



Cyber Risk and Compliance News and Alerts, February 2024

I do not always agree with the judgments of the Court of Justice of the European Union, but in risk and compliance management we have to learn, understand, and of course comply, if we serve EU citizens.



In Bulgaria, an **entry** was made in the police records concerning a person, for failing to tell the truth as a witness. That person was ultimately found guilty of that offence and given a one year suspended sentence.

After serving that sentence, that person was legally rehabilitated. He subsequently **applied to be removed** from the police records. Under Bulgarian law, the data relating to him are retained in those records and may be processed by the authorities, who have access to them **without any time limit other than his death**.

His application was **rejected** on the ground that a final criminal conviction, even after legal rehabilitation, is not one of the grounds for removal of the entry from the police records.

On appeal, the Bulgarian Supreme Administrative Court referred questions to the Court of Justice. In its judgment, the Court of Justice holds that the general and indiscriminate storage of biometric and genetic data of persons convicted of an intentional offence, until their death, is **contrary** to EU law.

Under EU law, national legislation must lay down an obligation for the data controller to **review** periodically whether that storage is **still necessary** and to

grant the data subject the right to have those data erased if that is no longer the case.

In Article 4(1)(c) and 4(1)(e) of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, we have:

Article 4(1)(c): Member States shall provide for personal data to be adequate, relevant, and **not excessive** in relation to the purposes for which they are processed.

Article 4(1)(e): Member States shall provide for personal data to be kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which they are processed.

Under EU law, national legislation must lay down an obligation for the data controller to review periodically whether that storage is still necessary and to grant the data subject the right to have those data erased if that is no longer the case.

This is an interesting judgment, from the Court of Justice of the European Union. I find interesting the fact that the police is not **obliged to remove** entries from the police records, but is **obliged to “review** periodically whether that storage is still **necessary** and to grant the data subject the right to have those data erased if that is no longer the case”. The approach “we keep everything until you die” is not legal in the EU, but with some more paperwork we may have the same result, if **necessary**, of course.

Francis of Assisi has said: “Start by doing what's necessary; then do what's possible; and suddenly you are doing the impossible”. This is not legal advice.

Read more at number 4 below.

We have four important Draft Implementing Technical Standards that make DORA (the Digital Operational Resilience Act, Regulation (EU) 2022/2554) a more serious and more difficult to implement regulation, especially for entities that use ICT **third-party** service providers from non-EU countries.

We read the first words at the new JC 2023 85:

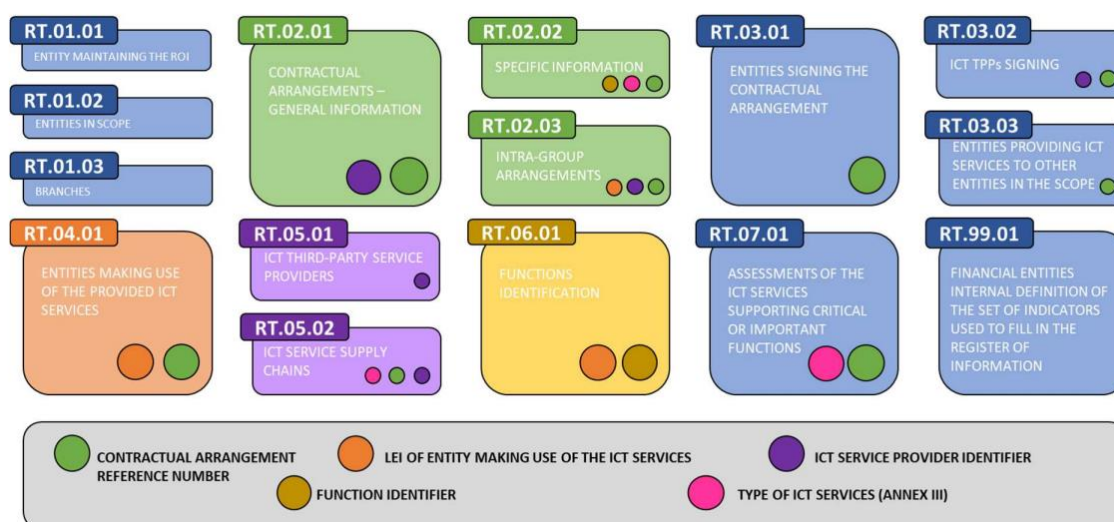
“One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to ensure a sound monitoring of ICT **third-party** risk in the financial sector. The conduct of such monitoring should follow a strategic approach to ICT third-party risk formalised through a dedicated ICT third-party risk strategy adopted by the management bodies of the financial entities (FEs), rooted in a **continuous** screening of all ICT third-party dependencies.”

In DORA it looked easier. According to Article 28(3), financial entities (FEs), must maintain and update at entity level, at sub consolidated and consolidated levels, a **register** of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

FEs must make available to the competent authorities (CAs) the register of information along with any information deemed necessary to enable the effective supervision of FEs, and for acquiring a broader understanding of the ICT dependencies of FEs with a view to support the Oversight Framework of critical ICT third-party service providers.

Now, in the Draft Implementing Technical Standards, it is **way more complex** and difficult.

Illustration 1: Structure of the Register of Information



The register of information is composed of **15 templates**. Illustration 1 shows the relational structure between the templates highlighting some of the relational keys used to link one template to another. You must read 113 pages, of course, to move from the illustration to a proper understanding of the regulatory obligation.

In 113 pages, the term “third-party” is repeated 273 times. The term “third-party service provider” is repeated 218 times. And this is just one of the four papers.

Read more at number 9 below.



I found this risk category (or this combination of risk categories) very interesting:

“**Digitalisation & cyber risks** - The category aims at monitoring potential **financial stability** risks related to an increased digitalisation, which exposes the IORP sector to risks from a digital operational resilience perspective (i.e. cyber security risks).”

This is part of the first (and very important) *Risk Dashboard on Institutions for*

Occupational Retirement Provisions (IORPs), from the European Insurance and Occupational Pensions Authority (EIOPA).

February 2024 IORP Risk Dashboard

























Risks	Level	Trend (Past 3 months)	Outlook (Next 12 months)
Digitalisation & cyber risks			

The Risk Dashboard includes a set of risk indicators covering “**traditional** risk categories, such as market and credit risks, liquidity risks, reserve & funding risks,” as well as “**emerging** threats like ESG and cyber risks”.

The **Macro Risks** category “depicts developments in the macro-economic environment that could impact the IORP sector. This category is based on **publicly available** data on macro variables that may be used for broader macroprudential monitoring and analysis.” I was thinking about Macro Intelligence and Macro OSINT experts for the quantification of risks, and actuaries reading intelligence reports.

According to the report, cyber risks are **emerging** threats. **Francis Bacon** believed that truth **emerges** more readily from **errors** than from confusion. But **Marcus Tullius Cicero** has also said that any man can make mistakes, but only an idiot persists in his **errors**. I am sure that he was not speaking about errors in the cyber domain.

February 2024 IORP Risk Dashboard

Risks	Level	Trend (Past 3 months)	Outlook (Next 12 months)
Macro risks			
Credit risks			
Market & asset return risks			
Liquidity risks			
Reserve & funding risks (DB Schemes)			
Concentration risks			
ESG related risks			
Digitalisation & cyber risks			

Read more at number 10 below.

Heracitus believed that there is nothing permanent except **change**.

Confucius has said that only the wisest and stupidest of men never **change**.

Changes are inherently risky. Fortunately, we have change management, where we acknowledge, anticipate, and manage risk. But what if we have “**accelerated innovation**”? This is accelerated change.

I have read carefully the *2024 Joint Cyber Defense Collaborative (JCDC) Priorities* from the Cybersecurity and Infrastructure Security Agency (CISA). This collaborative was established over two years ago to drive unified efforts across public and private partners, to achieve the most important cybersecurity outcomes. We read:

Anticipate Emerging Technology and Risks: Innovation can help to close off entire avenues of attack but may also create new cybersecurity risks. Our priorities in this focus area center on JCDC’s work with the cybersecurity community to support **accelerated innovation** in cyber defense and reduce known and suspected risks posed by the deployment of emerging technologies.

Then, we read:

Decrease the risk posed by Artificial Intelligence (AI) to critical infrastructure. In alignment and coordination with CISA’s Roadmap for Artificial Intelligence, JCDC will **work to decrease** the likelihood and impact of AI-related threats and vulnerabilities to critical infrastructure providers.

Lucius Annaeus Seneca, the stoic philosopher of Ancient Rome, was wrong. He has said: “Nothing is so wretched or foolish as to **anticipate** misfortunes. What madness is it to be expecting evil before it comes.” Seneca would never pass a risk management exam.

I agree with CISA. We must anticipate emerging technology and risks and support accelerated innovation. Perhaps it is time for an Accelerated Change Management book. No, I am not going to write it.

Read more at number 2 below.

We have some important developments in Switzerland. According to the Swiss Federal Department of Defence, Civil Protection and Sport, the Swiss Federal Council **approved** the report on strengthening the defence capability of the Armed Forces and deepening international cooperation.

The Report on Defence Capability and Cooperation addresses postulates submitted by the Council of States Security Policy Committee SPC-S (23.3000) and Council of States member Josef Dittli (23.3131). The report sets out how Switzerland intends to strengthen the defence capabilities of its Armed Forces and achieve closer, institutionalised cooperation with NATO while maintaining its neutrality.



Bern, 31. Januar 2024

Verteidigungsfähigkeit und Kooperation

Bericht des Bundesrates in Erfüllung des Postulats 23.3000 SiK-S vom 12. Januar 2023 und des Postulats 23.3131 Dittli vom 14. März 2023

In its supplementary report to the Security Policy Report of September 2022, the Federal Council stated that in view of the significant deterioration in the security situation there was a need to strengthen Switzerland's defence capability. In addition, security and defence policy will be geared more consistently to international cooperation, especially with NATO, the EU and neighbouring countries.

Strengthening the defence capability of the Armed Forces

Switzerland's military capability development is focused on improving defence. Hybrid methods of warfare that combine various means of warfare including armed conflict are becoming increasingly common. The Armed Forces must be able to meet these diverse threats now and in the future. Their capabilities will be developed in a broad and balanced manner; however, in light of the worsening security situation, a particular focus will be placed on defence capabilities. Services related to supporting civilian authorities and military peacekeeping continue to be part of the Armed Forces' mandate and will also be developed.

In responding to Postulate 23.3000, the Federal Council is setting out the conceptual basis for the 2024 Armed Forces Dispatch, which will enable the Federal Assembly to shape the longer-term development of the Armed Forces more strongly than before. The Federal Council will decide on this in February.

Intensifying cooperation

As a neutral state, Switzerland strives to ensure its defence independently. If attacked, however, it is free to organise its defence with other states. To this end,

interoperability should be extended without creating obligations, dependencies or constraints that would conflict with neutrality.

The current institutional framework for cooperation with NATO, the Partnership for Peace, also allows cooperation in the area of defence to be intensified in the future. More than in the past, cooperation should focus on aspects that are important for strengthening defence capabilities.

Since cooperation is a give and take, and the readiness of partners is required, Switzerland will make substantial contributions, for instance by participating in multinational centres of excellence and in military peace support in conflict areas.

Need for legislative amendments to be examined

The report sets out specific measures to strengthen defence capabilities and intensify multilateral cooperation. Based on its conclusions, the Federal Council will consider whether or not to examine these measures in greater detail and decide on their implementation.

This may include enabling conscript units to provide training services on training grounds in neighbouring countries or in multilateral exercises. It will also consider whether to deploy individual conscripts outside conventional military peace support operations for missions in multilateral staff structures or for training missions for third parties.

The clarifications will also cover military mobility, in particular rules on the possible transit of partner nations' military units.

Ob die Schweiz in einen Krieg verwickelt wird, dürfte auch von ihrer Fähigkeit abhängen, ihr Territorium zu verteidigen. Dazu muss die Armee fähig sein, einen Gegner von einem bewaffneten Angriff abzuhalten, und zwar in allen Wirkungsräumen, d. h. **am Boden, in der Luft, im Cyberraum, im elektromagnetischen Raum und im Informationsraum**. Dies beinhaltet auch, gegnerisches Angriffspotenzial auf grössere Distanz ausschalten zu können. Einem potenziellen Aggressor muss unmissverständlich aufgezeigt werden, dass die Armee einem bewaffneten Angriff entschlossen und wirksam entgegentreten würde. Ob die Verteidigungsfähigkeit glaubwürdig ist, liegt letztlich immer im Ermessen eines potenziellen Gegners.

3.2.4 Fähigkeiten im **Cyber- und elektromagnetischen Raum**

Aktionen im Cyberraum gehören heute nicht nur zu jedem Konfliktbild, sie sind alltäglich geworden. Die Technologien und Systeme entwickeln sich mit einer enormen Geschwindigkeit. Das neu konstituierte Kommando Cyber in der Gruppe Verteidigung soll in Zukunft den Wissens- und Entscheidungsvorsprung über alle Lagen und in allen Wirkungsräumen anstreben. Weiter soll es durch gezielte Aktionen im Cyber- und im elektromagnetischen Raum die gegnerische Führungsfähigkeit beeinträchtigen können.

Im Fähigkeitsaufbau im Cyber- und elektromagnetischen Raum geht es hauptsächlich darum, die notwendigen Fachkräfte und Expertise zu gewinnen, zu binden und weiterzubilden. Um die Wirkung im Cyber- und elektromagnetischen Raum zu verbessern, sind neben der Bereitstellung ausreichender Rechenkapazitäten insbesondere Massnahmen zum Schutz der eigenen Informations- und Telekommunikationssysteme erforderlich. Dadurch kann die Resilienz der eigenen Systeme und die Abwehr von Cyberangriffen auf militärische Infrastrukturen verbessert werden. Die weitere Fähigkeitsentwicklung sieht vor, zusätzliche Fähigkeiten im Bereich der elektronischen Kriegführung aufzubauen, namentlich zur Aufklärung und Störung von Signalübertragungen unterschiedlicher Art.



Verteidigungsfähigkeit und Kooperation

Bericht des Bundesrates



The report:

<https://www.news.admin.ch/newsd/message/attachments/85931.pdf>

We have a very interesting report from the Swiss National Cyber Security Centre:

Social engineering in the gaming community

The NCSC is currently receiving reports of several video game-related websites spreading malware. These sites are specifically designed to trap players who are trying to cheat games. In video games, the temptation to outdo your opponent or improve the gaming experience often leads players to seek unorthodox solutions:

‘Mods’, short for modifications, are programmes that are used to add new functions to the game or enable actions that were not originally intended. These can be aesthetic adjustments or significant changes to the gaming experience.

‘Cheats’ are ways of gaining unfair advantages by circumventing the normal rules and challenges of the game.

Players usually take the search engine route and combine the name of the game with terms such as 'mods', 'hack' or 'cheat'. These searches lead via developer portals to websites that claim to offer simple ways to achieve **gaming superiority**.

The screenshot shows a GitHub search page for the topic '# palworld-hack'. The page displays 25 public repositories matching the search. The top repository is 'palworld-hack' by 'matt-palworld', which has 139 stars and is updated last week. It features a banner with a yellow Pal character and the text 'PALWORD HACK'. Below the banner, there are tabs for 'world', 'battle', 'Other', 'Debug', 'Settings', and 'About'. A list of features is shown: 'Speed Modifier', 'Peeking', 'Auto-Dialogue', and 'Invisibility'. The repository description includes 'Code', 'Issues', and 'Pull requests' tabs, and a list of related repositories such as 'palworld-dedicated-server', 'palworld-crack', 'palworld-mod', 'palworld-speedhack', 'palworld-esp', 'palworld-instant-crafting', 'palworld-instant-build', 'palworld-instant-craft', 'palworld-instant-noclip', 'palworld-instant-fly', 'palworld-mod-menu', 'palworld-cheat-free-download', 'palworld-wh', 'palworld-radar', and 'palworld-instant-crafting-2024'. The second repository is 'palworld-hack' by 'matt-palworld', which has 1 star and is updated 3 weeks ago. It features a banner with a character and the text 'PALWORD'. Below the banner, there are tabs for 'Code', 'Issues', and 'Pull requests'. The repository description includes 'Do you want to gain a decisive advantage in Palworld? Phoenix is your faithful companion!' and a list of related repositories such as 'palworld-dedicated-server', 'palworld-crack', 'palworld-trainer', 'palworld-cheat', 'palworld-mod', 'palworld-speedhack', 'palworld-esp', 'palworld-bot', 'palworld-infinite', 'palworld-instant-crafting', 'palworld-godmode', 'palworld-script', 'palworld-craft', 'palworld-instant-build', 'palworld-instant-craft', 'palworld-instant-noclip', 'palworld-instant-fly', 'palworld-zero-weight', and 'palworld-no-item-weight'.

Risks

The search for advantages in video games with the help of such mods and hacks often leads players to websites where they are asked to download files that are misleadingly advertised as harmless programmes or tools.

The download usually takes place via well-known file hosting websites. This often involves a password-protected ZIP archive. Sometimes it is also possible to download the ZIP archive directly from the website itself.

There are often warning signals that should have your alarm bells ringing. The use of a password-protected ZIP file is reminiscent of methods used to spread malware. If a malicious file is password-protected, security measures such as virus scanners may no longer be effective.

What is even more worrying is that the installation instructions often require users to deactivate anti-virus software 'only during installation' along with any active VPN services. After downloading, users are asked to open the archive and execute the file.

Analysing such files reveals that they contain malware. In most cases, this malware either enables access to the system from outside (by the fraudsters) or steals information from the local device and transfers it to systems controlled by the fraudsters. Both of these threats jeopardise the victim's data and computer security.

For example, intrusions into e-banking could result in significant financial losses, or the user's accounts could be hijacked (email, social media, etc.). If that device is used by several members of a family, the impact will be great.

Precautions you should take, from the Swiss National Cyber Security Centre

- Only download software from trustworthy and official sources. This significantly reduces the risk of inadvertently installing malware.
- Do not just click on the first link that comes up in a search. The first hits are often paid search results. Not only companies, but also fraudsters pay to appear at the top of the results page.
- If the device is used by several family members, individual user accounts should be set up. In contrast to the privileged Administrator account, you cannot install programmes with simple user accounts. An ordinary user must request administrator rights in order to install a programme. This allows a certain degree of control over the use of the computer.
- Enable two-factor authentication: Using two-factor authentication adds an extra layer of security to your online accounts, making unauthorised access more difficult – even if the password has been leaked.
- If you suspect that your system has been compromised, have it cleaned

with the help of a specialist. The safest thing to do is to reset the system.

- If you suspect that fraudsters have had access to your passwords, it is essential to change all passwords immediately.
- Make regular backups of your system. In the event of a malware infection, you can ensure that your data is not lost for good.
- Inform yourself about current cyber security threats and scams. Raising awareness is an important pillar in the fight against cybercrime.

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
 Web: www.cyber-risk-gmbh.com

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

Our reading room: https://www.cyber-risk-gmbh.com/Reading_Room.html



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

1. Christina Lekati, interview, Schweizer Radio und Fernsehen (SRF): "Social Engineers und ihr Lieblingsnetzwerk".

Beim Social Engineering geht es darum, Menschen zu manipulieren, um an Infos oder Geld zu kommen. Kaum ein Hackerangriff kommt heute ohne eine gute Portion «Human Hacking» aus. Wie funktioniert es, was kann man dagegen tun und welche Rolle spielt LinkedIn?

<https://www.srf.ch/audio/digital-podcast/social-engineers-und-ihr-liebblingsnetzwerk?id=12484536>

SRF News Sport Meteo Kultur Dok Wissen TV

JETZT HÖREN DOWNLOAD + ABONNIEREN TEILEN

Der Podcast im Überblick:

- (00:00:50) Social Engineering
- (00:11:05) Christina Lekati, wie funktioniert Social Engineering?
- (00:20:37) LinkedIn
- (00:35:22) Christina Lekati, was kann man gegen Social Engineering tun?

Links:

- InsiderThreats bei Darknet Diaries (Fall 1 ab 18:37, Fall 2 ab 35:55): <https://darknetdiaries.com/episode/122/>
- Christina Lekati am Insomnihack: https://www.youtube.com/watch?v=5fBJ0xnd_XI
- Christina Lekati bei Hacktivity: <https://www.youtube.com/watch?v=DBZ69AsSFn0>
- Christina Lekati zur Kill-Chain: <https://feedly.com/ahead/posts/social-engineering-kill-chain-predicting-minimizing-and-disrupting-attack-verticals>

Number 1 (Page 16)

Revised Implementing Guidelines of the Cyber Diplomacy Toolbox
ENISA Single Programming Document 2024 – 2026

*Number 2 (Page 20)*

2024 Joint Cyber Defense Collaborative (JCDC) Priorities

*Number 3 (Page 23)*

Italian Data Protection Authority
ChatGPT: Italian DPA notifies breaches of privacy law to OpenAI

*Number 4 (Page 25)*

Judgment of the Court in Case C-118/22
Right to erasure: the general and indiscriminate storage of biometric and genetic data of persons convicted of criminal offences, until their death, is contrary to EU law

*Number 5 (Page 27)*

Artificial intelligence in central banking
Douglas Araujo, Sebastian Doerr, Leonardo Gambacorta, Bruno Tissot

*Number 6 (Page 29)*

INTERPOL-led operation targets growing cyber threats
Phishing, malware and ransomware incidents at heart of Operation Synergia



Number 7 (Page 31)

Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Number 8 (Page 34)

ENISA Single Programming Document 2024 – 2026



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Number 9 (Page 38)

The first set of final draft technical standards under the Digital Operational Resilience Act (DORA).



Number 10 (Page 41)

EIOPA's newly launched IORP Risk Dashboard highlights market and asset return risks as main concerns for occupational pension funds



Number 11 (Page 44)

Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies



Number 12 (Page 48)

Piloting new ways of protecting Android users from financial fraud

Google Security Blog

*Number 13 (Page 52)***Brazilian Federal Police against Grandoreiro Banking Trojan***Number 14 (Page 54)***Discovering Unknome Function (DUF)***Number 15 (Page 56)***The near-term impact of AI on the cyber threat**

An NCSC assessment focusing on how AI will impact the efficacy of cyber operations and the implications for the cyber threat over the next two years.

*Number 16 (Page 58)***The U.S. AI Safety Institute Consortium (AISIC).***Number 17 (Page 62)***U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure***Number 18 (Page 66)***AI in Support of StratCom Capabilities***Number 19 (Page 69)***Former CIA Officer Joshua Adam Schulte Sentenced To 40 Years In Prison For Espionage And Child Pornography Crimes**

Number 20 (Page 73)

AI breakthrough creates images from nothing

Innovative framework that generates images from nothing can enable new scientific applications



*Number 1**Revised Implementing Guidelines of the Cyber Diplomacy Toolbox*
ENISA Single Programming Document 2024 – 2026

In addition, to support Member States (MS) and European institutions, bodies and agencies (EUIBAs) in deterring and responding to cyberattacks from non-EU countries, the EU adopted a framework for a joint EU diplomatic response to malicious cyber activities, in the Council conclusions of 19 June 2017.

The European External Action Service (EEAS) recently published updated implementation guidelines for the cyber diplomacy toolbox detailing specific steps MSs could take.

The guidelines underline the importance of measures taken by MSs under the NISD to improve resilience, the role of ENISA in establishing information-sharing channels with industry to gain situational awareness, and the importance of cooperation between the Cyber Crisis Liaison Organisation Network (EU-Cyclone), the Computer Security Incidence Response Team (CSIRT) network, ENISA, the Computer Emergency Response Team for EU institutions, bodies and agencies (CERT-EU) and the European Union Agency for Law Enforcement Cooperation, and EEAS Single Intelligence Analysis Capacity, to ensure that internal and external EU initiatives are coherent.

Revised Implementing Guidelines of the Cyber Diplomacy Toolbox

1. In 2017, the EU adopted the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') to increase the EU's ability to prevent, discourage, deter and respond to malicious cyber activities.

With the adoption and implementation of the Cyber Diplomacy Toolbox, the EU took an important step towards a more secure and stable cyber domain, providing an answer to the increased willingness and ability of state and non-state actors to pursue their strategic objectives through malicious cyber activities.

In the last few years, however, and particularly since Russia's unjustified and unprovoked war of aggression against Ukraine, the EU and its Member States have seen a significant corrosion of international security, including in cyberspace.

Malicious cyber activities against critical infrastructure, including through the use of ransomware and wipers, as well as targeting of supply chains and **cyber-espionage**, including intellectual property theft activities or similar types of cyber-espionage, are increasingly more sophisticated, with disruptive and destructive effects posing a systemic threat to the EU's security, economy, democracy and society at large.

Such activities can also be used to conduct or enable **foreign information manipulation and interference (FIMI)**.

2. The increase of malicious cyber activities over recent years has provided lessons for the EU, its Member States and their partners on how to enhance cyber resilience, as well as on how to design and implement an appropriate response, including through the use of diplomatic measures.

With the unstable cyber threat landscape, the EU and its Member States need to step up their ability to strengthen situational awareness, prevent, discourage, deter and respond to malicious cyber activities, ensure solidarity and mutual assistance and enforce the United Nations framework for responsible state behaviour in cyberspace endorsed by consensus by the United Nations General Assembly, grounded in the application of international law in cyberspace.

3. At the same time, cyber diplomacy and cyber issues have gained momentum and importance as a component of EU Common Foreign and Security Policy (CFSP). With the pervasiveness and fast pace of digitalization and the magnitude of cyber challenges and of the threat landscape, cyber diplomacy needs to be strengthened and could be further complemented by making use of other policies and activities in order to effectively contribute and promote the European vision of a global, open, free, stable and secure cyberspace, grounded in the rule of law.

Strengthening global partnerships as well as pro-active, preventive and constructive diplomatic action is increasingly needed.

In this context, a more sustained, tailored, coherent and coordinated EU approach is necessary to advance a comprehensive and effective EU action against malicious cyber activities, large-scale cybersecurity incidents and an accumulation of those activities, as well as to persistent cyber threat actors that conduct, support or condone malicious cyber activities targeting the EU, its Member States and their partners.

4. Building on the main principles of the framework as set out in the 2017 Council conclusions on the Cyber Diplomacy Toolbox, the Council conclusions on the EU Cyber Posture of 2022, and the lessons learned from diplomatic responses and cyber exercises undertaken since 2017, this document responds to the need to further strengthen the EU Cyber Diplomacy Toolbox as expressed in the 2021 Council conclusions on the EU Cybersecurity Strategy, the 2022 Strategic Compass, the 2022 Council conclusions on the EU Cyber Posture and the 2023 Council Conclusions on the Joint Communication on the EU Policy on Cyber Defence.

The document also relates to the 2022 Council conclusions on EU Digital Diplomacy, specifically taking into account that the EU external policies on digital and cyber need to be coherent and mutually reinforcing.

This document outlines the revised implementing guidelines to further enhance situational awareness, ensure a strategic approach to persistent cyber threat

actors, provides additional response measures, and further enables timely decision-making and stronger cooperation with partners.

In addition, it includes guidance for the attribution of malicious cyber activities, strategic communications, as well as linkages to other EU toolboxes and crisis management mechanisms and activities, while preserving Member States competences on the matter.

5. Core to the EU Cyber Posture are the following five main components: its cyber resilience and capacities to prevent and protect against malicious cyber activities; its solidarity and comprehensive crisis management capabilities; its vision of a global, open, free, stable and secure cyberspace, with international law, the rules-based order and with the UN framework for responsible state behaviour in cyberspace at its centre; its strong global partnerships, including through capacity building efforts in third countries; and its ability to prevent, discourage, deter and respond to threat actors seeking to deny or disrupt our secure and open access to cyberspace as well as critical functions, and affect the EU's strategic interests, including the security of its partners.

6. In line with this posture, the Cyber Diplomacy Toolbox is part of the EU's full spectrum approach to resilience, response, conflict prevention, cooperation and stability in cyberspace.

It should be seen as complementary to existing and continuous cyber diplomacy engagement to advance conflict prevention, cooperation and stability in cyberspace, including substantive EU capacity building support to third countries.

In addition it complements the EU effort to enhance cyber resilience, prevent and tackle cybercrime as well as adds value to the development of the wider EU cyber cooperation, solidarity and crisis management ecosystem.

7. The joint EU diplomatic response builds on the UN framework for responsible state behaviour in cyberspace grounded in the reports of the UN Groups of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security and Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies, which concluded that existing international law is applicable to the use of cyber operations, and outlines eleven voluntary, non-binding norms of responsible State behaviour in cyberspace.

Through the use of diplomatic measures, the EU actively supports the global application of the UN framework of responsible state behaviour, contributes to its enforcement, and enhances transparency and predictability as regards states' conduct in cyberspace.

The use of confidence-building measures (CBMs) at regional and international level, notably in those of the Organization for Security and Cooperation in Europe (OSCE), could further reduce the risk of a potential conflict and misunderstanding between States as to their conduct in cyberspace.

8. The measures in the Cyber Diplomacy Toolbox could be used in tandem with other Union measures such as those reflected in the Network and Information Security Directive, the Directive on Attacks against Information Systems, as well as measures by EUIBAs, including by the EU Cybersecurity Agency (ENISA) and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), and EU networks, in line with their legal mandates and institutional autonomy, to prevent, discourage, deter and respond to and immediately recover from malicious cyber activities which may originate from a state or non-state actor or transit through a States' territory.

The measures could inter alia be used to encourage a State to ensure that its territory is not used for malicious cyber activities, or to induce a State to refrain from, or cease activities that are undertaken under its direction or its control.

To read more:

<https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2024-2024>

<https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf>

<https://www.cyber-diplomacy-toolbox.com>

This website belongs to Cyber Risk GmbH.

*Number 2***2024 Joint Cyber Defense Collaborative (JCDC) Priorities****CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

The Joint Cyber Defense Collaborative (JCDC) was established over two years ago to drive unified efforts across public and private partners to achieve our most important cybersecurity outcomes.

Each year, hundreds of JCDC partner organizations provide insight, expertise, and perspective to help identify our collective priorities for the coming year.

We are excited to introduce our 2024 Priorities.

Of course, these priorities are not CISA's alone; rather, they reflect shared goals across government, industry, and international partners that will enable cohesive planning and collaboration.

While these Priorities build on our **2023 Planning Agenda**, they also represent a critical step in JCDC's maturation.

The 2023 JCDC Planning Agenda: <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2023-jcdc-planning-agenda>

2023 JCDC Planning Agenda



The Joint Cyber Defense Collaborative (JCDC) is proud to announce its 2023 Planning Agenda—a major milestone in the collaborative's continued evolution and maturation. Economic prosperity, national defense, and public health and safety depend on interconnected digital technologies. Widespread security flaws and configuration missteps in these technologies create opportunities for malicious actors to

steal information, destroy valuable data, and cut off access to critical goods and services.

JCDC's planning agenda addresses these important and complex security challenges.

For the first time, we are aligning our priorities under **three broad focus areas**, which in turn will enable alignment of resources and strategic direction.

(1) Defend Against Advanced Persistent Threat (APT) Operations: Last year's ODNI Annual Threat Assessment makes clear the threat posed by malicious cyber actors, particularly those affiliated with the People's Republic of China (PRC).

No longer can our cyber defense focus on espionage and data theft; we must now posture to protect our country and allies against destructive attacks designed to cause real-world harm.

Our priorities in this focus area center on JCDC's strategic and operational efforts to counter known and suspected APT attack campaigns targeting entities that support national critical functions.

- Discover and defend against malicious abuse by APT actors, particularly those backed by the PRC, on and against U.S.-based infrastructure.
- Prepare for major cyber incidents. CISA, through the JCDC, will finalize and publish the **National Cyber Incident Response Plan (NCIRP)**, in close coordination with interagency and industry partners.

You may visit:

<https://www.cisa.gov/sites/default/files/2023-10/NCIRP-2024-Fact-Sheet-508C.pdf>



OVERVIEW

In 2016, the National Cyber Incident Response Plan (NCIRP) was published to provide a framework for significant cyber incident coordination. A lot has changed over the past eight years, including across the cyber threat landscape and the cyber defense ecosystem, and the NCIRP must evolve accordingly. As directed in the National Cybersecurity Strategy, the Cybersecurity and Infrastructure Security Agency (CISA) is leading the effort to update the NCIRP to provide a modern, agile, flexible framework to enable coherent and repeatable national incident response across the federal government, private sector, and other key partners.

WHAT IS THE NCIRP AND WHY WAS IT CREATED?

The NCIRP was developed in accordance with [Presidential Policy Directive 41 \(PPD-41\) on U.S. Cyber Incident Coordination](#) and describes how the federal government, private sector, and state, local, tribal, territorial (SLTT) government entities will organize to manage, respond to, and mitigate the consequences of significant cyber incidents. The NCIRP leverages principles from the National Preparedness System (NPS) to articulate how the nation responds to and recovers from significant cyber incidents. Alignment with the NPS also allows for significant cyber incident response to integrate with physical incident response in cases where cyber incidents may have physical impacts or vice versa.

(2) Raise the Cybersecurity Baseline: Too many successful intrusions are preventable, the result of inadequate investment in basic practices. Our priorities in this focus area center on JCDC's ability to organize and support efforts that raise the cybersecurity baseline of critical infrastructure entities.

- Help state and local election officials secure their networks and infrastructure against cyber threats as part of CISA's broader election security efforts.
- Measurably decrease the impact of ransomware on critical infrastructure.
- Make measurable progress toward a world where technology is Secure by Design. Even as we urgently work to help organizations implement the most effective cybersecurity measures, we know that scalable change requires a fundamental shift in how technology is designed, built, and maintained. We will continue to drive measurable commitments across the technology ecosystem that reduce the number of defective technology products by design and ensure that strong default settings are the norm.

(3) Anticipate Emerging Technology and Risks: Innovation can help to close off entire avenues of attack but may also create new cybersecurity risks. Our priorities in this focus area center on JCDC's work with the cybersecurity community to support **accelerated innovation** in cyber defense and reduce known and suspected risks posed by the deployment of emerging technologies.

- Decrease the risk posed by Artificial Intelligence (AI) to critical infrastructure. In alignment and coordination with **CISA's Roadmap for Artificial Intelligence**, JCDC will work to decrease the likelihood and impact of AI-related threats and vulnerabilities to critical infrastructure providers.

DHS Cybersecurity and Infrastructure Security Agency Releases Roadmap for Artificial Intelligence

Roadmap Will Guide CISA's Efforts to Manage the Risks and Harness the Opportunities Posed by Artificial Intelligence to Cybersecurity

Released: November 14, 2023

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#)

For CISA's Roadmap for Artificial Intelligence, you may visit:

<https://www.cisa.gov/news-events/news/dhs-cybersecurity-and-infrastructure-security-agency-releases-roadmap-artificial-intelligence>

To read more: <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2024-jcdc-priorities>

Number 3

Italian Data Protection Authority ChatGPT: Italian DPA notifies breaches of privacy law to OpenAI



The Italian DPA (Garante per la protezione dei dati personali) notified breaches of data protection law to OpenAI, the company behind ChatGPT's AI platform.

Following the temporary ban on processing imposed on OpenAI by the Garante on 30 March of last year, and based on the outcome of its fact-finding activity, the Italian DPA concluded that the available evidence pointed to the existence of breaches of the provisions contained in the EU GDPR.

OpenAI may submit its counterclaims concerning the alleged breaches within 30 days.

The Italian Garante will take account of the work in progress within the ad-hoc task force set up by the European Data Protection Framework in its final determination on the case.

To read more: <https://garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020#english>

The temporary ban (31 March 2023)

The Italian SA imposed an immediate temporary limitation on the processing of Italian users' data by OpenAI, the US-based company developing and managing the platform. An inquiry into the facts of the case was initiated as well.

A data breach affecting ChatGPT users' conversations and information on payments by subscribers to the service had been reported on 20 March. ChatGPT is the best known among relational AI platforms that are capable to emulate and elaborate human conversations.

In its order, the Italian SA highlights that no information is provided to users and data subjects whose data are collected by Open AI; more importantly, there appears to be no legal basis underpinning the massive collection and processing of personal data in order to 'train' the algorithms on which the platform relies.

As confirmed by the tests carried out so far, the information made available by ChatGPT does not always match factual circumstances, so that inaccurate personal data are processed.

Finally, the Italian SA emphasizes in its order that the lack of whatever age verification mechanism exposes children to receiving responses that are absolutely inappropriate to their age and awareness, even though the service is

allegedly addressed to users aged above 13 according to OpenAI's terms of service.

OpenAI is not established in the EU, however it has designated a representative in the European Economic Area. It will have to notify the Italian SA within 20 days of the measures implemented to comply with the order, otherwise a fine of up to EUR 20 million or **4% of the total worldwide annual turnover** may be imposed.

The temporary ban: <https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english>

Number 4

Judgment of the Court in Case C-118/22

Right to erasure: the general and indiscriminate storage of biometric and genetic data of persons convicted of criminal offences, until their death, is contrary to EU law



COURT OF JUSTICE
OF THE EUROPEAN UNION

In Bulgaria, an entry was made in the police records concerning a person in the course of a criminal investigation for failing to tell the truth as a witness.

That person was ultimately found guilty of that offence and given a one year suspended sentence.

After serving that sentence, that person was legally rehabilitated. He subsequently applied to be removed from the police records.

Under Bulgarian law, the data relating to him are retained in those records and may be processed by the authorities, who have access to them without any time limit other than his death.

His application was rejected on the ground that a final criminal conviction, even after legal rehabilitation, is not one of the grounds for removal of the entry from the police records.

On appeal, the Bulgarian Supreme Administrative Court referred questions to the Court of Justice.

In its judgment, the Court of Justice holds that the general and indiscriminate storage of biometric and genetic data of persons convicted of an intentional offence, until their death, is contrary to EU law.

The Court notes that the personal data stored in the police records in Bulgaria include, amongst other things, fingerprints, a photograph and a DNA sample taken for profiling purposes.

The records also contain data relating to the criminal offences committed by the data subject and to his or her convictions in that regard.

Those data may be essential for the purposes of verifying whether the data subject is involved in criminal offences other than that in respect of which he or she was convicted by final judgment.

However, such persons do not all present the same degree of risk of being involved in other criminal offences, justifying a uniform period of storage of the data relating to them. Thus, factors such as the nature and seriousness of the offence committed or the absence of recidivism may mean that the risk

represented by the convicted person does not necessarily justify the storage of the data relating to that person in the police records until his or her death.

Consequently, that time limit is appropriate only in specific circumstances which duly justify it. That is not the case where it is applicable generally and indiscriminately to any person convicted by final judgment of an intentional offence.

Under EU law, **national legislation must lay down an obligation for the data controller to review periodically whether that storage is still necessary** and to grant the data subject the right to have those data erased if that is no longer the case.

To read more: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-01/cp240020en.pdf>

<https://curia.europa.eu/juris/documents.jsf?num=C-118/22>

Number 5

Artificial intelligence in central banking

Douglas Araujo, Sebastian Doerr, Leonardo Gambacorta, Bruno Tissot



Key takeaways

1. Central banks have been early adopters of machine learning techniques for statistics, macro analysis, payment systems oversight and supervision, with considerable success.
2. Artificial intelligence brings many opportunities in support of central bank mandates, but also challenges – some general and others specific to central banks.
3. Central bank collaboration, for instance through knowledge-sharing and pooling of expertise, holds great promise in keeping central banks at the vanguard of developments in artificial intelligence.

Long before artificial intelligence (AI) became a focal point of popular commentary and widespread fascination, central banks were early adopters of machine learning methods to obtain valuable insights for statistics, research and policy (Doerr et al (2021), Araujo et al (2022, 2023)).

The greater capabilities and performance of the new generation of machine learning techniques open up further opportunities. Yet harnessing these requires central banks to build up the necessary infrastructure and expertise.

Central banks also need to address concerns about data quality and privacy as well as risks emanating from dependence on a few providers.

This Bulletin first provides a brief summary of concepts in the machine learning and AI space. It then discusses central bank use cases in four areas:

- (i) information collection and the compilation of official statistics;
- (ii) macroeconomic and financial analysis to support monetary policy;
- (iii) oversight of payment systems; and (iv) supervision and financial stability.

The Bulletin also summarises the lessons learned and the opportunities and challenges arising from the use of machine learning and AI.

It concludes by discussing how central bank cooperation can play a key role going forward.

Overview of machine learning methods and AI

Broadly speaking, machine learning comprises the set of techniques designed to extract information from data, especially with a view to making predictions.

Machine learning can be seen as an outgrowth of traditional statistical and econometric techniques, although it does not rely on a pre-specified model or on statistical assumptions such as linearity or normality.

The process of fitting a machine learning model to data is called training.

The criterion for successful training is the ability to predict outcomes on previously unseen (“out-of-sample”) data, irrespective of how the models predict them.

This section describes some of the most common techniques used in central banks, based on the regular stocktaking exercises organised in the central banking community under the umbrella of the BIS Irving Fisher Committee on Central Bank Statistics (IFC).

To read more: <https://www.bis.org/publ/bisbull84.pdf>



Number 6

INTERPOL-led operation targets growing cyber threats

Phishing, malware and ransomware incidents at heart of Operation Synergia



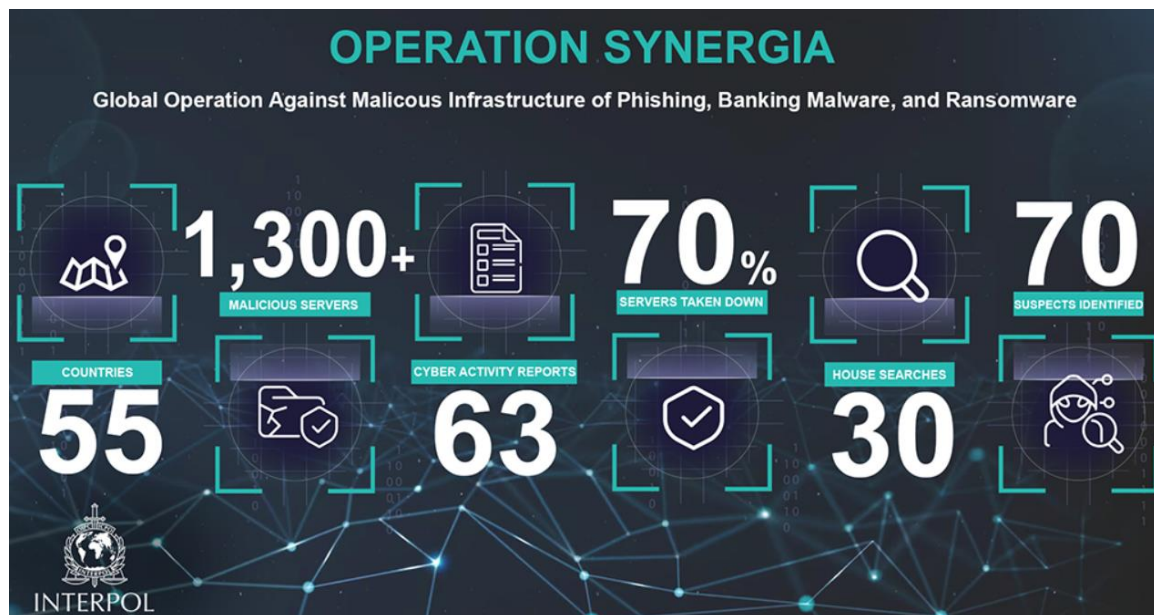
INTERPOL

SINGAPORE – Some 1,300 suspicious IP addresses or URLs have been identified as part of a global INTERPOL operation targeting phishing, malware and ransomware attacks.

Operation Synergia, which ran from September to November 2023, was launched in response to the clear growth, escalation and professionalisation of transnational cybercrime and the need for coordinated action against new cyber threats.

The operation involved 60 law enforcement agencies from more than 50 INTERPOL member countries, with officers conducting house searches and seizing servers as well as electronic devices.

To date, 70% of the command-and-control (C2) servers identified have been taken down, with the remainder currently under investigation.



Operational details

Authorities detained 31 individuals and identified an additional 70 suspects.

- Most of the C2 servers taken down were in Europe, where 26 people were arrested.
- Hong Kong and Singapore Police took down 153 and 86 servers, respectively.
- South Sudan and Zimbabwe reported the most takedowns on the African continent, arresting four suspects.
- Bolivia mobilized a range of public authorities to identify malware and resulting vulnerabilities.
- Kuwait's worked closely with Internet Service Providers to identify victims, conduct field investigations and offer technical guidance to mitigate impacts.

Operation Synergia demonstrated how cybersecurity is most effective when international law enforcement, national authorities, and private sector partners cooperate to share best practices and pro-actively combat cybercrime.

INTERPOL and its Gateway Partners Group-IB, Kaspersky, TrendMicro, Shadowserver and Ad hoc partner Team Cymru provided analysis and intelligence support throughout the operation.

Bernardo Pillot, Assistant Director to INTERPOL Cybercrime Directorate, said: "The results of this operation, achieved through the collective efforts of multiple countries and partners, show our unwavering commitment to safeguarding the digital space. By dismantling the infrastructure behind phishing, banking malware, and ransomware attacks, we are one step closer to protecting our digital ecosystems and a safer, more secure online experience for all."

Participating countries: Albania, Algeria, Australia , Bangladesh, Belarus, Belgium, Benin, Bolivia, Bosnia and Herzegovina, Brazil, Cameroon, Canada, China, Cyprus, Czech Republic, Dominican Republic, Ecuador, Estonia, Eswatini, France, Georgia, Greece, Guyana, India, Ireland, Israel, Kuwait, Latvia, Lebanon, Lichtenstein, Maldives, Mauritius, Moldova, Nepal, Nicaragua, Nigeria, Palestine, Poland, Qatar, Russia, San Marino, Singapore, South Korea, South Sudan, Spain, Sri Lanka, Switzerland, Tanzania, Thailand, Tonga, Tunisia, Türkiye, Uganda, United Arab Emirates, Uruguay, Zimbabwe.

To read more: <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats>

*Number 7***Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities**

The European Commission, ENISA, the EU Agency for Cybersecurity, CERT-EU, Europol and the network of the EU national computer security incident response teams (CSIRTs network), have been closely following the active exploitation of vulnerabilities in the Ivanti Connect Secure and Ivanti Policy Secure Gateway products, commercial virtual private network (VPN) solutions previously known as Pulse Connect Secure.



Following the initial disclosure of two vulnerabilities at the beginning of January, two additional vulnerabilities were disclosed on 31 January 2024, which impact all supported versions of Ivanti Connect Secure and Ivanti Policy Secure Gateway products and make it possible for attackers to run commands on the system. Broader exploitation of the initially disclosed vulnerabilities had been observed already as early as mid-January.

As this is a developing situation, we strongly recommend all organisations to regularly check the guidance provided by the CSIRTs Network members and CERT-EU for the latest assessment and advice. For detailed instructions on how to complete the advised factory reset, organisations may also follow the detailed vendor instructions.

It is crucial for organisations to respond appropriately to the latest developments in order to resume their critical business activities.

The latest advisories published by CSIRTs Network members can be found in their relevant official communication channels.

Organisations may also refer to guidance given by CERT-EU. ENISA maintains an advisory collection under:

<https://github.com/enisaeu/CNW/blob/main/advisories/2024/Multiple-Vulns-Ivanti-Secure-Gateways.md>



CSIRTs Network - Exploitation of Ivanti Connect Secure and Ivanti Policy Secure Gateway Zero-Days	
Date	10-01-2024 (last updated 06-02-2024)
Number	CNW-2024-01
Keywords	Ivanti Connect Secure (formerly known as Pulse Connect Secure) and Policy Secure Gateway
CVE	CVE-2023-46805 , CVE-2024-21887 , CVE-2024-21888 , CVE-2024-21893
Details	The mentioned vulnerabilities impact all supported versions – Version 9.x and 22.x – of Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS). On 31 January, Ivanti disclosed two additional vulnerabilities impacting the Connect and Policy Connect Secure products, CVE-2024-21888 and CVE-2024-21893. These vulnerabilities allow an unauthenticated threat actor to execute arbitrary commands on the appliance with elevated privileges. Zero-day exploitation in the wild seems to have started as early as 03 December, 2023, with broader exploitation starting around mid-January.
Mitigation	It is critically important that organisations take immediate action and respond appropriately to the latest developments in order to resume critical business activities. The application of patches now made available have to conclude a factory reset of the device. However, this will not necessarily resolve a past compromise. Systems should simultaneously be thoroughly analyzed per the details described in the Ivanti KB article. Furthermore, it is important that organisations running ICS VPN appliances review their logs, network telemetry, and Integrity Checker Tool results (past and present) to look for any signs of successful compromise. Initial sets of various indicators have been published by Volexity and Mandiant . For additional details please refer to the specific CNW member advisories referenced below.

ENISA and all relevant EU actors will continue to monitor this threat to contribute to the overall situational awareness at the Union level.

EU Policy

Organisations should be further aware that the EU Cyber Resilience Act (CRA), once in force, will require manufacturers of hardware and software products, including VPN solutions, to follow security-by-design principles throughout the lifecycle of such products.

This includes the remediation of vulnerabilities without delay.

Given their criticality, VPN solutions will be subject to strict conformity assessment requirements.

Resources for mitigate actions

Ivanti recovery instructions: https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US

[Home](#)[All Products](#)[More](#) [Log in](#)

Please note: we have observed the threat actor target the configuration and running cache of the system, which contains secrets important to the operation of the VPN. While we haven't observed this in every instance, out of an abundance of caution, Ivanti is recommending you rotate these secrets after rebuild. Detailed steps on how to rebuild impacted systems and rotate these secrets are documented below.

If exploitation has occurred, we believe it is likely that the threat actor has taken an export of your running configurations with the private certs loaded on the gateway at time of exploit and left behind a Web shell file enabling backdoor future access. We believe the purpose of this Web shell is to provide a backdoor to the gateway after the vulnerability is mitigated, for this reason we are recommending customers revoke and replace certificates to prevent further exploitation after mitigation. Steps for how to revoke and replace the certificates can be found below.

Ivanti expects threat actors to change their behavior after sharing this information. Customers can assume that this information is relevant to activity observed between 01/11 and 01/15. Some additional information that is helpful for defenders:

- The mitigation we have provided blocks the vulnerabilities and the web shell currently being used in the post-advisory activity we are tracking.
- Both the internal and external ICT successfully identifies the post-advisory activity.
- The post-advisory activity that occurred before PoC was released appears to be automated, and we have not observed or had any reports of additional actions taken by the threat actor after deploying the shell and obtaining the configuration.
- We are recommending customers rebuild impacted systems and take actions highlighted below.

To read more: <https://www.enisa.europa.eu/news/joint-statement-on-ivanti>

Number 8

ENISA Single Programming Document 2024 – 2026



Strategy

EMPOWERING COMMUNITIES

Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in MSs and the EU institutions and agencies.

It strives to ensure the complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

CYBERSECURITY POLICY

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives.

Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity must therefore be embedded across all domains of EU policies. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

OPERATIONAL COOPERATION

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyberattacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large-scale and cross-border) cyber-attacks and cyber crisis.

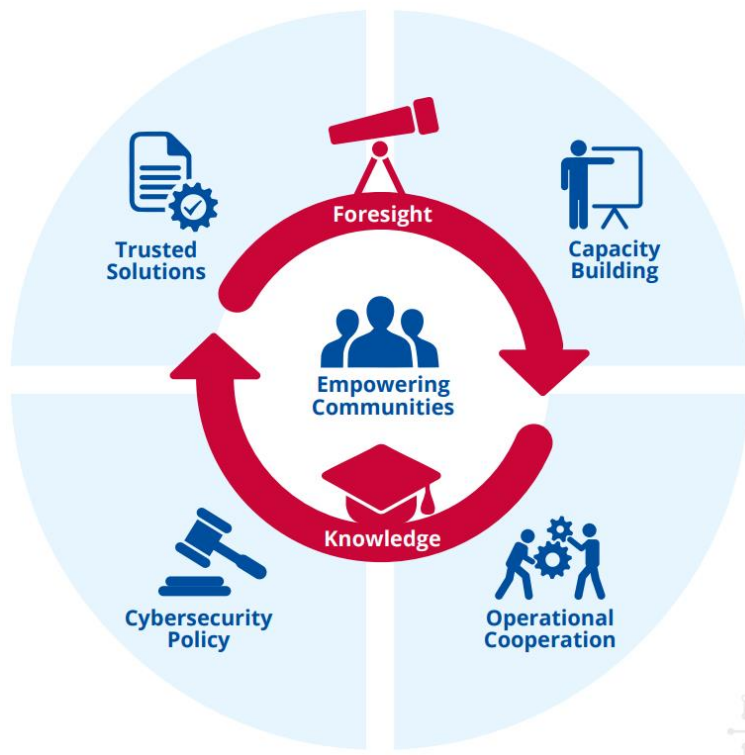
Cross-border interdependencies have highlighted the need for effective cooperation between MSs and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of information and communications technology (ICT) infrastructures and technologies by individuals, organisations and industries is

increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply.

The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the MSs but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.



TRUSTED SOLUTIONS

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating the security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust in digital solutions and the wider digital environment.

FORESIGHT

Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policymakers would be able to define early mitigation strategies that improve the EU's resilience to cybersecurity threats and find solutions to address emerging challenges.

KNOWLEDGE

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge is clearly needed. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

NIS2	Adopted	<p>The European Parliament and the Council of the European Union approved legislation that sets clearer rules for entities in a wider range of sectors. NIS2 reinforces and extends the existing approach under the NIS1 directive, strengthening and streamlining the cybersecurity risk management and incident reporting provisions, and extending the scope by adding additional sectors, such as space or telecom (important for securing satellite communications, a vital infrastructure in remote rural areas, but also as a fail over in times of a natural disaster or military conflict). NIS2 underlines the special role of telecoms as a highly mature sector, a conduit for cyberattacks, and a possible filter, protecting less mature and harder to protect sectors such as health care. In addition, the NIS2 ambitions need to be supported, for instance to improve incident reporting, to create a better situational picture, of vulnerability disclosure policies and an EU vulnerability database, of supply chain security and other coordinated EU-wide cybersecurity risk assessments, including expanding the scope in terms of sectors covered, and of creating the right culture and environment for essential and important entities to share cybersecurity-relevant information such as cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. MSs have 21 months to transpose NIS2 into national law and to implement it. In parallel, ENISA is developing its service and expertise for this with the introduction of service catalogue based on existing NIS1 expertise that is reflected in this single programming document (SPD).</p> <p>ENISA is already invested in activities linked to the development and implementation of NIS2, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the implementation of the directive in the coming years, using existing resources and building on these wherever necessary.</p>
The EU Cybersecurity Act	Amendment	<p>On 18 April 2023, the Commission proposed a targeted amendment to the EU CSA (ENISA's founding regulation).</p> <p>The proposed targeted amendment aims to enable, by means of Commission implementing acts, the adoption of European cybersecurity certification schemes for 'managed security services'. This is in addition to ICT products, services and processes, which are already covered under the CSA. Such security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents.</p>

Regulation on digital operational resilience for the financial sector (DORA)	Adopted	In parallel with NIS2, in December 2022 the Parliament and the Council adopted DORA (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector). The regulation aims to ensure that all participants in the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyberattacks and other risks. The regulation aims to ensure that all participants in the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyberattacks and other risks. DORA requires financial entities to ensure that they can withstand all types of ICT-related disruptions and threats. ENISA is actively supporting the mapping of cyber legislation initiatives in the finance sector and works closely with the Commission and relevant EU bodies on cybersecurity aspects of DORA including crisis management, incident reporting and information sharing.
Cyber diplomacy toolbox	Adopted	In addition, to support MS and European institutions, bodies and agencies (EUIBAs) in deterring and responding to cyberattacks from non-EU countries, the EU adopted a framework for a joint EU diplomatic response to malicious cyber activities, in the Council conclusions of 19 June 2017 ⁽²⁾ . The European External Action Service (EEAS) recently published updated implementation guidelines for the cyber diplomacy toolbox detailing specific steps MSs could take ⁽³⁾ . The guidelines underline the importance of measures taken by MSs under the NISD to improve resilience, the role of ENISA in establishing information-sharing channels with industry to gain situational awareness, and the importance of cooperation between the Cyber Crisis Liaison Organisation Network (EU-Cyclone), the Computer Security Incidence Response Team (CSIRT) network, ENISA, the Computer Emergency Response Team for EU institutions, bodies and agencies (CERT-EU) and the European Union Agency for Law Enforcement Cooperation, and EEAS Single Intelligence Analysis Capacity, to ensure that internal and external EU initiatives are coherent.

To read more: <https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2024-2024>

Number 9

The first set of final draft technical standards under the Digital Operational Resilience Act (DORA).



The three European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published the first set of final draft technical standards under the Digital Operational Resilience Act (DORA) aimed at enhancing the digital operational resilience of the EU financial sector by strengthening financial entities' Information and Communication Technology (ICT) and third-party risk management and incident reporting frameworks. The joint final draft technical standards include:

1. Final report, Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Executive Summary	2
2. Background and rationale	7
3. Draft regulatory technical standards	36
4. Accompanying documents	90

2. Final report on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Executive Summary	3
2. Background and rationale	4
3. Draft regulatory technical standards	6
4. Accompanying documents	19
4.1 Draft cost-benefit analysis / impact assessment	19
4.2 Summary of responses to the consultation	28

3. Final report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554.



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

1. Executive Summary	3
2. List of abbreviations	4
3. Background and Rationale	5
4. Draft regulatory technical standards	18
5. Accompanying documents	31

4. Final Report On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554



JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

ABBREVIATIONS	3
1. EXECUTIVE SUMMARY	4
2. BACKGROUND AND RATIONALE	6
3. NEXT STEPS	16
4. DRAFT IMPLEMENTING TECHNICAL STANDARDS	17
5. DRAFT COST- BENEFIT ANALYSIS / IMPACT ASSESSMENT	6
6. FEEDBACK ON THE PUBLIC CONSULTATION	18
7. FEEDBACK FROM THE STAKEHOLDER GROUPS	39

To read more: <https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party>

We carefully monitor the developments at: <https://www.digital-operational-resilience-act.com>

This website belongs to Cyber Risk GmbH.

Note

The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 solves an important problem in the EU financial regulation.

Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience.

After DORA, they must also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.

This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.

Number 10

EIOPA's newly launched IORP Risk Dashboard highlights market and asset return risks as main concerns for occupational pension funds



The European Insurance and Occupational Pensions Authority (EIOPA) published its first Risk Dashboard on Institutions for occupational retirement provisions (IORPs).

Based on individual occupational pensions regulatory reporting, EIOPA's IORP Risk Dashboard **summarises the main risks and vulnerabilities** in the IORPs sector of the European Economic Area (EEA) for the different schemes, i.e. defined contributions (DC) and defined benefits (DB).

It includes a set of risk indicators covering traditional risk categories, such as market and credit risks, liquidity risks, reserve & funding risks, as well as emerging threats like ESG and cyber risks.

February 2024 IORP Risk Dashboard			
Risks	Level	Trend (Past 3 months)	Outlook (Next 12 months)
Macro risks	Yellow circle	Blue arrow pointing right	Blue arrow pointing right
Credit risks	Yellow circle	Blue arrow pointing right	Blue arrow pointing up and right
Market & asset return risks	Orange circle	Blue arrow pointing right	Blue arrow pointing right
Liquidity risks	Yellow circle	Blue arrow pointing up	Blue arrow pointing right
Reserve & funding risks (DB Schemes)	Yellow circle	Blue arrow pointing right	Blue arrow pointing right
Concentration risks	Yellow circle	Blue arrow pointing right	Blue arrow pointing right
ESG related risks	Yellow circle	Blue arrow pointing right	Blue arrow pointing right
Digitalisation & cyber risks	Yellow circle	Blue arrow pointing right	Blue arrow pointing up and right

The risk dashboard was developed in cooperation with National Competent Authorities with the objective to systematically:

- monitor and assess the risks and evolution thereof in the IORP sector from a macroprudential perspective; and
- analyse the potential vulnerabilities of IORPs' financial position and their implication to financial stability at the EEA level.

Description of risk categories

Macro risks

This category depicts developments in the macro-economic environment that could impact the IORP sector. This category is based on publicly available data on macro variables that may be used for broader macroprudential monitoring and analysis.

Credit risks

The category assesses the vulnerability of the IORP sector towards credit risks. To achieve this aim, credit-relevant asset class exposures of the IORPs are combined with the relevant risk metrics applicable to these asset classes.

Market & asset return risks

The risk category depicts the main risks IORPs are exposed to on financial markets and the level of asset returns and costs (e.g. administrative, investments and other). For most asset classes these risks are being assessed by analysing both the investment exposure of the IORP sector and an underlying risk metric. The exposures give a picture of the vulnerability of the sector to adverse developments; the risk metric, usually the volatility of the yields of the associated indices, gives a picture of the current level of riskiness.

Liquidity risk can be defined as the risk that an institution will not be able to meet its payment obligations timely or without generating excessive cost.

Reserve & funding risks

This category aims to assess the level of the own funds of IORPs and the robustness of its technical provisions. This risk category is only relevant for IORPs executing defined benefit pension schemes (DB).

Concentration risks

This section assesses different concentration risks IORPs are exposed to via their portfolio investments. It depicts various concentration types.

Environmental, Social and Governance (ESG) related risks¹

ESG risks aim at assessing the vulnerability of the European IORPs market to environmental, social and governance risks such as transition risk.

Digitalisation & cyber risks

The category aims at monitoring potential financial stability risks related to an increased digitalisation, which exposes the IORP sector to risks from a digital operational resilience perspective (i.e. cyber security risks).

Results

The first edition shows that the IORPs' exposure to market & asset return risks is currently at a high level, making this the most relevant risk category for the sector given the still high volatility in bond markets.

Macro risks are at a medium level: there are positive developments related to a reduction in forecasted inflation, partially offset by a GDP growth outlook that remains weak by historical standards.

Liquidity risks are at a medium level but show an increasing trend compared to the previous quarter, driven by developments in derivative positions.

The net asset value of IORP's derivative positions went further into negative territory due to the continued increase of interest rates in Q3-2023.

All other risk categories are currently assessed at a medium level, with increases expected for credit risks as well as digitalisation and cyber risks over the next 12 months.

Key observations:

IORPs' exposure to market & asset return risks is currently at a high level, making this the most relevant risk category for the sector given the still high volatility in bond markets.

Macro risks are at a **medium** level: there are positive developments related to a reduction in forecasted inflation, partially offset by a GDP growth outlook that remains weak by historical standards.

Liquidity risks are at a **medium** level but show an **increasing trend** compared to the previous quarter, driven by developments in derivative positions. The net asset value of IORP's derivative positions went further into negative territory due to the continued increase of interest rates in Q3-2023.

All other risk categories are currently assessed at a medium level, with increases expected for credit risks as well as digitalisation and cyber risks over the next 12 months.

To read more: https://www.eiopa.europa.eu/eiopas-newly-launched-iorp-risk-dashboard-highlights-market-and-asset-return-risks-main-concerns-2024-02-01_en

*Number 11***Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies****Protect Your Organization from the Foreign Intelligence Threat - Enterprise Risk Mitigation Blueprint***Preamble*

Nothing in this document shall be construed as authorization for any organization to conduct activities not otherwise authorized under statutes, executive order, or other applicable law, policy, or regulation nor does this document obviate an organization's responsibility to conduct activities that are otherwise mandated, directed, or recommended for execution under the same.

Threats are not limited to only cyber, insider, foreign intelligence and/or criminal activities.

Introduction

Today's global threat environment is more diverse and dynamic than ever. The 2023 Annual Threat Assessment of the U.S. Intelligence Community (IC) identified a growing number of foreign intelligence entities (FIE), state actors, and non-state actors targeting the United States Government (USG) and the private sector. The Assessment:

<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>



They are no longer interested just in obtaining classified U.S. secrets, but are also collecting sensitive unclassified information from most government agencies and virtually every sector of our economy.

Personal data, trade secrets, intellectual property, technology, and research and development are being aggressively targeted by adversaries who have the capability, patience, and resources to obtain them.

To achieve their objectives, FIEs are employing a wide range of illegal techniques including insider threats, cyber penetrations, supply chain attacks, and blended operations that combine some or all of these methods.

They are also using a variety of legal and quasi-legal methods, including mergers and acquisitions, investment, joint ventures, partnerships, and talent recruitment programs to acquire U.S. technology and innovation.

Ultimately, FIEs seek to degrade our economic power and national security, compromise our critical infrastructure, and undermine our democratic institutions.

This new form of conflict is not fought on a foreign battlefield but in our power grids, our computer networks, our laboratories and research facilities, our financial institutions, our healthcare systems, and our federal, state, local, and tribal governments.

This challenge can be met only by hard work, determination and diligence, and public and private sector partnership.

NCSC is working closely with partners to implement holistic, integrated enterprise risk mitigation (ERM) programs to develop a “blended” enterprise approach, actively engaging the entire enterprise to protect their organizations.

Our citizens as well as our government and institutions need capabilities that deter our adversaries capabilities. These capabilities can be provided by an integrated and layered ERM program.

This document includes links to risk mitigation information that can help organizations enhance their physical security, personnel security, operations security (OPSEC), cybersecurity, defensive counterintelligence (CI), insider threat mitigation capabilities, and supply chain risk management (SCRM).

ERM programs mitigate vulnerabilities to protect critical assets from collection, theft, disruption, and exploitation.

A well-developed program likely will have the added benefit of protecting the organization against criminal exploitation as well. Successful threat mitigation requires leveraging the workforce at all levels across an organization.

Threat Overview

Some foreign governments combine civilian and military capabilities with criminal activity to steal information to gain an advantage.

These practices illustrate the blurred lines between traditional intelligence collection and economic espionage. Rapid technological advancements are enabling FIEs to refine cyber capabilities and target organizations in the United States.

Their cyber operations penetrate our government and private sector in pursuit of policy insights, research, intellectual property, military and trade secrets, and personal identifiable information (PII), all to obtain a competitive advantage.

There are also significant risks associated with our nation's ever-increasing reliance on interconnected information technologies, particularly across critical infrastructure sectors such as the defense industrial base, energy, finance, healthcare, and telecommunications.

Additionally, many state actors view economic espionage—often using commercial enterprises owned or influenced by the state—as essential to achieving their own national security and economic goals. This comes at our expense.

FIEs attempt to exploit vulnerabilities in government and industry supply chains to steal our intellectual property, corrupt our software, surveil our critical infrastructure, and carry out other malicious activities through cyber or technical operations.

FIE tactics have included elicitation, economic espionage, human targeting, and cyber intrusions. We are increasingly concerned about state and nonstate-sponsored attempts to control or debilitate critical infrastructure systems, corrupt supply chains, or gain access to systems that control our nation's critical infrastructure.

The systemic and persistent vulnerabilities continue to grow, intensifying traditional FIE threats, placing critical infrastructure and emerging and proprietary technologies at risk, eroding competitive advantage, and weakening our global influence.

The federal workforce is one of our nation's greatest assets, but it faces an increasingly challenging risk environment ranging from insider threats, unauthorized disclosures, workplace violence, and being targeted by adversaries.

These workforce challenges will persist. Threat actors are conducting malicious influence campaigns that employ cyber operations, propaganda, and manipulation to try to sow divisions in society and undermine confidence in democratic institutions.

To read more:

https://www.dni.gov/files/NCSC/documents/products/Risk_Mitigation_Web_2023.pdf

Protect Your Organization.....	1
Preamble.....	1
Introduction.....	1
Threat Overview.....	2
Enterprise Risk Mitigation – Blueprint.....	3
Enterprise Risk Mitigation – Self Evaluation.....	3
Enterprise Risk Management – Best Practices.....	5
Put It All Together.....	9
References, Resources, and Terms.....	10
Notes.....	11

Number 12

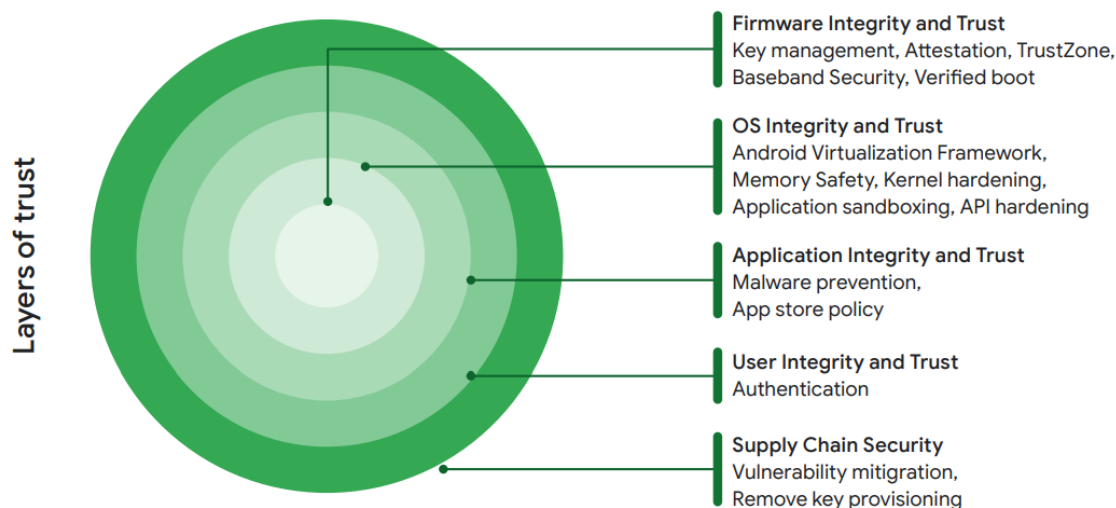
Piloting new ways of protecting Android users from financial fraud

Google Security Blog

From its founding, Android has been guided by principles of openness, transparency, safety, and choice. Android gives you the freedom to choose which device best fits your needs, while also providing the flexibility to download apps from a variety of sources, including preloaded app stores such as the Google Play Store or the Galaxy Store; third-party app stores; and direct downloads from the Internet.

Keeping users safe in an open ecosystem takes sophisticated defenses. That's why Android provides multiple layers of protections, powered by AI and backed by a large, dedicated security & privacy team, to help to protect our users from security threats while continually making the platform more resilient.

We also provide our users with numerous built-in protections like Google Play Protect, the world's most widely deployed threat detection service, which actively scans over 125 billion apps on devices every day to monitor for harmful behavior. That said, our data shows that a disproportionate amount of bad actors take advantage of select APIs and distribution channels in this open ecosystem.

Security by design*Elevating app security in an open ecosystem*

While users have the flexibility to download apps from many sources, the safety of an app can vary depending on the download source. Google Play, for example, carries out rigorous operational reviews to ensure app safety, including proper high-risk API use and permissions handling.

Other app stores may also follow established policies and procedures that help reduce risks to users and their data. These protections often include requirements for developers to declare which permissions their apps use and how

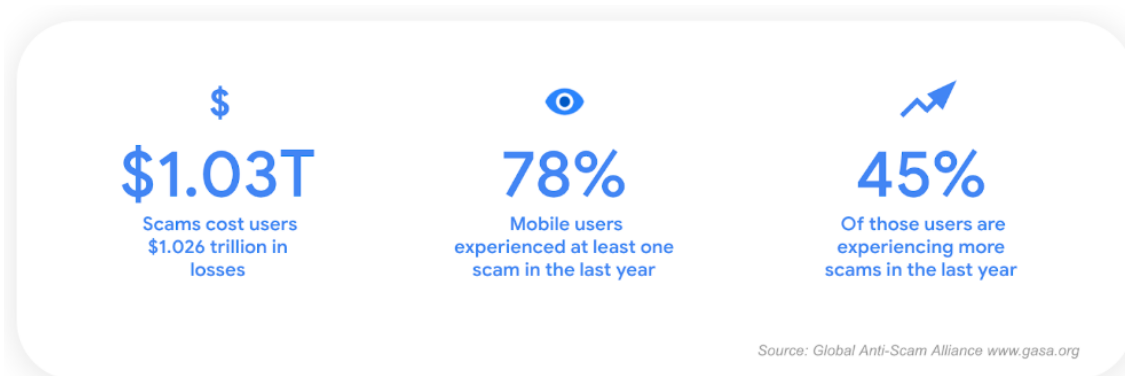
developers plan to use app data. Conversely, standalone app distribution sources like web browsers, messaging apps or file managers – which we commonly refer to as Internet-sideloaded – do not offer the same rigorous requirements and operational reviews. Our data demonstrates that users who download from these sources today face unusually high security risks due to these missing protections.

We recently launched enhanced Google Play Protect real-time scanning to help better protect users against novel malicious Internet-sideloaded apps. This enhancement is designed to address malicious apps that leverage various methods, such as AI, to avoid detection. This feature, now deployed on Android devices with Google Play Services in India, Thailand, Singapore and Brazil, has already made a significant impact on user safety.

As a result of the real-time scanning enhancement, Play Protect has identified 515,000 new malicious apps and issued more than 3.1 million warnings or blocks of those apps. Play Protect is constantly improving its detection capabilities with each identified app, allowing us to strengthen our protections for the entire Android ecosystem.

A new pilot to combat financial fraud

Cybercriminals continue to invest in advanced financial fraud scams, costing consumers more than \$1 trillion in losses. According to the 2023 Global State of Scams Report by the Global Anti-Scam Alliance, 78 percent of mobile users surveyed experienced at least one scam in the last year. Of those surveyed, 45 percent said they're experiencing more scams in the last 12 months. The Global Scam Report also found that scams were most often initiated by sending scam links via various messaging platforms to get users to install malicious apps and very often paired with a phone call posing to be from a valid entity.



Scammers frequently employ social engineering tactics to deceive mobile users. Using urgent pretenses that often involve a risk to a user's finances or an opportunity for quick wealth, cybercriminals convince users to disable security safeguards and ignore proactive warnings for potential malware, scams, and phishing. We've seen a large percentage of users ignore, or are tricked into dismissing, these proactive Android platform warnings and proceed with installing malicious apps.

This can lead to users ultimately disclosing their security codes, passwords, financial information and/or transferring funds unknowingly to a fraudster.

To help better protect Android users from these financial fraud attacks, we are piloting enhanced fraud protection with Google Play Protect. As part of a continued strategic partnership with the Cyber Security Agency of Singapore (CSA), we will launch this first pilot in Singapore in the coming weeks to help keep Android users safe from mobile financial fraud.

This enhanced fraud protection will analyze and automatically block the installation of apps that may use sensitive runtime permissions frequently abused for financial fraud when the user attempts to install the app from an Internet-sideloaded source (web browsers, messaging apps or file managers).

This enhancement will inspect the permissions the app declared in real-time and specifically look for four runtime permission requests: RECEIVE_SMS, READ_SMS, BIND_Notifications, and Accessibility. These permissions are frequently abused by fraudsters to intercept one-time passwords via SMS or notifications, as well as spy on screen content.

Based on our analysis of major fraud malware families that exploit these sensitive runtime permissions, we found that over 95 percent of installations came from Internet-sideloaded sources.

During the upcoming pilot, when a user in Singapore attempts to install an application from an Internet-sideloaded source and any of these four permissions are declared, Play Protect will automatically block the installation with an explanation to the user.

Collaborating to combat mobile fraud

This enhanced fraud protection has undergone testing by the Singapore government and will be rolling out to Android devices with Google Play services.

“The fight against online scams is a dynamic one. As cybercriminals refine their methods, we must collaborate and innovate to stay ahead,” said Mr Chua Kuan Seah, Deputy Chief Executive of CSA. “Through such partnerships with technology players like Google, we are constantly improving our anti-scam defenses to protect Singaporeans online and safeguard their digital assets.”

Together with CSA, we will be closely monitoring the results of the pilot program to assess its impact and make adjustments as needed. We will also support CSA by continuing to assist with malware detection and analysis, sharing malware insights and techniques, and creating user and developer education resources.

How developers can prepare

For developers distributing apps that may be affected by this pilot, please take the time to review the device permissions your app is requesting and ensure you're following developer best practices. Your app should only request permissions that

the app needs to complete an action and ensure it does not violate the Mobile Unwanted Software principles. Always ensure that your app does not engage in behavior that could be considered potentially harmful or malware.

If you find that your app is affected by the app protection pilot you can refer to our updated developer guidance for Play Protect warnings for tips on how to help fix potential issues with your app and instructions for filing an appeal if needed.

Our commitment to protecting Android users

We believe industry collaboration is essential to protect users from mobile security threats and fraud. Piloting these new protections will help us stay ahead of new attacks and evolve our solutions to defeat scammers and their expanding fraud attempt. We have an unwavering commitment to protecting our users around the world and look forward to continuing to partner with governments, ecosystem partners and other stakeholders to improve user protections.

Device management for any scenario

	Work Profile	Fully managed
	Personally-owned	Company-owned
Management of work apps & data	✓	✓
Management of personal apps & data	✗	✓
Privacy of personal apps & data	✓	✓

Not intended for personal use.

All apps and data are treated as if they were work, and thus are visible to IT.

To read more: <https://security.googleblog.com/2024/02/piloting-new-ways-to-protect-Android-users-from%20financial-fraud.html>

<https://services.google.com/fh/files/misc/android-enterprise-security-paper-2023.pdf>

Number 13

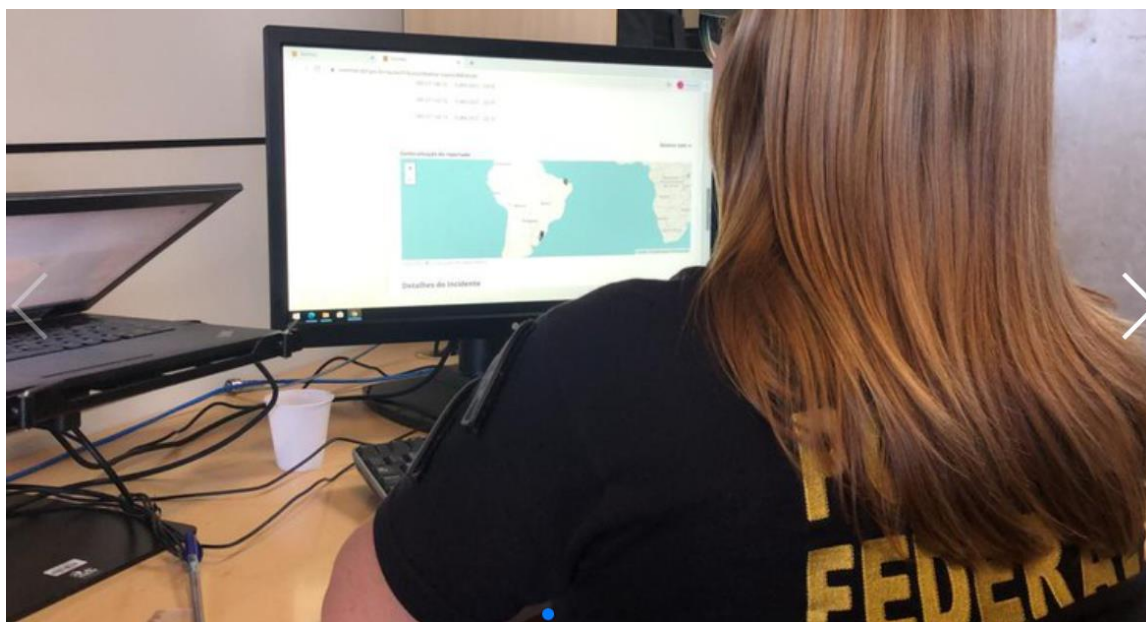
Brazilian Federal Police against Grandoreiro Banking Trojan



January 30 - the Federal Police launched Operation Grandoreiro to investigate the activities of a criminal group responsible for electronic banking fraud, using banking malware with victims outside Brazil.

The criminal structure is suspected of moving at least 3.6 million euros through fraud since 2019.

Federal police officers serve five temporary arrest warrants and another 13 search and seizure warrants, in the states of São Paulo, Santa Catarina, Pará, Goiás and Mato Grosso.



According to Caixa Bank, a financial institution in Spain, in addition to the damage caused, it was identified that there were fraud attempts using Brazilian banking malware that would amount to 110 million euros in losses.

The investigations began based on information sent by Caixa Bank, which identified that the programmers and operators of the banking malware were in Brazil.

Those investigated used cloud servers to host the infrastructure used in the Grandoreiro malware campaigns.

The use of command-and-control programs allowed remote access to victims' computers, an opportunity to steal valuables cybernetically. The infection of victims' equipment was carried out by sending emails containing malicious messages (**phishing**) that induced victims to believe that it was official

information such as, for example, court subpoenas, overdue invoice collections, invoices, among others.

To read more: <https://www.gov.br/pf/pt-br/assuntos/noticias/2024/01/pf-combate-organizacao-criminosa-que-praticava-fraudes-bancarias-eletronicas-contra-vitimas-no-exterior>

Number 14

Discovering Unknome Function (DUF)



Despite over 20 years of extensive genome function annotation, certain genes have been neglected (i.e., the Unknome).



Annotating these genes is technically challenging and often goes unfunded. The result is a bias in biological research toward previously studied genes, leaving a large area of fundamental research ripe for scientific discovery.

Cellular processes are inherently complex due to the large number of molecules and interactions, which are often nonlinear and occur at drastically different spatiotemporal scales that can span orders of magnitude.

Generating cellular datasets for gene function discovery is thus laborious and time-consuming; this leads to integrated experimental datasets from various strains, cellular states, and laboratory conditions.

Consequently, efforts to build useful predictive models of genotype-phenotype relationships are hindered by batch effects in training datasets and unannotated genes that still affect cell phenotype.

This ARC Opportunity is soliciting ideas to explore the question: Can high-throughput workflows be developed to generate high-confidence functional annotations of unknown coding and noncoding genes.

The DUF Opportunity on SAM.gov - Topic 5: Discovering Unknome Function (DUF) at: <https://sam.gov/opp/4e86ad556e184738b83ebb1coeobf6aa/view>

Discovering Unknown Function (DUF)

DARPA-EA-24-01-02
Discovering Unknown Function (DUF)

I. ARC Opportunity

The Defense Advanced Research Projects Agency (DARPA) Defense Sciences Office (DSO) is issuing an Advanced Research Concepts (ARC) Opportunity, inviting submissions of Abstracts for innovative exploratory research concepts in the technical domain of Biology. This ARC Opportunity, methods to Discovering Unknown Function (DUF), is issued under the master ARC Exploration Announcement (EA), DARPA-EA-24-01.

ARC Topic Solicitations

- Topic 1: Imagining Practical Applications
for a Quantum Tomorrow
(IMPAQT) (Closed)
- Topic 2: Separation and Purification of
Rare Earth Elements (SPREE) (Closed)
- Topic 3: Collaborative Knowledge
Curation (CKC) (Closed)
- Topic 4: Grip Likelihood in Underwater
Environments (GLUE)
- Topic 5: Discovering Unknown Function
(DUF)
- Topic 6: Fuel Access Anywhere,
Regardless of Means (FAARM)

To read more: <https://www.darpa.mil/ARC/DUF>

Number 15

The near-term impact of AI on the cyber threat

An NCSC assessment focusing on how AI will impact the efficacy of cyber operations and the implications for the cyber threat over the next two years.



During the Bletchley AI Safety Summit in November 2023, international leaders came together to discuss the vast potential of AI models in promoting economic growth, propelling scientific advances, and providing a wide range of public benefits. They also underscored the security risks that could arise from the irresponsible development and use of AI technologies. The UK government is evaluating and addressing the potential threats and risks associated with AI.

While it is essential to focus on the risks posed by AI, we must also seize the substantial opportunities it presents to cyber defenders. For example, AI can improve the detection and triage of cyber attacks and identify malicious emails and phishing campaigns, ultimately making them easier to counteract.

The Summit Declaration highlighted the importance of ensuring that AI is designed, developed, deployed, and used in a manner that is safe, human-centric, trustworthy, and responsible for the benefit of all.

The NCSC continues to work with international partners and industry to provide guidance on the secure development and use of AI, so that we can realise the benefits that AI offers to society, publishing Guidelines for Secure AI System Development in November 2023.

NCSC Assessment

NCSC Assessment (NCSC-A) is the authoritative voice on the cyber threat to the UK. We fuse all-source information – classified intelligence, industry knowledge, academic material and open source – to provide independent key judgements that inform policy decision making and improve UK cyber security.

We work closely with government, industry and international partners for expert input into our assessments.

NCSC-A is part of the Professional Heads of Intelligence Assessment (PHIA). PHIA leads the development of the profession through analytical tradecraft, professional standards, and building and sustaining a cross-government community.

This report uses formal probabilistic language (see yardstick) from NCSC-A product to inform readers about the near-term impact on the cyber threat from AI. To learn more about NCSC-A, please contact enquiries@ncsc.gov.uk.

	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	Moderate uplift	Moderate uplift	Uplift
Social engineering, phishing, passwords	Uplift	Uplift	Significant uplift (from low base)
Tools (malware, exploits)	Realistic possibility of uplift	Minimal uplift	Moderate uplift (from low base)
Lateral movement	Minimal uplift	Minimal uplift	No uplift
Exfiltration	Uplift	Uplift	Uplift

To read more: <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>

*Number 16***The U.S. AI Safety Institute Consortium (AISIC).**

On February 7, 2024 US Secretary of Commerce Gina Raimondo announced key members of the executive leadership team to lead the U.S. AI Safety Institute (USAISI), which will be established at the National Institute of Standards and Technology (NIST).

In support of efforts to create safe and trustworthy artificial intelligence (AI), NIST is establishing the U.S. Artificial Intelligence Safety Institute (USAISI).

To support this Institute, NIST has created the U.S. AI Safety Institute Consortium.

The Consortium brings together more than 200 organizations to develop science-based and empirically backed guidelines and standards for AI measurement and policy, laying the foundation for AI safety across the world.

This will help ready the U.S. to address the capabilities of the next generation of AI models or systems, from frontier models to new applications and approaches, with appropriate risk management strategies.

Consortium members contributions will support one of the following areas:

- Develop new guidelines, tools, methods, protocols and best practices to facilitate the evolution of industry standards for developing or deploying AI in safe, secure, and trustworthy ways
- Develop guidance and benchmarks for identifying and evaluating AI capabilities, with a focus on capabilities that could potentially cause harm
- Develop approaches to incorporate secure-development practices for generative AI, including special considerations for dual-use foundation models, including:
 - Guidance related to assessing and managing the safety, security, and trustworthiness of models and related to privacy-preserving machine learning;
 - Guidance to ensure the availability of testing environments
- Develop and ensure the availability of testing environments
- Develop guidance, methods, skills and practices for successful red-teaming and privacy-preserving machine learning
- Develop guidance and tools for authenticating digital content

- Develop guidance and criteria for AI workforce skills, including risk identification and management, test, evaluation, validation, and verification (TEVV), and domain-specific expertise
- Explore the complexities at the intersection of society and technology, including the science of how humans make sense of and engage with AI in different contexts
- Develop guidance for understanding and managing the interdependencies between and among AI actors along the lifecycle

NIST received over 600 Letters of Interest from organizations across the AI stakeholder community and the United States. As of February 8, 2024, the consortium includes more than 200 member companies and organizations.

The AI Safety Institute Consortium (AISIC) is pleased to announce its inaugural cohort of members:

A	F	P
<ul style="list-style-type: none"> • Accel AI Institute • Accenture LLP • Adobe • Advanced Micro Devices (AMD) • AFL-CIO Technology Institute (Provisional Member) • AI Risk and Vulnerability Alliance • AlandYou • Allen Institute for Artificial Intelligence • Alliance for Artificial Intelligence in Healthcare • Altana • Alteryx • Amazon.com • American University, Kogod School of Business • AmpSight • Anika Systems Incorporated • Anthropic • Apollo Research • Apple • Ardent Management Consulting • Aspect Labs • Atlanta University Center 	<ul style="list-style-type: none"> • FAIR Institute • FAR AI • Federation of American Scientists • FISTA • ForHumanity • Fortanix, Inc. • Free Software Foundation • Frontier Model Forum • Financial Services Information Sharing and Analysis Center (FS-ISAC) • Future of Privacy Forum 	<ul style="list-style-type: none"> • Palantir • Partnership on AI (PAI) • Pfizer • Preamble • PwC • Princeton University • Purdue University, Governance and Responsible AI Lab (GRAIL)
	G	Q
	<ul style="list-style-type: none"> • Gate Way Solutions • George Mason University • Georgia Tech Research Institute • GitHub • Gladstone AI • Google • Gryphon Scientific • Guidepost Solutions 	<ul style="list-style-type: none"> • Qualcomm Incorporated • Queer in AI
	H	R
		<ul style="list-style-type: none"> • RAND Corporation • Redwood Research Group • Regions Bank • Responsible AI Institute • Robust Intelligence • RTI International
		S
		<ul style="list-style-type: none"> • SaferAI • Salesforce • SAS Institute

- Atlanta University Center Consortium
 - Autodesk, Inc.
- B**
- BABL AI Inc.
 - Backpack Healthcare
 - Bank of America
 - Bank Policy Institute
 - Baylor College of Medicine
 - Beck's Superior Hybrids
 - Benefits Data Trust
 - Humane Intelligence
 - Booz Allen Hamilton
 - Boston Scientific
 - BP
 - BSA | The Software Alliance
 - BSI Group America
- C**
- Canva
 - Capitol Technology University
 - Carnegie Mellon University
 - Casepoint
 - Center for a New American Security
 - Center For AI Safety
 - Center for Security and Emerging Technologies (Georgetown University)
 - Center for Democracy and Technology
 - Centers for Medicare & Medicaid Services
 - Centre for the Governance of AI
 - Cisco Systems
 - Citadel AI
 - Citigroup
 - CivAI
 - Civic Hacker LLC
 - Cleveland Clinic
 - Coalition for Health AI (CHAI) (Provisional Member)
 - Cohere
 - Common Crawl Foundation
 - Cornell University
- Hewlett Packard Enterprise
 - Hispanic Tech and Telecommunications Partnership (HTTP)
 - Hitachi Vantara Federal
 - Hugging Face
 - Human Factors and Ergonomics Society
 - Humane Intelligence
 - Hypergame AI
- I**
- IBM
 - Imbue
 - Indiana University
 - Inflection AI
 - Information Technology Industry Council
 - Institute for Defense Analyses
 - Institute for Progress
 - Institute of Electrical and Electronics Engineers, Incorporated (IEEE)
 - Institute of International Finance
 - Intel Corporation
 - Intertrust Technologies
 - Iowa State University, Translational AI Center (TrAC)
 - Iowa State University, Translational AI Center (TrAC)
- J**
- JPMorgan Chase
 - Johns Hopkins University
- K**
- Kaiser Permanente
 - Keysight Technologies
 - Kitware, Inc.
 - Knexus Research
 - KPMG
- L**
- LA Tech4Good
 - Leadership Conference Education Fund, Center for Civil Rights and Technology
 - Leela AI
- SAS Institute
 - SandboxAQ
 - Scale AI
 - Science Applications International Corporation
 - Scripps College
 - SecureBio
 - Society of Actuaries Research Institute
 - Software & Information Industry Association
 - SonarSource
 - SRI International
 - Stability AI (Provisional Member)
 - stackArmor
 - Stanford Institute for Human-Centered AI, Stanford Center for Research on Foundation Models, Stanford Regulation, Evaluation, and Governance Lab
 - State of California, Department of Technology
 - State of Kansas, Office of Information Technology Services
 - StateRAMP
 - Subtextive
 - Syracuse University
- T**
- T**
- Taraaz
 - TensTorrent USA
 - Texas A&M University
 - Thomson Reuters (Provisional Member)
 - Touchstone Evaluations
 - Trustible
 - TrueLaw
 - Trufo
- U**
- UnidosUS
 - UL Research Institutes
 - University at Albany, SUNY Research Foundation
 - University at Buffalo, Institute for Artificial Intelligence and Data Science

- Cranium AI
- Credo AI
- CrowdStrike
- Cyber Risk Institute

D

- Dark Wolf Solutions
- Data & Society Research Institute
- Databricks
- Dataiku
- DataRobot
- Deere & Company
- Deloitte
- Beckman Coulter
- Digimarc
- DLA Piper
- Drexel University
- Drummond Group
- Duke University
- The Carl G Grefenstette Center for Ethics at Duquesne University

E

- EBG Advisors
- EDM Council
- Eightfold AI
- Elder Research
- Electronic Privacy Information Center
- Elicit
- EleutherAI Institute
- Emory University
- Enveil
- EqualAI
- Erika Britt Consulting
- Ernst & Young, LLP
- Exponent

- Linux Foundation, AI & Data
- Lucid Privacy Group
- Lumenova AI

M

- Magnit Global Solutions
- Manatt, Phelps & Phillips
- MarkovML
- Massachusetts Institute of Technology, Lincoln Laboratory
- Mastercard
- Meta
- Microsoft
- MLCommons
- Model Evaluation and Threat Research (METR, formerly ARC Evals)
- Modulate
- MongoDB

N

- National Fair Housing Alliance
- National Retail Federation
- New York Public Library
- New York University
- NewsGuard Technologies
- Northrop Grumman
- NVIDIA

O

- ObjectSecurity LLC
- Ohio State University
- O'Neil Risk Consulting & Algorithmic Auditing, Inc. (ORCAA)
- OpenAI
- OpenPolicy
- OWASP (AI Exchange & Top 10 for LLM Apps)
- University of Oklahoma, Data Institute for Societal Challenges (DISC)
- University of Oklahoma, NSF AI Institute for Research on Trustworthy AI in Weather, Climate, and Coastal Oceanography (AI2ES)

- University at Buffalo, Center for Embodied Autonomy and Robotics
- University of Texas at San Antonio (UTSA)
- University of Maryland, College Park
- University Of Notre Dame Du Lac
- University of Pittsburgh
- University of South Carolina, AI Institute
- University of Southern California
- U.S. Bank National Association

V

- Vanguard
- Vectice
- Visa

W

- Wells Fargo & Company
- Wichita State University, National Institute for Aviation Research
- William Marsh Rice University
- Wintrust Financial Corporation
- Workday

To read more: <https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute>

Number 17

U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure



Office of Public Affairs
U.S. Department of Justice

Court-Authorized Operation Removed Malware from U.S.-Based Victim Routers and Took Steps to Prevent Reinfection

A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People’s Republic of China (PRC) state-sponsored hackers.

The hackers, known to the private sector as “Volt Typhoon,” used privately-owned SOHO routers infected with the “KV Botnet” malware to conceal the PRC origin of further hacking activities directed against U.S. and other foreign victims.

These further hacking activities included a campaign targeting critical infrastructure organizations in the United States and elsewhere that was the subject of a May 2023 FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and foreign partner advisory.

The same activity has been the subject of private sector partner advisories in May and December 2023, as well as an additional secure by design alert released by CISA.



The vast majority of routers that comprised the KV Botnet were Cisco and NetGear routers that were vulnerable because they had reached “end of life” status; that is, they were no longer supported through their manufacturer’s security patches or other software updates. The court-authorized operation deleted the KV Botnet malware from the routers and took additional steps to

sever their connection to the botnet, such as blocking communications with other devices used to control the botnet.

“The Justice Department has disrupted a PRC-backed hacking group that attempted to target America’s critical infrastructure utilizing a botnet,” said Attorney General Merrick B. Garland. “The United States will continue to dismantle malicious cyber operations – including those sponsored by foreign governments – that undermine the security of the American people.”

“In wiping out the KV Botnet from hundreds of routers nationwide, the Department of Justice is using all its tools to disrupt national security threats – in real time,” said Deputy Attorney General Lisa O. Monaco. “Today’s announcement also highlights our critical partnership with the private sector – victim reporting is key to fighting cybercrime, from home offices to our most critical infrastructure.”

“China’s hackers are targeting American civilian critical infrastructure, pre-positioning to cause real-world harm to American citizens and communities in the event of conflict,” said FBI Director Christopher Wray. “Volt Typhoon malware enabled China to hide as they targeted our communications, energy, transportation, and water sectors. Their pre-positioning constitutes a potential real-world threat to our physical safety that the FBI is not going to tolerate. We are going to continue to work with our partners to hit the PRC hard and early whenever we see them threaten Americans.”

“Today, the FBI and our partners continue to stand firmly against People's Republic of China cyber actors that threaten our nation's cyber security,” said FBI Deputy Director Paul Abbate. “We remain committed to thwarting malicious activities of this type and will continue to disrupt and dismantle cyber threats, safeguarding the fabric of our cyber infrastructure.”

“This operation disrupted the efforts of PRC state-sponsored hackers to gain access to U.S. critical infrastructure that the PRC would be able to leverage during a future crisis,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “The operation, together with the release of valuable network defense guidance by the U.S. government and private sector partners, demonstrates the Department of Justice’s commitment to enhance cybersecurity and disrupt efforts to hold our critical infrastructure at risk.”

“Using traditional law enforcement tools to disrupt state-of-the-art technologies, the U.S. Attorney’s Office for the Southern District of Texas protected Americans from PRC government-sponsored cyber-criminals who used U.S. based routers to hack into American targets,” said U.S. Attorney Alamdar S. Hamdani for the Southern District of Texas. “This case demonstrates my office’s ongoing commitment to defending our critical infrastructure from PRC initiated cyber-attacks. We thank the FBI and the Justice Department’s National Security Division for its work, and we will continue to work shoulder to shoulder with them to shield our country from state-sponsored hackers.”

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

IN THE MATTER OF THE SEARCH OF
SPECIFIED ROUTERS IN THE UNITED
STATES INFECTED WITH KV BOTNET
MALWARE

Case No. 4:23-MC-5432

(UNDER SEAL)

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41(b)(6)(B) FOR A SEARCH AND SEIZURE WARRANT**

I [REDACTED] a Special Agent with the Federal Bureau of Investigation (“FBI”), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. The FBI is investigating foreign state-sponsored actors (“hackers”) who have intruded into small-office/home-office (“SOHO”) routers in this District and elsewhere and infected them with malware. This malware links the SOHO routers into a network of nodes, or a botnet, which the hackers use as proxies to conceal their identities while committing additional computer intrusions against separate U.S. victims.

“The FBI’s dismantling of the KV Botnet sends a clear message that the FBI will take decisive action to protect our nation’s critical infrastructure from cyber-attacks,” said Special Agent in Charge Douglas Williams of the FBI Houston Field Office. “By ensuring home and small-business routers are replaced after their end-of-life expiration, everyday citizens can protect both their personal cyber security and the digital safety of the United States. We need the American public’s vigilance and support to continue our fight against malicious PRC-sponsored cyber actors.”

As described in court documents, the government extensively tested the operation on the relevant Cisco and NetGear routers. The operation did not impact the legitimate functions of, or collect content information from, hacked routers. Additionally, the court-authorized steps to disconnect the routers from the KV Botnet and prevent reinfection are temporary in nature. A router’s owner can reverse these mitigation steps by restarting the router. However, a restart that is not accompanied by mitigation steps similar to those the court order authorized will make the router vulnerable to reinfection.

The FBI is providing notice of the court-authorized operation to all owners or operators of SOHO routers that were infected with the KV Botnet malware and remotely accessed pursuant to the operation. For those victims whose contact information was not publicly available, the FBI has contacted providers (such as a victim’s internet service provider) and has asked those providers to provide notice to the victims.

FBI Houston Field Office and Cyber Division, U.S. Attorney’s Office for the Southern District of Texas, and National Security Cyber Section of the Justice Department’s National Security Division led the disruption effort. The Justice Department’s Criminal Division’s Computer Crime and Intellectual Property Section and Office of International Affairs provided valuable assistance. These efforts would not have been successful without the partnership of numerous private-sector entities.

If you believe you have a compromised router, please visit the FBI’s Internet Crime Complaint Center or report online to CISA. The remediated routers remain vulnerable to future exploitation by Volt Typhoon and other hackers, and the FBI strongly encourages router owners to remove and replace any end-of-life SOHO router currently in their networks.

The FBI continues to investigate Volt Typhoon’s computer intrusion activity.

To read more: <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States Courts
Southern District of Texas
FILED
January 09, 2024
Nathan Ochsner, Clerk of Court

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

SPECIFIED ROUTERS IN THE UNITED STATES
INFECTED WITH KV BOTNET MALWARE

)

)

)

)

Case No. **4:24-mc-5018**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

Number 18

AI in Support of StratCom Capabilities



The report aims to guide information environment assessment (IEA) practitioners. This includes understanding the information environment and audiences, particularly in online campaigns, and covers necessary technical elements and legal factors.

Contents

Abstract	5
Understanding the role of StratCom in NATO	5
The social perspective: what is required	6
PsyOps requirements	6
Target audience analysis	7
Audience segmentation	8
Construct validity	8
Fundamental attribution error	9
Operationalising the variables	10
When we fail, why do we fail?	11
Introducing the behaviour model: COM-B as a framework for TAA	11
Capability	11
Opportunity	12
Motivation	12
Overview	12
Example: TAA in a marketing company's digital advertising campaign	15
Technical prerequisites of a successful campaign	16
Borrowing useful tools from IEA	16
Hashtags and entities	17
Challenges with sentiment analysis: from polar sentiment towards directional sentiment	19
From topics to narratives	23
Network analysis	24
Deriving insights from surveys, interviews and focus groups	25
Multimodal perspectives	26
Fusing everything together	28

Steering towards an AI toolbox for targeted communication	31
The legal perspective	37
The Artificial Intelligence Act	39
Ethics Guidelines for Trustworthy AI	40
Legal framework for military purposes	41
North Atlantic Treaty Organization	41
The European Union	41
Conclusions and recommendations	42
The legal considerations	44
Endnotes	45

Key questions addressed include:

- What artificial intelligence (AI) functions are essential for Strategic Communications?
- Which models need improvement?
- What is the projected future of AI in this field?

The report offers current knowledge to enhance practitioners' ability to navigate an AI-driven information environment securely, efficiently and in line with legal requirements.

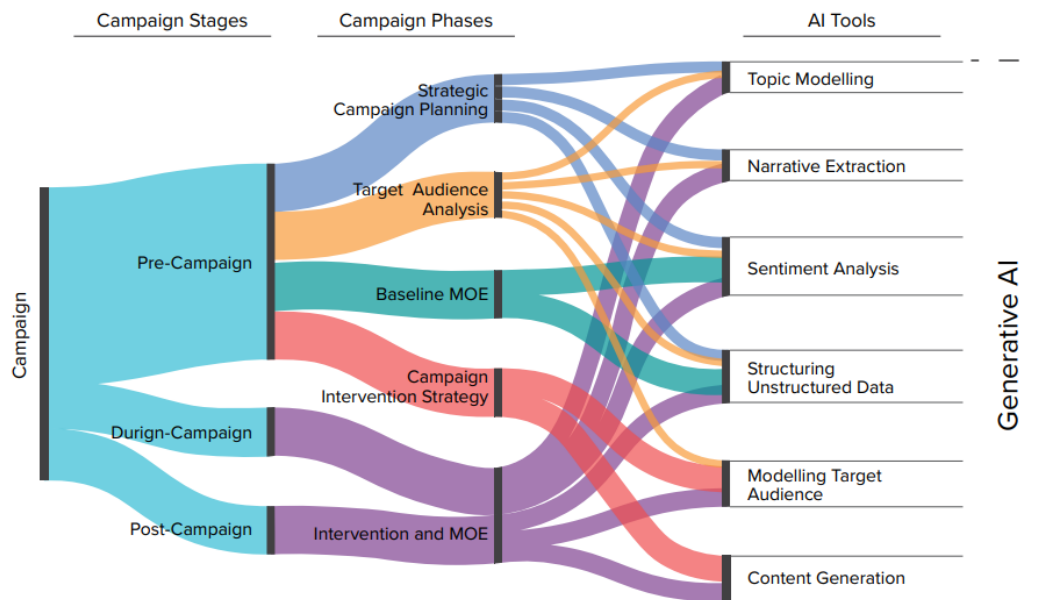


FIGURE 9. Summary of usage of AI tools in various stages of a StratCom campaign

To read more: <https://stratcomcoe.org/publications/ai-in-support-of-stratcom-capabilities/296>

AI in Support of StratCom Capabilities

PREPARED AND PUBLISHED BY THE
**NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE**



Number 19

Former CIA Officer Joshua Adam Schulte Sentenced To 40 Years In Prison For Espionage And Child Pornography Crimes



February 1, 2024 - Damian Williams, the United States Attorney for the Southern District of New York; Matthew G. Olsen, the Assistant Attorney General for National Security; and James Smith, the Assistant Director in Charge of the New York Field Office of the Federal Bureau of Investigation (“FBI”), announced that JOSHUA ADAM SCHULTE was sentenced to 40 years in prison by U.S. District Judge Jesse M. Furman for crimes of espionage, computer hacking, contempt of Court, making false statements to the FBI, and child pornography.

SCHULTE’s theft is the largest data breach in the history of the CIA, and his transmission of that stolen information to WikiLeaks is one of the largest unauthorized disclosures of classified information in the history of the U.S.

This sentencing followed SCHULTE’s convictions at trials that concluded on March 9, 2020, July 13, 2022, and September 13, 2023.

U.S. Attorney Damian Williams said: “Joshua Schulte betrayed his country by committing some of the most brazen, heinous crimes of espionage in American history. He caused untold damage to our national security in his quest for revenge against the CIA for its response to Schulte’s security breaches while employed there.

When the FBI caught him, Schulte doubled down and tried to cause even more harm to this nation by waging what he described as an ‘information war’ of publishing top secret information from behind bars.

And all the while, Schulte collected thousands upon thousands of videos and images of children being subjected to sickening abuse for his own personal gratification. The outstanding investigative work of the FBI and the career prosecutors in this Office unmasked Schulte for the traitor and predator that he is and made sure that he will spend 40 years behind bars – right where he belongs.”

According to court documents and evidence at trial:

From 2012 to 2016, SCHULTE was employed as a software developer in the Center for Cyber Intelligence (“CCI”), which conducts offensive cyber operations: cyber espionage relating to terrorist organizations and foreign governments.

SCHULTE and other CCI developers worked on tools that were used in, among other things, human-enabled operations: cyber operations that involved a person with access to the computer network being targeted by the cyber tool. In addition to being a developer, SCHULTE was also temporarily one of the administrators of one of the servers and suite of development programs used to build cyber tools.

In March 2016, SCHULTE was moved within branches of CCI as a result of personnel disputes between SCHULTE and another developer. Following that transfer, in April 2016, SCHULTE abused his administrator powers to grant himself administrator privileges over a development project from which he had been removed as a result of the branch change.

SCHULTE's abuse of administrator privileges was detected, and CCI leadership directed that administrator privileges would immediately be transferred from developers, including SCHULTE, to another division. SCHULTE was also given a warning about self-granting administrator privileges that had previously been revoked.

SCHULTE had, however, secretly opened an administrator session on one of the servers before his privileges were removed. On April 20, 2016, after other developers had left the CCI office, SCHULTE used his secret server administrator session to execute a series of cyber-maneuvers on the CIA network to restore his revoked privileges, break in to the backups, steal copies of the entire CCI tool development archives (the "Stolen CIA Files"), revert the network back to its prior state, and delete hundreds of log files in an attempt to cover his tracks. SCHULTE's theft of the Stolen CIA Files is the largest data breach in CIA history.

From his home computer, SCHULTE then transmitted the Stolen CIA Files to WikiLeaks, using anonymizing tools recommended by WikiLeaks to potential leakers, such as the Tails operating system and the Tor browser. On May 5, 2016, having transmitted the Stolen CIA Files to WikiLeaks, SCHULTE wiped and reformatted his home computer's internal hard drives.

On March 7, 2017, WikiLeaks began publishing classified data from the Stolen CIA Files. Between March and November 2017, there were a total of 26 disclosures of classified data from the Stolen CIA Files that WikiLeaks denominated as Vault 7 and Vault 8 (the "WikiLeaks Disclosures").

The WikiLeaks Disclosures were one of the largest unauthorized disclosures of classified information in the history of the U.S., and SCHULTE's theft and disclosure immediately and profoundly damaged the CIA's ability to collect foreign intelligence against America's adversaries; placed CIA personnel, programs, and assets directly at risk; and cost the CIA hundreds of millions of dollars. The effect was described at trial by the former CIA Deputy Director of Digital Innovation as a "digital Pearl Harbor," and the disclosure caused exceptionally grave harm to the national security of the U.S.

Following the WikiLeaks Disclosures, SCHULTE was voluntarily interviewed on multiple occasions by the FBI in March 2017. During those interviews, SCHULTE repeatedly lied, including denying being responsible for the theft of the Stolen CIA Files or for the WikiLeaks Disclosures and spinning fake narratives about ways the Stolen CIA Files could have been obtained from CIA computers, in the hope of deflecting suspicion away from SCHULTE and diverting law enforcement resources to false leads.

In March 2017, the FBI searched SCHULTE's apartment in New York pursuant to a search warrant and recovered, among other things, multiple computers, servers, and other electronic storage devices, including SCHULTE's personal desktop computer (the "Desktop Computer"), which SCHULTE built while living in Virginia and then transported to New York in November 2016.

On the Desktop Computer, FBI agents found layers of encryption hiding tens of thousands of videos and images of child sexual abuse materials, including approximately 3,400 images and videos of disturbing and horrific child pornography and the rape and sexual abuse of children as young as two years old, as well as images of bestiality and sadomasochism. SCHULTE collected some of these files during his employment with the CIA and continued to stockpile child pornography from the dark web and Russian websites after moving to New York.

While detained pending trial, in approximately April 2018, SCHULTE sent a copy of the affidavit in support of the warrant to search his apartment, which a protective order entered by the Court prohibiting SCHULTE from disseminating, to reporters from two different newspapers, and SCHULTE acknowledged in recorded phone calls that he knew he was prohibited from sharing protected material like the affidavit.

Despite being warned by the Court not to violate the protective order further, in the summer and fall of 2018, SCHULTE made plans to wage what he proclaimed to be an "information war" against the U.S. government. To pursue these ends, SCHULTE obtained access to contraband cellphones while in jail that he used to create anonymous, encrypted email and social media accounts.

SCHULTE also attempted to use the contraband cellphones to transmit protected discovery materials to WikiLeaks and planned to use the anonymous email and social media accounts to publish a manifesto and various other postings containing classified information about CIA cyber techniques and cyber tools. In a journal, SCHULTE wrote that he planned to "breakup diplomatic relationships, close embassies, [and] end U.S. occupation across the world[.]"

SCHULTE successfully sent emails containing classified information about the CCI development network and the number of employees in particular CIA cyber intelligence groups to a reporter.

As a result of this conduct, on March 9, 2020, SCHULTE was found guilty at trial of contempt of court and making material false statements.

On July 13, 2022, SCHULTE was found guilty at trial of eight counts: illegal gathering and transmission of national defense information in connection with his theft and dissemination of the Stolen CIA Files, illegal transmission and attempted transmission of national defense information, unauthorized access to a computer to obtain classified information and information from a department or agency of the U.S. in connection with his theft of the Stolen CIA Files, and two counts of causing transmission of harmful computer commands in connection with his theft of the Stolen CIA Files.

Finally, on September 13, 2023, SCHULTE was found guilty at trial on charges of receiving, possessing, and transporting child pornography.

In addition to the prison term, SCHULTE, 35, of New York, New York, was sentenced to a lifetime of supervised release.

Mr. Williams praised the outstanding efforts of the Counterintelligence Division and the Child Exploitation and Human Trafficking Task Force of the FBI's New York Field Office, as well as the extraordinary work of FBI computer scientists from the Cyber Action Team. Mr. Williams also thanked the FBI Washington Field Office, the CIA Office of General Counsel, and the National Security Division's Counterintelligence and Export Control Section for their assistance.

This case is being handled by the Office's National Security and International Narcotics Unit. Assistant U.S. Attorneys David W. Denton Jr., Michael D. Lockard, and Nicholas S. Bradley are in charge of the prosecution.

To read more: <https://www.justice.gov/usao-sdny/pr/former-cia-officer-joshua-adam-schulte-sentenced-40-years-prison-espionage-and-child>

Number 20

AI breakthrough creates images from nothing

Innovative framework that generates images from nothing can enable new scientific applications



A new, potentially revolutionary artificial intelligence framework called “**Blackout Diffusion**” generates images from a completely empty picture, meaning that the machine-learning algorithm, unlike other generative diffusion models, does not require initiating a “random seed” to get started.

Blackout Diffusion, presented at the recent International Conference on Machine Learning, generates samples that are comparable to the current diffusion models such as DALL-E or Midjourney, but require fewer computational resources than these models.

“Generative modeling is bringing in the next industrial revolution with its capability to assist many tasks, such as generation of software code, legal documents and even art,” said Javier Santos, an AI researcher at Los Alamos National Laboratory and co-author of Blackout Diffusion.

“Generative modeling could be leveraged for making scientific discoveries, and our team’s work laid down the foundation and practical algorithms for applying generative diffusion modeling to scientific problems that are not continuous in nature.”

Diffusion models create samples similar to the data they are trained on. They work by taking an image and repeatedly adding noise until the image is unrecognizable. Throughout the process the model tries to learn how to revert it back to its original state.

Current models require input noise, meaning they need some form of data to start producing images.

“We showed that the quality of samples generated by Blackout Diffusion is comparable to current models using a smaller computational space,” said Yen Ting Lin, the Los Alamos physicist who led the Blackout Diffusion collaboration.

Another unique aspect of Blackout Diffusion is the space it works in. Existing generative diffusion models work in continuous spaces, meaning the space they work in is dense and infinite. However, working in continuous spaces limits their potential for scientific applications.

“In order to run existing generative diffusion models, mathematically speaking, diffusion has to be living on a continuous domain; it cannot be discrete,” Lin said.

The theoretical framework the team developed, on the other hand, works in discrete spaces (meaning each point in the space is isolated from the others by

some distance), which opens up opportunities for a variety of applications such as text and scientific applications.

The team tested Blackout Diffusion on a number of standardized datasets, including the Modified National Institute of Standards and Technology database; the CIFAR-10 dataset, which has images of objects in 10 different classes; and the CelebFaces Attributes Dataset, which consists of more than 200,000 images of human faces.

In addition, the team used the discrete nature of Blackout Diffusion to clarify several widely conceived misconceptions about how diffusion models internally, providing a critical understanding of generative diffusion models.

They also provide design principles for future scientific applications. “This demonstrates the first foundational study on discrete-state diffusion modeling and points the way toward future scientific applications with discrete data,” Lin said. The team explains that generative diffusion modeling can potentially drastically speed up the time spent running many scientific simulations on supercomputers, which would both support scientific progress and reduce the carbon footprint of computational science.

Some of the diverse examples they mention are subsurface reservoir dynamics, chemical models for drug discovery and single-molecule and single-cell gene expression for understanding biochemical mechanisms in living organisms.

To read more: <https://discover.lanl.gov/news/0111-ai-breakthrough/>

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:

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

Cyber Risk GmbH

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

Cyber Risk GmbH offers:

1. In-House Instructor-Led Training programs,
2. Online Live Training programs,
3. Video-Recorded Training programs,
4. Distance Learning with Certificate of Completion programs.



In the core of our training approach is to ensure that our delivery is 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.

Instructor-led training
in Baur au Lac, Zurich

BAUR AU LAC

- Great training, exceptional venues.
- Presentations for the Board and the C-Suite.



CEO Briefings
in Baur au Lac, Zurich

BAUR AU LAC

- CEO Briefings, answering the questions of the CEO.



Our reading room: https://www.cyber-risk-gmbh.com/Reading_Room.html



ABOUT TRAINING FOR THE BOARD ASSESSMENT READING ROOM CONTACT CYBER RISK LINKS IMPRESSUM



2. Presentation at the Insomni'hack conference in Lausanne, Switzerland, in 2023: "Targeted Social Engineering Attacks: Weaponizing Psychology".

Targeted social engineering attacks that weaponize psychology have become tools employed by cybercriminals to infiltrate organizations in the public and private sector, steal sensitive information, recruit insiders, and help threat actors breach an organization's security. This presentation covers some of the most recent social engineering techniques and case studies.

https://www.youtube.com/watch?v=SfBjOxnd_XI



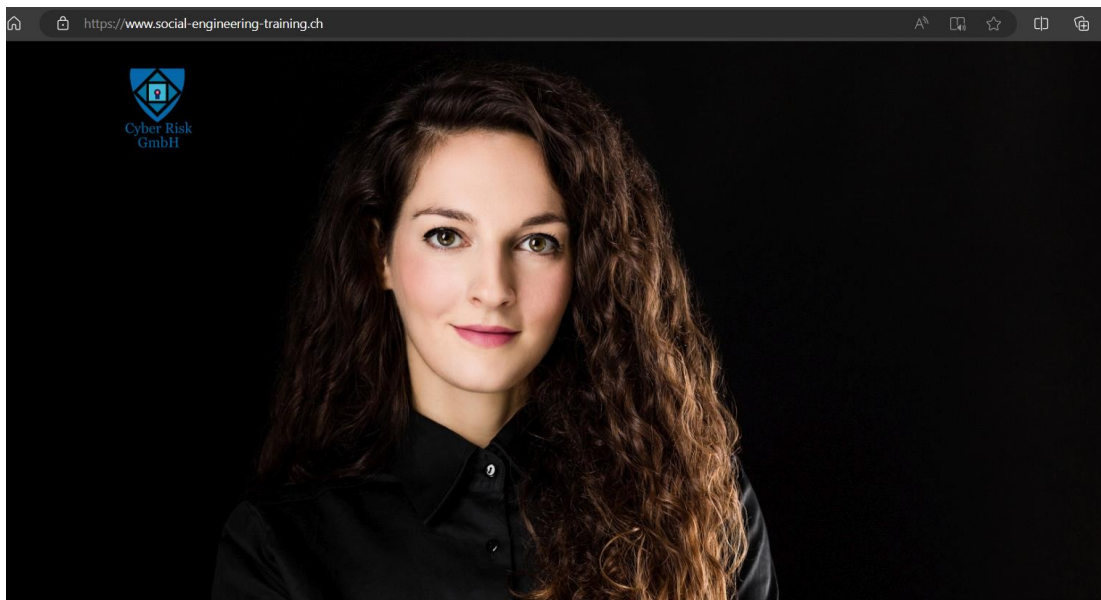
Our websites include:

a. Sectors and Industries.

1. Cyber Risk GmbH - <https://www.cyber-risk-gmbh.com>
2. Social Engineering - <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. Oil Cybersecurity - <https://www.oil-cybersecurity.com>

Cyber Risk GmbH, CHE-244.099.341, Dammstrasse 16, 8810 Horgen, Switzerland - www.cyber-risk-gmbh.com

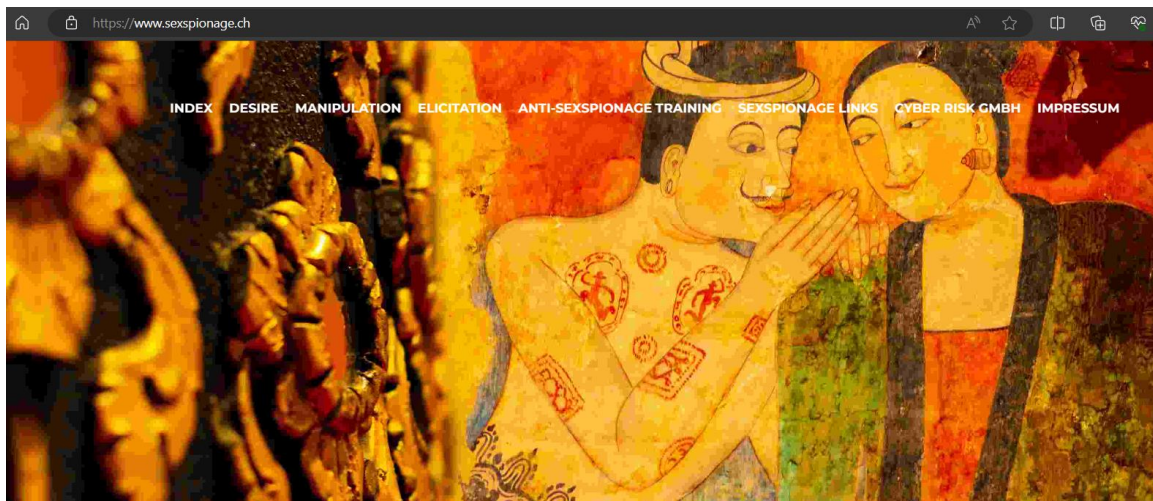
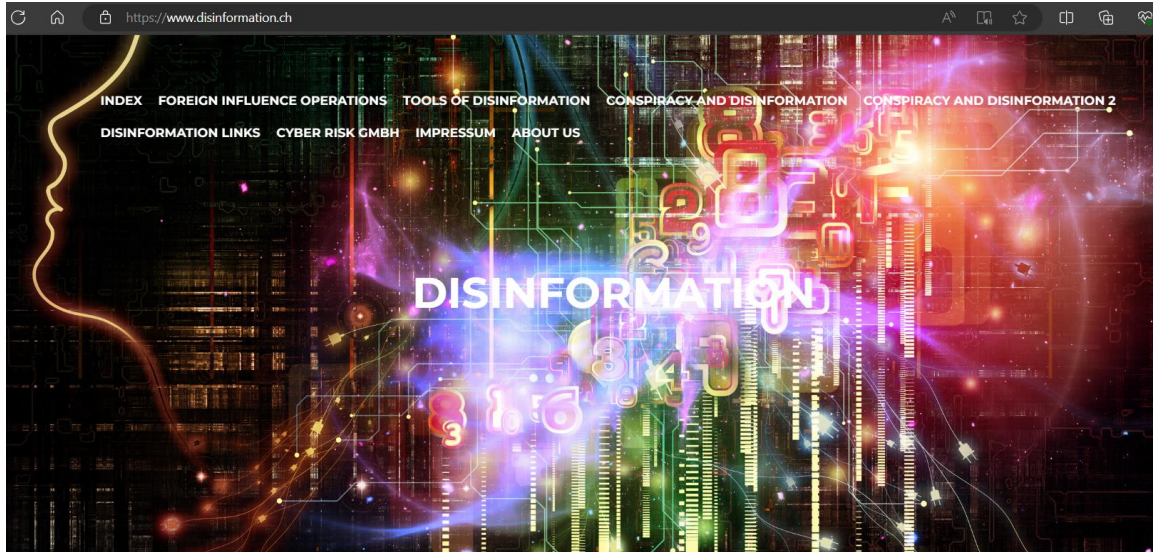
8. Electricity Cybersecurity - <https://www.electricity-cybersecurity.com>
9. Gas Cybersecurity - <https://www.gas-cybersecurity.com>
10. Hydrogen Cybersecurity - <https://www.hydrogen-cybersecurity.com>
11. Transport Cybersecurity - <https://www.transport-cybersecurity.com>
12. Transport Cybersecurity Toolkit - <https://www.transport-cybersecurity-toolkit.com>
13. Hotel Cybersecurity - <https://www.hotel-cybersecurity.ch>
14. Sanctions Risk - <https://www.sanctions-risk.com>
15. Travel Security - <https://www.travel-security.ch>



b. Understanding Cybersecurity.

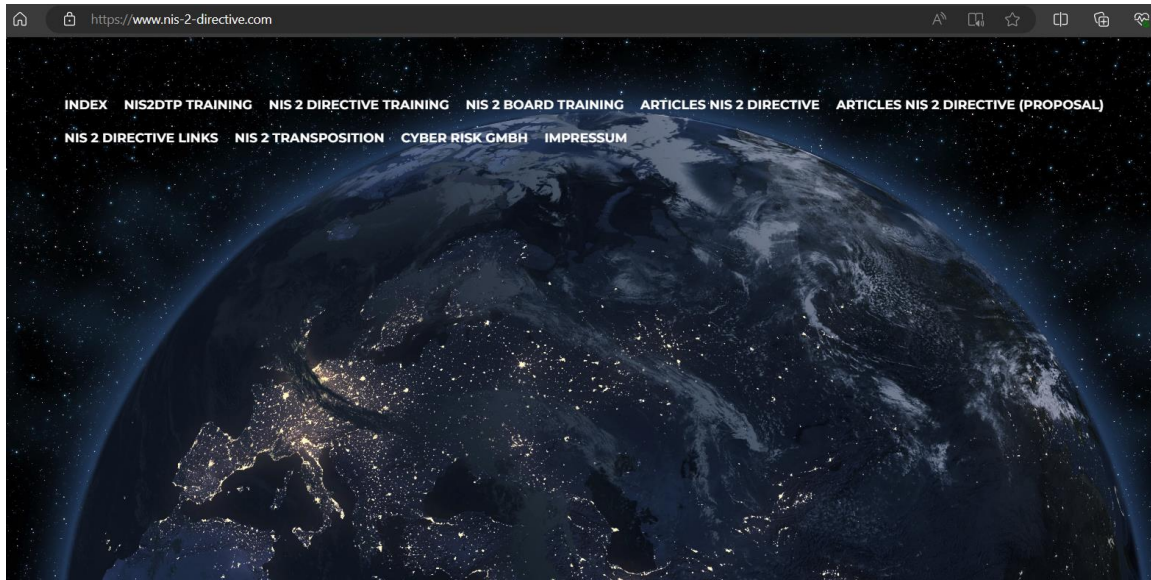
1. What is Disinformation? - <https://www.disinformation.ch>
2. What is Steganography? - <https://www.steganography.ch>
3. What is Cyberbiosecurity? - <https://www.cyberbiosecurity.ch>
4. What is Synthetic Identity Fraud? - <https://www.synthetic-identity-fraud.com>
5. What is a Romance Scam? - <https://www.romance-scams.ch>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

8. What is the RESTRICT Act? - <https://www.restrict-act.com>



c. Understanding Cybersecurity in the European Union.

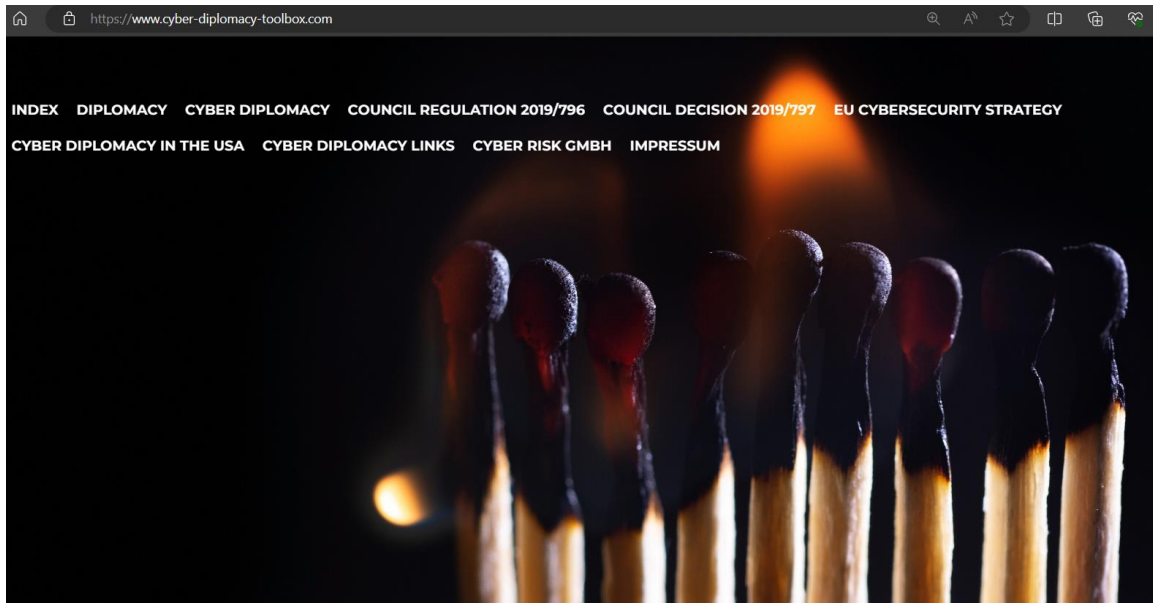
1. The NIS 2 Directive - <https://www.nis-2-directive.com>
2. The European Cyber Resilience Act - <https://www.european-cyber-resilience-act.com>
3. The Digital Operational Resilience Act (DORA) - <https://www.digital-operational-resilience-act.com>
4. The Critical Entities Resilience Directive (CER) - <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 EU Cyber Solidarity Act - <https://www.eu-cyber-solidarity-act.com>
12. The Digital Networks Act (DNA) - <https://www.digital-networks-act.com>
13. The Artificial Intelligence Act - <https://www.artificial-intelligence-act.com>
14. The Artificial Intelligence Liability Directive - <https://www.ai-liability-directive.com>
15. The Framework for Artificial Intelligence Cybersecurity Practices (FAICP) - <https://www.faicp-framework.com>
16. The European ePrivacy Regulation - <https://www.european-eprivacy-regulation.com>
17. The European Digital Identity Regulation - <https://www.european-digital-identity-regulation.com>
18. The European Media Freedom Act (EMFA) - <https://www.media-freedom-act.com>
19. The European Cyber Defence Policy - <https://www.european-cyber-defence-policy.com>

20. The Strategic Compass of the European Union <https://www.strategic-compass-european-union.com>

21. 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
Web: www.cyber-risk-gmbh.com

