our communities. Where an earthquake or catastrophic storm intensifies already historic levels of migration in our hemisphere.

Where criminals 3D print weapons or modify consumer technologies like drones to evade law enforcement. Where cyber criminals are emboldened to the point of holding for ransom the critical services of an entire city.

At the Department of Homeland Security, we have the tools and talent to meet the moment today. We are taking the actions and making the investments to ensure we will continue to adapt and meet the moment into the future. We are more fit for purpose than at any time in our 20-year history.

This is a collective effort: we must all come together in the service of our homeland security. We must call upon our collective imagination, our commitment to a better future, and our fundamental love of country that binds us together, to protect our homeland.

Thank you.

To read more: <https://www.dhs.gov/news/2023/04/21/2023-state-homeland-security-remarks-tackling-evolving-threat-landscape-homeland>

## *Number 11*

### Awareness campaigns



INTERPOL's campaigns draw attention to online risks and give advice on how to stay safe.

Cybercrime affects us all: as individuals and society as a whole. On the one hand, new technologies have made many aspects of our lives easier, from social interactions to banking, shopping and more. On the other hand, our increasing reliance on the Internet has created more risks and opened new paths for criminal activity.

We run regular awareness campaigns to highlight major forms of cybercrime and provide tips on how to stay safe.



#### *#YouMayBeNext*

Cyberattacks can happen to anyone at any time. The #YouMayBeNext campaign focuses on digital extortion threats including:

- Sextortion
- Ransomware
- Distributed Denial-of-Services (DDoS)

The campaign offers practical tips to ensure that individuals and businesses are better equipped with the knowledge to safeguard their systems, networks and devices.



You may visit: <https://www.interpol.int/Crimes/Cybercrime/Awareness-campaigns>



*Number 12***Project Polaris: secure and resilient CBDC systems, offline and online**

This handbook provides a comprehensive overview of the key aspects of offline payments with CBDC and is intended to serve as a guide for central banks considering implementing offline payments capabilities.

In this handbook, an offline payment is defined as a transfer of value (CBDC) between devices that takes place without requiring connection to any ledger system.

This could be due to a system outage or in the absence of internet or telecommunications connectivity.

A survey conducted by the BIS Innovation Hub as part of the development of this handbook shows that 49% of central banks surveyed consider offline payments with retail CBDC to be vital, while another 49% deemed it to be advantageous.

Providing offline payments with CBDC is an important requirement for many central banks, but its implementation is complex and involves a number of technology, security and operational considerations that need to be planned and designed for at the earliest possible stages.

These considerations have implications on decisions related to policy, ecosystem roles and responsibilities, design, architecture, security, technology, investment, ongoing operations, change management and risk management.

The research for this handbook has found there is no one-size-fits-all solution, with each country having multiple reasons for providing offline payments with CBDC.

The types and suitability of solutions for offline payments will vary by country depending on local requirements.

This handbook provides some of the main reasons and usage scenarios for offline payments; a map and an explanation of the technology components; and a set of design criteria for risk management, privacy, inclusion and resilience.

It also provides a set of considerations that central banks can use to inform their planning, policy development, technology and business requirements, procurement activities and future operations.

This handbook is intended to help central banks to:

- understand the available technologies and security measures;
- understand the main threats, risks and risk management measures;
- understand the privacy issues, inclusion needs and resilience options;
- understand the design and architecture principles involved; and
- gain perspective on potential operational and change management issues.

Project Polaris: - Offline payments with CBDC



Project Polaris: - Offline payments with CBDC



## Contents

<b>Acronyms, abbreviations and definitions</b>	<b>7</b>
<b>1. Executive summary</b>	<b>13</b>
<b>2. Introduction</b>	<b>16</b>
<b>3. Offline payments with CBDC</b>	<b>19</b>
3.1 Reasons for offline payments with CBDC	19
3.2 Modes of offline payment	22
3.3 Key lessons from history relevant to offline payments with CBDC	26
<b>4. Offline payment solutions for CBDC</b>	<b>28</b>
4.1 Logical architecture for offline payment solutions	28
4.2 Tamper-resistant user devices	30
4.2.1 Secure element (SE)-based	31
4.2.2 Trusted execution environment (TEE)-based	32
4.2.3 Secure software-based	32
4.3 User onboarding	33
4.4 Provisioning and life cycle management	34
4.4.1 Secure provisioning processes	34
4.4.2 Cryptographic key generation processes	35
4.4.3 Lifecycle management activities	35
4.6 Offline risk management	37
4.6.1 Risk parameter management	37
4.6.2 Transaction history management	37
4.6.3 Limiting the lifetime or uses of cryptographic keys	38
4.6.4 Block list management	38
4.7 Purses	38
4.8 Value transfer protocol	39
4.9 Value-form	40
4.10 Online updates	41
4.11 Value transfer mechanism	41
4.12 Interoperability	42

4.12.1	Between different offline solutions	42
4.12.2	Between online and offline solutions	43
<b>5.</b>	<b>Risk management by design</b>	<b>45</b>
5.1	Key assumptions	46
5.2	Threats and vulnerabilities	46
5.2.1	Counterfeiting via physical breaches	46
5.2.2	Counterfeiting via cryptographic protocol analysis (cryptanalysis)	47
5.2.3	Side-channel attacks	47
5.2.4	Fault-inducing attacks	47
5.2.5	Cryptography strength, lifetime and ability to update	48
5.2.6	Master cryptographic key compromise	48
5.2.7	Third-party device compromise	48
5.3	Risks	49
5.3.1	Device obsolescence	49
5.3.2	Double-spending	49
5.3.3	Fraud	49
5.3.4	Lost value	50
5.3.5	Third-party vendors and supply chains	51
5.3.6	Lack of risk management and breach detection	52
5.3.7	Complexity of the technology stack	52
5.3.8	Insider threats	52
5.4	Risk management measures	52
5.5	Technology risk management	53
5.5.1	General criteria	54
5.5.2	Measures to mitigate the risk of counterfeiting	55
5.5.3	Measures to mitigate side-channel attacks	56
5.5.4	Measures to mitigate crypto-durability and crypto-agility risks	56
5.5.5	Measures to mitigate risks of master cryptographic key compromise	56
5.5.6	Measures to mitigate risks from third-party device compromise	57
5.5.7	Measures to mitigate risks from obsolescence	57
5.5.8	Measures to mitigate double-spending risks	58
5.5.9	Measures to mitigate fraud risks	58
5.5.10	Measures to mitigate third-party vendor and supply chain risks	60

5.5.11 Measures to mitigate lack of real-time transaction monitoring and breach detection	61
5.6 Operational risk management	63
5.7 Reputational risk management	64
<b>6. Privacy by design</b>	<b>66</b>
6.1 Privacy principles	66
6.2 Privacy considerations for offline payments with CBDC	67
<b>7. Inclusion by design</b>	<b>70</b>
7.1 Inclusion considerations	70
7.2 Supporting multiple ways to pay	73
<b>8. Resilience by design</b>	<b>75</b>
8.1 Short-term resilience	75
8.2 Ongoing resilience	75
8.3 Civil contingency resilience	76
8.4 Resilience considerations	76
8.5 Design considerations to improve resilience	77
<b>9. Conclusion</b>	<b>79</b>

To read more: <https://www.bis.org/about/bisih/topics/cbdc/polaris.htm>

<https://www.bis.org/publ/othp64.pdf>



*Number 13*

## European Court of Justice (CJEU), requirements under which data subjects affected by a breach of the GDPR can claim for compensation of non-material damages under Art. 82 GDPR



**InfoCuria**  
Case-law

### JUDGMENT OF THE COURT

Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 82(1) – Right to compensation for damage caused by data processing that infringes that regulation – Conditions governing the right to compensation – Mere infringement of that regulation not sufficient – Need for damage caused by that infringement – Compensation for non-material damage resulting from such processing – Incompatibility of a national rule making compensation for such damage subject to the exceeding of a threshold of seriousness – Rules for the determination of damages by national courts.

The dispute in the main proceedings and the questions referred for a preliminary ruling

11 From 2017, Österreichische Post, a company incorporated under Austrian law, an address broker, collected information on the political affinities of the Austrian population. Using an algorithm that takes into account various social and demographic criteria, it defined ‘target group addresses’. The data thus generated were sold to various organisations, to enable them to send targeted advertising.

12 In the course of its activity, Österreichische Post processed data which, by way of statistical extrapolation, led it to infer that the applicant in the main proceedings had a high degree of affinity with a certain Austrian political party. That information was not communicated to third parties, but the applicant in the main proceedings, who had not consented to the processing of his personal data, felt offended by the fact that an affinity with the party in question had been attributed to him.

The fact that data relating to his supposed political opinions were retained within that company caused him great upset, a loss of confidence and a feeling of exposure. It is apparent from the order for reference that no harm other than those adverse emotional effects of a temporary nature has been established.



13 In that context, the applicant in the main proceedings brought an action before the Landesgericht für Zivilrechtssachen Wien (Regional Court for Civil Matters, Vienna, Austria) seeking, first, an injunction for Österreichische Post to cease processing the personal data in question and, second, an order requiring that company to pay him the sum of EUR 1 000 by way of compensation for the non-material damage which he claims to have suffered. By decision of 14 July 2020, that court upheld the application for an injunction but rejected the claim for compensation.

14 On appeal, the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria) confirmed, by judgment of 9 December 2020, the decision at first instance. As regards the claim for compensation, that court referred to recitals 75, 85 and 146 of the GDPR and held that the Member States' provisions of national law on civil liability supplement the provisions of that regulation, in so far as the latter does not contain special rules. In that regard, it noted that, under Austrian law, a breach of the rules on the protection of personal data is not automatically associated with non-material damage and gives rise to a right to compensation only where such damage reaches a certain 'threshold of seriousness'. In its view, that is not the case with regard to the negative feelings which the applicant in the main proceedings has invoked.

15 Hearing the action brought by the two parties in the main proceedings, the Oberster Gerichtshof (Supreme Court, Austria), by interim judgment of 15 April 2021, did not uphold the appeal on a point of law brought by Österreichische Post against the injunction imposed on it. Therefore, only the appeal on a point of law which the applicant in the main proceedings brought against the rejection of his claim for compensation which had been raised against him remains before that court.

16 In support of its request for a preliminary ruling, the referring court states that it is apparent from recital 146 of the GDPR that Article 82 of that regulation established its own rules on liability for the protection of personal data, which superseded the rules in force in the Member States. Therefore, the concepts contained in Article 82, in particular the concept of 'damage' referred to in paragraph 1 thereof, should be interpreted autonomously and the conditions for the implementation of that liability should be defined in the light not of the rules of national law, but of the requirements of EU law.

17 Specifically, in the first place, as regards the right to compensation for a breach of personal data protection, that court tends to consider, in the light of the sixth sentence of recital 146 of the GDPR, that compensation based on Article 82 of that regulation presupposes that material or non-material damage has actually been suffered by the data subject. It argues

that the award of such compensation is subject to proof of specific damage distinct from that breach, which does not in itself establish the existence of non-material damage. In its view, recital 75 of that regulation refers to the mere possibility that non-material damage may result from the breaches listed therein and, although recital 85 refers to the risk of a ‘loss of control’ of the data affected, that risk is, however, uncertain in the present case, since those data were not transmitted to a third party.

18 In the second place, as regards the assessment of the compensation that may be awarded under Article 82 of the GDPR, that court considers that the principle of effectiveness of EU law must have a limited impact, on the grounds that that regulation already provides for severe penalties for breaches thereof and that it is therefore not necessary to award a high level of compensation in addition to ensure its effectiveness. In its view, any compensation due on that basis must be proportionate, effective and dissuasive, so that the damages awarded may fulfil a compensatory function, but not be punitive in nature, which is extraneous to EU law.

19 In the third place, the referring court questions the argument put forward by Österreichische Post that the award of such compensation is subject to the condition that the breach of personal data protection has caused particularly serious harm. In that regard, it notes that recital 146 of the GDPR advocates a broad interpretation of the concept of ‘damage’ within the meaning of that regulation. It takes the view that non-material damage must be compensated, under Article 82 of that regulation, if it is tangible, even if it is minor. By contrast, such damage should not be compensated if it appears to be completely negligible, as would be the case for the merely unpleasant feelings that are typically associated with such a breach.

20 In those circumstances, the Oberster Gerichtshof (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Does the award of compensation under Article 82 of [the GDPR] also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?’

(2) Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?

(3) Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a

consequence [or effect] of the infringement of at least some weight that goes beyond the upset caused by that infringement?’

*The Court (Third Chamber) hereby rules:*

1. Article 82(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) **must be interpreted as meaning that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation.**
2. Article 82(1) of Regulation 2016/679 **must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness.**
3. Article 82 of Regulation 2016/679 **must be interpreted as meaning that for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with.**

To read more:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4947438>

*Number 14***Responsible Cyber Power in Practice**

A Defence and Intelligence Partnership

Established in 2020, the National Cyber Force (NCF) is a partnership between GCHQ and the Ministry of Defence which carries out cyber operations on a daily basis to protect against threats to the UK, further the UK's foreign policy, support military operations, and prevent serious crime.



A Defence and Intelligence Partnership

**The National Cyber Force:****Responsible Cyber Power in Practice**

There are three broad categories of NCF operations:



Countering threats from terrorists, criminals and states using the internet to operate across borders in order to do harm in the UK and elsewhere.



Countering threats which undermine the confidentiality, integrity and availability of data, and effective use of systems by users. This can involve conducting cyber operations, when necessary, alongside the range of other mitigations available to counter threats to our cyber security, including improved cyber resilience, coordinated action with allied governments, and collaboration with the private sector.



Contributing to UK Defence operations and helping to deliver the UK's foreign policy agenda. Cyber operations can support the full range of Defence activity. And they can make a particular contribution in support of key foreign policy and security objectives.

## Licence to operate

The UK's approach to cyber operations has traditionally been kept highly secret. But this kind of work clearly prompts questions about how the UK can act in a responsible way that is consistent with its commitment to a free, open, peaceful and secure internet. With the creation of the NCF, and the degree of investment involved, it is right that we enable greater transparency and engage with the public more widely than has been done before. This document is part of that process. Doing so is a crucial part of assuring the force's 'licence to operate' in the public mind and demonstrating the UK's commitment to being a responsible and democratic cyber power. We do not take this for granted.

### To read more:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1148278/Responsible\\_Cyber\\_Power\\_in\\_Practice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf)

*Number 15*

## Meta's Q1 2023 Security Reports: Protecting People and Businesses

Guy Rosen, Chief Information Security Officer



### *Takeaways*

1. As part of our quarterly integrity reporting, we're sharing Q1 updates on our work to combat a range of threats.
2. We detected and took action against malware campaigns targeting people and businesses online, shared our findings with other technology companies and rolled out new security features to help protect people.
3. We took actions against nine separate adversarial networks around the world for engaging in covert influence operations and cyber espionage, and shared our threat insights with industry peers, researchers and governments.

We know that safety and security are top of mind for people using our apps, including businesses and advertisers. Today, as part of our quarterly integrity reporting, we're sharing updates on our work to combat a range of threats, including covert influence operations, cyber espionage and malware campaigns.

In my first year as Meta's chief information security officer, my focus has been bringing together teams working on integrity, security, support, and operations so that we can work together in the most effective way possible.

Each of these efforts has been ongoing for many years, and a key focus for us has been sharing progress, bringing in outside experts and working with other companies to tackle industry-wide threats.

It's been more than 10 years since our bug bounty program began working with the security research community, 10 years since we first published transparency reports on government data requests, over five years since we started sharing takedowns of covert influence operations and five years since we published our first community standards enforcement report.

We've learned a lot through this work, including the importance of sharing both qualitative and quantitative insights into our integrity work. And it's been encouraging to see our peers join us in expanding their trust and

safety reporting. We're committed to continuing these efforts, and today's updates are good examples of this work.

### *Countering Malware Campaigns Across the Internet*

My teams track and take action against hundreds of threat actors around the world, including malware campaigns. Here are a few things that stood out from our latest malware work.

*First*, our threat research has shown time and again that malware operators, just like spammers, are very attuned to what's trendy at any given moment. They latch onto hot-button issues and popular topics to get people's attention. The latest wave of malware campaigns have taken notice of generative AI technology that's captured people's imagination and excitement.

Since March alone, our security analysts have found around 10 malware families posing as ChatGPT and similar tools to compromise accounts across the internet. For example, we've seen threat actors create malicious browser extensions available in official web stores that claim to offer ChatGPT-related tools.

In fact, some of these malicious extensions did include working ChatGPT functionality alongside the malware. This was likely to avoid suspicion from the stores and from users.

We've detected and blocked over 1,000 of these unique malicious URLs from being shared on our apps, and reported them to our industry peers at file-sharing services where malware was hosted so they, too, can take appropriate action.

This is not unique to the generative AI space. As an industry, we've seen this across other topics popular in their time, such as crypto scams fueled by the interest in digital currency. The generative AI space is rapidly evolving and bad actors know it, so we should all be vigilant.

*Second*, we've seen that our and industry's efforts are forcing threat actors to rapidly evolve their tactics in attempts to evade detection and enable persistence.

One way they do this is by spreading across as many platforms as they can to protect against enforcement by any one service. For example, we've seen malware families leveraging services like ours and LinkedIn, browsers like Chrome, Edge, Brave and Firefox, link shorteners, file-hosting services like Dropbox and Mega, and more. When they get caught, they mix in more



services including smaller ones that help them disguise the ultimate destination of links.

Another example is when some malware families masquerading as ChatGPT apps switched their lures to other popular themes like Google's Bard or TikTok marketing support, in response to detection.

These changes are likely an attempt by threat actors to ensure that any one service has only limited visibility into the entire operation. When bad actors count on us to work in silos while they target people far and wide across the internet, we need to work together as an industry to protect people.

That's why we designed our threat research to help us scale our security work in a number of ways — it disrupts malicious operations on our platform and helps inform our industry's defenses against threats that rarely target one platform. The insights we gain from this research help drive our continuous product development to protect people and businesses.

In the months and years ahead, we'll continue to highlight how these malicious campaigns operate, share threat indicators with our industry peers and roll out new protections to address new tactics. For instance, we're launching a new support flow for businesses impacted by malware. Read more about our work to help businesses stay safe on our apps.

### *Disrupting Cyber Espionage and Covert Influence Operations*

In today's Q1 Adversarial Threat report, we shared findings about nine adversarial networks we took action against for various security violations.

Six of these networks engaged in coordinated inauthentic behavior (CIB) that originated in the US, Venezuela, Iran, China, Georgia, Burkina Faso and Togo, and primarily targeted people outside of their countries. We removed the majority of these networks before they were able to build authentic audiences.

Nearly all of them ran fictitious entities — news media organizations, hacktivist groups and NGOs — across the internet, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, WordPress, Freelancer[.]com, hacking forums and their own websites.

Half of these operations were linked to private entities including an IT company in China, a US marketing firm and a political marketing consultancy in the Central African Republic.

We also disrupted three cyber espionage operations in South Asia, including an advanced persistent threat (APT) group we attributed to state-linked actors in Pakistan, a threat actor in India known in the security industry as Patchwork APT, and the threat group known as Bahamut APT in South Asia.

Each of these APTs relied heavily on social engineering to trick people into clicking on malicious links, downloading malware or sharing personal information across the internet.

This investment in social engineering meant that these threat actors did not have to invest as much on the malware side. In fact, for at least two of these operations, we saw a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.

In response to the security community continuing to disrupt these malicious efforts, we've seen these APTs to be forced to set up new infrastructure, change tactics and invest more in hiding and diversifying their operations, which likely degraded their operations. Read more about this threat research in our Q1 Adversarial Threat Report (at Number 10, below).

To read more: <https://about.fb.com/news/2023/05/metasploit-q1-2023-security-reports/>

*Number 16*

## Quarterly Adversarial Threat Report



Our public threat reporting began about six years ago when we first shared our findings about **coordinated inauthentic behavior (CIB)** by a Russian influence operation.

Since then, we have expanded our ability to respond to a wider range of adversarial behaviors as global threats have continued to evolve.

To provide a more comprehensive view into the risks we tackle, we've also expanded our regular threat reports to include cyber espionage and other emerging threats — all in one place, as part of the quarterly reporting series.

In addition to sharing our analysis and threat research, we're also publishing threat indicators to contribute to the efforts by the security community to detect and counter malicious activity elsewhere on the internet (See Appendix).

We expect the make-up of these reports to continue to evolve in response to the changes we see in the threat environment and as we expand to cover new areas of our Trust & Safety work.

This report is not meant to reflect the entirety of our security enforcements, but to share notable trends and investigations to help inform our community's understanding of the evolving security threats we see.

We welcome ideas from our peers across the defender community to help make these reports more informative, and we'll adjust as we learn from feedback.

For a quantitative view into our Community Standards' enforcement, including content-based actions we've taken at scale and our broader integrity work, please visit Meta's Transparency Center here:

<https://transparency.fb.com/data/>

*Summary of our findings*

1. Our quarterly threat report provides a view into the risks we see across multiple adversarial behaviors including CIB and cyber espionage.

2. We took action against three cyber espionage operations in South Asia. One was linked to a group of hackers known in the security industry as Bahamut APT (advanced persistent threat), the other to the group known as Patchwork APT and one to the state-linked actors in Pakistan. Here is what stood out from our threat research (See Section 1 for details):

**2a. Diversifying social engineering efforts:** These APTs relied heavily on social engineering and invested in making some of their fake accounts into more varied and elaborate fictitious personas with backstops across the internet so they can withstand scrutiny by their targets, platforms and researchers.

While we saw them continue using traditional lures like women looking for a romantic connection, they also developed personas posing as recruiters, journalists or military personnel.

**2b. Continued reliance on low-sophistication malware:** This investment in social engineering to trick people into clicking on malicious links or sharing sensitive information means that threat actors did not have to invest as much on the malware side.

In fact, our investigations showed that cheaper, low-sophistication malware can be effective in targeting people when used together with social engineering. For at least two of these operations, we observed a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.

**2c. Impact of public disruptions and threat reporting:** As the security community continued to disrupt these APTs, they have been forced to set up new infrastructure, change tactics, and invest more in hiding and diversifying their operations in order to persist, which likely degraded their operations.

3. In our Q1 Adversarial Threat report, we're sharing findings about six separate covert influence operations we took down for violating our policy against CIB. They originated in the United States and Venezuela, Iran, China, Georgia, Burkina Faso and Togo.

More than half of them targeted audiences outside of their countries. We removed the majority of these networks before they were able to build authentic audiences. Here is what stood out from our CIB threat research (See Section 2 for details):

**4. Creating fictitious entities across the internet:** In an attempt to build credibility, nearly all of these operations invested in creating

fictitious entities across the internet, including news media organizations, hacktivist groups, and NGOs.

They operated on many platforms, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, Wordpress, freelancer[.]com, hacking forums and their own websites.

**5. Fake hacktivists from Iran:** The operation from Iran posted claims of having hacked organizations in Israel, Bahrain and France, including news media, logistics and transport companies, educational institutions, an airport, a dating service and a government institution.

Some of these individual claims have been reported by the press in these countries, but we cannot confirm if any of them are credible. This is not the first time an Iran-origin operation claimed to have hacked government systems; a similar claim was promoted by another CIB network we removed ahead of the US 2020 election.

**6. For-hire operations:** As we called out in our past reporting, we continue to see for-hire organizations behind covert influence operations globally, with half of the operations in this report attributed to private entities. This included an IT company in China, a marketing firm in the United States and a political marketing consultancy in the Central African Republic.

**7. The evolution of China-origin operations:** Finally, this report brings the total of the China-origin CIB networks we removed since 2017 to six, with half of them reported in the last seven months.

These latest takedowns signal a shift in the nature of the China-based CIB activity we've found with new threat actors, novel geographic targeting, and new adversarial tactics. Yet, we continue to find and remove them before they are able to build their audience.

These latest networks experimented with a range of tactics we haven't seen in China-based operations before (though we've observed them elsewhere over the years, including in operations linked to troll farms, and marketing and PR firms).


The latest behaviors included creating a front media company in the West, hiring freelance writers around the world, offering to recruit protesters, and co-opting an NGO in Africa.


**M MOVIE DATE**      HOME   ABOUT   WORKING   REVIEWS   CONTACT US

# Host a **MOVIE DATE** with friends while social distancing


Movie Date is an entertainment app that provides you the comfort of cinema at home absolutely free of charge!

[DOWNLOAD](#)



 **CV**  
**WRITER**

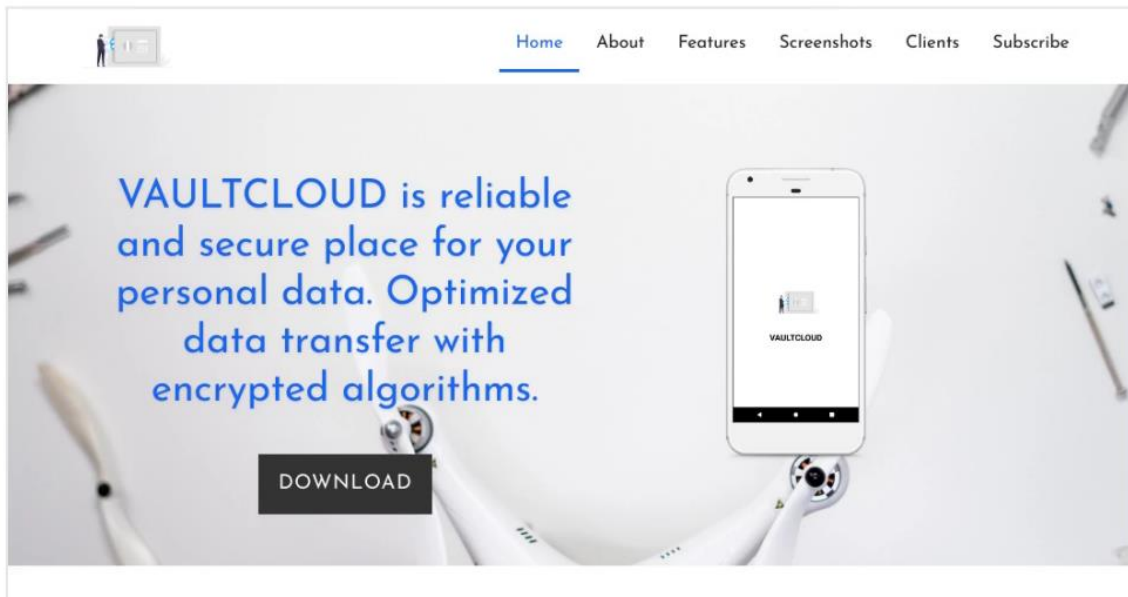
[DOWNLOAD](#)   [ABOUT US](#)   [OUR CLIENTS](#)   [OUR WORK](#)   [CONTACT US](#)



## Upgrade Your CV Upgrade Your Career.

● ● ●





## Coordinated inauthentic behavior (CIB)

**We view CIB** as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. In each case, people coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. When we investigate and remove these operations, we focus on behavior rather than content — no matter who's behind them, what they post or whether they're foreign or domestic.

**Continuous CIB enforcement:** We monitor for efforts to come back by the networks we previously removed. Using both automated and manual detection, we continuously remove accounts and Pages connected to networks we took down in the past.

The report: <https://about.fb.com/wp-content/uploads/2023/05/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf>



*Number 17*

## Using math to map social connections



Imagine being able to predict how a group of people will behave before they even know it themselves. From the dynamics of a sports team to the complexities of a nation, the ability to anticipate human interactions has long been a goal of scientists and analysts. Now, a team of researchers at Sandia National Laboratories is pioneering a new approach to social analysis.

Sandia cybersecurity expert Mike Brzustowicz believes a well-known mathematical function may provide the key to predicting that level of social interaction.

“The Fourier transform is a mathematical principle that very simply tells you the frequency — the count — of things that you’re observing. A famous use of the principle is transforming sound waves and time into frequency,” Brzustowicz explained.

“We are working with the non-Abelian Fourier transform. This is a totally different thing. It tells you about combinations of entities. So instead of understanding what individual things are happening, it tells you what connections exist between groups of things.”



## Nonabelian Fourier Transforms: A Path to Solving Epistasis

The work builds upon what was started with one of Brzustowicz’s collaborators, David Uminsky. Uminsky began the work at the University of San Francisco when trying to analyze genetic sequences and identify mutations. You may visit:

[https://research.latinxinai.org/papers/neurips/2018/slides/Slide\\_David\\_Uminsky.pdf](https://research.latinxinai.org/papers/neurips/2018/slides/Slide_David_Uminsky.pdf)



Eventually Uminsky and his team reached a point where they lacked the computing power to analyze large number sets and needed the computational capability that Sandia can offer.

“When you talk about a combination of things, there are almost infinitely many combinations of very small groups,” Brzustowicz explained. “The basketball team idea is something my collaborator David Uminsky published a long time ago: There are 15 players on the bench and there are five on the floor at a time. And then with those five on the floor, you look at thousands of combinations of the different players.”

But that is a small system to look at when compared to a community, a state or a nation, or groups of people that are not even geographically related.

“Ten years ago, it took forever to process that on a computer, and now it takes me like a second. But when you think of a social network, you may be thinking of hundreds or thousands of people,” Brzustowicz said.

“If you have 20 people together or 30 people, there are so many possible group combinations. You couldn’t maybe write them all down because you wouldn’t have enough memory on your computer, or you wouldn’t be able to annotate them. If we wanted to look at social networks and understand how subgroups interact with social networks, we’re barely getting there. So that’s our challenge.”

Now Brzustowicz and his team are trying to figure out how big a transform they can compute, and what kinds of groups they can predict.

“We’re already doing stuff that’s really cool,” Brzustowicz said. “It’s enviable that we can get to this level, but if we can go further, you know, like no one’s doing this, the non-Abelian Fourier transform.”

He added that Sandia is ideally positioned to figure out where the math goes next.

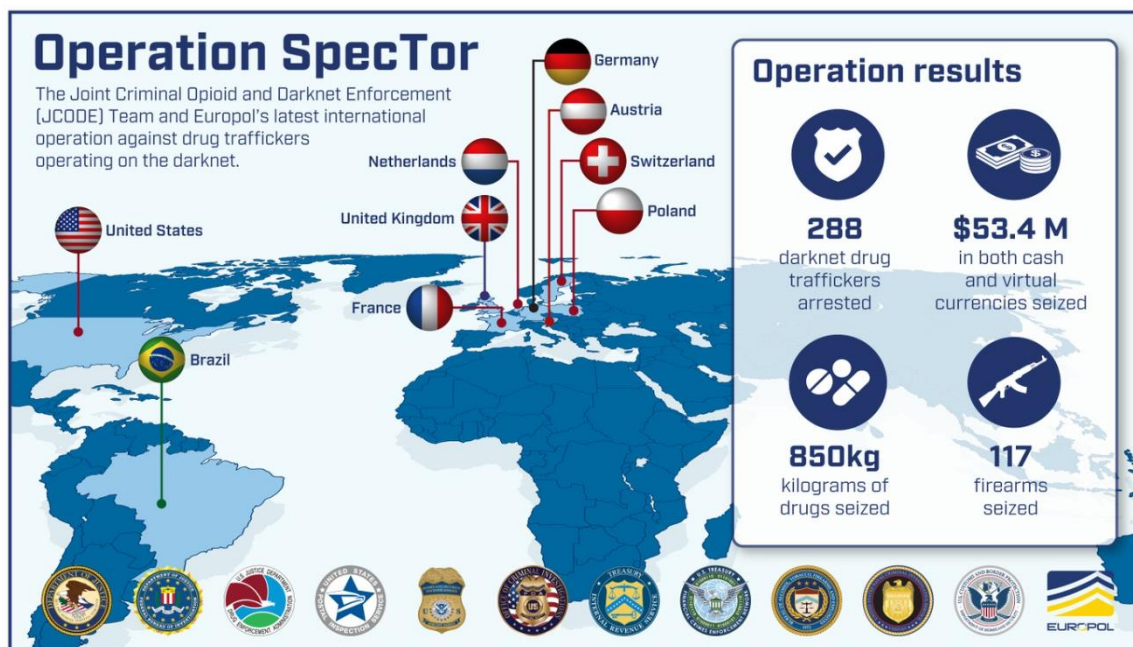
“I think that’s what the national labs are good at,” Brzustowicz concluded. “We’re not academics, we’re not industry. We’re not bound by those two extremes, bounded by ‘what can you do that will get published’ and bound by, ‘does this make the submit button at Google work better, or make the timeline at Facebook more appealing?’ We’re in the middle where we solve practical problems, but we have these huge resources available to us.”

To read more: [https://newsreleases.sandia.gov/social\\_connections/](https://newsreleases.sandia.gov/social_connections/)

## Number 18

### Sweep Targets Darknet Markets

**Operation SpecTor** spanned three continents, seized millions of dollars, and removed tens of thousands of potentially lethal drugs from circulation



A massive coordinated operation spanning nine countries and dozens of law enforcement agencies across the United States, Europe, and South America targeting darknet drug markets culminated recently with seizures of more than \$50 million in cash and virtual currency, 1,875 pounds of potentially lethal pills and other drugs, and 288 arrests.

Operation SpecTor uncovered vast networks of manufacturers, online supply chains, buyers, re-sellers, and users, revealing that the darknet—a part of the internet accessible through an encrypted browser—provides only a veneer of anonymity.

The drug seizures included about 152 pounds of fentanyl, a synthetic opioid so dangerous that two milligrams—like a few grains of salt—is a potentially lethal dose.

"The availability of dangerous substances like fentanyl on darknet marketplaces is helping to fuel the crisis that has claimed far too many American lives," FBI Director Christopher Wray said in a statement.

"That's why we will continue to join forces with our law enforcement partners around the globe to attack this problem together."

The operation began in late 2021. The Joint Criminal and Opioid Darknet Enforcement (JCODE) team, which the Department of Justice created in 2018, led the effort. The team coordinates complex, multi-agency investigations into virtual marketplaces selling dangerous and illegal drugs around the globe. The FBI was among 12 U.S. agencies working with local partners in the operation.

Overseas, the Bureau worked closely with authorities in Brazil and Europol (which provides investigative support to European law enforcement agencies) to conduct 135 arrests and seize more than \$38 million.

"These darknet marketplaces and vendors are not limited by geographical boundaries, requiring us to work closely with our international partners," said Kristen Varel, a supervisory special agent in the FBI's High Tech Organized Crime Unit, which coordinates the JCODE operations. "We focus on those vendors operating on U.S. soil, but we also investigate the marketplace infrastructure, which is frequently located overseas, often in European countries."

To read more: <https://www.fbi.gov/news/stories/operation-spector-targets-darknet-markets>

## *Number 19*

The European Commission adopted the first designation decisions under the Digital Services Act (DSA).



The European Commission designated 17 Very Large Online Platforms (VLOPs) and 2 Very Large Online Search Engines (VLOSEs) that reach at least 45 million monthly active users.

### *Very Large Online Platforms:*

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

### *Very Large Online Search Engines:*

- Bing
- Google Search

Following their designation, the companies will now have to comply, within four months, with the full set of new obligations under the DSA.

These aim at empowering and protecting users online, including minors, by requiring the designated services to assess and mitigate their systemic risks and to provide robust content moderation tools.

This includes:

### *More user empowerment:*

- Users will get clear information on why they are recommended certain information and will have the right to opt-out from recommendation systems based on profiling;
- Users will be able to report illegal content easily and platforms have to process such reports diligently;
- Advertisements cannot be displayed based on the sensitive data of the user (such as ethnic origin, political opinions or sexual orientation);
- Platforms need to label all ads and inform users on who is promoting them;
- Platforms need to provide an easily understandable, plain-language summary of their terms and conditions, in the languages of the Member States where they operate.

*Strong protection of minors:*

- Platforms will have to redesign their systems to ensure a high level of privacy, security, and safety of minors;
- Targeted advertising based on profiling towards children is no longer permitted;
- Special risk assessments including for negative effects on mental health will have to be provided to the Commission 4 months after designation and made public at the latest a year later;
- Platforms will have to redesign their services, including their interfaces, recommender systems, terms and conditions, to mitigate these risks.

*More diligent content moderation, less disinformation:*

- Platforms and search engines need to take measures to address risks linked to the dissemination of illegal content online and to negative effects on freedom of expression and information;
- Platforms need to have clear terms and conditions and enforce them diligently and non-arbitrarily;
- Platforms need to have a mechanism for users to flag illegal content and act upon notifications expeditiously;



- Platforms need to analyse their specific risks, and put in place mitigation measures – for instance, to address the spread of disinformation and inauthentic use of their service.

*More transparency and accountability:*

- Platforms need to ensure that their risk assessments and their compliance with all the DSA obligations are externally and independently audited;

- They will have to give access to publicly available data to researchers; later on, a special mechanism for vetted researchers will be established;

- They will need to publish repositories of all the ads served on their interface;

- Platforms need to publish transparency reports on content moderation decisions and risk management.

By 4 months after notification of the designated decisions, the designated platforms and search engines need to adapt their systems, resources, and processes for compliance, set up an independent system of compliance and carry out, and report to the Commission, their first annual risk assessment.

*Risk assessment*

Platforms will have to identify, analyse and mitigate a wide array of systemic risks ranging from how illegal content and disinformation can be amplified on their services, to the impact on the freedom of expression and media freedom.

Similarly, specific risks around gender-based violence online and the protection of minors online and their mental health must be assessed and mitigated.

The risk mitigation plans of designated platforms and search engines will be subject to an independent audit and oversight by the Commission.

To read more:

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_2413](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413)

*Number 20*

## Developing Agile, Reliable Sensing Systems with Microbes

DARPA's Tellus program seeks to advance remote environmental sense-and-respond platforms with enhanced breadth, resolution



Current environmental monitoring approaches can rely on both distributed sensor networks - on the ground or in the water - and remote sensing platforms, like satellites, to collect information important for the protection of people and property.

The Department of Defense (DOD) is interested in developing new, complementary sensors to monitor the environment with high spatial resolution, and reduced power and logistical burden, to further enhance monitoring capabilities and significantly reduce potential risk to personnel.

Recent research has demonstrated that microbes, such as bacteria, fungi, or microalgae, offer promise for detecting different types of input signals, including both chemical (e.g., toxic or radioactive materials, heavy metal pollutants) and physical phenomena (e.g., light, electric current, magnetic fields).

Microbes can also generate both chemical and physical output signals in response to sensing these inputs. The ability to detect and convert signals, be self-powering, and environmental resilience are microbial features that may complement other sensing approaches.

DARPA's new Tellus program will explore the development of an interactive, platform methodology for the rapid design of microbe-based sense-and-respond devices for monitoring DOD-relevant environments.

Specifically, DARPA seeks to establish the range of chemical and physical signals that microbial devices can detect, environmental conditions they can tolerate, and types of output signals that can be generated.

To this end, Tellus will focus on developing the methodology to enable the rapid design of agile, robust, reliable, and durable microbial sensors for environmental monitoring.

The microbial devices developed during the 2.5-year program must be able to translate detected signals into a variety of physical or chemical output signals, including light, non-toxic organic compounds, or electric current, which can then be measurable by conventional receiver systems (e.g., optoelectronic, photonic, imaging, electrode).

In addition to method development, Tellus is focused on assessing sensor functionality across many different environments and conditions. As remote environmental monitoring for chemicals, pollutants, or changing conditions is an area of national security interest, microbial sensing systems that are capable of detecting multiple types input targets, relaying a variety of output signals at a distance, and operating unattended for long durations are desired.

“As part of the program, DARPA will test how quickly new, functional devices can be designed, built, and tested using specific parameters,” stated Dr. Linda Chrisey, Tellus program manager.

“Ultimately, we envision a dashboard or interface where a user would dial in features of their environment, the inputs they want to detect, and the output signals that are useful to them, and the system would design a safe, effective microbial device to meet those needs.”

To read more: <https://www.darpa.mil/news-events/2023-04-21>

*Number 21*

## Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service



Through Operation MEDUSA, the FBI, and the U.S. Attorney's Office for the Eastern District of New York Neutralized the FSB's Premier Cyberespionage Malware Implant in Coordination with Multiple Foreign Governments.

The Justice Department announced the completion of a court-authorized operation, codenamed MEDUSA, to disrupt a global peer-to-peer network of computers compromised by sophisticated malware, called "Snake", that the United States Government attributes to a unit within Center 16 of the Federal Security Service of the Russian Federation (FSB).

For nearly 20 years, this unit, referred to in court documents as "Turla," has used versions of the Snake malware to steal sensitive documents from hundreds of computer systems in at least 50 countries, which have belonged to North Atlantic Treaty Organization (NATO) member governments, journalists, and other targets of interest to the Russian Federation.

After stealing these documents, Turla exfiltrated them through a covert network of unwitting Snake-compromised computers in the United States and around the world.

Operation MEDUSA disabled Turla's Snake malware on compromised computers through the use of an FBI-created tool named PERSEUS, which issued commands that caused the Snake malware to overwrite its own vital components.

Within the United States, the operation was executed by the FBI pursuant to a search warrant issued by United States Magistrate Judge Cheryl L. Pollak of the Eastern District of New York, which authorized remote access to the compromised computers.

This morning, the Court unsealed redacted versions of the affidavit submitted in support of the application for the search warrant, and of the search warrant issued by the Court.

For victims outside the United States, the FBI is engaging with local authorities to provide both notice of Snake infections within those authorities' countries and remediation guidance.

Merrick B. Garland, United States Attorney General; Breon Peace, United States Attorney for the Eastern District of New York; Lisa O. Monaco, Deputy Attorney General of the Justice Department; and Michael J. Driscoll, Assistant Director-in-Charge, FBI, New York Field Office, announced the operation.

“The Justice Department, together with our international partners, has dismantled a global network of malware-infected computers that the Russian government has used for nearly two decades to conduct cyber-espionage, including against our NATO allies,” stated Attorney General Garland.

“We will continue to strengthen our collective defenses against the Russian regime’s destabilizing efforts to undermine the security of the United States and our allies.”

“Russia used sophisticated malware to steal sensitive information from our allies, laundering it through a network of infected computers in the United States in a cynical attempt to conceal their crimes. Meeting the challenge of cyberespionage requires creativity and a willingness to use all lawful means to protect our nation and our allies,” stated United States Attorney Peace.

“The court-authorized remote search and remediation announced today demonstrates my Office and our partners’ commitment to using all of the tools at our disposal to protect the American people.”

“Through a high-tech operation that turned Russian malware against itself, U.S. law enforcement has neutralized one of Russia’s most sophisticated cyber-espionage tools, used for two decades to advance Russia’s authoritarian objectives,” stated Deputy Attorney General Monaco.

“By combining this action with the release of the information victims need to protect themselves, the Justice Department continues to put victims at the center of our cybercrime work and take the fight to malicious cyber actors.”

“The operation we announced today successfully disrupted the foremost cyber espionage tool of the Russian government. For two decades, the malware allowed Russian Intelligence to compromise computer systems

and steal sensitive information - harming not only the United States Government and our allies but also private sector organizations. This action should serve as a reminder to Russia and any other hostile nation willing to steal information, the FBI and our partners are united in our efforts to protect our countries,” stated FBI Assistant Director-in-Charge Driscoll.

“For 20 years, the FSB has relied on the Snake malware to conduct cyberespionage against the United States and our allies – that ends today,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division.

“The Justice Department will use every weapon in our arsenal to combat Russia’s malicious cyber activity, including neutralizing malware through high-tech operations, making innovative use of legal authorities, and working with international allies and private sector partners to amplify our collective impact.”

As detailed in court documents, the U.S. government has been investigating Snake and Snake-related malware tools for nearly 20 years. The U.S. government has monitored FSB officers assigned to Turla conducting daily operations using Snake from a known FSB facility in Ryazan, Russia.

Although Snake has been the subject to several cybersecurity industry reports throughout its existence, Turla has applied numerous upgrades and revisions, and selectively deployed it, all to ensure that Snake remains the FSB’s most sophisticated long-term cyberespionage malware implant.

Unless disrupted, the Snake implant persists on a compromised computer’s system indefinitely, typically undetected by the machine’s owner or authorized users. The FBI has observed Snake persist on particular computers despite a victim’s efforts to remediate the compromise.

Snake provides its Turla operators the ability to remotely deploy selected malware tools to extend Snake’s functionality to identify and steal sensitive information and documents stored on a particular machine.

Most importantly, the worldwide collection of Snake-compromised computers acts as a covert peer-to-peer network, which utilizes customized communication protocols designed to hamper detection, monitoring, and collection efforts by Western and other signals intelligence services.

Turla uses the Snake network to route data exfiltrated from target systems through numerous relay nodes scattered around the world back to Turla



operators in Russia. For example, the FBI, its partners in the U.S. Intelligence Community, together with allied foreign governments, have monitored the FSB's use of the Snake network to exfiltrate data from sensitive computer systems, including those operated by NATO member governments, by routing the transmission of these stolen data through unwitting Snake-compromised computers in the United States.

As described in court documents, through analysis of the Snake malware and the Snake network, the FBI developed the capability to decrypt and decode Snake communications.

With information gleaned from monitoring the Snake network and analyzing Snake malware, the FBI developed a tool, named PERSEUS, that establishes communication sessions with the Snake malware implant on a particular computer, and issues commands that causes the Snake implant to disable itself without affecting the host computer or legitimate applications on the computer.

Today, to empower network defenders worldwide, the FBI, the National Security Agency, the Cybersecurity and Infrastructure Security Agency, the U.S. Cyber Command Cyber National Mission Force, and six other intelligence and cybersecurity agencies from each of the Five Eyes member nations, issued a joint cybersecurity advisory (the "Joint Advisory") with detailed technical information about the Snake malware that will allow cybersecurity professionals to detect and remediate Snake malware infections on their networks.

The Joint Advisory is available [here](#). The FBI and U.S. Department of State are also providing additional information to local authorities in countries where computers that have been targeted by the Snake malware have been located.

Although Operation MEDUSA disabled the Snake malware on compromised computers, victims should take additional steps to protect themselves from further harm.

The operation to disable Snake did not patch any vulnerabilities or search for or remove any additional malware or hacking tools that hacking groups may have placed on victim networks.

The Department of Justice strongly encourages network defenders to review the Joint Advisory for further guidance on detection and patching.

Moreover, as noted in court documents, Turla frequently deploys a "keylogger" with Snake that Turla can use to steal account authentication credentials, such as usernames and passwords, from legitimate users.

Victims should be aware that Turla could use these stolen credentials to fraudulently re-access compromised computers and other accounts. The FBI has is providing notice of the court-authorized operation to all owners or operators of the computers remotely accessed pursuant to the search warrant.

The criminal investigation into the FSB's use of the Snake malware is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorney Ian C. Richardson is in charge of the investigation, with assistance from the National Security Division's Counterintelligence and Export Control Section.

The efforts to disrupt the Snake malware network were led by the FBI's New York Field Office, FBI's Cyber Division, the U.S. Attorney's Office for the Eastern District of New York, and the National Security Division's Counterintelligence and Export Control Section. Assistance was also provided by the Criminal Division's Computer Crime and Intellectual Property Section.

Those efforts would not have been successful without the partnership of numerous private-sector entities, including those victims who allowed the FBI to monitor Snake communications on their systems.

To read more: <https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network>

*Number 22***Hunting Russian Intelligence “Snake” Malware**

The Snake implant is considered the most sophisticated cyber espionage tool designed and used by Center 16 of Russia’s Federal Security Service (FSB) for long-term intelligence collection on sensitive targets.

To conduct operations using this tool, the FSB created a covert peer-to-peer (P2P) network of numerous Snake-infected computers worldwide.

Many systems in this P2P network serve as relay nodes which route disguised operational traffic to and from Snake implants on the FSB’s ultimate targets.

Snake’s custom communications protocols employ encryption and fragmentation for confidentiality and are designed to hamper detection and collection efforts.

We have identified Snake infrastructure in over 50 countries across North America, South America, Europe, Africa, Asia, and Australia, to include the United States and Russia itself.

Although Snake uses infrastructure across all industries, its targeting is purposeful and tactical in nature.

Globally, the FSB has used Snake to collect sensitive intelligence from high-priority targets, such as government networks, research facilities, and journalists.

As one example, FSB actors used Snake to access and exfiltrate sensitive international relations documents, as well as other diplomatic communications, from a victim in a North Atlantic Treaty Organization (NATO) country.

Within the United States, the FSB has victimized industries including education, small businesses, and media organizations, as well as critical infrastructure sectors including government facilities, financial services, critical manufacturing, and communications.

This Cybersecurity Advisory (CSA) provides background on Snake’s attribution to the FSB and detailed technical descriptions of the implant’s

host architecture and network communications. This CSA also addresses a recent Snake variant that has not yet been widely disclosed.

The technical information and mitigation recommendations in this CSA are provided to assist network defenders in detecting Snake and associated activity.

For more information on FSB and Russian state-sponsored cyber activity, please see the joint advisory Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure and CISA's Russia Cyber Threat Overview and Advisories webpage.

You may visit: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>

<https://www.cisa.gov/russia>



# Russia Cyber Threat Overview and Advisories



This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Russian government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes [a complete list of related CISA publications](#), many of which are jointly authored with other U.S. government agencies

## TABLE OF CONTENTS

Summary .....	1
Introduction .....	4
What is Snake? .....	4
Background .....	4
Attribution .....	5
Victimization .....	5
Other Tools and TTPs Employed with Snake .....	6
Snake Architecture .....	6
Capitalizing on Mistakes .....	7

---

Snake Host-Based Technical Details .....	8
Installer .....	8
On-Disk Components .....	8
The Queue .....	11
Snake Network Communications .....	17
Network Obfuscation .....	17
Snake's Network Authentication Technique ("ustart") .....	17
Snake UDP .....	19
Snake HTTP .....	20
Snake TCP .....	21
Snake "enc" Layer .....	23

To read more: [https://www.cisa.gov/sites/default/files/2023-05/aa23-129a\\_snake\\_malware\\_1.pdf](https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_1.pdf)

*Number 23*

## Joint Communication to the European Parliament, the Council, and the European Economic and Social Committee on the fight against corruption



HIGH REPRESENTATIVE  
OF THE UNION FOR  
FOREIGN AFFAIRS AND  
SECURITY POLICY

Corruption is highly damaging to society, to our democracies, to the economy and to individuals. It undermines the institutions on which we depend, diluting their credibility as well as their ability to deliver public policies and quality public services. It acts as an enabler for organised crime and hostile foreign interference.

Successfully preventing and fighting corruption is essential both to safeguard EU values and the effectiveness of EU policies, and to maintain the rule of law and trust in those who govern and public institutions.

Corruption is an impediment to sustainable economic growth, diverting resources from productive outcomes, undermining the efficiency of public spending and deepening social inequalities. It hampers the effective and smooth functioning of the single market, creates uncertainties in doing business and holds back investment.

Corruption is by its nature difficult to quantify, but even conservative estimates suggest that it costs the EU economy at least EUR 120 billion per year.

The negative effects of corruption are felt worldwide, undercutting efforts to bring good governance and prosperity, and to meet the United Nations Sustainable Development Goals.

Effective anti-corruption policies are an essential part of the enabling environment required for the rule of law, alongside on respect for judicial independence, free and pluralistic media, a transparent and high-quality public administration, and a free and active civil society.

A constant commitment to prevention, maintaining a culture of integrity and the active enforcement of anti-corruption legislation, including effective prosecution of corruption crimes, is needed to keep corruption in check.

This approach is also reflected in EU external action on anti-corruption underpinned by support to the rule of law and public financial management of partner countries.

Global corruption indices put many EU Member States among the countries seen as the least corrupt in the world. However, as also set out in the Rule of Law reports, there are many issues to address and corruption remains a concern for people across the EU, as shown by Eurobarometer data.

In 2022, almost seven in ten Europeans (68%) believed that corruption was widespread in their country and only 31% were of the opinion that their government's efforts to combat corruption are effective.

In addition, over half of the companies based in the EU (51%) think that it is unlikely that corrupt people or businesses in their country would be caught, or reported to the police or prosecutors.

In the 2022 State of the Union address, President von der Leyen set out the need for decisive action against corruption.

The EU can play a major role: not only in the way it manages its own work, but also through ongoing efforts to integrate measures to prevent corruption into the design of EU policies and programmes, and by actively supporting Member States' work to put strong anti-corruption policies and legislation in place.

Today the Commission has adopted two targeted proposals to strengthen EU law in this area.

First, the Commission is proposing a directive to update and harmonise EU rules on the definitions of and penalties for corruption offences, to ensure high standards against the full range of corruption offences, to better prevent corruption and to improve enforcement.

Second, the High Representative of the Union for Foreign Affairs and Security Policy, with the Commission's support, is proposing to complement the Common Foreign and Security Policy (CFSP sanctions) toolbox of restrictive measures (sanctions) with a dedicated CFSP sanctions regime to fight corruption when and where acts of corruption seriously affect or risk affecting the fundamental interests of the Union and the objectives of the CFSP as set out in Article 21 of the Treaty on European Union.

The High Representative is therefore submitting a proposal for a Council Decision and, jointly with the Commission, a proposal for a Council Regulation for a thematic framework for CFSP sanctions targeting corruption, to complement our internal and external policy actions to fight corruption.



The Commission will step up its action and the anti-corruption proposals presented today represent a milestone in the fight against corruption at national and EU level.

This Communication shows how these building blocks will accompany a broader effort to build a comprehensive and systematic strategic approach. This needs to bring together existing work and develop new directions and new tools at both EU and Member State level, also feeding into a clear commitment to tackling corruption at the global level.

Success will depend on a joint and continuous effort at EU, national, regional, and local level, involving public authorities, civil society, and the private sector, as well as international organisations.

This will not only make the public aware of the consequences of corruption, but it will also give citizens and businesses the confidence to challenge it.

To read more: [https://commission.europa.eu/system/files/2023-05/JOIN\\_2023\\_12\\_1\\_EN.pdf](https://commission.europa.eu/system/files/2023-05/JOIN_2023_12_1_EN.pdf)

*Number 24***Proposal for a Directive on combating corruption***Article 1, Subject matter and scope*

This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of corruption, as well as measures to better prevent and fight corruption.

*Article 2, Definitions*

For the purposes of this Directive, the following definitions apply:

1. '*prevention of corruption*' refers to the detection and elimination of the causes of and conditions for corruption, through development and implementation of a system of appropriate measures, as well as deterrence against corruption-related acts.

2. '*property*' means funds or assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or an interest in, such assets.

3. '*public official*' means:

(a) a Union official or a national official of a Member State or of a third country,

(b) any other person assigned and exercising a public service function in Member States or third countries, for an international organisation or for an international court.

4. '*Union official*' means a person who is:

(a) a member of an institution, body, office or agency of the Union and the staff of such bodies shall be assimilated to Union officials.

(b) an official or other servant engaged under contract by the Union within the meaning of the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 (the 'Staff Regulations');

(c) seconded to the Union by a Member State or by any public or private body, who carries out functions equivalent to those performed by Union officials or other servants.

5. '*national official*' means any person holding an executive, administrative, or judicial office at national, regional or local level, whether appointed or elected, whether permanent or temporary, whether paid or unpaid, irrespective of that person's seniority. Any person holding a legislative office at national, regional or local level is considered a national official for the purpose of this Directive.

6. '*breach of duty*' covers as a minimum any disloyal behaviour constituting a breach of a statutory duty, or, as the case may be, a breach of professional regulations or instructions, which apply within the business of a person who in any capacity directs or works for a private sector entity.

7. '*legal person*' means any entity having legal personality under the applicable national law, except for States or public bodies in the exercise of State authority and for public international organisations.

8. '*high level officials*' are heads of state, heads of central and regional government, members of central and regional government, as well as other political appointees who hold a high level public office such as deputy ministers, state secretaries, heads and members of a minister's private office, and senior political officials, as well as members of parliamentary chambers, members of highest Courts, such as Constitutional and Supreme Courts, and members of Supreme Audit Institutions.

To read more: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0234>

## *Number 25*

From CNIL, the French Data Protection Agency  
**Artificial intelligence: the action plan of the CNIL**



Note – what is CNIL?: Back in the seventies, the French Government announced a plan designed to identify each citizen with a specific number and, using that unique identifier, to interconnect all government records.

This plan, known as SAFARI, led to great controversy in the public opinion. It underlined the dangers inherent to certain uses of information technology and aroused fears that the entire French population would soon be recorded in files. This fear led the Government to set up a commission mandated to recommend concrete measures intended to guarantee that any developments in information technology would remain respectful of privacy, individual rights and public liberties.

After broad debates and public consultation, this “Commission on Information Technology and Liberties” recommended that an independent oversight authority be set up. Such was the purpose of the January 6, 1978 Act creating the “*Commission Nationale de l’Informatique et des Libertés*” (CNIL).

- The CNIL has been undertaking work for several years to anticipate and respond to the issues raised by AI.
- In 2023, it will extend its action on augmented cameras and wishes to expand its work to generative AIs, large language models and derived applications (especially chatbots).
- Its action plan is structured around four strands:
  - to understand the functioning of AI systems and their impact on people;
  - enabling and guiding the development of privacy-friendly AI;
  - federate and support innovative players in the AI ecosystem in France and Europe;
  - audit and control AI systems and protect people.
- This work will also make it possible to prepare for the entry into application of the draft European AI Regulation, which is currently under discussion.

## *The protection of personal data, a fundamental challenge in the development of AI*

The development of AI is accompanied by challenges in the field of data protection and individual freedoms that the CNIL has been working to address for several years now. Since the publication in 2017 of its report on the ethical challenges of algorithms and artificial intelligence, the CNIL repeatedly pronounced on the issues raised by the new tools brought about by this new technology.

In particular, generative artificial intelligence (see box below) has been developing rapidly for several months, whether in the field of text and conversation, via large language models (LLMs in English), such as GPT-3, BLOOM or Megatron NLG and derived chatbots (ChatGPT or Bard), but also in those of imaging (Dall-E, Midjourney, Stable Diffusion, etc.) or speech (Vall-E).

These foundation models and the technological bricks that rely on them seem to already find many cases of application in a variety of sectors. Nevertheless, the understanding of their functioning, their possibilities and their limitations, as well as the legal, ethical and technical issues surrounding their development and use remain largely under debate.

Considering that the protection of personal data is a major challenge for the design and use of these tools, the CNIL publishes its action plan on artificial intelligence, which aims – among other things – to frame the development of generative AI.

### *What is generative AI?*

Generative artificial intelligence is a system capable of creating text, images or other content (music, video, voice, etc.) from a human user's instruction. These systems can produce new content from training data.

Their performance is now close to some productions made by people because of the large amount of data that has been used for their training. However, these systems require the user to clearly specify their queries in order to achieve the expected results. A real know-how is therefore developed around the composition of the user's queries (quick engineering).

For example, the image below, entitled 'Space Opera Theatre', was generated by user Jason M. Allen using the Midjourney tool on the basis of a textual instruction describing his expectations (theatrical decor, toges, pictorial inspirations, etc.).

### *A four-pronged action plan*

For several years, the CNIL has been undertaking work aimed at anticipating and responding to the challenges posed by artificial intelligence, its different variations (classification, prediction, content generation, etc.) and its various use cases. Its new artificial intelligence service will be dedicated to these issues, and will support other CNIL services that also face uses of these algorithms in many contexts.

Faced with challenges related to the protection of freedoms, the acceleration of AI and news related to generative AI, the regulation of artificial intelligence is a main focus of the CNIL's action.

This regulation is structured around *four objectives*:

- Understanding the functioning of AI systems and their impacts for people
- Enabling and guiding the development of AI that respects personal data
- Federating and supporting innovative players in the AI ecosystem in France and Europe
- Audit and control AI systems and protect people

To read more: <https://www.cnil.fr/en/artificial-intelligence-action-plan-cnil>

*Number 26***Pre-Infected - Over 8.9 Million Android Phones Worldwide**

Fyodor Yarochkin, Zhengyu Dong, Paul Pajares



An overview of the Lemon Group's use of preinfected mobile devices, and how this scheme is potentially being developed and expanded to other internet of things (IoT) devices. This research was presented in full at the Black Hat Asia 2023 Conference in Singapore in May 2023.

The size of the mobile device market has reached the billions, and it is estimated to reach 18 billion by 2025. Around 2010, reflashing (described as reprogramming and/or replacing the existing firmware of a device with a new one) and silent installation became common.

The ROM image of phones can be reflashed to modify the said image with new software features, firmware updates, or arrive preinstalled to run a different operating system (OS) from the original.

Developers, hobbyists, and enthusiasts knowledgeable and keen on improving their respective devices did this to maximize the features of their respective phones and/or customize their ROMs for better hardware, user experience, or battery life performance, among other purposes.

In time, threat actors turned to reflashing and silent installation as techniques for malicious activities. These became rampant as phones got infected when threat actors implanted unwanted apps to monetize pay-per-install schemes. These apps were accompanied by a silent plugin that pushed apps to the victim's device whenever they wanted.

To read more: [https://www.trendmicro.com/en\\_us/research/23/e/lemon-group-cybercriminal-businesses-built-on-preinfected-devices.html](https://www.trendmicro.com/en_us/research/23/e/lemon-group-cybercriminal-businesses-built-on-preinfected-devices.html)



## *Number 27*

### Why more transparency around cyber attacks is a good thing for everyone

Eleanor Fairford, Deputy Director of Incident Management at the NCSC, and Mihaela Jembei, Director of Regulatory Cyber at the Information Commissioner's Office (ICO).



At the NCSC and ICO, we deal with the fallout from serious cyber attacks every day. Our responsibilities are different, but we both work on incidents that can take down businesses, severely impact national services and infrastructure, and massively disrupt people's day-to-day lives. You'll be familiar with some of the headlines and it's not a pretty picture.

But we are increasingly concerned about what happens behind the scenes of the attacks we don't hear about, particularly the ransomware ones. They are the attacks that aren't reported to us and pass quietly by, pushed to one side, the ransoms paid to make them go away. And if attacks are covered up, the criminals enjoy greater success, and more attacks take place. We know how damaging this is.

In this blog we look at why it's in everyone's interests to be more open about cyber attacks, by exploring – and dispelling – some of the myths around responding to cyber attacks.

#### *Myth 1: If I cover up the attack, everything will be ok*

Imagine that you come home from work to find your house has been burgled. Instead of reporting it to the police and seeking support, you quickly tidy everything up and carry on as if nothing had happened, hoping no one finds out, and without investigating further.

The next week your neighbour is burgled too, although you might not know about it because they don't mention it. And then the burglars return to your place again because you didn't spot that the unlocked window is still unlocked, so it's easy for them to get back in.

This is often how it works in a cyber incident, particularly ransomware. Every successful cyber attack that is hushed up, with no investigation or information sharing, makes other attacks more likely because no one learns from it. Every ransom that is quietly paid gives the criminals the message that these attacks work and it's worth doing more.

So if attacks pass by without full investigation and information sharing, particularly with those who can help mitigate it, everything definitely won't be ok.

### *How to share?*

We understand it's hard for organisations to open up about the stressful experience of a cyber attack, and lay bare the things you wish had been different. But there are secure and trusted environments where you can do this safely. The NCSC has CISP to facilitate information sharing between organisations, as well as our sector information exchanges (IEs) and other trust groups. Your sector or region may have other forums too.

Keeping your cyber incident a secret doesn't help anyone except the criminals.

### *Myth 2: Reporting to the authorities makes it more likely your incident will go public*

If your organisation experiences a cyber attack, reporting it to the NCSC or law enforcement means you can access the wealth of support available. One of the responsibilities of NCSC Incident Management is to provide direct support to affected organisations where there is a national impact, working with the appointed incident response provider. We know how these things play out – we manage cyber incidents every day, and can help you. We respect your confidentiality and don't proactively make information public, or share it with regulators without your consent.

In fact, the NCSC has extensive communications support available to help you navigate the incident and to manage media coverage and active communications. We encourage organisations to be open when an incident happens, but ultimately, it's your choice, and we will support you either way.

### **Remember your regulatory responsibilities**

As the regulator, over at the ICO, our role is to provide guidance and support to the organisations we regulate, as well as to monitor and enforce the regulations we oversee. But in the immediate aftermath of an incident, we don't disclose details beyond confirming whether or not an incident has been reported to us. It's important to remember that there may be a regulatory requirement to report (and you can find out more about your responsibilities and when you need to report a breach, including a self-assessment tool, on the ICO website).

When it comes to deciding the regulatory response, it's really important to emphasise that we've always taken into account how proactive an organisation is about getting the right support, which includes engaging with the NCSC and implementing any advice. In our next process review, we're even considering making explicit the amount saved in a fine when an organisation has positively engaged. Being open and transparent is the right thing to do for the greater good, but we're looking into making it business savvy as well.

And where information about an incident does need to be made public – not always the case – we will usually be in dialogue with a company about this so there aren't any surprises.

### *Myth 3: Paying a ransom makes the incident go away*

In a ransomware attack, your files and computers are encrypted, and there is now the added sting that an attacker often also steals data from your network and threatens to leak it if you don't pay up.

But paying the ransom quickly to get the decryption key and restore services doesn't always help. Why not?

- The decryption process can be lengthy and cumbersome – attackers sometimes accidentally double-encrypt data meaning it can't be decrypted, or they delete data that is then unrecoverable. In one case, restoration from backups was actually quicker than using the decryption key itself.
- Paying a ransom is basically accepting a pinky promise from criminals that they will decrypt your network or not leak stolen data. Nothing is guaranteed and bear in mind that organisations that pay the ransom are likely to be targeted again. Estimates vary but it's suggested that around one third of all organisations affected by ransomware are attacked again.
- It's basically rewarding criminals for their efforts and makes it more likely they'll carry out more attacks against other organisations, ultimately making the broader threat landscape worse.
- From the ICO point of view, paying ransoms doesn't reduce the risk to individuals, it's not a mitigation under data protection law, and isn't considered a reasonable step to safeguard data.

The NCSC position, along with law enforcement, is that we don't endorse, promote or encourage the payment of ransoms. But we know that an unprepared organisation, in the aftermath of an attack, may take the view

that paying a ransom is the only way out. If that's the case, we ask that you still stay in touch with the NCSC and our law enforcement partners so we can understand the full picture and try to establish how they got into your systems in the first place so you can fix that.

Don't leave that window unlocked for them to come back next time.

*Myth 4: I've got good offline backups, I won't need to pay a ransom*

We'd like it to be true that if you implemented all our excellent cyber security guidance, your backups would be safely offline and you could rebuild if the worst happened.

Unfortunately the data extortion angle adds a whole new level of complexity. If the attackers have access to sensitive data, they could threaten to leak it unless you pay the ransom.

So you need to think really carefully about the data you hold and how you protect it.

It's a bit like storing someone else's valuables in your house in a cardboard box with the words 'valuable stuff in here!' on it, and your window left unlocked for the thieves to get in. You are responsible for protecting the valuable items you hold – except in this case, it's other people's personal data.

Keeping people's data safe is also a requirement under data protection law – see the ICO's guidance on security for more on that.

*Myth 5: If there is no evidence of data theft, you don't need to report to the ICO*

You might not be able to see in your logging data whether or not data was stolen. But if there is any suggestion that the actor has accessed the systems holding your data, you should start from the assumption that it has been taken. As the quote goes: absence of evidence isn't evidence of absence.

In the NCSC we've seen many examples of organisations affected by ransomware that were convinced no data had been taken, only to find it crop up in a dark web data leak weeks or months later. But if you seek early support and communicate openly, you will reduce the risk of an unpleasant surprise of future data leaks.

From an ICO point of view, we'd reiterate the earlier point that organisations have responsibilities under data protection law, and other

legislation including NIS, to report incidents where the thresholds are met. And remember that point about lack of evidence – poor situational awareness isn't an adequate technical control. You could be living in blissful ignorance while also being in breach of data protection law.

*Myth 6: You'll only get a fine if your data is leaked*

This isn't necessarily the case. A data leak isn't the only reason for a fine, and you won't always be fined if data is leaked. A personal data breach is more than just a loss of data: it also includes its destruction, alteration, and unauthorised disclosure or access to it. The ICO looks at the context of each individual case – it's not just about whether or not data was leaked.

As a fair and proportionate regulator, the ICO understands that helping organisations to improve their data protection practices is also the best way to protect people's data. If we find serious, systemic or negligent behaviour that puts people's information at risk, enforcement action may be an option. But this isn't a blanket approach.

The ICO also recognises when organisations have taken steps to fully understand what has happened, and learn from it. As we say above, if your organisation has raised the incident with the NCSC, and you can show you've followed guidance and support, it could positively impact our response.

. . . but the gangs may tell you otherwise

Be aware that cyber criminal gangs prey on the misconception that the data leak is the source of a fine. The NCSC has seen ransomware messages to organisations that say things like: "The ransom demand is £50 million. If you pay, you'll avoid a regulator fine of £600 million which is 0.5% of your annual profit." Don't succumb to their techniques! Seek support and communicate early to avoid an investigation later into an incident you tried to hide.

*Don't feed the cycle!*

We hope this blog has helped persuade you of the value of being open if the worst happens.

Being open about an attack by seeking support and communicating openly with the NCSC and ICO in the days following it can only help you, while sharing information about the attack with your trust communities later on will ultimately improve the threat landscape for everyone.

And don't just take our word for it; others are saying the same thing. In the US, CISA Director Jen Easterly has written about how reluctance to report to government creates a race to the bottom, while the Google President of Global Affairs talks about the need to 'weave transparency' into a cyber security response.

Make sure cyber security lessons are learned to protect yourself and help prevent future attacks for everyone. And remember the cyber incident reporting service helps UK organisations access the right support if you need it.

To read more: <https://www.ncsc.gov.uk/blog-post/why-more-transparency-around-cyber-attacks-is-a-good-thing-for-everyone>

## Cyber Risk GmbH

Cyber Risk GmbH has been established in Horgen, Switzerland, by George Lekatis, a well-known expert in risk management and compliance.



### Online Training

Recorded on-demand training and live webinars.

[More »](#)



### In-house Training

Engaging training classes and workshops.

[More »](#)



### Social Engineering

Developing the human perimeter to deal with cyber threats.

[More »](#)



### For the Board

Short and comprehensive briefings for the board of directors.

[More »](#)



### Assessments

Open source intelligence (OSINT) reports and recommendations.

[More »](#)



### High Value Targets

They have the most skilled adversaries. We can help.

[More »](#)

## Cyber security training

### Overview

The world of cyber security and privacy is constantly changing. Today, effective cyber security programs involve the entire organization and not only the IT or the information security teams. Employees that have access to critical assets of an organization, have become primary targets of cyber attacks. Those that have access to technology and organizational assets are also responsible for the protection of those assets. Are they fit and proper to handle this responsibility? Do they have the awareness and skills necessary to meet these expectations?

Our training programs have the objective to help managers and employees not only understand the cyber security threats, but also their responsibility towards protecting the assets they handle. We explain how to proactively



apply good cyber security practices, how to identify threats and attacks, and what to do to protect themselves and their organizations. Cyber security is a shared responsibility.

## **Duration**

We tailor each program to the needs of each client. We can provide trainings as short as one hour, but we can also deep dive into our topics for one or two days. The duration depends entirely on the needs, the agreed content of the program, and the case studies.

## **Our Education Method**

In the core of our training approach is to ensure that our delivery is relatable, engaging, and interesting. We always make cyber security training an exciting adventure for our attendees. Our instructors have trained thousands of employees across the globe and have the skills and experience necessary to ensure that our attendees will enjoy the process while they learn. Our training programs may have workshop elements that get everyone involved.

## **Our Instructors**

They are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

## **Our websites include:**

### **a. Sectors and Industries.**

1. Cyber Risk GmbH - <https://www.cyber-risk-gmbh.com>
2. Social Engineering Training - <https://www.social-engineering-training.ch>
3. Healthcare Cybersecurity - <https://www.healthcare-cybersecurity.ch>
4. Airline Cybersecurity - <https://www.airline-cybersecurity.ch>
5. Railway Cybersecurity - <https://www.railway-cybersecurity.com>
6. Maritime Cybersecurity - <https://www.maritime-cybersecurity.com>
7. Transport Cybersecurity - <https://www.transport-cybersecurity.com>

8. Transport Cybersecurity Toolkit - <https://www.transport-cybersecurity-toolkit.com>
9. Hotel Cybersecurity - <https://www.hotel-cybersecurity.ch>
10. Sanctions Risk - <https://www.sanctions-risk.com>
11. Travel Security - <https://www.travel-security.ch>

## **b. Understanding Cybersecurity.**

1. What is Disinformation? - <https://www.disinformation.ch>
2. What is Steganography? - <https://www.steganography.ch>
3. What is Cyberbiosecurity? - <https://www.cyberbiosecurity.ch>
4. What is Synthetic Identity Fraud? - <https://www.synthetic-identity-fraud.com>
5. What is a Romance Scam? - <https://www.romance-scams.ch>
6. What is Cyber Espionage? - <https://www.cyber-espionage.ch>
7. What is Sexspionage? - <https://www.sexspionage.ch>

## **c. Understanding Cybersecurity in the European Union.**

1. The NIS 2 Directive - <https://www.nis-2-directive.com>
2. The European Cyber Resilience Act - <https://www.european-cyber-resilience-act.com>
3. The Digital Operational Resilience Act (DORA) - <https://www.digital-operational-resilience-act.com>
4. The Critical Entities Resilience Directive (CER) - <https://www.critical-entities-resilience-directive.com>
5. The Digital Services Act (DSA) - <https://www.eu-digital-services-act.com>
6. The Digital Markets Act (DMA) - <https://www.eu-digital-markets-act.com>

7. The European Health Data Space (EHDS) - <https://www.european-health-data-space.com>
8. The European Chips Act - <https://www.european-chips-act.com>
9. The European Data Act - <https://www.eu-data-act.com>
10. European Data Governance Act (DGA) - <https://www.european-data-governance-act.com>
11. The Artificial Intelligence Act - <https://www.artificial-intelligence-act.com>
12. The European ePrivacy Regulation - <https://www.european-eprivacy-regulation.com>
13. The European Cyber Defence Policy - <https://www.european-cyber-defence-policy.com>
14. The Strategic Compass of the European Union - <https://www.strategic-compass-european-union.com>
15. The EU Cyber Diplomacy Toolbox - <https://www.cyber-diplomacy-toolbox.com>

You may contact:

George Lekatis  
General Manager, Cyber Risk GmbH  
Dammstrasse 16, 8810 Horgen  
Phone: +41 79 505 89 60  
Email: [george.lekatis@cyber-risk-gmbh.com](mailto:george.lekatis@cyber-risk-gmbh.com)  
Web: [www.cyber-risk-gmbh.com](http://www.cyber-risk-gmbh.com)

## Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of Cyber Risk GmbH.

Readers will make their own determination of how suitable the information is for their usage and intent. Cyber Risk GmbH expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

Cyber Risk GmbH and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. Cyber Risk GmbH does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of interpretative;
- does not prejudice the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudice the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

*Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.*

General Terms and Conditions for all visitors to the Cyber Risk GmbH websites, and all legal transactions made through the Cyber Risk GmbH websites (hereinafter “GTC”):

<https://www.cyber-risk-gmbh.com/Impressum.html>