



Cyber Risk and Compliance News and Alerts, March 2024

Friedrich Nietzsche believed that we often refuse to accept an idea, merely because the **tone of voice** in which it has been expressed is unsympathetic to us.



But what if we hear a person we like or love? Today, this can easily be generated with AI-enabled voice cloning technology.

AI-enabled voice cloning is the process of creating a synthetic imitation of a person's voice, that sounds exactly like the person's voice. First, voice data is collected. Then it is analysed for unique characteristics, used to train a machine learning model, and converted to synthetic speech.

Voice was a unique identifier, but it **cannot be trusted** any more. Criminals, spies, and everybody else can use voice cloning to impersonate individuals in phone calls, voice messages, or any other audio communication medium. This can trick the recipient into believing they are communicating with someone they trust, leading to the unauthorized sharing of sensitive or classified information, or financial loss.

Voice cloning can be used to create fake audio recordings to spread disinformation, manipulate public opinion, or create political unrest. We must not forget that it can also be used for **marketing**, and it works 24 x 7 x 365.

What is new? The U.S. Federal Communications Commission announced the unanimous adoption of a Declaratory Ruling that recognizes calls made with AI-generated voices are “artificial” under the Telephone Consumer Protection Act

(TCPA). The ruling, which takes effect immediately, makes [voice cloning](#) technology used in [common robocall scams targeting consumers illegal](#).

Frank Sinatra has said: “May you live to be 100 and may the **last voice** you hear be mine”. Today, with use of AI-enabled voice cloning technology, we can even hear Frank asking for a meeting in heaven or metaverse.

Read more at number 22 below.

The Bundesamt für Verfassungsschutz (BfV) together with the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners are releasing this joint Cybersecurity Advisory to warn of Russian state-sponsored cyber actors' use of compromised Ubiquiti EdgeRouters to facilitate malicious cyber operations worldwide.



The FBI, NSA, US Cyber Command and international partners - including authorities from Belgium, Brazil, France, Germany, Latvia, Lithuania, Norway, Poland, South Korea, and the United Kingdom - assess the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS), also known as APT 28, Fancy Bear, and Forest Blizzard (Strontium), have used compromised EdgeRouters globally to harvest credentials, collect NTLMv2 digests, proxy network traffic, and host spear-phishing landing pages and custom tools.

Threat Actor Activity

As early as 2022, APT28 actors had utilized compromised EdgeRouters to facilitate covert cyber operations against governments, militaries, and organizations around the world. These operations have targeted various industries, including Aerospace & Defense, Education, Energy & Utilities, Governments, Hospitality, Manufacturing, Oil & Gas, Retail, Technology, and Transportation. Targeted countries include Czech Republic, Italy, Lithuania, Jordan, Montenegro, Poland, Slovakia, Turkey, Ukraine, United Arab Emirates, and the US[1][2]. Additionally, the actors have strategically targeted many individuals in Ukraine.

An FBI investigation revealed APT28 actors accessed EdgeRouters compromised by Moobot, a botnet that installs OpenSSH trojans on compromised hardware [T1588]. While the compromise of EdgeRouters has been documented in open-source reporting, FBI investigation revealed each compromised router accessed by APT28 actors housed a collection of Bash scripts and ELF binaries designed to exploit backdoor OpenSSH daemons and related services [T1546] for a variety of purposes.

APT28 actors have used compromised EdgeRouters to collect credentials, proxy network traffic, and host spoofed landing pages and custom post-exploitation tools. For example, in early 2023, APT28 actors authored custom Python scripts to collect account credentials for specifically targeted webmail users. APT28 actors uploaded these custom Python scripts [T1587] to a subset of compromised Ubiquiti routers to validate stolen webmail account credentials collected via cross-site scripting and browser-in-the-browser spear-phishing campaigns [T1566].

The U. S. Department of Justice, including the FBI, BfV, and international partners recently disrupted a GRU botnet consisting of such routers. However, owners of relevant devices should take the remedial actions described below to ensure the long-term success of the disruption effort and to identify and remediate any similar compromises.

To read more:

https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/cyber/2024-02-28-joint-cyber-security-advisory.pdf?__blob=publicationFile&v=1

Which is more important, to protect the society from actual and potential adverse impacts on *human rights*, or from actual and potential adverse impacts on the *environment*?

I believe that the European Commission could not make a choice, so we have the proposal for a [Corporate Sustainability Due Diligence Directive \(CSDDD\)](#), which aims to enhance the protection of the environment **and** human rights in the EU and globally.

The directive sets obligations for large companies regarding actual and potential adverse impacts on human rights and the environment, with respect to their own operations, those of their **subsidiaries**, and those carried out by their **business partners**.

In December 2023 the Council and the European Parliament reached a *provisional deal* on the CSDDD that frames the scope of the directive, clarifies the liabilities for non-compliant companies, better defines the different penalties, and completes the list of rights and prohibitions that companies should respect.

The agreement fixes the scope of the directive on large companies that have more than 500 employees and a net worldwide turnover over €150 million. For **non-EU companies** it will apply if they have over €150 million net turnover generated in the EU, three years from the entry into force of the directive.

Compliance with the CSDDD could be qualified as a criterion for the award of public contracts and concessions.

The Commission will publish a [list of non-EU companies](#) that fall under the scope of the directive.

According to the deal, **financial services** will be **temporarily excluded** from the scope of the directive, but there will be a review clause for a possible future inclusion of the financial downstream sector based on a sufficient impact assessment. Perhaps they give them time to comply with the Digital Operational Resilience Act (DORA) that has become very complex after the first set of final draft technical standards (17 January 2024).

Next steps - The provisional agreement reached by the Council and the European Parliament needs to be endorsed and formally adopted by both institutions.

We did not avoid the Latin phrase *vacatio legis* in the directive (an embarrassing way that legal experts use to communicate with IT, risk, and compliance experts involved in the implementation). *Vacare* in Latin means to be empty, to be free, to have leisure. It took some time, but now from *vacare* we have the word vacation. In the proposed directive, **vacatio legis** means absence of law. This is the period between the announcement of a legislation and its entering into force.

This “**vacatio legis**” only adds to the uncertainty caused by the phrases “**entry into force**” (our advice: ignore it), and “**date of applicability**” (our advice: this is for you), in the EU legal acts. The entry into force is the date when the regulation has legal existence in the legal order. Usually, an EU regulation enters into force 20 days after its publication in the Official Journal of the EU. A period of time may be needed between the date the regulation enters into force, and the date it can actually be applied. This period is deliberately introduced for Member States, competent authorities, operators, organisations etc. to prepare for compliance with the new rules.

Read more at number 4 below. Grab a cup of coffee and read the Top 10 news below. *Plenus venter non studet libenter* (a full belly does not like studying).

Washington’s “My Health My Data Act” was passed in April 2023, and expands privacy protections for personal health data. It is the first privacy-focused law in the U.S. that protects personal health data that falls **outside** the ambit of the Health Insurance Portability and Accountability Act (HIPAA).

On **March 31, 2024**, the Act’s requirements will come into force for all organizations subject to the law. Small businesses have until June 30, 2024, to comply.

I find interesting that the Act is “making it **unlawful to utilize a geofence** around a facility that provides health care services”. According to Section 3, “**Geofence means** technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wifi data, and/or any other form of spatial or location detection to establish a virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary. For purposes of this definition, “geofence” means a virtual boundary that is **2,000 feet** or less from the perimeter of the physical location”.

In Section 10 we read: “It is unlawful for any person to implement a geofence around an entity that provides in-person health care services where such geofence is used to:

- (1) Identify or track consumers seeking health care services;
- (2) collect consumer health data from consumers; or
- (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.

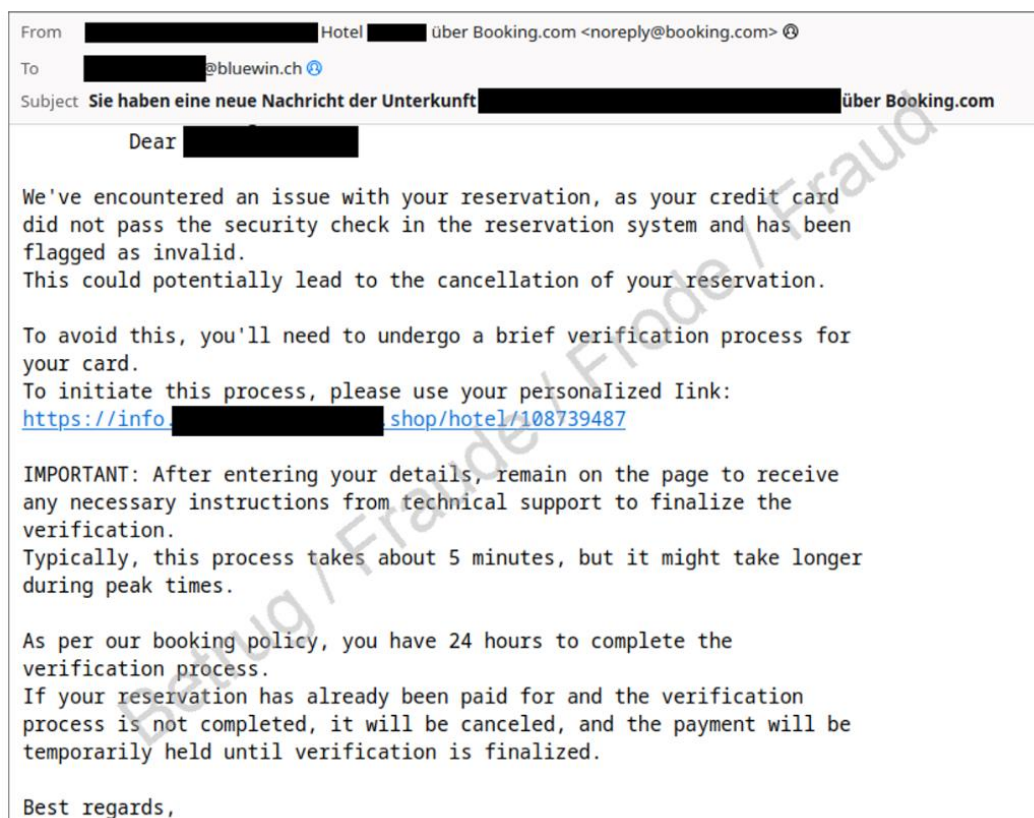
The Act protects **consumer health data**, defined as “personal information that is linked or reasonably linkable to a consumer and that identifies the consumer’s past, present, or future physical or mental health status.”

It is interesting that “physical or mental **health status**” includes “**precise location** information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies.”

Washington’s “My Health My Data Act” has **nothing to do** with the “European Data Act” that makes **more data available** for use, and sets up rules on who can use and access what data for which purposes across all economic sectors in the EU.

Read more at number 19 below.

According to the Swiss National Cyber Security Center (NCSC), most of the **phishing-related** complaints received by the NCSC relate to emails or text messages designed to look like they originate from the Swiss Post, the SBB/SwissPass, or banks. There is an interesting variation targeting users of **booking.com**.



Typical scenarios generally follow the same pattern. After a guest makes a hotel booking, they **receive an email** claiming that their credit card has to be checked again, or that their booking can only be confirmed once they have re-entered their credit card information.

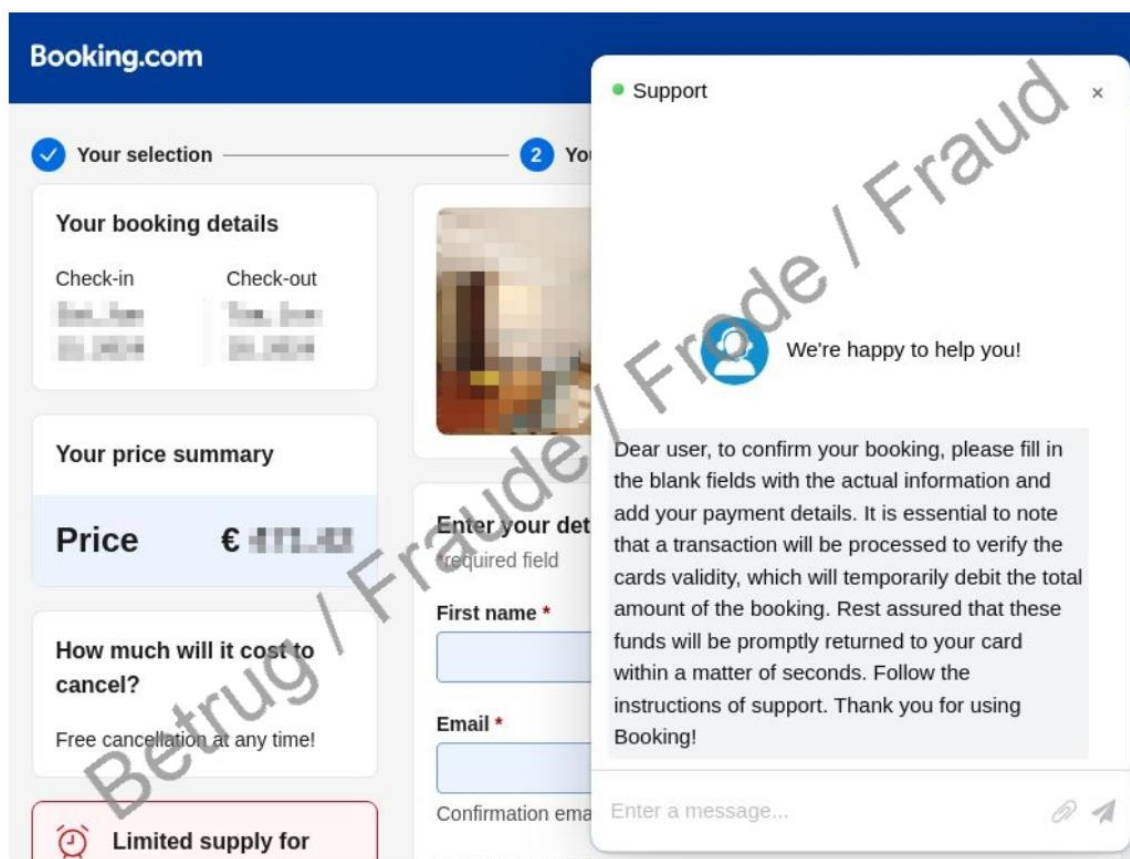
The email does in fact originate from booking.com and is sent **from the account of the hotel** that the guest has made a booking with – because the fraudsters have taken over the hotel's account and are using it to send fraudulent messages.

Recipients **accept the messages as trustworthy** because of their apparent (and verifiable) origin and because they contain the correct booking information.

If a source email looks legitimate, many recipients will click on links without looking at them carefully. Furthermore, the links sent in these emails contain correct personalised information about the guest and their booking.

The links do not lead to booking.com, however – instead, the user is taken to a phishing web page that is a professional-looking copy. The fake web page also shows correct information about the booking, and its design looks like that of the authentic booking.com site.

Once the guest enters their credit card details on the web form, the unexpected charges quickly begin.



Recommendations from the Swiss National Cyber Security Center (NCSC),

- Always think carefully about suspicious requests, and never enter information on a web page that you have accessed using a link sent by unknown parties.
- If you realise you have entered your password on a phishing website,

change the password immediately everywhere that you use it.

- If the password in question is an email password, reset your password for every service connected with this email address. This will prevent the fraudsters from using your email account to reset those other passwords.
- If you realise you have entered your credit card data on a phishing website, contact your credit card provider immediately so that they can block the card . If fraudulent charges have already been made on the card, the NCSC recommends making a report of a criminal offence with the local police.
- Activate two-factor authentication, which provides your online accounts with an additional layer of protection. This makes it more difficult for unauthorised parties to access them, even if they have managed to find out your password. Many online services offer this protection, including booking.com.

To read more:

https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/wochenrueckblick_10.html

Welcome to our monthly newsletter.

Best regards,



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



[INDEX](#) [CRA TRAINING](#) [CRA BOARD TRAINING](#) [CRA TEXT 15.9.2022](#) [CRA LINKS](#) [CYBER RISK GMBH](#) [IMPRE](#)

12 March 2024 - the European Parliament approved the Cyber Resilience Act.

The Cyber Resilience Act was approved with 517 votes in favour, 12 against and 78 abstentions.

Text adopted: "European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))".

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html

Next step: It must be formally adopted by the Council.

Number 1 (Page 12)

Disrupting malicious uses of AI by state-affiliated threat actors

*Number 2 (Page 16)*

WhatsApp, text messages, Off-Channel Communications – **Be careful**

This time the compliance failure comes from Broker-Dealers and Investment Advisers

*Number 3 (Page 18)*

NIST Releases Version 2.0 of Landmark Cybersecurity Framework

*Number 4 (Page 21)*

Revisiting the deal after Christmas

Corporate sustainability due diligence: Council and Parliament strike deal to protect environment and human rights

*Number 5 (Page 24)*

NIST SP 800-66 Rev. 2 - Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide, February 2024

*Number 6 (Page 27)*

Peer Review of Switzerland

Review report

*Number 7 (Page 30)*

Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment



Number 8 (Page 33)

CISA and MS-ISAC Release Advisory on Compromised Account Used to Access State Government Organization

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Number 9 (Page 34)

Researchers develop a tantalizing method to study cyberdeterrence



Number 10 (Page 37)

ARTIFICIAL INTELLIGENCE - Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity



United States Government Accountability Office
Report to Congressional Addressees

Number 11 (Page 39)

Using AI to develop enhanced cybersecurity measures

New research helps identify an unprecedented number of malware families



Number 12 (Page 41)

EU Digital Markets Act: the application by Bytedance (TikTok) seeking suspension of the Commission decision designating it as a gatekeeper is dismissed



Number 13 (Page 43)

EU list of non-cooperative jurisdictions for tax purposes



Number 14 (Page 44)

Announcing Microsoft's open automation framework to red team generative AI Systems

By Ram Shankar Siva Kumar, Microsoft AI Red Team Lead



Number 15 (Page 47)

Reward Offers for Information on LockBit Leaders and Designating Affiliates

U.S. DEPARTMENT of STATE

Number 16 (Page 51)

NIST, Nonprofit Research Consortium to Develop Safety Tools for Synthetic Biology to Defend Against Potential Misuse of AI



Number 17 (Page 53)

Are Russian Narratives Amplified by PRC Media?

A Case Study on Narratives Related to Sweden's and Finland's NATO Applications



Number 18 (Page 57)

#StopRansomware: ALPHV Blackcat



Number 19 (Page 59)

My Health My Data Act



Number 20 (Page 62)

The EBA consults on Guidelines on redemption plans under the Markets in Crypto-Assets Regulation



Number 21 (Page 65)

Android and Windows RATs Distributed Via Online Meeting Lures - Zscaler Blog



Number 22 (Page 66)

FCC Makes AI-Generated Voices in Robocalls Illegal



Number 23 (Page 68)

Basel Committee agrees to revisions to Basel Core Principles



Number 24 (Page 70)

Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google

Defendant Allegedly Pilfered Technology from Google While Secretly Working for Two PRC-Based Technology Companies



Number 25 (Page 75)

Researchers Develop Missing LINC to Help Vehicles Adapt to Unknowns



Number 26 (Page 77)

Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

THE WHITE HOUSE



Number 1

Disrupting malicious uses of AI by state-affiliated threat actors



We terminated accounts associated with state-affiliated threat actors. Our findings show our models offer only limited, incremental capabilities for malicious cybersecurity tasks.

We build AI tools that improve lives and help solve complex challenges, but we know that malicious actors will sometimes try to abuse our tools to harm others, including in furtherance of cyber operations. Among those malicious actors, state-affiliated groups—which may have access to advanced technology, large financial resources, and skilled personnel—can pose unique risks to the digital ecosystem and human welfare.

In partnership with Microsoft Threat Intelligence, we have disrupted five state-affiliated actors that sought to use AI services in support of malicious cyber activities. We also outline our approach to detect and disrupt such actors in order to promote information sharing and transparency regarding their activities.

Disruption of threat actors

Based on collaboration and information sharing with Microsoft, we disrupted five state-affiliated malicious actors: two China-affiliated threat actors known as Charcoal Typhoon and Salmon Typhoon; the Iran-affiliated threat actor known as Crimson Sandstorm; the North Korea-affiliated actor known as Emerald Sleet; and the Russia-affiliated actor known as Forest Blizzard. The identified OpenAI accounts associated with these actors were terminated.

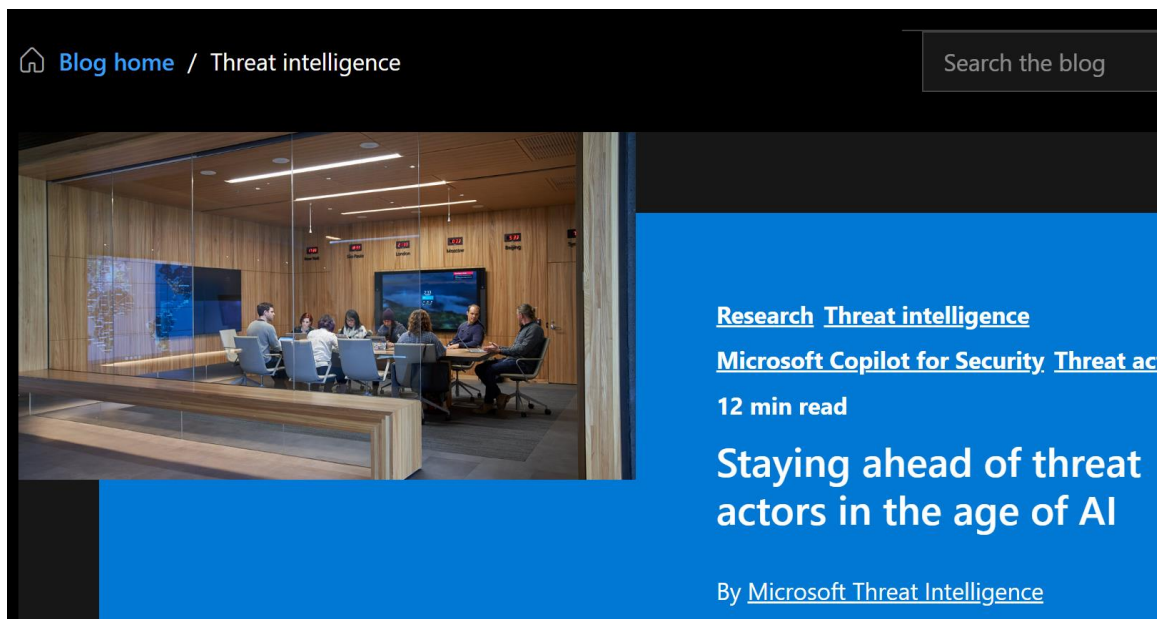
These actors generally sought to use OpenAI services for querying open-source information, translating, finding coding errors, and running basic coding tasks.

Specifically:

- Charcoal Typhoon used our services to research various companies and cybersecurity tools, debug code and generate scripts, and create content likely for use in phishing campaigns.
- Salmon Typhoon used our services to translate technical papers, retrieve publicly available information on multiple intelligence agencies and regional threat actors, assist with coding, and research common ways processes could be hidden on a system.
- Crimson Sandstorm used our services for scripting support related to app and web development, generating content likely for spear-phishing campaigns, and researching common ways malware could evade detection.

- Emerald Sleet used our services to identify experts and organizations focused on defense issues in the Asia-Pacific region, understand publicly available vulnerabilities, help with basic scripting tasks, and draft content that could be used in phishing campaigns.
- Forest Blizzard used our services primarily for open-source research into satellite communication protocols and radar imaging technology, as well as for support with scripting tasks.

Additional technical details on the nature of the threat actors and their activities can be found in the Microsoft blog post: <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>



The activities of these actors are consistent with previous red team assessments we conducted in partnership with external cybersecurity experts, which found that GPT-4 offers only limited, incremental capabilities for malicious cybersecurity tasks beyond what is already achievable with publicly available, non-AI powered tools.

A multi-pronged approach to AI safety

Although the capabilities of our current models for malicious cybersecurity tasks are limited, we believe it's important to stay ahead of significant and evolving threats. To respond to the threat, we are taking a multi-pronged approach to combating malicious state-affiliate actors' use of our platform:

- *Monitoring and disrupting malicious state affiliated actors.* We invest in technology and teams to identify and disrupt sophisticated threat actors' activities.

Our Intelligence and Investigations team—working in concert with our Safety, Security, and Integrity teams—investigates malicious actors in a

variety of ways, including using our models to pursue leads, analyze how adversaries are interacting with our platform, and assess their broader intentions.

Upon detection, OpenAI takes appropriate action to disrupt their activities, such as disabling their accounts, terminating services, or limiting access to resources.

- *Working together with the AI ecosystem.* OpenAI collaborates with industry partners and other stakeholders to regularly exchange information about malicious state-affiliated actors' detected use of AI.

This collaboration reflects our voluntary commitment to promote the safe, secure and transparent development and use of AI technology, and aims to promote collective responses to ecosystem-wide risks via information sharing.

- *Iterating on safety mitigations.* Learning from real-world use (and misuse) is a key component of creating and releasing increasingly safe AI systems over time. We take lessons learned from these actors' abuse and use them to inform our iterative approach to safety.

Understanding how the most sophisticated malicious actors seek to use our systems for harm gives us a signal into practices that may become more widespread in the future, and allows us to continuously evolve our safeguards.

- *Public transparency.* We have long sought to highlight potential misuses of AI and share what we have learned about safety [link 1, link 2] with the industry and the public.

As part of our ongoing efforts to advance responsible use of AI, OpenAI will continue to inform the public and stakeholders about the nature and extent of malicious state-affiliated actors' use of AI detected within our systems and the measures taken against them, when warranted.

We believe that sharing and transparency foster greater awareness and preparedness among all stakeholders, leading to stronger collective defense against ever-evolving adversaries. You may visit:

<https://openai.com/research/language-model-safety-and-misuse>

<https://openai.com/blog/best-practices-for-deploying-language-models>

The vast majority of people use our systems to help improve their daily lives, from virtual tutors for students to apps that can transcribe the world for people who are seeing impaired.

As is the case with many other ecosystems, there are a handful of malicious actors that require sustained attention so that everyone else can continue to enjoy the

benefits. Although we work to minimize potential misuse by such actors, we will not be able to stop every instance.

But by continuing to innovate, investigate, collaborate, and share, we make it harder for malicious actors to remain undetected across the digital ecosystem and improve the experience for everyone else.

To read more: <https://openai.com/blog/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors>

Number 2

WhatsApp, text messages, Off-Channel Communications – Be careful

This time the compliance failure comes from Broker-Dealers and Investment Advisers



Sixteen Firms to Pay More Than \$81 Million Combined to Settle Charges for Widespread Recordkeeping Failures.

The Securities and Exchange Commission announced charges against five broker-dealers, seven dually registered broker-dealers and investment advisers, and four affiliated investment advisers for widespread and longstanding failures by the firms and their employees to **maintain and preserve electronic communications**.

The firms admitted the facts set forth in their respective SEC orders, acknowledged that their conduct violated recordkeeping provisions of the federal securities laws, agreed to pay combined civil penalties of more than \$81 million, as outlined below, and have begun implementing improvements to their compliance policies and procedures to address these violations.

“Today’s actions against these 16 firms result from our continuing efforts to ensure that all regulated entities comply with the recordkeeping requirements, which are essential to our ability to monitor and enforce compliance with the federal securities laws,” said Gurbir S. Grewal, Director of the SEC’s Division of Enforcement. “Once again, one of these orders is not like the others: Huntington’s penalty reflects its voluntary self-report and cooperation.”

The SEC’s investigations uncovered pervasive and longstanding uses of **unapproved communication** methods, known as off-channel communications, at all 16 firms. As described in the SEC’s orders, the broker-dealer firms admitted that, from at least 2019 or 2020, their employees communicated through **personal text messages** about the business of their employers.

The investment adviser firms admitted that their employees sent and received **off-channel** communications related to **recommendations** made or proposed to be made and advice given or proposed to be given.

The firms did not maintain or preserve the substantial majority of these off-channel communications, in violation of the federal securities laws. By failing to maintain and preserve required records, some of the firms likely deprived the SEC of these off-channel communications in various SEC investigations.

The failures involved employees at multiple levels of authority, including supervisors and senior managers.

In addition to the significant financial penalties, each of the firms was ordered to cease and desist from future violations of the relevant recordkeeping provisions and was censured.

The firms also agreed to retain independent compliance consultants to, among other things, conduct comprehensive reviews of their policies and procedures relating to the retention of electronic communications found on personal devices and their respective frameworks for addressing non-compliance by their employees with those policies and procedures.

To read more: <https://www.sec.gov/news/press-release/2024-18>

Number 3

NIST Releases Version 2.0 of Landmark Cybersecurity Framework



- NIST’s cybersecurity framework (CSF) now explicitly aims to help all organizations — not just those in critical infrastructure, its original target audience — to manage and reduce risks.
- NIST has updated the CSF’s core guidance and created a suite of resources to help all organizations achieve their cybersecurity goals, with added emphasis on governance as well as supply chains.
- This update is the outcome of a multiyear process of discussions and public comments aimed at making the framework more effective.

The National Institute of Standards and Technology (NIST) has updated the widely used Cybersecurity Framework (CSF), its landmark guidance document for reducing cybersecurity risk.

The new 2.0 edition is designed for all audiences, industry sectors and organization types, from the smallest schools and nonprofits to the largest agencies and corporations — regardless of their degree of cybersecurity sophistication.

In response to the numerous comments received on the draft version, NIST has expanded the CSF’s core guidance and developed related resources to help users get the most out of the framework. These resources are designed to provide different audiences with tailored pathways into the CSF and make the framework easier to put into action.

“The CSF has been a vital tool for many organizations, helping them anticipate and deal with cybersecurity threats,” said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio.

“CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization’s cybersecurity needs change and its capabilities evolve.”

The CSF 2.0, which supports implementation of the National Cybersecurity Strategy, has an expanded scope that goes beyond protecting critical infrastructure, such as hospitals and power plants, to all organizations in any sector.

It also has a new focus on governance, which encompasses how organizations make and carry out informed decisions on cybersecurity strategy.

The CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk that senior leaders should consider alongside others such as finance and reputation.

“Developed by working closely with stakeholders and reflecting the most recent cybersecurity challenges and management practices, this update aims to make the framework even more relevant to a wider swath of users in the United States and abroad,” according to Kevin Stine, chief of NIST's Applied Cybersecurity Division.

Following a presidential Executive Order, NIST first released the CSF in 2014 to help organizations understand, reduce and communicate about cybersecurity risk. The framework's core is now organized around six key functions: Identify, Protect, Detect, Respond and Recover, along with CSF 2.0's newly added Govern function. When considered together, these functions provide a comprehensive view of the life cycle for managing cybersecurity risk.

The updated framework anticipates that organizations will come to the CSF with varying needs and degrees of experience implementing cybersecurity tools. New adopters can learn from other users' successes and select their topic of interest from a new set of implementation examples and quick-start guides designed for specific types of users, such as small businesses, enterprise risk managers, and organizations seeking to secure their supply chains.

A new CSF 2.0 Reference Tool now simplifies the way organizations can implement the CSF, allowing users to browse, search and export data and details from the CSF's core guidance in human-consumable and machine-readable formats.

In addition, the CSF 2.0 offers a searchable catalog of informative references that shows how their current actions map onto the CSF. This catalog allows an organization to cross-reference the CSF's guidance to more than 50 other cybersecurity documents, including others from NIST, such as SP 800-53 Rev. 5, a catalog of tools (called controls) for achieving specific cybersecurity outcomes.

Organizations can also consult the Cybersecurity and Privacy Reference Tool (CPRT), which contains an interrelated, browsable and downloadable set of NIST guidance documents that contextualizes these NIST resources, including the CSF, with other popular resources. And the CPRT offers ways to communicate these ideas to both technical experts and the C-suite, so that all levels of an organization can stay coordinated.

NIST plans to continue enhancing its resources and making the CSF an even more helpful resource to a broader set of users, Stine said, and feedback from the community will be crucial.

“As users customize the CSF, we hope they will share their examples and successes, because that will allow us to amplify their experiences and help others,” he said. “That will help organizations, sectors and even entire nations better understand and manage their cybersecurity risk.”

The CSF is used widely internationally; Versions 1.1 and 1.0 have been translated into 13 languages, and NIST expects that CSF 2.0 also will be translated by volunteers around the world. Those translations will be added to NIST's expanding portfolio of CSF resources.

Over the last 11 years, NIST's work with the International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), has helped to align multiple cybersecurity documents.

ISO/IEC resources now allow organizations to build cybersecurity frameworks and organize controls using the CSF functions. NIST plans to continue working with ISO/IEC to continue this international alignment.



<h3>CSF 2.0</h3> <p>For industry, government, and organizations to reduce cybersecurity risks</p> <p>Read the Document</p>	<h3>Quick Start Guides</h3> <p>For users with specific common goals</p> <p>View the Quick Start Guides</p>
<h3>CSF 2.0 Profiles</h3> <p>Templates and useful resources for creating and using both CSF profiles</p> <p>See the Profiles</p>	<h3>Informative References (Mappings)</h3> <p>See how NIST's resources overlap and share themes</p> <p>See the Mappings</p>

To read more: <https://www.nist.gov/cyberframework>

Number 4

Revisiting the deal after Christmas

Corporate sustainability due diligence: Council and Parliament strike deal to protect environment and human rights



The Council and the European Parliament reached a provisional deal on the corporate sustainability due diligence directive (CSDDD), which aims to enhance the protection of the environment and human rights in the EU and globally.

The due diligence directive will set obligations for large companies regarding actual and potential adverse impacts on human rights and the environment, with respect to their own operations, those of their subsidiaries, and those carried out by their business partners.

Obligations for companies

The due diligence directive lays down rules on obligations for large companies regarding actual and potential adverse impacts on the environment and human rights for their business chain of activities which covers the upstream business partners of the company and partially the downstream activities, such as distribution or recycling.

The directive also lays down rules on penalties and civil liability for infringing those obligations; it requires companies to adopt a plan ensuring that their business model and strategy are compatible with the Paris agreement on climate change.

Main elements of the agreement

The provisional agreement reached today between the two co-legislators frames the scope of the directive, clarifies the liabilities for non-compliant companies, better defines the different penalties, and completes the list of rights and prohibitions that companies should respect.

Scope of the directive

The agreement fixes the scope of the directive on large companies that have more than 500 employees and a net worldwide turnover over €150 million.

For non-EU companies it will apply if they have over €150 million net turnover generated in the EU, three years from the entry into force of the directive.

The Commission will have to publish a list of non-EU companies that fall under the scope of the directive.

Financial Sector

According to the deal reached today, financial services will be temporarily excluded from the scope of the directive, but there will be a review clause for a possible future inclusion of the financial downstream sector based on a sufficient impact assessment.

Climate change and civil liability

The compromise struck today strengthens the provisions related to the obligation of means for large companies to adopt and put into effect, through best efforts, a transition plan for climate change mitigation.

On civil liability, the agreement reinforces the access to justice of persons affected. It establishes a period of five years to bring claims by those concerned by adverse impacts (including trade unions or civil society organisations). It also limits the disclosure of evidence, injunctive measures, and cost of the proceedings for claimants.

As a last resort, companies that identify adverse impacts on environment or human rights by some of their business partners will have to end those business relationships when these impacts cannot be prevented or ended.

Penalties

For companies that fail to pay fines imposed on them in the event of violation of the directive, the provisional agreement includes several injunction measures, and takes into consideration the turnover of the company to impose pecuniary penalties (i.e. a minimum maximum of 5% of the company's net turnover). The deal includes the obligation for companies to carry out meaningful engagement including a dialogue and consultation with affected stakeholders, as one of the measures of the due diligence process.

Public procurement

The deal establishes that compliance with the CSDDD could be qualified as a criterion for the award of public contracts and concessions.

Definitions

The provisional agreement clarifies the obligations for companies described in Annex I, a list of specific rights and prohibitions which constitutes an adverse human rights impact when they are abused or violated. The list makes references to international instruments that have been ratified by all member states and that set sufficiently clear standards that can be observed by companies.

The compromise adds new elements to the obligations and instruments listed in the Annex as regards human rights, particularly for vulnerable groups. Core International Labour Organisation (ILO) Conventions can also be added to the list, by delegated acts, once they have been ratified by all member states.

The provisional agreement also introduces in the annex references to other UN conventions, such as the International covenant on civil and political rights or the International covenant on economic, social and cultural rights, or the Convention on the rights of the child.

Likewise, the compromise clarifies the nature of environmental impacts covered by this directive as any measurable environmental degradation, such as harmful soil change, water or air pollution, harmful emissions or excessive water consumption or other impacts on natural resources.

Next steps

The provisional agreement reached with the European Parliament now needs to be endorsed and formally adopted by both institutions.

To read more: <https://www.consilium.europa.eu/en/press/press-releases/2023/12/14/corporate-sustainability-due-diligence-council-and-parliament-strike-deal-to-protect-environment-and-human-rights/#:~:text=The%20due%20diligence%20directive%20lays,the%20downstream%20activities%2C%20such%20as>

*Number 5***NIST SP 800-66 Rev. 2 - Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide, February 2024**

This publication aims to help educate readers about the security standards included in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, as amended by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act and Other Modifications to the HIPAA Rules.

**NIST Special Publication 800
NIST SP 800-66r2**

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

A Cybersecurity Resource Guide

Jeffrey A. Marron

In general, the requirements, standards, and implementation specifications of the Security Rule apply to the following regulated entities:

- **Covered Healthcare Providers** — Any provider of medical or other health services or supplies who transmits any health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services (HHS) has adopted a standard.
- **Health Plans** — Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- **Healthcare Clearinghouses** — A public or private entity that processes another entity's healthcare transactions from a standard format to a non-standard format or vice versa.
- **Business Associate** — A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on

behalf of or provides services to a covered entity. A business associate is liable for their own HIPAA violations.

The Security Rule is separated into six main sections that each include several standards that a regulated entity must meet.

Many of the standards contain implementation specifications.

An implementation specification is a more detailed description of the method or approach that regulated entities can use to meet a particular standard.

Implementation specifications are either required or addressable. Regulated entities must comply with required implementation specifications. Regulated entities must perform an assessment to determine whether each addressable implementation specification is a reasonable and appropriate safeguard to implement in the regulated entity's environment.

The assessment, analysis, and management of risk to ePHI provide the foundation for a regulated entity's Security Rule compliance efforts and the protection of ePHI. Readers are reminded of the Security Rule's flexibility of approach. The HHS Office for Civil Rights (OCR) does not prescribe any particular risk assessment or risk management methodology.

Section 3 and Sec. 4 provide background information about risk assessment and risk management processes, respectively, as well as approaches that regulated entities may choose to use in assessing and managing risk to ePHI.

Many regulated entities may benefit from more specific guidance concerning how to comply with the standards and implementation specifications of the Security Rule.

To that end, Sec. 5 highlights considerations for a regulated entity when implementing the Security Rule. Key activities, descriptions, and sample questions are provided for each standard. The key activities suggest actions that are often associated with the security functions suggested by that standard.

Many of these key activities are often included in a robust security program and may be useful to regulated entities. The descriptions provide expanded explanations about each of the key activities and the types of activities that a regulated entity may pursue when implementing the standard.

The sample questions are a non-exhaustive list of questions that a regulated entity may ask itself to determine whether the standard has been adequately implemented.

Regulated entities may implement the Security Rule more effectively if they are shown controls catalogs and cybersecurity activities that align with each standard. To assist regulated entities, this publication includes mappings of the Security Rule's standards and implementation specifications to Cybersecurity Framework [NIST CSF] Subcategories and applicable security controls detailed in

NIST Special Publication (SP) 800-53r5 (Revision 5), Security and Privacy Controls for Information Systems and Organizations [SP 800-53].

The mapping also lists additional NIST publications relevant to each Security Rule standard. Readers may draw upon these NIST publications and mappings for assistance in implementing the Security Rule.

Additionally, Appendix F links to a wide variety of resources (e.g., guidance, templates, tools) that regulated entities may find useful for complying with the Security Rule and improving the security posture of their organizations.

For ease of use, the resources are organized by topic. Regulated entities could consult these resources when they need additional information or guidance about a particular topic.

To read more:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf>

Number 6

Peer Review of Switzerland

Review report



Main findings

The Swiss authorities have made important strides toward implementing an effective TBTF regime for G-SIBs. Switzerland introduced capital and liquidity requirements beyond the international minimum standards to increase G-SIBs' abilities to cope with stress scenarios. Supervision of G-SIBs has increased in intensity over time and under the Swiss Financial Market Supervisory Authority's (FINMA's) proportional and systematic risk-oriented approach, relatively more resources are devoted to the supervision of G-SIBs than for other Swiss banks. FINMA has streamlined routine regulatory audits to re-deploy resources to conducting more risk-focused supervisory activities. FINMA has also increased the transparency of its supervisory activities, and in so doing helps alert banks and the public of risks facing the Swiss financial market.

Financial Stability Board (FSB) member jurisdictions have committed, under the FSB Charter and in the FSB Framework for Strengthening Adherence to International Standards, to undergo periodic peer reviews.

To fulfil this responsibility, the FSB has established a regular programme of country and thematic peer reviews of its member jurisdictions.

Country reviews focus on the implementation and effectiveness of regulatory, supervisory or other financial sector policies in a specific FSB jurisdiction.

They examine the steps taken or planned by national/regional authorities to address IMF-World Bank Financial Sector Assessment Program (FSAP) and Reports on the Observance of Standards and Codes recommendations on financial regulation and supervision as well as on institutional and market infrastructure that are deemed most important and relevant to the FSB's core mandate of promoting financial stability.

Country reviews can also focus on regulatory, supervisory or other financial sector policy issues not covered in the FSAP that are timely and topical for the jurisdiction and for the broader FSB membership.

Unlike the FSAP, a peer review does not comprehensively analyse a jurisdiction's financial system structure or policies, or its compliance with international financial standards.

FSB jurisdictions have committed to undergo an FSAP assessment every five years; peer reviews taking place typically two to three years following an FSAP will complement that cycle.

As part of this commitment, Switzerland volunteered to undergo a peer review in 2022-2023. This report describes the findings and conclusions of the Switzerland peer review, including the key elements of the discussion in the FSB's Standing Committee on Standards Implementation (SCSI) in November 2023.

It is the second FSB peer review of Switzerland and is based on the objectives and guidelines for the conduct of peer reviews set forth in the Handbook for FSB Peer Reviews.

The analysis and conclusions of this peer review are based on the responses to questionnaires by financial authorities in Switzerland and reflect information on the progress of relevant reforms as of December 2023.

The review has also benefited from dialogue with the Swiss authorities as well as discussion in the FSB SCSI. The draft report for discussion was prepared by a team chaired by Arthur Yuen (Hong Kong Monetary Authority) and comprising Marc-Oliver Thurner (Reserve Bank of Australia), Stefania Gallo (Banca d'Italia), Adam Cull (Bank of England), Kristin Malcarney (Federal Reserve Bank of New York) and Milada McCabe (Single Resolution Board). Michael Januska, Hans Sassen and Marianne Klumpp (FSB Secretariat) provided support to the team and contributed to the preparation of the report.

Annex 1: Switzerland's implementation of G20 reforms (as of September 2023)

This table presents the status of implementation of G20 financial regulatory reforms, drawing on information from various sources. The tables below distinguish between **priority areas** that undergo more intensive monitoring and detailed reporting via progress reports and peer reviews, and **other areas** of reform whose monitoring is based on annual survey responses by FSB member jurisdictions. See [here](#) for further information.

IMPLEMENTATION STATUS OF REFORMS IN PRIORITY AREAS																		
Reform Area	BASEL III					COMPENSATION	OVER-THE-COUNTER (OTC) DERIVATIVES				RESOLUTION				NON-BANK FINANCIAL INTERMEDIATION			
	Risk-based capital	Requirements for SIBs	Large exposures framework	Leverage ratio	Net Stable Funding Ratio (NSFR)		Trade reporting	Central clearing	Platform trading	Margin	Minimum external TLAC for G-SIBs	Transfer / bail-in / temporary stay powers for banks	Recovery and resolution planning for systemic banks	Transfer / bridge / run-off powers for insurers	Resolution planning for SIB-1 CCPs	Money market funds (MMFs)	Securitisation	Securities financing transactions (SFTs)
Agreed phase-in (completed) date	2023	2016 (2019)	2019	2023	2018		end-2012	end-2012	end-2012	2016 (2022)	2019/2025 (2022/2028)						2017/2023	
Status		C																***
Legend	■ Final rule or framework implemented. ■ Final rule published but not implemented, draft regulation published or framework being implemented. ■ Draft regulation not published or no framework in place (dark red colour indicates that deadline has lapsed). ■ Requirements reported as non-applicable. Basel III: C=Compliant, LC=Largely compliant, MNC=Materially non-compliant, NC=Non-compliant. Compensation: B=Principles and Standards deemed applicable only for banks (B) and/or insurers (I). OTC derivatives: RF=Further action required to remove barriers to full trade reporting (R) or to access trade repository data by foreign authority (F). Non-bank financial intermediation: **=Implementation is more advanced in one or more/all elements of at least one reform area (money market funds), or in one or more / all sectors of the market (securitisation). Further information on the legend.																	
Notes	CCPs=Central counterparties. G-SIBs=Global Systemically Important Banks. TLAC=Total Loss-Absorbing Capacity. SIB-1=Systemically important in more than one jurisdiction.																	
Source	FSB, <i>Promoting Global Financial Stability: 2023 FSB Annual Report</i> , October 2023.																	

IMPLEMENTATION STATUS OF REFORMS IN OTHER AREAS												
Reform area	Hedge funds			Securitisation			Supervision				Macroprudential frameworks and tools	
	Registration, appropriate disclosures and oversight of hedge funds	Establishment of international information sharing framework	Enhancing counterparty risk management	Strengthening of regulatory and capital framework for monolines	Strengthening supervisory requirements or best practices for investment in structured products	Enhanced disclosure of securitised products	Consistent, consolidated supervision and regulation of SIFIs	Establishing supervisory colleges and conducting risk assessments	Supervisory exchange of information and coordination	Strengthening resources and effective supervision	Establishing regulatory framework for macroprudential oversight	Enhancing system-wide monitoring and the use of macroprudential instruments
Status	REF*	REF	REF*	N/A*	N/A	N/A	REF	N/A*	REF	REF	REF	REF
Reform area	Credit rating agencies		Accounting standards	Risk management		Deposit insurance	Integrity and efficiency of financial markets		Financial consumer protection			
	Enhancing regulation and supervision of CRAs	Reducing the reliance on ratings	Consistent application of high-quality accounting standards	Enhancing guidance to strengthen banks' risk management practices	Enhanced risk disclosures by financial institutions		Enhancing market integrity and efficiency	Regulation and supervision of commodity markets				
Status	REF*	REF	REF	REF	REF	IOG	REF	REF	REF			
Legend	REF=Implementation reported as completed. IOG=Implementation reported as ongoing. ABN=Applicable but no action envisaged at the moment. N/A=Not applicable. *="collected in previous year(s) for all members.											
Notes	The FSB has not undertaken an evaluation of survey responses to verify the status or assess the effectiveness of implementation. In a number of cases, the complexity of the reforms and the summarised nature of the responses does not allow for straightforward comparisons across jurisdictions or reform areas. In particular, reforms whose status in a particular area is reported as complete should not be interpreted to mean that no further policy steps (or follow-up supervisory work) are anticipated in that area. CRA = Credit Rating Agency, SIFI = Systemically important financial institution.											
Source	FSB, <i>Jurisdictions' Responses to the IMN Survey</i> .											

Box 2: Roles of Swiss federal authorities in bank supervision

The Swiss Financial Market Supervisory Authority (FINMA) is the prudential and conduct authority for financial supervision in Switzerland. FINMA was established in 2009 from the merger of its three predecessor institutions: the Swiss Federal Banking Commission (SFBC), the Federal Office of Private Insurance (FOPI) and the Anti-Money Laundering Control Authority (AMLCO). Whilst its Board of Directors is FINMA's strategic management body, the Executive Board manages the operations of the authority.

The Swiss National Bank (SNB) is the monetary authority and the lender of last resort. The National Bank Act of 3 October 2003 serves as the statutory basis for the SNB and its activity. SNB has an explicit mandate to contribute to the stability of the financial system. The SNB is responsible for designating (after consulting FINMA) the SIBs and their systemically important functions, and for submitting proposals on the countercyclical capital buffer to the Federal Council.

The Swiss Federal Department of Finance (FDF) is responsible for financial stability policies and relevant laws and ordinances. The head of the FDF is a member of the Swiss Federal Council. The State Secretariat for International Finance represents Switzerland's interests on financial, monetary and tax matters and is responsible for implementing the financial market policy of the Federal Council.

The Federal Audit Oversight Authority (FAOA) is an institution under public law with its own legal identity. It is responsible for the licensing of audit firms which offer statutory audit services. In addition, it is responsible for overseeing audit firms' work on auditing public interest companies. The FAOA commenced its activities in September 2007. Since 2015 it has also assumed all of FINMA's responsibilities on audit oversight and the oversight of audit firms.

The report: <https://www.fsb.org/wp-content/uploads/P290224.pdf>

Table of Contents

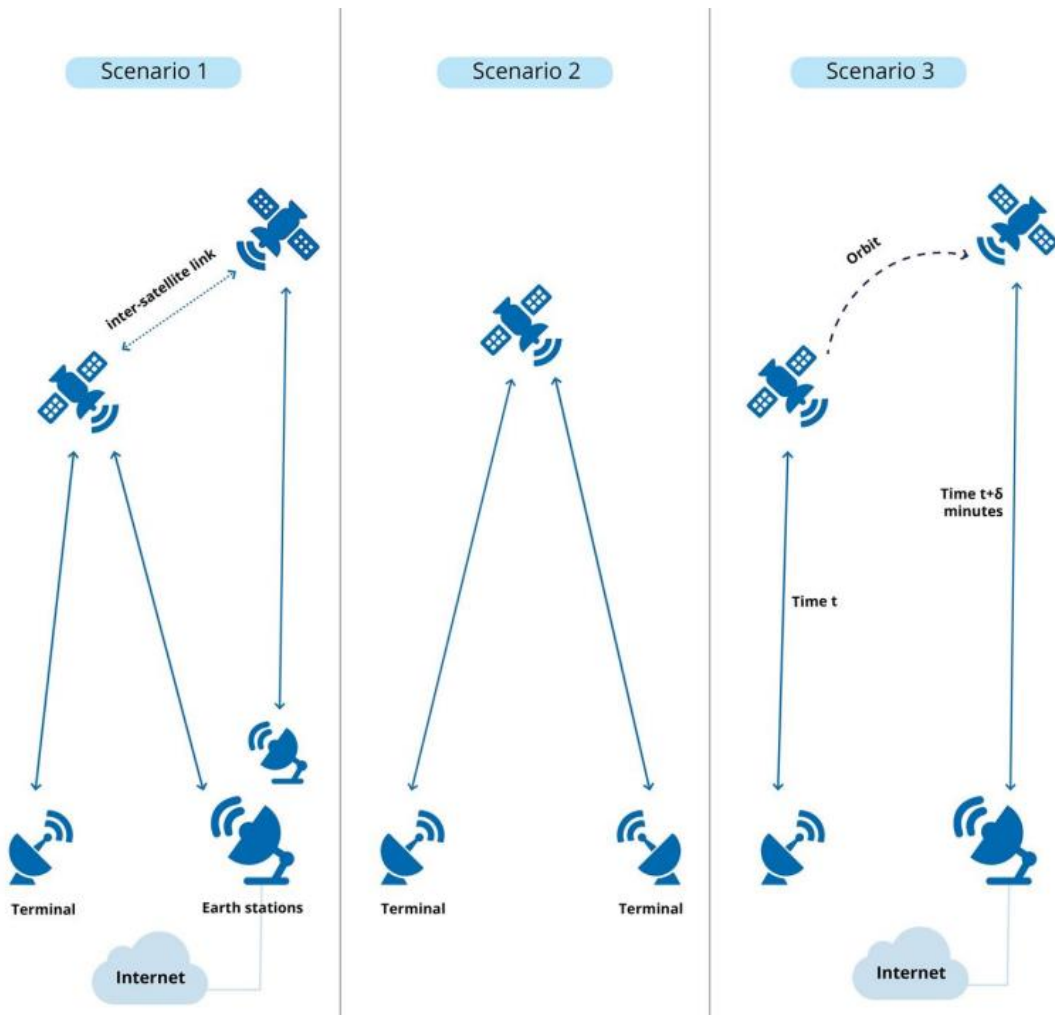
Foreword	1
Abbreviations	2
Executive summary	3
1. Introduction	7
2. Overview of the banking system and of the Swiss G-SIBs	8
3. Steps taken and actions planned	9
3.1. Capital and liquidity requirements	9
3.2. Approach to bank supervision	11
3.3. Framework for recovery and resolution of banks	17
4. Conclusions and recommendations	29
4.1. Increasing resources for supervision, recovery and resolution	30
4.2. Strengthening the supervisory framework and early intervention powers	30
4.3. Enhancing the recovery and resolution framework	32
Annex 1: Switzerland's implementation of G20 reforms (as of September 2023)	36

Number 7

Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment



This report covers the topic of cybersecurity of Low Earth Orbit (LEO) constellations delivering telecommunications services (LEO satcom in short).

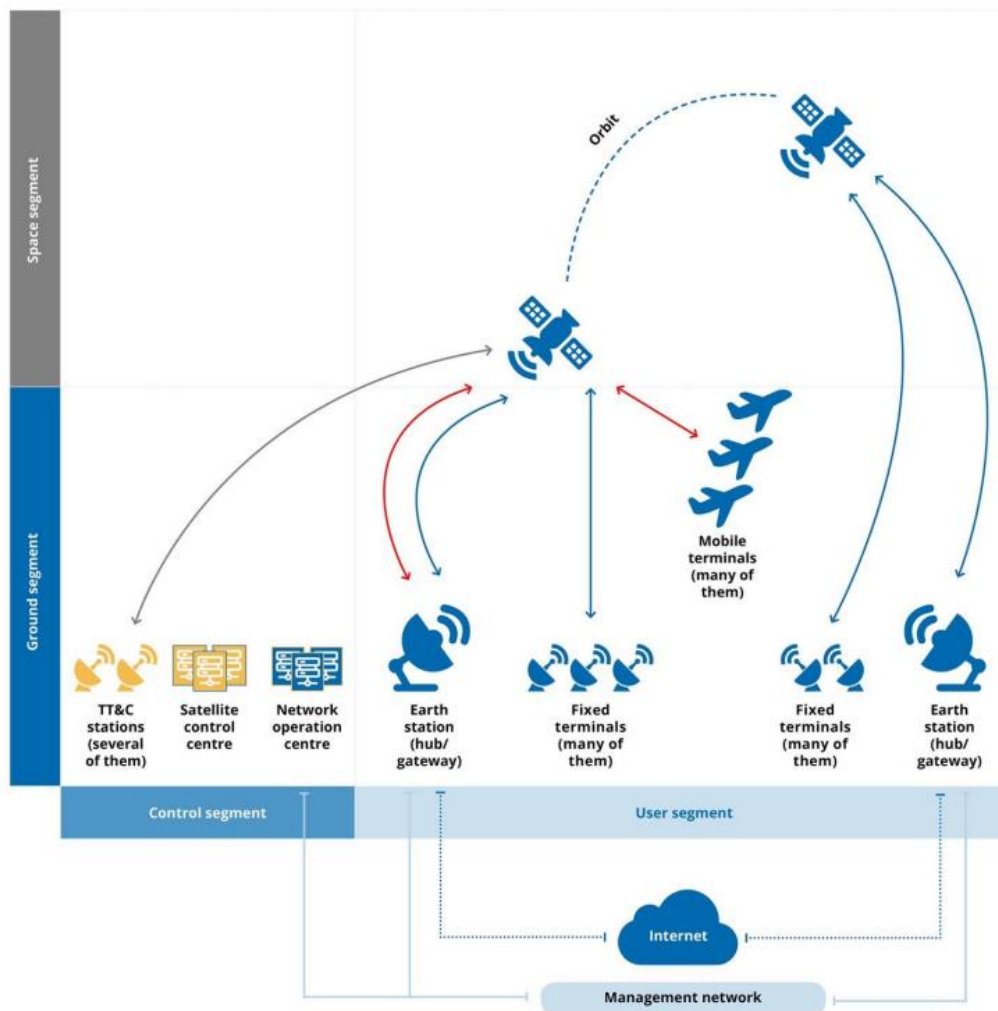


The key specifics of an LEO satcom system may be summed up as:

- many assets forming the space and ground segments, and
- a worldwide distribution of the services delivered by those assets.

These two aspects usually differentiate satcom systems from terrestrial and other space systems (such as geostationary satellites), where the service coverage under the responsibility of a single organisation/system is smaller.

Figure 2: Organisation in segments of an LEO satcom system



The global nature of LEO satcom also calls for tailored cybersecurity treatment. When looking at different threats and incurred risks (whether technical, financial or commercial), the landscape of possible attacks is rich.

It includes classic cyber threats as found in terrestrial systems that target the user and control segments (terminals, gateways, telemetry tracking and command stations, and interconnection networks).

But it also extends to attacks focusing specifically on the satellites forming the space segment. For these reasons, LEO satcom systems deserve a tailored approach when it comes to their security.

This situation is acknowledged by actors in the sector and has resulted in several initiatives, among them the European Space Agency (ESA) Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD).

The survey on past cyber incidents shows that most attacks fall roughly into two categories: data theft through reverse engineering of user link transmission

techniques; and denial of service, targeting either the ground or space segments, possibly resulting in a service degradation or outage.

The first category of incidents calls for the use of common encryption techniques. The second calls for standards and recommendations in cyber protection, which are applicable to all segments of space systems.

The report also includes a comparison of LEO satcom and broadband terrestrial cellular networks based on cyber threat exposure and impact severity.

The case of cellular networks is believed to be a representative case of more generic terrestrial networks. Based on technical considerations only, the comparison reveals that the cyber risk is higher for space systems.

Concluding, the report shows that the cyber protection needs of LEO satcom systems extend beyond what exists for terrestrial systems.

The advent of commercial mega-constellations is a clear call for a coordinated approach in space systems security by means of standards, recommendations, information sharing and training.

To read more: <https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment>

Number 8

CISA and MS-ISAC Release Advisory on Compromised Account Used to Access State Government Organization

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



CISA and the Multi-State Information Sharing & Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA), Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization to provide network defenders with the tactics, techniques, and procedures (TTPs) utilized by a threat actor and methods to protect against similar exploitation.

**JOINT
CYBERSECURITY
ADVISORY**

Co-Authored by:

TLP: CLEAR Product ID: AA24-046A
February 15, 2024

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

The banner features a dark blue background with a futuristic cityscape and network lines. The text "JOINT CYBERSECURITY ADVISORY" is prominently displayed in white. Below this, it states "Co-Authored by:" followed by the logos for CISA and MS-ISAC. To the right, it includes the classification "TLP: CLEAR", the product ID "AA24-046A", and the date "February 15, 2024".

Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization

Following an incident response assessment of a state government organization's network environment, analysis confirmed compromise through network administrator credentials of a former employee. This allowed the threat actor to successfully authenticate to an internal virtual private network (VPN) access point.

CISA and MS-ISAC encourage network defenders and organizations review the TTPs and implement the mitigations provided in the joint CSA. For more information, visit CISA's Cross-Sector Cybersecurity Performance Goals.

To read more: <https://www.cisa.gov/news-events/alerts/2024/02/15/cisa-and-ms-isac-release-advisory-compromised-account-used-access-state-government-organization>

Number 9

Researchers develop a tantalizing method to study cyberdeterrence



Experimental **war gaming** provides insightful data for real-world cyberattacks

In Greek mythology, Tantalus was the king of Sipylus who so angered Zeus with his treachery that his punishment was to go thirsty and hungry while standing in a pool of water with bountiful fruit trees just above his reach. His fate serves as a reminder to humanity that foolish actions can lead to unpredictable and enduring consequences.

At Sandia, the name Tantalus is associated with an experimental multiplayer online war game used to study different conditions within cyberdeterrence strategy. More importantly, the game is a human research study to gather data about how people's decisions during a threatening situation can impact national security.



“We’re interested in understanding the theory of cyberdeterrence — the notion that the threat of cyberattacks can modify or inhibit the actions of others,” explained the lead online game designer, Jon Whetzel.

To learn more about the human element of cyberdeterrence, researchers pursued increasing Sandia's experimental war-gaming capabilities, and the Program for Experimental Gaming & Analysis of Strategic Interaction Scenarios created Tantalus.

As part of the PEGASIS portfolio, Tantalus was a three-year Laboratory Directed Research and Development project on cyber deterrence. The project recently ended, and the team published their preliminary findings in September 2022.

Combining scientific rigor with the art of war game design

Tantalus is unlike most war games because it is experimental instead of experiential — the immersive game differs by overlapping scientific rigor and quantitative assessment methods with the experimental sciences.

“We consider real-world problems,” said systems research analyst Jason Reinhardt. “And the war games are a laboratory where we can experiment on deterrence problems and understand how they change under different circumstances,” he said.

Tantalus is a three-player war game where players navigate between building and defending their nation. Players act as the leader of a hypothetical country with a mission to increase key "metrics" in their country's mining, infrastructure and manufacturing while fending off attacks from rival countries. The game consists of 12 to 18 randomly selected rounds, with four phases per round: Planning, Threats, Revision and Execution. Players choose to influence or deter each other by force (e.g., kinetic, cyber or nuclear) or engage in espionage.

“We wanted to have the players strive for something that could be taken out of reach by the other players,” explained Whetzel.

During the game, players might threaten to conduct a cyberattack, also known as cyber brandishing. However, in cyberwarfare, revealing a threat can decrease its effectiveness and render the threat powerless, causing a capability - communication tradeoff.

Researchers analyzed the game's data to see how this tradeoff impacted the players' strategies and ability to manage cyberattacks, including the efficacy of threatening opponents.

“We modify game conditions by altering the available threats to player groups. We examine the gameplay across different conditions to see if players favor certain deterrence measures and how other players respond to those threats,” said Whetzel.

Players must earn three victory points to win, and there can be multiple winners — or no victors at all.



To read more: <https://www.sandia.gov/research/news/researchers-develop-a-tantalizing-method-to-study-cyberdeterrence/>

Number 10

ARTIFICIAL INTELLIGENCE - Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity



United States Government Accountability Office
Report to Congressional Addressees

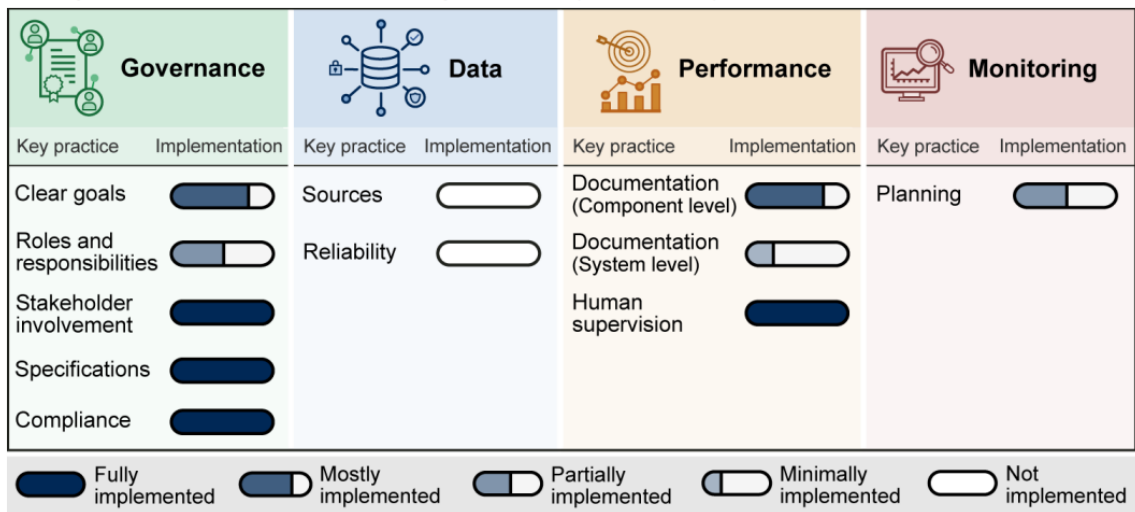
What GAO Found

To promote transparency and inform the public about how artificial intelligence (AI) is being used, federal agencies are required by Executive Order No. 13960 to maintain an inventory of AI use cases. The Department of Homeland Security (DHS) has established such an inventory, which is posted on the Department’s website.

However, DHS's inventory of AI systems for cybersecurity is not accurate. Specifically, the inventory identified two AI cybersecurity use cases, but officials told us one of these two was incorrectly characterized as AI. Although DHS has a process to review use cases before they are added to the AI inventory, the agency acknowledges that it does not confirm whether uses are correctly characterized as AI. Until it expands its process to include such determinations, DHS will be unable to ensure accurate use case reporting.

DHS has implemented some but not all of the key practices from GAO’s AI Accountability Framework for managing and overseeing its use of AI for cybersecurity. GAO assessed the one remaining cybersecurity use case known as Automated Personally Identifiable Information (PII) Detection—against 11 AI practices selected from the Framework (see figure).

Status of the Department of Homeland Security’s Implementation of Selected Key Practices to Manage and Oversee Artificial Intelligence for Cybersecurity







Source: GAO analysis of agency documents and interviews with Department of Homeland Security officials; GAO (icons). | GAO-24-106246

GAO found that DHS fully implemented four of the 11 key practices and implemented five others to varying degrees in the areas of governance,

performance, and monitoring. It did not implement two practices: documenting the sources and origins of data used to develop the PII detection capabilities, and assessing the reliability of data, according to officials.

GAO's AI Framework calls for management to provide reasonable assurance of the quality, reliability, and representativeness of the data used in the application, from its development through operation and maintenance. Addressing data sources and reliability is essential to model accuracy. Fully implementing the key practices can help DHS ensure accountable and responsible use of AI.

Figure 1: Principles, Selected Key Practices, and Questions to Consider for Managing and Overseeing Artificial Intelligence

Principle	Practice	Key considerations
Governance 	Clear goals	What goals and objectives does the entity expect to achieve throughout the AI life cycle? To what extent do stated goals and objectives represent a balanced set of priorities and adequately reflect stated values? How does the AI system help the entity meet its goals and objectives? To what extent does the entity communicate its AI strategic goals and objectives to the community of stakeholders? To what extent does the entity have the necessary resources to achieve the goals and objectives outlined for the AI life cycle? To what extent does the entity consistently measure progress towards stated goals and objectives?
	Roles and responsibilities	What are the roles, responsibilities, and delegation of authorities of personnel involved throughout the AI life cycle? To what extent has the entity clarified the roles, responsibilities, and delegated authorities to relevant stakeholders?
	Stakeholder involvement	What factors were considered when identifying the community of stakeholders involved throughout the life cycle? Which stakeholders did the entity include throughout the life cycle? What specific perspectives did stakeholders share, and how were they integrated throughout the life cycle? To what extent has the entity addressed stakeholder perspectives on the potential negative impacts of the AI system on end users and impacted populations?
	Technical specifications	What challenge/constraint is the AI system intended to solve? To what extent has the entity clearly defined technical specifications and requirements for the AI system? How do the technical specifications and requirements align with the AI system's goals and objectives? What justifications, if any, has the entity provided for the assumptions, boundaries, and limitations of the AI system?
	Compliance	To what extent has the entity identified the relevant laws, regulations, standards, and guidance, applicable to the AI system's use? How does the entity ensure that the AI system complies with relevant laws, regulations, standards, federal guidance, and policies? To what extent is the AI system in compliance with applicable laws, regulations, standards, federal guidance, and entity policies?
Data 	Sources	How has the entity documented the AI system's data provenance, including sources, origins, transformations, augmentations, labels, dependencies, constraints, and metadata?
	Reliability	To what extent are data used to develop the AI system accurate, complete, and valid?
Performance 	Component-level documentation	How is each model component solving a defined problem? How are the operating specifications and parameters of model and non-model components selected, evaluated, and optimized? How suitable are the components to the available data and operating conditions?
	System-level documentation	To what extent has the entity documented the AI system's development, testing methodology, metrics, and performance outcomes? To what extent does the documentation describe test results, limitations, and corrective actions, including efforts to minimize undesired effects in the outcomes?
	Human supervision	How has the entity considered an appropriate degree of human involvement in the automated decision-making processes? What procedures have been established for human supervision of the AI system? To what extent has the entity followed its procedures for human supervision to ensure accountability?
Monitoring 	Planning	What plans has the entity developed to monitor the AI system? To what extent do the plans describe processes and procedures to continuously monitor the AI system? What is the established frequency for monitoring the AI system?

Source: GAO AI Accountability Framework; GAO (icons). | GAO-24-106246

To read more: <https://www.gao.gov/assets/d24106246.pdf>

*Number 11***Using AI to develop enhanced cybersecurity measures**

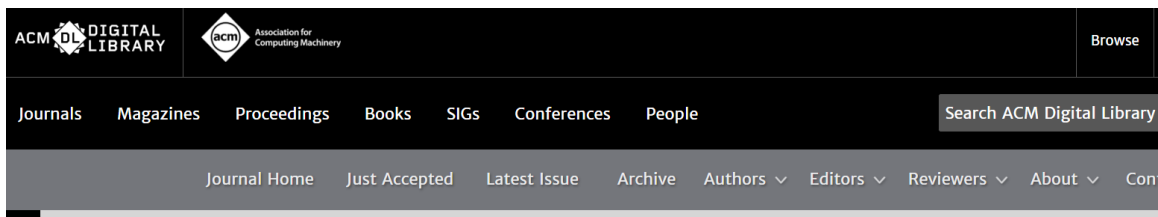
New research helps identify an unprecedented number of malware families



A research team at Los Alamos National Laboratory is using artificial intelligence to address several critical shortcomings in large-scale malware analysis, making significant advancements in the classification of Microsoft Windows malware and paving the way for enhanced cybersecurity measures. Using their approach, the team set a new world record in classifying malware families.

“Artificial intelligence methods developed for cyber-defense systems, including systems for large-scale malware analysis, need to consider real-world challenges,” said Maksim Eren, a scientist in Advanced Research in Cyber Systems at Los Alamos. “Our method addresses several of them.”

The team’s paper was recently published in the Association for Computing Machinery’s journal, Transactions on Privacy and Security. The paper: <https://dl.acm.org/doi/10.1145/3624567>



Semi-Supervised Classification of Malware Families Under Extreme Class Imbalance via Hierarchical Non-Negative Matrix Factorization with Automatic Model Selection

This research introduces an innovative method using AI that is a significant breakthrough in the field of Windows malware classification. The approach achieves realistic malware family classification by leveraging semi-supervised tensor decomposition methods and selective classification, specifically, the reject option.

“The reject option is the model’s ability to say, ‘I do not know,’ instead of making a wrong decision, giving the model the knowledge discovery capability,” Eren said.

Cyber defense teams need to quickly identify infected machines and malicious programs. These malicious programs can be uniquely crafted for their victims, which makes gathering large numbers of samples for traditional machine learning methods difficult.

This new method can accurately work with samples with both larger and smaller datasets at the same time — called class imbalance — allowing it to detect both rare and prominent malware families. It can also reject predictions if it is not confident in its answer.

This could give security analysts the confidence to apply these techniques to practical high-stakes situations like cyber defense for detecting novel threats.

Distinguishing between novel threats and known types of malware specimens is an essential capability to develop mitigation strategies. Additionally, this method can maintain its performance even when limited data is used in its training.

Altogether, the use of the reject option and tensor decomposition methods to extract multi-faceted hidden patterns in data, sets a superior capability in characterizing malware. This achievement underscores the groundbreaking nature of the team's approach.

“To the best of our knowledge, our paper sets a new world record by simultaneously classifying an unprecedented number of malware families, surpassing prior work by a factor of 29, in addition to operating under extremely difficult real-world conditions of limited data, extreme class-imbalance and with the presence of novel malware families,” Eren said.

The team's tensor decomposition methods, with high performance computing and graphics processing unit capabilities, are now available as a user-friendly Python library in GitHub.

Paper: “Semi-supervised Classification of Malware Families Under Extreme Class Imbalance via Hierarchical Non-Negative Matrix Factorization with Automatic Model Determination.” Journal Transactions on Privacy and Security. LANL contributors: Eren (A-4), Manish Bhattarai (T-1), Boian Alexandrov (T-1).

To read more: <https://discover.lanl.gov/news/0215-ai-cybersecurity-measures/>

Number 12

EU Digital Markets Act: the application by Bytedance (TikTok) seeking suspension of the Commission decision designating it as a gatekeeper is dismissed



COURT OF JUSTICE
OF THE EUROPEAN UNION

Bytedance has failed to demonstrate the urgency required for an interim order in order to avoid serious and irreparable damage.

Bytedance Ltd is a non-operating holding company established in China in 2012 which, through local subsidiaries, provides the entertainment platform TikTok.

By decision of 5 September 2023, the Commission designated Bytedance as a gatekeeper under the Digital Markets Act.

In November 2023, Bytedance brought an **action for annulment** of that decision.

By separate document, Bytedance lodged an application for interim measures seeking suspension of that decision.

By today's order, the President of the General Court **dismisses** Bytedance's application for interim measures.

According to the President of the General Court, Bytedance has not shown that it is necessary to suspend the contested decision until the proceedings on the substance of the case are closed in order to avoid serious and irreparable harm to Bytedance.

Bytedance argued, inter alia, that the immediate implementation of the contested decision **risks causing the disclosure** of highly strategic information concerning TikTok's **user profiling** practices, which is not otherwise in the public domain.

That disclosure would enable TikTok's competitors and other third parties to obtain insight into TikTok's business strategies in a way that would significantly harm its business.

According to the President of the General Court, Bytedance has not shown that there is a real risk of disclosure of confidential information or that such a risk would give rise to serious and irreparable harm.

NOTE: The General Court will deliver final judgment on the substance of this case at a later date. An order as to interim measures is without prejudice to the outcome of the main proceedings. An appeal, limited to points of law only, may be brought before the Vice-President of the Court of Justice against the decision of the President of the General Court within two months and ten days of notification of the decision.

NOTE: An action for annulment seeks the annulment of acts of the institutions of the European Union that are contrary to EU law. The Member States, the European institutions and individuals may, under certain conditions, bring an action for annulment before the Court of Justice or the General Court. If the action is well founded, the act is annulled. The institution concerned must fill any legal vacuum created by the annulment of the act.

To read more: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-02/cp240028en.pdf>

*Number 13***EU list of non-cooperative jurisdictions for tax purposes**













The EU list of non-cooperative jurisdictions for tax purposes is part of the EU's work to fight tax evasion and avoidance. It is composed of countries which have failed to fulfil their commitments to comply with tax good governance criteria within a specific timeframe, and countries which have refused to do so.

Which countries are listed?

On 20 February 2024, the Council adopted the EU list of non-cooperative jurisdictions for tax purposes. It is composed of 12 countries.

The list becomes official upon publication in the Official Journal.

Listed: these countries do not cooperate with the EU or have not fully met their commitments

 American Samoa	 Anguilla	 Antigua and Barbuda
 Fiji	 Guam	 Palau
 Panama	 Russia	 Samoa
 Trinidad and Tobago	 US Virgin Islands	 Vanuatu

The countries listed are within the scope of the EU screening process

To read more: <https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/>

Number 14

Announcing Microsoft's open automation framework to red team generative AI Systems

By Ram Shankar Siva Kumar, Microsoft AI Red Team Lead



Today we are releasing an open automation framework, **PyRIT (Python Risk Identification Toolkit for generative AI)**, to empower security professionals and machine learning engineers to proactively find risks in their generative AI systems.

The Python Risk Identification Tool for generative AI (PyRIT) is an open access automation framework to empower security professionals and machine learning engineers to proactively find risks in their generative AI systems.

At Microsoft, we believe that security practices and generative AI responsibilities need to be a collaborative effort.

We are deeply committed to developing tools and resources that enable every organization across the globe to innovate responsibly with the latest artificial intelligence advances.

This tool, and the previous investments we have made in red teaming AI since 2019, represents our ongoing commitment to democratize securing AI for our customers, partners, and peers.

The need for automation in AI Red Teaming

Red teaming AI systems is a complex, multistep process. Microsoft's AI Red Team leverages a dedicated interdisciplinary group of security, adversarial machine learning, and responsible AI experts.

The Red Team also leverages resources from the entire Microsoft ecosystem, including the Fairness center in Microsoft Research; AETHER, Microsoft's cross-company initiative on AI Ethics and Effects in Engineering and Research; and the Office of Responsible AI.

Our red teaming is part of our larger strategy to map AI risks, measure the identified risks, and then build scoped mitigations to minimize them.

Over the past year, we have proactively red teamed several high-value generative AI systems and models before they were released to customers.

Through this journey, we found that red teaming generative AI systems is markedly different from red teaming classical AI systems or traditional software in three prominent ways.

1. Probing both security and responsible AI risks simultaneously

We first learned that while red teaming traditional software or classical AI systems mainly focuses on identifying security failures, red teaming generative AI systems includes identifying both security risk as well as responsible AI risks.

Responsible AI risks, like security risks, can vary widely, ranging from generating content that includes fairness issues to producing ungrounded or inaccurate content. AI red teaming needs to explore the potential risk space of security and responsible AI failures simultaneously.

2. Generative AI is more probabilistic than traditional red teaming

Secondly, we found that red teaming generative AI systems is more probabilistic than traditional red teaming.

Put differently, executing the same attack path multiple times on traditional software systems would likely yield similar results. However, generative AI systems have multiple layers of non-determinism; in other words, the same input can provide different outputs.

This could be because of the app-specific logic; the generative AI model itself; the orchestrator that controls the output of the system can engage different extensibility or plugins; and even the input (which tends to be language), with small variations can provide different outputs.

Unlike traditional software systems with well-defined APIs and parameters that can be examined using tools during red teaming, we learned that generative AI systems require a strategy that considers the probabilistic nature of their underlying elements.

3. Generative AI systems architecture varies widely

Finally, the architecture of these generative AI systems varies widely: from standalone applications to integrations in existing applications to the input and output modalities, such as text, audio, images, and videos.

These three differences make a triple threat for manual red team probing.

To surface just one type of risk (say, generating violent content) in one modality of the application (say, a chat interface on browser), red teams need to try different strategies multiple times to gather evidence of potential failures. Doing this manually for all types of harms, across all modalities across different strategies, can be exceedingly tedious and slow.

This does not mean automation is always the solution. Manual probing, though time-consuming, is often needed for identifying potential blind spots.

Automation is needed for scaling but is not a replacement for manual probing. We use automation in two ways to help the AI red team: automating our routine tasks and identifying potentially risky areas that require more attention.

In 2021, Microsoft developed and released a red team automation framework for classical machine learning systems. Although Counterfit still delivers value for traditional machine learning systems, we found that for generative AI applications, Counterfit did not meet our needs, as the underlying principles and the threat surface had changed.

Because of this, we re-imagined how to help security professionals to red team AI systems in the generative AI paradigm and our new toolkit was born.

We like to acknowledge out that there have been work in the academic space to automate red teaming such as PAIR and open source projects including garak.

To read more: <https://www.microsoft.com/en-us/security/blog/2024/02/22/announcing-microsofts-open-automation-framework-to-red-team-generative-ai-systems/>

Number 15

Reward Offers for Information on LockBit Leaders and Designating Affiliates

U.S. DEPARTMENT *of* STATE

The Department of State is announcing reward offers totaling up to \$15 million for information leading to the arrest and/or conviction of any individual participating in a LockBit ransomware variant attack and for information leading to the identification and/or location of any key leaders of the LockBit ransomware group.



The screenshot shows the top portion of a press release page from the U.S. Department of State. It features a dark blue header with the text 'U.S. DEPARTMENT of STATE'. Below the header is a breadcrumb trail: 'Home > Office of the Spokesperson > Press Releases > Reward Offers for Information on LockBit Leaders and Designating Affiliates'. The main title of the press release is 'Reward Offers for Information on LockBit Leaders and Designating Affiliates', preceded by three stars. Below the title, it is identified as a 'PRESS STATEMENT' by 'MATTHEW MILLER, DEPARTMENT SPOKESPERSON'.

Since January 2020, LockBit actors have executed over 2,000 attacks against victims in the United States, and around the world, causing costly disruptions to operations and the destruction or exfiltration of sensitive information. More than \$144 million in ransom payments have been made to recover from LockBit ransomware events.

The reward offer complements announcements by the Department of Justice and the Federal Bureau of Investigation with the United Kingdom's National Crime Agency, along with other international partners, of a coordinated series of law enforcement actions that will disrupt the LockBit ransomware criminal organization.

To further strengthen our fight against malicious cyber actors, the United States also designated two individuals involved in LockBit pursuant to Executive Order 13694 . We will continue to stand with our partners to disrupt ransomware actors that threaten our economies and critical infrastructure. For more information on this designation, please see Treasury's press release .

To read more: <https://www.state.gov/reward-offers-for-information-on-lockbit-leaders-and-designating-affiliates/>

FBI Cyber Deputy Assistant Director Brett Leatherman's Remarks
at Press Conference Announcing the Disruption of the LockBit Ransomware Group I'm pleased to represent the FBI here today, as I oversee the FBI's Cyber Operations Branch.

I am excited to speak about our multi-year disruption campaign against the LockBit ransomware group.

LockBit has hurt thousands of victims across the country and around the world to include in recent years, targeting all sectors, from government and public sector companies, such as hospitals and schools, to high-profile, global companies.

Today, a joint sequenced operation among 10 countries disrupted LockBit's front- and back-end infrastructure in the U.S. and abroad.

The FBI seized four servers in the U.S. as part of this technical disruption, and we are announcing a total of five LockBit affiliates charged by the Department of Justice.

Two of those indictments are being publicly released today.

In addition, the cyber-related sanctions program implemented by the US Office of Foreign Assets Control (OFAC) imposed sanctions on two LockBit threat actors responsible for malicious cyber-enabled activities.

Lastly, we can proudly announce through the U.S. Department of State a reward of up to \$15 million via the Transnational Organized Crime Rewards Program for anyone with information about LockBit associates.

This includes a reward of up to \$10 million for information leading to the identification or location of any individual(s) who hold a leadership position in the LockBit ransomware variant transnational organized crime group and a reward offer of up to \$5 million for information leading to the arrest and/or conviction of any individual conspiring to participate in or attempting to participate in LockBit ransomware activities.

This large operation could not have happened without the contributions of the National Crime Agency, FBI Newark, our international partners, the FBI's Cyber Division—including our field office personnel across the country—and the FBI personnel stationed overseas, who led the collaboration with our foreign law enforcement partners all, standing shoulder to shoulder, pursuing the same goals, seeking to remediate victims and prevent LockBit from continuing its nefarious activities, it was these partnerships that were essential to today's success.

I cannot go on without mentioning some of the other international partners who contributed to this effort including South West Regional Organized Crime Unit in the U.K., Metropolitan Police Service in the U.K., Europol, Gendarmerie-C3N in France, the State Criminal Police Office L-K-A and Federal Criminal Police Office in Germany, Fedpol and Zurich Cantonal Police in Switzerland, the National Police Agency in Japan, the Australian Federal Police in Australia, the Swedish Police Authority in Sweden, the National Bureau of Investigation in Finland, the Royal Canadian Mounted Police in Canada, and the National Police in the Netherlands.

This coordinated disruption of LockBit's networks illustrates the power of collaboration between the FBI and our international partners.

The FBI's strategy to combat ransomware leverages both our law enforcement and intelligence authorities to go after the whole cybercrime ecosystem by targeting the key services, namely the actors, their finances, their communications, their malware, and their supporting infrastructure.

And since 2021, that's exactly how we've targeted the LockBit ransomware.

Our access to LockBit's infrastructure was no accident.

Now, as we move to the next phase of the investigation, we've worked with our international partners to seize the infrastructure used by these criminal actors including nearly 11,000 domains and servers located all over the globe—hindering LockBit's ability to sting again.

Through this operation, we have access to nearly 1,000 potential decryption capabilities, and the FBI, NCA, and Europol will be conducting victim engagement with over 1,600 known US victims.

I'm here today to ask those US victims and private sector partners who have been a victim of a LockBit ransomware attack to please go to our IC3 website to complete a questionnaire to see if the FBI can provide you with decryption capabilities found during this infrastructure disruption.

One example of our success helping victims occurred in October of 2023.

A Boeing distribution business, Boeing Distribution Inc. (BDI), was the victim of a LockBit ransomware attack.

Boeing immediately engaged the FBI, which provided timely coordination and information sharing that was instrumental to BDI's investigation and recovery.

Today's lesson for businesses large and small, hospitals and police departments, and all the other many victims of ransomware is this:

Reach out to your local FBI field office today and introduce yourselves, so you know who to call if you become the victim of a cyberattack. If you are a victim of LockBit, please reach out to your local FBI office or fill out the form on lockbitvictims.ic3.gov. The FBI is in possession of nearly 1,000 decryption keys, which we intend to provide to victims.

We're ready to help you build a crisis response plan, so when an intruder does come knocking, you'll be prepared.

And, like the LockBit victims here, when you talk to us in advance—as so many others have—you'll know how we operate: quickly and quietly, giving you the assistance, intelligence, and technical information you want and need.

When victims report attacks to us, we can help them—and others, too.

Today's announcement is only the beginning.

We'll continue gathering evidence, building out our map of LockBit developers, administrators, and affiliates, and using that knowledge to drive arrests, seizures, and other operations, whether by the FBI or our partners here and abroad.

While this is, yes, a fight to protect our country, our citizens, and our national security, make no mistake—the fight for cybersecurity spans the globe. But the FBI's presence and partnerships do, too.

So, a reminder to cybercriminals: No matter where you are, and no matter how much you try to twist and turn to cover your tracks—your infrastructure, your criminal associates, your money, and your liberty are all at risk. And there will be consequences.

To read more: https://www.fbi.gov/news/speeches/fbi-cyber-deputy-assistant-director-brett-leathermans-remarks-at-press-conference-announcing-the-disruption-of-the-lockbit-ransomware-group?_gl=1*17cxb48*_gcl_au*Mzg5NDc3NDIxLjE3MDg2Nzk0MTc.



Learn More About the Transnational Organized Crime Rewards Program Targets

Number 16

NIST, Nonprofit Research Consortium to Develop Safety Tools for Synthetic Biology to Defend Against Potential Misuse of AI



Cooperative agreement with public-private partnership is the next step in NIST's fulfillment of Executive Order on Artificial Intelligence.

- Artificial intelligence (AI) has the potential to help develop biotechnologies that can improve human health or that may increase harm.
- Organizations performing nucleic acid synthesis must be aware of AI-related risks and need guidance in identifying and mitigating those risks.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has entered a two-year cooperative research agreement with the nonprofit **Engineering Biology Research Consortium (EBRC)** to develop screening and safety tools to defend against the potential misuse of artificial intelligence (AI) related to nucleic acid synthesis, a growing field of synthetic biology with great promise but also serious risks.



NIST initiated this collaboration to fulfill a task within the recent Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence that charges multiple agencies — including NIST — with developing standards, best practices and implementation guides for nucleic acid synthesis, in light of advances in AI. The Executive Order on AI calls on NIST to initiate an effort to engage with industry and other stakeholders to develop safeguards to defend against potential misuse of AI related to the synthesis of genetic material. NIST will work with EBRC to identify best practices and policies to ensure public safety.



OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

[BRIEFING ROOM](#)[PRESIDENTIAL ACTIONS](#)

“This agreement is the first step toward promoting safe research in engineering biology as tasked to NIST under the recent AI executive order,” said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. “The promise of this technology is immense, but clearly safeguards are needed to protect the public, and this is an important first step toward creating them.”

Researchers have used synthetic nucleic acids to achieve groundbreaking biotechnology innovations, such as new drugs and therapies, but the growing availability and ease of synthesizing nucleic acids has raised safety concerns — particularly in light of advances in artificial intelligence — that could pose risks to the public, environment and national security.

The partnership between NIST and EBRC aims to identify and describe the necessary infrastructure for ensuring safety and security in the synthesis of nucleic acids. As part of the cooperative agreement, the organizations will solicit input from industry, universities, government agencies and other relevant stakeholders.

Based in Emeryville, California, EBRC is a nonprofit public-private partnership dedicated to bringing together an inclusive community committed to advancing engineering biology to address national and global needs.

To read more: <https://www.nist.gov/news-events/news/2024/02/nist-nonprofit-research-consortium-develop-safety-tools-synthetic-biology>

*Number 17***Are Russian Narratives Amplified by PRC Media?**

A Case Study on Narratives Related to Sweden's and Finland's NATO Applications



After the launch of Russia's full-scale invasion of Ukraine on 24 February 2022, state media in the People's Republic of China (PRC) and the Russian Federation have employed similar tactics in their information operations and have often disseminated similar narratives about the war.

PRC state media, which insist on referring to the Russian aggression as the 'Ukrainian crisis', have among other things amplified conspiracy theories about purported United States (US) biological weapons facilities in Ukraine and spread Russian narratives claiming US and NATO culpability for the war.

Moreover, Russian officials and commentators significantly outnumber their Ukrainian counterparts in the coverage of state-owned Chinese news organisations targeting foreign audiences, such as Xinhua, the Chinese state news agency, and China Daily.

The many similarities between the Chinese and Russian media coverage of the war are hardly surprising; the two parties share an apprehension towards NATO and the West at large. Merely three weeks before the launch of Russia's invasion, presidents Vladimir Putin and Xi Jinping voiced their opposition to 'further enlargement of NATO' in a joint statement where they also declared that their friendship had 'no limits'.

One concrete example of the Sino-Russian partnership is collaboration in the information space, where officials have signed several agreements for state media organisations to increase exchanges and mutual support.

In a bilateral agreement signed in July 2021 by both state media outlets and private firms, the parties vowed to jointly promote 'objective, comprehensive and accurate coverage' of international events.

They would, among other things, exchange news content and cooperate on digital media strategies and on the co-production of television shows. There is also evidence that journalists working for Russian state media have helped amplify Chinese narratives.

Russia's war of aggression against Ukraine has rapidly transformed the European security architecture and prompted Finland and Sweden to initiate their NATO membership applications in the spring of 2022.

Introduction	5
Sweden's relations with Russia and China before 2022	6
Recent historical background to Sweden's relations with Russia	6
Recent historical background to Sweden's relations with China	7
Finland's relations with Russia and China before 2022	7
Recent historical background to Finland's relations with Russia	7
Recent historical background to Finland's relations with China	8
Media systems in Russia and China	8
Russian media	8
Chinese media	9
Sweden's NATO application	10
Methods and sources	11
Results	13
On intensity of reporting	13
On topics and narratives related to Sweden's bid to join NATO	15
Discussion of narratives related to Sweden	20
Finland's NATO application	22
Methods and sources	22
Results	24
Russian narrative: 'The US-driven NATO expansion leads to Finland giving up its neutrality'	24
Chinese narrative: 'Security deterioration caused by the US's hegemonic enlargement'	29
Discussion of narratives related to Finland	34
Are Russian narratives relating to the NATO membership bids by Sweden and Finland amplified by PRC media?	35
Sweden's NATO bid: convergence in media narratives	35
Finland's NATO bid: divergence in narrative strategies	36
Conclusion	37
Endnotes	38

Following brief governmental consultations, Finland and Sweden officially applied for membership of the alliance on 18 May 2022. The application process evoked strong negative reactions in Russian and Chinese state-owned media networks, which attempted to frame the move as being fundamentally detrimental for European and even global security.

Considering the shared concern in Moscow and Beijing over new members potentially joining NATO, their collaboration within the information space could be utilised to hamper such an expansion.

This report aims to identify the main narratives that characterise the separate coverage of Sweden and Finland in Russia and China from 21 July 2021 to 21 July 2023.

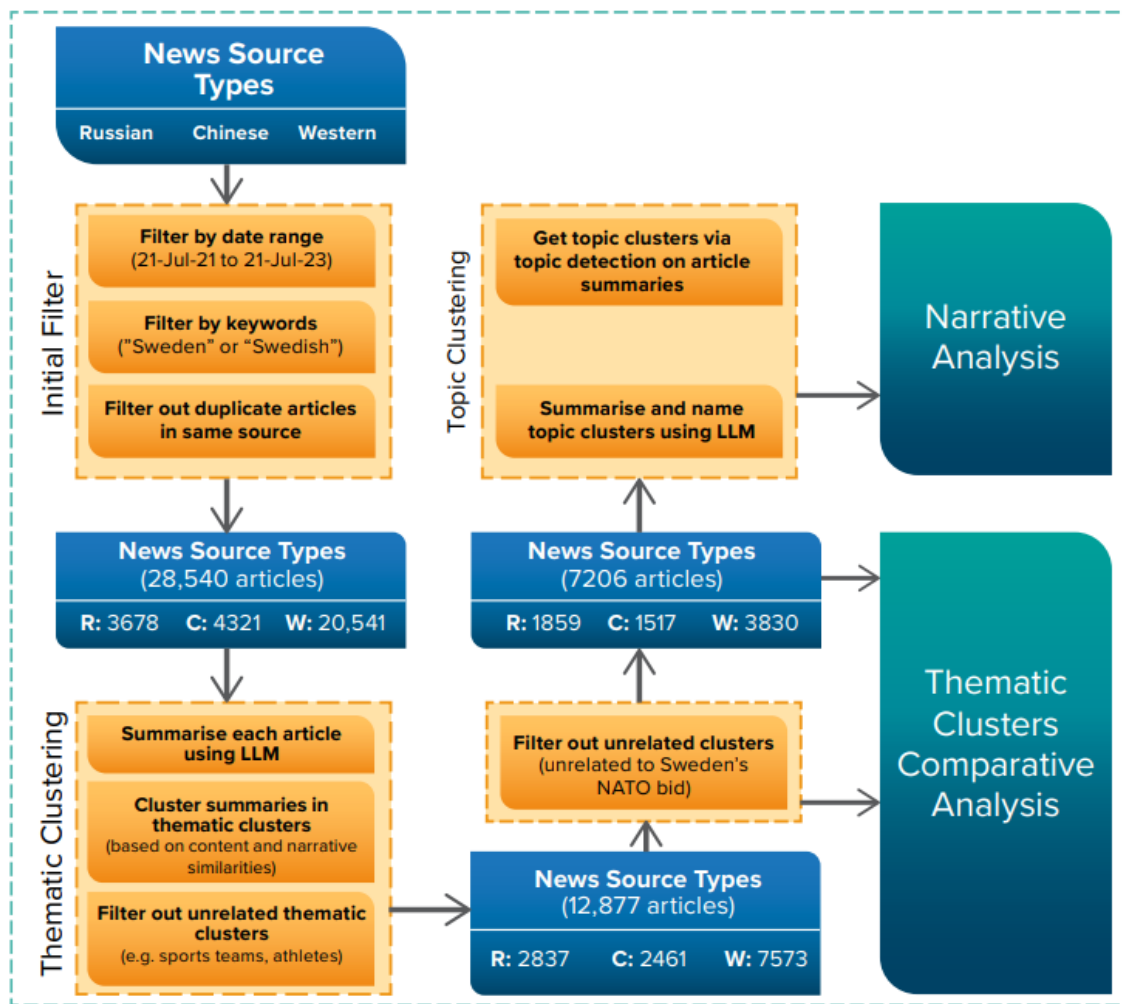


FIGURE 1: Narrative analysis framework method for Sweden's NATO application

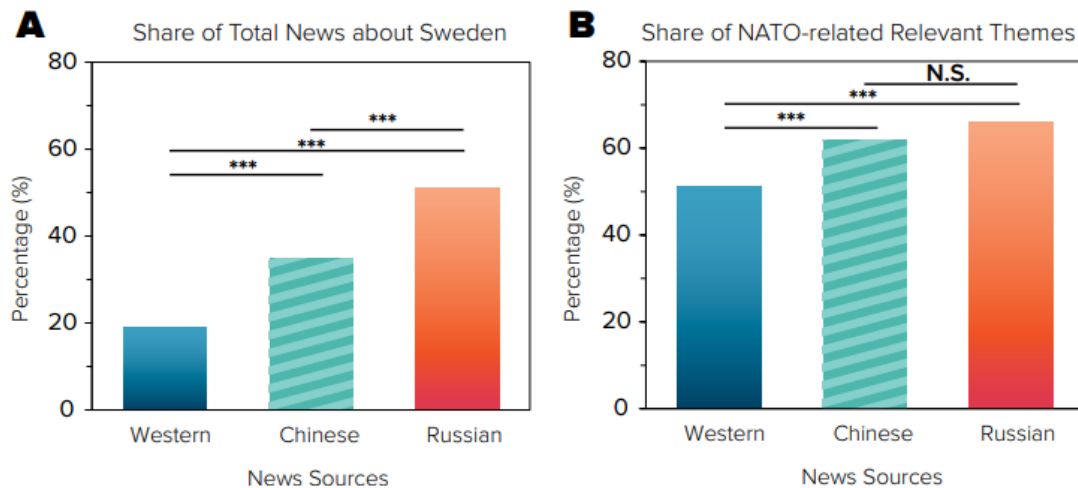


FIGURE 2: Comparison of NATO-related reporting on Sweden in difference sources for (A) the share of total news about Sweden and, after filtering, (B) the share of NATO-related relevant themes. Chi-square test for independence p-values indicate statistical significance at 0.05 significance level (***) $P < 0.001$, N.S.: not significant).

The following research questions are analysed and discussed:

- (1) what are the narratives propagated by both Russia and China to international audiences with respect to Sweden and Finland separately;
- (2) in quantitative terms, what is the overlap between Russian and Chinese narratives; and
- (3) to what extent do the results support the hypothesis that China and Russia are coordinating their strategic communications?

In this report we conduct two distinct analyses, one focused on Sweden and the other on Finland, in examining Russian and Chinese narratives regarding their NATO membership bids.

The separation of these two analyses is crucial for a comprehensive understanding of the situation, acknowledging that each country's bid may evoke unique narratives due to their different historical, geopolitical, and strategic contexts.

While Sweden and Finland share certain similarities in their geopolitical positions, they also possess distinct characteristics and relationships with China and Russia, which could result in divergent narrative strategies from Russian and Chinese media. To read more: <https://stratcomcoe.org/publications/are-russian-narratives-amplified-by-prc-media-a-case-study-on-narratives-related-to-swedens-and-finlands-nato-applications/298>



*Number 18***#StopRansomware: ALPHV Blackcat**

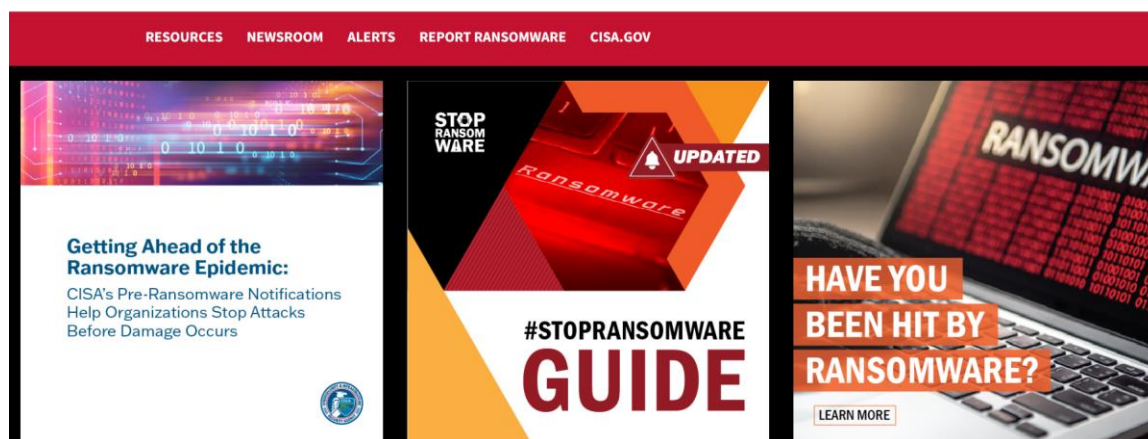
**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**



This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors.

These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware.

Visit <https://www.cisa.gov/stopransomware> to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.



The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (HHS) are releasing this joint CSA to disseminate known IOCs and TTPs associated with the ALPHV Blackcat ransomware as a service (RaaS) identified through FBI investigations as recently as February 2024.

This advisory provides updates to the FBI FLASH BlackCat/ALPHV Ransomware Indicators of Compromise released April 19, 2022, and to this advisory released December 19, 2023.

ALPHV Blackcat actors have since employed improvised communication methods by creating victim-specific emails to notify of the initial compromise. Since mid-December 2023, of the nearly 70 leaked victims, the healthcare sector has been the most commonly victimized.

This is likely in response to the ALPHV Blackcat administrator's post encouraging its affiliates to target hospitals after operational action against the group and its infrastructure in early December 2023.

FBI, CISA, and HHS encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ALPHV Blackcat ransomware and data extortion incidents.

In February 2023, ALPHV Blackcat administrators announced the ALPHV Blackcat Ransomware 2.0 Sphynx update, which was rewritten to provide additional features to affiliates, such as better defense evasion and additional tooling.

This ALPHV Blackcat update has the capability to encrypt both Windows and Linux devices, and VMWare instances. ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations.

To read more: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a>

https://www.cisa.gov/sites/default/files/2024-02/aa23-353a-stopransomware-alphv-blackcat-update_o.pdf



ACTIONS TO TAKE TODAY TO MITIGATE AGAINST THE THREAT OF RANSOMWARE:

1. Routinely take inventory of assets and data to identify authorized and unauthorized devices and software.
2. Prioritize remediation of known exploited vulnerabilities.
3. Enable and enforce multifactor authentication with strong passwords.
4. Close unused ports and remove applications not deemed necessary for day-to-day operations.

*Number 19***My Health My Data Act**

The **My Health My Data Act** is the first privacy-focused law in the country to protect personal health data that falls **outside** the ambit of the Health Insurance Portability and Accountability Act, or HIPAA.

The Act was developed to protect a consumer's sensitive health data from being collected and shared without that consumer's consent.

Washington's concern for the urgent need to enhance privacy protections for health data is widely shared: 76% of Washingtonians express support for the My Health My Data Act.

Under the law, regulated entities must follow specific requirements about how and when they may collect and share personal health data.

*Frequently Asked Questions***1: What are the effective dates for the My Health My Data Act?**

The My Health My Data Act includes effective dates on a section-by-section basis.

All persons, as defined in the Act, must comply with section 10 beginning July 23, 2023. Regulated entities that are not small businesses must comply with sections 4 through 9 beginning March 31, 2024. Small businesses, as defined in the Act, must comply with sections 4 through 9 beginning June 30, 2024. For sections 4 through 9, the effective dates apply to the entirety of the section and are not limited to the subsections in which the effective dates appear.

2: What is the Attorney General's role in enforcing the My Health My Data Act?

Section 11 of the My Health My Data Act provides that any violation of the Act is a per se violation of the Washington Consumer Protection Act (CPA), RCW 19.86, which is enforced by the Attorney General as well as through private action.

3: How will a business located outside of the state of Washington but that stores its data in Washington be impacted?

Generally, all persons and businesses that conduct business in Washington (or provide services or products to Washington), and that collect, process, share, or sell consumer health data are impacted by the Act.

Subject to some exceptions, a regulated entity is a legal entity that (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of

consumer health data. An entity that only stores data in Washington is not a regulated entity.

A processor is as a person that processes consumer health data on behalf of a regulated entity or a small business. Out-of-state entities that are processors for regulated entities or a small business must comply with the Act.

Sections 9 and 10 of the Act apply to persons, which generally includes natural persons, corporations, trusts, unincorporated associations, and partnerships. Out-of-state entities that fall within the definition of person must comply with sections 9 and 10 of the Act.

4: Is a business that is covered by the My Health My Data Act required to place a link to its Consumer Health Data Privacy Policy on the company's homepage?

Yes. Section 4(1)(b) of the My Health My Data Act explicitly provides that “[a] regulated entity and a small business shall prominently publish a link to its consumer health data privacy policy on its homepage.”

The Consumer Health Privacy Policy must be a separate and distinct link on the regulated entity's homepage and may not contain additional information not required under the My Health My Data Act.

5: Does the definition of consumer health data include the purchase of toiletry products (such as deodorant, mouthwash, and toilet paper) as these products relate to “bodily functions”?

Information that does not identify a consumer's past, present, or future physical or mental health status does not fall within the Act's definition of consumer health data. Ordinarily, information limited to the purchase of toiletry products would not be considered consumer health data.

For example, while information about the purchase of toilet paper or deodorant is not consumer health data, an app that tracks someone's digestion or perspiration is collecting consumer health data.

6: If a regulated entity or small business draws inferences about a consumer's health status from purchases of products, could that information be considered consumer health data?

Yes. The definition of consumer health data includes information that is derived or extrapolated from nonhealth data when that information is used by a regulated entity or their respective processor to associate or identify a consumer with consumer health data. This would include potential inferences drawn from purchases of toiletries.

For example, in 2012 the media reported that a retailer was assigning shoppers a “pregnancy prediction score” based on the purchase of certain products; this information is protected consumer health data even though it was inferred from

nonhealth data. Likewise, any inferences drawn from purchases could be consumer health data.

In contrast, nonhealth data that a regulated entity collects but does not process to identify or associate a consumer with a physical or mental health status is not consumer health data.

7: How may a regulated entity or a small business comply with its obligation to retain copies of a consumer's valid authorization for sale of consumer health data under section 9 and a consumer's request to delete their consumer health data under section 6 of the Act?

Under section 9 of the My Health My Data Act, it is unlawful for anyone to sell or offer to sell consumer health data without first obtaining valid authorization from the consumer.

When a consumer grants a person valid authorization to sell their consumer health data, both the seller and purchaser are required to retain a copy of the valid authorization for six years.

Section 6 of the My Health My Data Act empowers consumers to have their consumer health data deleted from a regulated entity's or small business' network, including archived or backup systems.

If after executing a valid authorization, a consumer exercises their section 6 right to have their consumer health data deleted, a regulated entity or small business may meet its obligation to delete the consumer's health data and its obligation to retain a copy of the valid authorization by redacting the portion of the valid authorization that specifies the consumer health data for sale (for example, by applying a redaction that states: "REDACTED pursuant to consumer deletion request on [insert date]").

To read more: <https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy>

<https://app.leg.wa.gov/billsummary?BillNumber=1155&Initiative=false&Year=2023>

Number 20

The EBA consults on Guidelines on redemption plans under the Markets in Crypto-Assets Regulation



The European Banking Authority (EBA) launched a consultation on the Guidelines for the plans to orderly redeem asset-referenced or e-money tokens in the event that the issuer fails to fulfil its obligations under the Markets in Crypto assets Regulation (MiCAR).

The Guidelines specify the content of the redemption plan, the timeframe for review and the triggers for its implementation. The Guidelines are addressed to issuers of asset-referenced tokens (ART) and of e-money tokens (EMT), and to competent authorities under MiCAR. The consultation run until 10 June 2024.

In particular, the draft Guidelines:

- clarify the main principles governing the redemption plan, such as the equitable treatment of token holders, and describe the main steps for the orderly and timely implementation of the plan, including the communication plan, the content of the redemption claims and the distribution plan;
- cover the case of pooled issuance, where the same token is issued by multiple issuers; and
- outline the triggers for the activation of the plan by the competent authority and the cooperation with the prudential and resolution authorities.

Consultation process

Comments to the consultation paper can be sent by clicking on the "send your comments" button on the EBA's consultation page at:

<https://www.eba.europa.eu/publications-and-media/events/consultation-guidelines-redemption-plans-under-micar>

The deadline for the submission of comments is **10 June 2024**.

The EBA will hold a virtual public hearing on the consultation paper on 22 May from 14:00 to 16:00 Paris time. The EBA invites interested stakeholders to register using this link: <https://www.eba.europa.eu/micar-gl-redemption-plans> by 17 May at 16:00 CEST. The dial-in details will be communicated to those who have registered for the meeting.

All contributions received will be published following the end of the consultation, unless requested otherwise.

Legal basis

The EBA has developed the draft Guidelines on redemption plans based on the mandate set out in Article 47(5) of MiCAR. By virtue of the cross-reference set out in Article 55 MiCAR, the Guidelines also cover issuers of e-money tokens, as applicable.

Background

Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCAR) establishes a regime for the regulation and supervision of crypto-asset issuance and crypto-asset service provision in the European Union (EU). It came into force on 29 June 2023, and the provisions relating to ARTs and EMTs will be applicable from 30 June 2024. You may visit: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance)

PE/54/2022/REV/1

OJ L 150, 9.6.2023, p. 40–205 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

● In force: This act has been changed. Current consolidated version: 09/01/2024

ELI: <http://data.europa.eu/eli/reg/2023/1114/oj>

✕ Expand all ⚡ Collapse all

Languages, formats and link to OJ	
	BG ES CS DA DE ET EL EN FR GA HR IT LV LT HU MT NL PL PT RO SK SL FI SV
HTML	                            
PDF	                            
Official Journal	                            

Article 1

Subject matter

1. This Regulation lays down uniform requirements for the offer to the public and admission to trading on a trading platform of crypto-assets other than asset-referenced tokens and e-money tokens, of asset-referenced tokens and of e-money tokens, as well as requirements for crypto-asset service providers.
2. In particular, this Regulation lays down the following:
 - (a) transparency and disclosure requirements for the issuance, offer to the public and admission of crypto-assets to trading on a trading platform for crypto-assets ('admission to trading');
 - (b) requirements for the authorisation and supervision of crypto-asset service providers, issuers of asset-referenced tokens and issuers of e-money tokens, as well as for their operation, organisation and governance;
 - (c) requirements for the protection of holders of crypto-assets in the issuance, offer to the public and admission to trading of crypto-assets;
 - (d) requirements for the protection of clients of crypto-asset service providers;
 - (e) measures to prevent insider dealing, unlawful disclosure of inside information and market manipulation related to crypto-assets, in order to ensure the integrity of markets in crypto-assets.

Among the activities within the scope of MiCAR are the activities of offering to the public or seeking admission to trading of ARTs and EMTs and issuing such tokens.

Supervision tasks are conferred on the EBA for ARTs and EMTs that are determined by the EBA to be significant.

Additionally, the EBA is mandated to develop 17 technical standards and guidelines under MiCAR to further specify the requirements for ARTs and EMTs, and an additional 3 mandates jointly with ESMA (and, in one case, also with the European Insurance and Occupational Pensions Authority - EIOPA).

To read more: <https://www.eba.europa.eu/publications-and-media/press-releases/eba-consults-guidelines-redemption-plans-under-markets-crypto>

Number 21[Android and Windows RATs Distributed Via Online Meeting Lures - Zscaler Blog](#)

- A threat actor is distributing multiple malware families using fake Skype, Zoom, and Google Meet websites.
- The threat actor is distributing Remote Access Trojans (RATs) including SpyNote RAT for Android platforms, and NjRAT and DCRat for Windows systems.

To read more: <https://www.zscaler.com/blogs/security-research/android-and-windows-rats-distributed-online-meeting-lures>

Number 22

FCC Makes AI-Generated Voices in Robocalls Illegal



The Federal Communications Commission regulates U.S. interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the Commission is the federal agency responsible for implementing and enforcing America's communications law and regulations.

The Federal Communications Commission announced the unanimous adoption of a Declaratory Ruling that recognizes calls made with AI-generated voices are “artificial” under the Telephone Consumer Protection Act (TCPA).

The ruling, which takes effect immediately, [makes voice cloning technology used in common robocall scams targeting consumers illegal](#). This would give State Attorneys General across the country new tools to go after bad actors behind these nefarious robocalls.

“Bad actors are using AI-generated voices in unsolicited robocalls to extort vulnerable family members, imitate celebrities, and misinform voters. We’re putting the fraudsters behind these robocalls on notice,” said FCC Chairwoman Jessica Rosenworcel. “State Attorneys General will now have new tools to crack down on these scams and ensure the public is protected from fraud and misinformation.”

The rise of these types of calls has escalated during the last few years as this technology now has the potential to confuse consumers with misinformation by imitating the voices of celebrities, political candidates, and close family members.

While currently State Attorneys General can target the outcome of an unwanted AI-voice generated robocall—such as the scam or fraud they are seeking to perpetrate—this action now makes the act of using AI to generate the voice in these robocalls itself illegal, expanding the legal avenues through which state law enforcement agencies can hold these perpetrators accountable under the law.

In November of 2023, the FCC launched a Notice of Inquiry to build a record on how the agency can combat illegal robocalls and how AI might be involved.

The agency asked questions on how AI might be used for scams that arise out of junk calls, by mimicking the voices of those we know, and whether this technology should be subject to oversight under the TCPA.

Similarly, the FCC also asked about how AI can help us with pattern recognition so that we turn this technology into a force for good that can recognize illegal robocalls before they ever reach consumers on the phone.

The Telephone Consumer Protection Act is the primary law the FCC uses to help limit junk calls.

It restricts the making of telemarketing calls and the use of automatic telephone dialing systems and artificial or prerecorded voice messages. Under FCC rules, it also requires telemarketers to obtain prior express written consent from consumers before robocalling them.

This Declaratory Ruling ensures AI-generated voices in calls are also held to those same standards. The TCPA gives the FCC civil enforcement authority to fine robocallers.

The Commission can also take steps to block calls from telephone carriers facilitating illegal robocalls. In addition, the TCPA allows individual consumers or an organization to bring a lawsuit against robocallers in court.

Lastly, State Attorneys General have their own enforcement tools which may be tied to robocall definitions under the TCPA. A coalition of 26 State Attorneys General—more than half of the nation's AGs—recently wrote to the FCC supporting this approach.

By taking this step, the FCC is building on its work to establish partnerships with law enforcement agencies in states across the country to identify and eliminate illegal robocalls.

These partnerships can provide critical resources for building cases and coordinating efforts to protect consumers and businesses nationwide. The FCC offers partner states not only the expertise of its enforcement staff but also important resources and remedies to support state investigations.

To read more: <https://www.fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal>

Number 23

Basel Committee agrees to revisions to Basel Core Principles



- Basel Committee approves revisions to Core principles for effective banking supervision.
- Decides to consult on potential measures to address window-dressing behaviour by some banks in the context of the framework for global systemically important banks.
- Reaffirms expectation that all aspects of Basel III will be implemented in full, consistently and as soon as possible.

The Basel Committee on Banking Supervision met on 28–29 February 2024 in Madrid to take stock of recent market developments and risks to the global banking system, and to discuss a range of policy and supervisory initiatives.

Risks and vulnerabilities to the global banking system

The Committee discussed the outlook for the global banking system in the light of recent economic and financial market developments. It discussed risks to banks from sectors facing headwinds, including segments of commercial real estate.

Members also discussed banks' interconnections with non-bank financial intermediaries, including the growing role of private credit. Banks and supervisors need to remain vigilant to emerging risks in these areas.

Basel Core Principles

The Committee discussed the comments received to its consultation on revisions to the Core principles for effective banking supervision (Basel Core Principles). Drawing on the inputs received from a wide range of stakeholders, the Committee **approved** the final revisions to the Core Principles, which draw on supervisory insights and structural changes to the banking system since the previous update in 2012.

[The final standard will be published following the International Conference of Banking Supervisors on 24–25 April 2024.](#)

Global systemically important banks and window-dressing

Building on the discussion at its previous meeting, the Committee looked at a range of empirical analyses that highlight window-dressing behaviour by some banks in the context of the framework for global systemically important banks (G-SIBs).

Such regulatory arbitrage behaviour seeks to temporarily reduce banks' perceived systemic footprint around the reference dates used for the reporting and public disclosure of the G-SIB scores.

As noted previously by the Committee, window-dressing by banks undermines the intended policy objectives of the Committee's standards and risks disrupting the operations of financial markets. To that end, the Committee agreed to consult on potential measures aimed at reducing window-dressing behaviour.

The consultation paper, and an accompanying working paper summarising the empirical analyses, will be published next month. The Committee also agreed to publish a working paper on an assessment of the G-SIB score dynamics over the past decade.

Climate-related financial risks

As part of its holistic approach to addressing climate-related financial risks, the Committee discussed the role of scenario analysis in assessing the resilience of banks' business models, strategies and overall risk profile to a range of plausible climate-related pathways. Members noted that the field of scenario analysis is dynamic, with practices expected to evolve rapidly as climate science advances.

Building on its existing supervisory principles, the Committee agreed to publish a discussion paper on the use of climate scenario analysis by banks and supervisors to help inform potential future work in this area. The discussion paper will be published in the coming months.

Implementation of Basel III reforms

The Committee took stock of the implementation status of the outstanding Basel III standards, which were finalised in 2017. Committee members have continued to make good progress with implementation, though it remains uneven.

Members unanimously reaffirmed their expectation of implementing all aspects of the Basel III framework in full, consistently and as soon as possible. Members also approved a workplan for the jurisdictional assessments of the implementation of these standards as part of the Committee's Regulatory Consistency Assessment Programme.

To read more: <https://www.bis.org/press/p240229.htm>

*Number 24***Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google**

Defendant Allegedly Pilfered Technology from Google While Secretly Working for Two PRC-Based Technology Companies



A federal grand jury indicted Linwei Ding, aka Leon Ding, charging him with four counts of theft of trade secrets in connection with an alleged plan to steal from Google LLC (Google) proprietary information related to artificial intelligence (AI) technology.

The announcement was made by Attorney General Merrick B. Garland this afternoon while participating in a “Fireside Chat” at the American Bar Association’s 39th National Institute on White Collar Crime in San Francisco.

According to the indictment, returned on March 5 and unsealed earlier today, Ding, 38, a national of the People’s Republic of China and resident of Newark, California, transferred sensitive Google trade secrets and other confidential information from Google’s network to his personal account while secretly affiliating himself with PRC-based companies in the AI industry. Ding was arrested earlier this morning in Newark.

“The Justice Department will not tolerate the theft of artificial intelligence and other advanced technologies that could put our national security at risk,” said Attorney General Garland. “In this case, we allege the defendant stole artificial intelligence-related trade secrets from Google while secretly working for two companies based in China. We will fiercely protect sensitive technologies developed in America from falling into the hands of those who should not have them.”

“While we work to responsibly harness the benefits of AI, the Justice Department is on high alert to its risks, including global threats to our national security,” said Deputy Attorney General Lisa Monaco. “As alleged in today’s charges, the defendant stole from Google over 500 confidential files containing AI trade secrets, while covertly working for China-based companies seeking an edge in the AI technology race. The Justice Department will relentlessly pursue and hold accountable those who would siphon disruptive technologies – especially AI – for unlawful export.”

“Today’s charges are the latest illustration of the lengths affiliates of companies based in the People’s Republic of China are willing to go to steal American innovation,” said FBI Director Christopher Wray. “The theft of innovative technology and trade secrets from American companies can cost jobs and have devastating economic and national security consequences. The FBI will continue its efforts to vigorously pursue those responsible for stealing U.S. companies’ intellectual property and most closely guarded secrets.”

“Mr. Ding allegedly schemed to siphon off cutting-edge AI technology from Google while secretly trying to go into business with Chinese competitors,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “Through the Disruptive Technology Strike Force, we will work relentlessly to find and hold accountable those who would steal advanced American technology and jeopardize our national security and economic prosperity.”

“While Linwei Ding was employed as a software engineer at Google, he was secretly working to enrich himself and two companies based in the People’s Republic of China,” said U.S. Attorney Ismail Ramsey. “By stealing Google’s trade secrets about its artificial intelligence supercomputing systems, Ding gave himself and the companies that he affiliated with in the PRC an unfair competitive advantage. This office is committed to protecting the innovation of our Silicon Valley companies. To that end, we will aggressively investigate and prosecute the theft of sensitive trade secrets by insiders like Ding, including criminal efforts to jump start illegitimate competition.”

“In the one year since its inception, the Disruptive Technology Strike Force has been relentless in protecting advanced U.S. technologies, like artificial intelligence, from malign actors,” said Assistant Secretary Matthew S. Axelrod of the Commerce Department’s Office for Export Enforcement. “Let today’s announcement serve as further warning – those who would steal sensitive U.S. technology risk finding themselves on the wrong end of a criminal indictment.”

According to court documents, the technology Ding allegedly stole involves the building blocks of Google’s advanced supercomputing data centers, which are designed to support machine learning workloads used to train and host large AI models.

According to the indictment, large AI models are AI applications capable of understanding nuanced language and generating intelligent responses to prompts, tasks, or queries.

The indictment describes how Google developed both proprietary hardware and software to facilitate the machine learning process powered by its supercomputing data centers.

With respect to hardware, Google uses advanced computer chips with the extraordinary processing power required to facilitate machine learning and run AI applications.

With respect to software, Google deploys several layers of software, referred to in the indictment as the “software platform,” to orchestrate machine learning workloads efficiently.

For example, one component of the software platform is the Cluster Management System (CMS), which functions as the “brain” of Google’s supercomputing data centers. The CMS organizes, prioritizes, and assigns tasks to the hardware

infrastructure, allowing the advanced chips to function efficiently when executing machine learning workloads or hosting AI applications.

According to the indictment, Google hired Ding as a software engineer in 2019. Ding's responsibilities included developing the software deployed in Google's supercomputing data centers.

In connection with his employment, Ding was granted access to Google's confidential information related to the hardware infrastructure, the software platform, and the AI models and applications they supported.

The indictment alleges that on May 21, 2022, Ding began secretly uploading trade secrets that were stored in Google's network by copying the information into a personal Google Cloud account.

According to the indictment, Ding continued periodic uploads until May 2, 2023, by which time Ding allegedly uploaded more than 500 unique files containing confidential information.

In addition, the indictment alleges that Ding secretly affiliated himself with two PRC-based technology companies. According to the indictment, on or about June 13, 2022, Ding received several emails from the CEO of an early-stage technology company based in the PRC indicating Ding had been offered the position of Chief Technology Officer for the company.

Ding allegedly traveled to the PRC on Oct. 29, 2022, and remained there until March 25, 2023, during which time he participated in investor meetings to raise capital for the new company.

The indictment alleges potential investors were told Ding was the new company's Chief Technology Officer and that Ding owned 20% of the company's stock.

According to the indictment, unbeknownst to Google, by no later than May 30, 2023, Ding had founded his own technology company in the AI and machine learning industry and was acting as the company's CEO. Ding's company touted the development of a software platform designed to accelerate machine learning workloads, including training large AI models.

As alleged in the indictment, Ding applied to a PRC-based startup incubation program and traveled to Beijing, to present his company at an investor conference on Nov. 24, 2023.

As set forth in the indictment, a document related to Ding's startup company stated, "we have experience with Google's ten-thousand-card computational power platform; we just need to replicate and upgrade it - and then further develop a computational power platform suited to China's national conditions."

The indictment alleges Ding's conduct violated his employment agreement as well as a separate code of conduct that Ding signed when he became a Google

employee. Further, the indictment describes measures that Ding allegedly took to conceal his theft of the trade secrets.

For example, he allegedly copied data from Google source files into the Apple Notes application on his Google-issued MacBook laptop.

By then converting the Apple Notes into PDF files and uploading them from the Google network into a separate account, Ding allegedly evaded detection by Google's data loss prevention systems. Likewise, the indictment describes how in December 2023 Ding allegedly permitted another Google employee to use his Google-issued access badge to scan into the entrance of a Google building – making it appear he was working from his U.S. Google office when, in fact, he was in the PRC.

Ding is charged with four counts of theft of trade secrets. If convicted, Ding faces a maximum penalty of 10 years in prison and up to a \$250,000 fine for each count. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI and Commerce Department are investigating the case.

The U.S. Attorney's Office for the Northern District of California and Justice Department National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

Today's action was coordinated through the Justice and Commerce Departments' Disruptive Technology Strike Force.

The Disruptive Technology Strike Force is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation-states.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

To read more: <https://www.justice.gov/opa/pr/chinese-national-residing-california-arrested-theft-artificial-intelligence-related-trade>

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED

Mar 05 2024

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

The video: <https://www.youtube.com/watch?v=l64VlrA-GUA>



This morning, United States Attorney General Merrick Garland announced the unsealing of an indictment here in the Northern District of



*Number 25***Researchers Develop Missing LINC to Help Vehicles Adapt to Unknowns**

DARPA's Learning Introspective Control (LINC) program successfully demonstrated machine learning technologies that help systems adapt to challenges encountered in the real world.

Imagine a world where the number of vehicle accidents is cut in half.

DARPA's Learning Introspective Control (LINC) program is developing machine learning (ML) methods that may bring that scenario closer to reality. You may visit: <https://www.darpa.mil/program/learning-introspective-control>

The Learning Introspective Control (LINC) program aims to develop machine learning-based introspection technologies that enable physical systems, with specific interest in ground vehicles, ships, drone swarms, and robotic systems, to respond to events not predicted at design time. LINC technologies endeavor to update control laws as required in real time while providing guidance and situational awareness to the operator, whether that operator is human or an autonomous controller.

LINC aims to fundamentally improve the safety of mechanical systems – specifically in ground vehicles, ships, drone swarms, and robotics – using various ML-driven methods that require minimal computing power. The result is an AI-powered controller the size of a cell phone.

At Sandia National Laboratories' Robotic Vehicle Range, LINC researchers used U.S. Army robots as surrogates for larger vehicles to test their solutions, allowing the small vehicles to respond to obstacles in real-time.

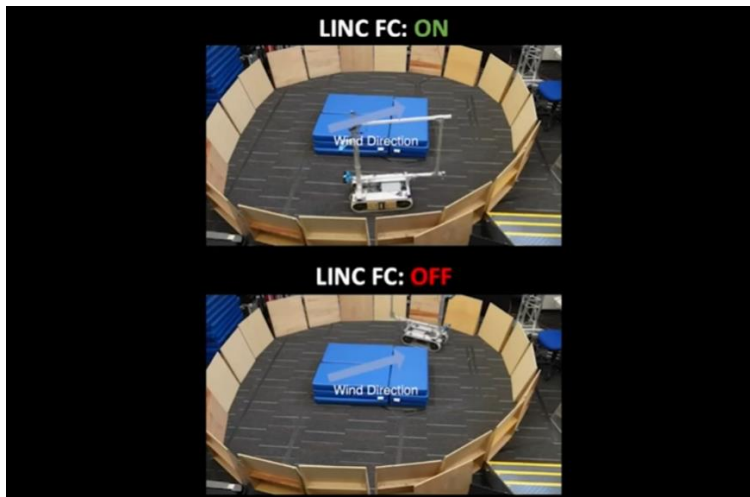
"These systems use sensors while operating but have difficulty adapting when encountering unforeseen situations," said John-Francis Mergen, DARPA's LINC program manager.

"Humans are very good at figuring out how to keep going when faced with a challenge, but the same cannot be said for machines. So, if we could make systems safer with enhanced controls enabled by machine learning, we'd save many people's lives."

Not only did the ML algorithms work as intended, but new behaviors also emerged as pleasant surprises to the research teams.

In one instance, high winds damaged the robot's treads; however, the robot figured out how to leverage the wind and position its body as if it were a sail to help propel itself to finish the obstacle course up an incline.

Experimentation will continue in 2024 in larger systems such as light aerial multipurpose vehicles (LAMVs) and boats.



To read more: <https://www.darpa.mil/news-events/2024-3-7>

https://youtu.be/D8Wbi_lcN4I

*Number 26***Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern**

THE WHITE HOUSE



By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, hereby expand the scope of the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries).

The continuing effort of certain countries of concern to access Americans' sensitive personal data and United States Government-related data constitutes an unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security and foreign policy of the United States.

Access to Americans' bulk sensitive personal data or United States Government-related data increases the ability of countries of concern to engage in a wide range of malicious activities.

Countries of concern can rely on advanced technologies, including artificial intelligence (AI), to analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations or to identify other potential strategic advantages over the United States.

Countries of concern can also use access to bulk data sets to fuel the creation and refinement of AI and other advanced technologies, thereby improving their ability to exploit the underlying data and exacerbating the national security and foreign policy threats.

In addition, access to some categories of sensitive personal data linked to populations and locations associated with the Federal Government — including the military — regardless of volume, can be used to reveal insights about those populations and locations that threaten national security.

The growing exploitation of Americans' sensitive personal data threatens the development of an international technology ecosystem that protects our security, privacy, and human rights.

Accordingly, to address this threat and to take further steps with respect to the national emergency declared in Executive Order 13873, it is hereby ordered that:

Section 1. Policy. It is the policy of the United States to restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States.

At the same time, the United States continues to support open, global, interoperable, reliable, and secure flows of data across borders, as well as maintaining vital consumer, economic, scientific, and trade relationships that the United States has with other countries.

The continuing effort by countries of concern to access Americans' bulk sensitive personal data and United States Government-related data threatens the national security and foreign policy of the United States.

Such countries' governments may seek to access and use sensitive personal data in a manner that is not in accordance with democratic values, safeguards for privacy, and other human rights and freedoms.

Such countries' approach stands in sharp contrast to the practices of democracies with respect to sensitive personal data and principles reflected in the Organisation for Economic Co-operation and Development Declaration on Government Access to Personal Data Held by Private Sector Entities.

Unrestricted transfers of Americans' bulk sensitive personal data and United States Government-related data to such countries of concern may therefore enable them to exploit such data for a variety of nefarious purposes, including to engage in malicious cyber-enabled activities.

Countries of concern can use their access to Americans' bulk sensitive personal data and United States Government-related data to track and build profiles on United States individuals, including Federal employees and contractors, for illicit purposes, including blackmail and espionage.

Access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern through data brokerages, third-party vendor agreements, employment agreements, investment agreements, or other such arrangements poses particular and unacceptable risks to our national security given that these arrangements often can provide countries of concern with direct and unfettered access to Americans' bulk sensitive personal data.

Countries of concern can use access to United States persons' bulk sensitive personal data and United States Government-related data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

This risk of access to Americans' bulk sensitive personal data and United States Government-related data is not limited to direct access by countries of concern. Entities owned by, and entities or individuals controlled by or subject to the jurisdiction or direction of, a country of concern may enable the government of a country of concern to indirectly access such data.

For example, a country of concern may have cyber, national security, or intelligence laws that, without sufficient legal safeguards, obligate such entities and individuals to provide that country's intelligence services access to Americans' bulk sensitive personal data and United States Government-related data.

These risks may be exacerbated when countries of concern use bulk sensitive personal data to develop AI capabilities and algorithms that, in turn, enable the use of large datasets in increasingly sophisticated and effective ways to the detriment of United States national security.

Countries of concern can use AI to target United States persons for espionage or blackmail by, for example, recognizing patterns across multiple unrelated datasets to identify potential individuals whose links to the Federal Government would be otherwise obscured in a single dataset.

While aspects of this threat have been addressed in previous executive actions, such as Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended, additional steps need to be taken to address this threat.

At the same time, the United States is committed to promoting an open, global, interoperable, reliable, and secure Internet; protecting human rights online and offline; supporting a vibrant, global economy by promoting cross-border data flows required to enable international commerce and trade; and facilitating open investment.

To ensure that the United States continues to meet these important policy objectives, this order does not authorize the imposition of generalized data localization requirements to store Americans' bulk sensitive personal data or United States Government-related data within the United States or to locate computing facilities used to process Americans' bulk sensitive personal data or United States Government-related data within the United States.

This order also does not broadly prohibit United States persons from conducting commercial transactions, including exchanging financial and other data as part of the sale of commercial goods and services, with entities and individuals located in or subject to the control, direction, or jurisdiction of countries of concern, or impose measures aimed at a broader decoupling of the substantial consumer, economic, scientific, and trade relationships that the United States has with other countries.

In addition, my Administration has made commitments to increase public access to the results of taxpayer-funded scientific research, the sharing and interoperability of electronic health information, and patient access to their data.

The national security restrictions established in this order are specific, carefully calibrated actions to minimize the risks associated with access to bulk sensitive personal data and United States Government-related data by countries of concern while minimizing disruption to commercial activity.

This order shall be implemented consistent with these policy objectives, including by tailoring any regulations issued and actions taken pursuant to this order to address the national security threat posed by access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern.

Sec. 2. Prohibited and Restricted Transactions. (a) To assist in addressing the national emergency described in this order, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, shall issue, subject to public notice and comment, regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest (transaction), where the transaction:

(i) involves bulk sensitive personal data or United States Government-related data, as further defined by regulations issued by the Attorney General pursuant to this section;

(ii) is a member of a class of transactions that has been determined by the Attorney General, in regulations issued by the Attorney General pursuant to this section, to pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency described in this order;

(iii) was initiated, is pending, or will be completed after the effective date of the regulations issued by the Attorney General pursuant to this section;

(iv) does not qualify for an exemption provided in, or is not authorized by a license issued pursuant to, the regulations issued by the Attorney General pursuant to this section; and

(v) is not, as defined by regulations issued by the Attorney General pursuant to this section, ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any Federal statutory or regulatory requirements, including any regulations, guidance, or orders implementing those requirements.

(b) The Attorney General, in consultation with the heads of relevant agencies, is authorized to take such actions, including the promulgation of rules and regulations, and to employ all other powers granted to the President by IEEPA, as may be necessary or appropriate to carry out the purposes of this order. Executive departments and agencies (agencies) are directed to take all appropriate measures within their authority to implement the provisions of this order.

(c) Within 180 days of the date of this order, the Attorney General, in coordination with the Secretary of Homeland Security, and in consultation with the heads of relevant agencies, shall publish the proposed rule described in subsection (a) of this section for notice and comment. This proposed rule shall:

(i) identify classes of transactions that meet the criteria specified in subsection (a)(ii) of this section that are to be prohibited (prohibited transactions);

(ii) identify classes of transactions that meet the criteria specified in subsection (a)(ii) of this section and for which the Attorney General determines that security requirements established by the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency, in accordance with the process described in subsection (d) of this section, adequately mitigate the risk of access by countries of concern or covered persons to bulk sensitive personal data or United States Government-related data (restricted transactions);

(iii) identify, with the concurrence of the Secretary of State and the Secretary of Commerce, countries of concern and, as appropriate, classes of covered persons for the purposes of this order;

(iv) establish, as appropriate, mechanisms to provide additional clarity to persons affected by this order and any regulations implementing this order (including by designations of covered persons and licensing decisions);

(v) establish a process to issue (including to modify or rescind), in concurrence with the Secretary of State, the Secretary of Commerce, and the Secretary of Homeland Security, and in consultation with the heads of other relevant agencies, as appropriate, licenses authorizing transactions that would otherwise be prohibited transactions or restricted transactions;

(vi) further define the terms identified in section 7 of this order and any other terms used in this order or any regulations implementing this order;

(vii) address, as appropriate, coordination with other United States Government entities, such as the Committee on Foreign Investment in the United States, the Office of Foreign Assets Control within the Department of the Treasury, the Bureau of Industry and Security within the Department of Commerce, and other entities implementing relevant programs, including those implementing Executive Order 13873; Executive Order 14034; and Executive Order 13913 of April 4, 2020 (Establishing the Committee for the Assessment of

Foreign Participation in the United States Telecommunications Services Sector); and

(viii) address the need for, as appropriate, recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts.

(d) The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall, in coordination with the Attorney General and in consultation with the heads of relevant agencies, propose, seek public comment on, and publish security requirements that address the unacceptable risk posed by restricted transactions, as identified by the Attorney General pursuant to this section. These requirements shall be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology.

(i) The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall, in coordination with the Attorney General, issue any interpretive guidance regarding the security requirements.

(ii) The Attorney General shall, in coordination with the Secretary of Homeland Security acting through the Director of the Cybersecurity and Infrastructure Security Agency, issue enforcement guidance regarding the security requirements.

(e) The Secretary of Homeland Security, in coordination with the Attorney General, is hereby authorized to take such actions, including promulgating rules, regulations, standards, and requirements; issuing interpretive guidance; and employing all other powers granted to the President by IEEPA as may be necessary to carry out the purposes described in subsection (d) of this section.

(f) In exercising the authority delegated in subsection (b) of this section, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, may, in addition to the rulemaking directed in subsection (c) of this section, propose one or more regulations to further implement this section, including to identify additional classes of prohibited transactions; to identify additional classes of restricted transactions; with the concurrence of the Secretary of State and the Secretary of Commerce, to identify new or remove existing countries of concern and, as appropriate, classes of covered persons for the purposes of this order; and to establish a mechanism for the Attorney General to monitor whether restricted transactions comply with the security requirements established under subsection (d) of this section.

(g) Any proposed regulations implementing this section:

(i) shall reflect consideration of the nature of the class of transaction involving bulk sensitive personal data or United States Government-related data, the volume of bulk sensitive personal data involved in the transaction, and other factors, as appropriate;

(ii) shall establish thresholds and due diligence requirements for entities to use in assessing whether a transaction is a prohibited transaction or a restricted transaction;

(iii) shall not establish generalized data localization requirements to store bulk sensitive personal data or United States Government-related data within the United States or to locate computing facilities used to process bulk sensitive personal data or United States Government-related data within the United States;

(iv) shall account for any legal obligations applicable to the United States Government relating to public access to the results of taxpayer-funded scientific research, the sharing and interoperability of electronic health information, and patient access to their data; and

(v) shall not address transactions to the extent that they involve types of human 'omic data other than human genomic data before the submission of the report described in section 6 of this order.

(h) The prohibitions promulgated pursuant to this section apply except to the extent provided by law, including by statute or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of the applicable regulations directed by this order.

(i) Any transaction or other activity that has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions promulgated pursuant to this section is prohibited.

(j) Any conspiracy formed to violate any of the prohibitions promulgated pursuant to this section is prohibited.

(k) In regulations issued by the Attorney General under this section, the Attorney General may prohibit United States persons from knowingly directing transactions if such transactions would be prohibited transactions under regulations issued pursuant to this order if engaged in by a United States person.

(l) The Attorney General may, consistent with applicable law, redelegate any of the authorities conferred on the Attorney General pursuant to this section within the Department of Justice. The Secretary of Homeland Security may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary of Homeland Security pursuant to this section within the Department of Homeland Security.

(m) The Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, is hereby authorized to submit recurring and final reports to the Congress related to this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 3. Protecting Sensitive Personal Data. (a) Access to bulk sensitive personal data and United States Government-related data by countries of concern can be enabled through the transmission of data via network infrastructure that is subject to the jurisdiction or control of countries of concern.

The risk of access to this data by countries of concern can be, and sometime is, exacerbated where the data transits a submarine cable that is owned or operated by persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that connects to the United States and terminates in the jurisdiction of a country of concern.

Additionally, the same risk of access by a country of concern is further exacerbated in instances where a submarine cable is designed, built, and operated for the express purpose of transferring data, including bulk sensitive personal data or United States Government-related data, to a specific data center located in a foreign jurisdiction.

To address this threat, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee) shall, to the extent consistent with its existing authority and applicable law:

(i) prioritize, for purposes of and in reliance on the process set forth in section 6 of Executive Order 13913, the initiation of reviews of existing licenses for submarine cable systems that are owned or operated by persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that terminate in the jurisdiction of a country of concern;

(ii) issue policy guidance, in consultation with the Committee's Advisors as defined in section 3(d) of Executive Order 13913, regarding the Committee's reviews of license applications and existing licenses, including the assessment of third-party risks regarding access to data by countries of concern; and

(iii) address, on an ongoing basis, the national security and law enforcement risks related to access by countries of concern to bulk sensitive personal data described in this order that may be presented by any new application or existing license reviewed by the Committee to land or operate a submarine cable system, including by updating the Memorandum of Understanding required under section 11 of Executive Order 13913 and by revising the Committee's standard mitigation measures, with the approval of the Committee's Advisors, which may include, as appropriate, any of the security requirements contemplated by section 2(d) of this order.

(b) Entities in the United States healthcare market can access bulk sensitive personal data, including personal health data and human genomic data, through partnerships and agreements with United States healthcare providers and research institutions. Even if such data is anonymized, pseudonymized, or de-identified, advances in technology, combined with access by countries of concern to large data sets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data, which may reveal the exploitable health

information of United States persons. While the United States supports open scientific data and sample sharing to accelerate research and development through international cooperation and collaboration, the following additional steps must be taken to protect United States persons' sensitive personal health data and human genomic data from the threat identified in this order:

(i) The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall consider taking steps, including issuing regulations, guidance, or orders, as appropriate and consistent with the legal authorities authorizing relevant Federal assistance programs, to prohibit the provision of assistance that enables access by countries of concern or covered persons to United States persons' bulk sensitive personal data, including personal health data and human genomic data, or to impose mitigation measures with respect to such assistance, which may be consistent with the security requirements adopted under section 2(d) of this order, on the recipients of Federal assistance to address this threat.

The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall, in consultation with each other, develop and publish guidance to assist United States research entities in ensuring protection of their bulk sensitive personal data.

(ii) Within 1 year of the date of this order, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation shall jointly submit a report to the President through the Assistant to the President for National Security Affairs (APNSA) detailing their progress in implementing this subsection.

(c) Entities in the data brokerage industry enable access to bulk sensitive personal data and United States Government-related data by countries of concern and covered persons. These entities pose a particular risk of contributing to the national emergency described in this order because they routinely engage in the collection, assembly, evaluation, and dissemination of bulk sensitive personal data and of the subset of United States Government-related data regarding United States consumers.

The Director of the Consumer Financial Protection Bureau (CFPB) is encouraged to consider taking steps, consistent with CFPB's existing legal authorities, to address this aspect of the threat and to enhance compliance with Federal consumer protection law, including by continuing to pursue the rulemaking proposals that CFPB identified at the September 2023 Small Business Advisory Panel for Consumer Reporting Rulemaking.

Sec. 4. Assessing the National Security Risks Arising from Prior Transfers of United States Persons' Bulk Sensitive Personal Data. Within 120 days of the effective date of the regulations issued pursuant to section 2(c) of this order, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, in consultation with the heads of relevant agencies, shall recommend to the APNSA appropriate actions to detect, assess, and mitigate

national security risks arising from prior transfers of United States persons' bulk sensitive personal data to countries of concern. Within 150 days of the effective date of the regulations issued pursuant to section 2(c) of this order, the APNSA shall review these recommendations and, as appropriate, consult with the Attorney General, the Secretary of Homeland Security, and the heads of relevant agencies on implementing the recommendations consistent with applicable law.

Sec. 5. Report to the President. (a) Within 1 year of the effective date of the regulations issued pursuant to section 2(c) of this order, the Attorney General, in consultation with the Secretary of State, the Secretary of the Treasury, the Secretary of Commerce, and the Secretary of Homeland Security, shall submit a report to the President through the APNSA assessing, to the extent practicable:

(i) the effectiveness of the measures imposed under this order in addressing threats to the national security of the United States described in this order; and

(ii) the economic impact of the implementation of this order, including on the international competitiveness of United States industry.

(b) In preparing the report described in subsection (a) of this section, the Attorney General shall solicit and consider public comments concerning the economic impact of this order.

Sec. 6. Assessing Risks Associated with Human 'omic Data. Within 120 days of the date of this order, the APNSA, the Assistant to the President and Director of the Domestic Policy Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Pandemic Preparedness and Response Policy, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, the Director of the National Science Foundation, the Director of National Intelligence, and the Director of the Federal Bureau of Investigation, shall submit a report to the President, through the APNSA, assessing the risks and benefits of regulating transactions involving types of human 'omic data other than human genomic data, such as human proteomic data, human epigenomic data, and human metabolomic data, and recommending the extent to which such transactions should be regulated pursuant to section 2 of this order. This report and recommendation shall consider the risks to United States persons and national security, as well as the economic and scientific costs of regulating transactions that provide countries of concern or covered persons access to these data types.

Sec. 7. Definitions. For purposes of this order:

(a) The term "access" means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information technology systems, cloud computing platforms, networks, security systems, equipment, or software.

(b) The term “bulk” means an amount of sensitive personal data that meets or exceeds a threshold over a set period of time, as specified in regulations issued by the Attorney General pursuant to section 2 of this order.

(c) The term “country of concern” means any foreign government that, as determined by the Attorney General pursuant to section 2(c)(iii) or 2(f) of this order, has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons, and poses a significant risk of exploiting bulk sensitive personal data or United States Government-related data to the detriment of the national security of the United States or the security and safety of United States persons, as specified in regulations issued by the Attorney General pursuant to section 2 of this order.

(d) The term “covered person” means an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern; a foreign person who is an employee or contractor of such an entity; a foreign person who is an employee or contractor of a country of concern; a foreign person who is primarily resident in the territorial jurisdiction of a country of concern; or any person designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a country of concern, as acting on behalf of or purporting to act on behalf of a country of concern or other covered person, or as knowingly causing or directing, directly or indirectly, a violation of this order or any regulations implementing this order.

(e) The term “covered personal identifiers” means, as determined by the Attorney General in regulations issued pursuant to section 2 of this order, specifically listed classes of personally identifiable data that are reasonably linked to an individual, and that — whether in combination with each other, with other sensitive personal data, or with other data that is disclosed by a transacting party pursuant to the transaction and that makes the personally identifiable data exploitable by a country of concern — could be used to identify an individual from a data set or link data across multiple data sets to an individual. The term “covered personal identifiers” does not include:

(i) demographic or contact data that is linked only to another piece of demographic or contact data (such as first and last name, birth date, birthplace, zip code, residential street or postal address, phone number, and email address and similar public account identifiers); or

(ii) a network-based identifier, account-authentication data, or call-detail data that is linked only to another network-based identifier, account-authentication data, or call-detail data for the provision of telecommunications, networking, or similar services.

(f) The term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(g) The term “foreign person” means any person that is not a United States person.

(h) The term “human genomic data” refers to data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a cell.

(i) The term “human ‘omic data” means data generated from humans that characterizes or quantifies human biological molecule(s), such as human genomic data, epigenomic data, proteomic data, transcriptomic data, microbiomic data, or metabolomic data, as further defined by regulations issued by the Attorney General pursuant to section 2 of this order, which may be informed by the report described in section 6 of this order.

(j) The term “person” means an individual or entity.

(k) The term “relevant agencies” means the Department of State, the Department of the Treasury, the Department of Defense, the Department of Commerce, the Department of Health and Human Services, the Office of the United States Trade Representative, the Office of the Director of National Intelligence, the Office of the National Cyber Director, the Office of Management and Budget, the Federal Trade Commission, the Federal Communications Commission, and any other agency or office that the Attorney General determines appropriate.

(l) The term “sensitive personal data” means, to the extent consistent with applicable law including sections 203(b)(1) and (b)(3) of IEEPA, covered personal identifiers, geolocation and related sensor data, biometric identifiers, human ‘omic data, personal health data, personal financial data, or any combination thereof, as further defined in regulations issued by the Attorney General pursuant to section 2 of this order, and that could be exploited by a country of concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals. The term “sensitive personal data” does not include:

(i) data that is a matter of public record, such as court records or other government records, that is lawfully and generally available to the public;

(ii) personal communications that are within the scope of section 203(b)(1) of IEEPA; or

(iii) information or informational materials within the scope of section 203(b)(3) of IEEPA.

(m) The term “United States Government-related data” means sensitive personal data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a country of concern to harm United States national security and that:

(i) a transacting party identifies as being linked or linkable to categories of current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of this order;

(ii) is linked to categories of data that could be used to identify current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of this order; or

(iii) is linked or linkable to certain sensitive locations, the geographical areas of which will be specified publicly, that are controlled by the Federal Government, including the military.

(n) The term “United States person” means any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States.

Sec. 8. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) Nothing in this order shall prohibit transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.

(c) Any disputes that may arise among agencies during the consultation processes described in this order may be resolved pursuant to the interagency process described in National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System), or any successor document.

(d) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

To read more: <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/>

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



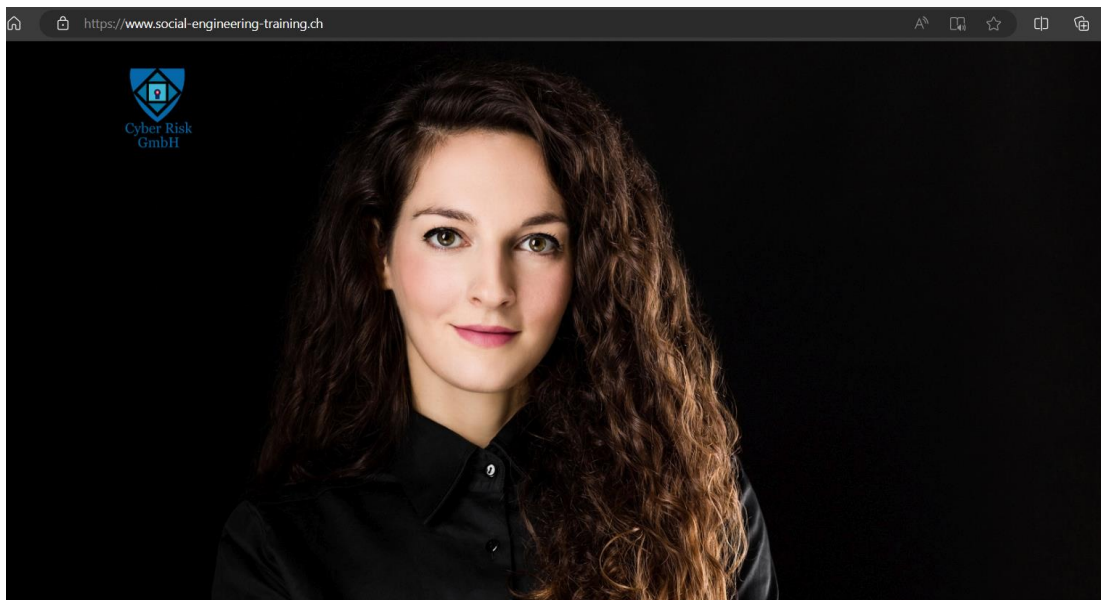
Our websites include:

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

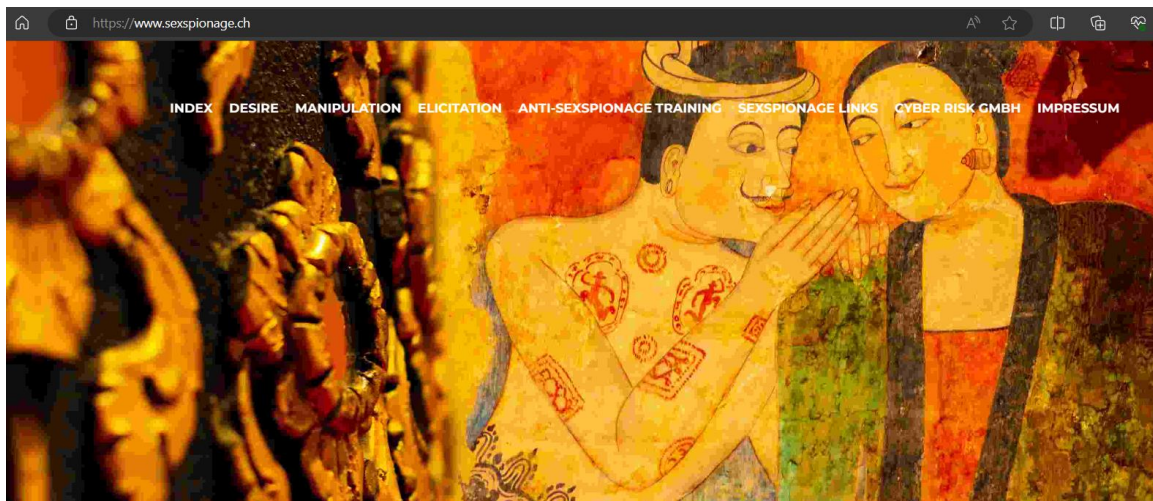
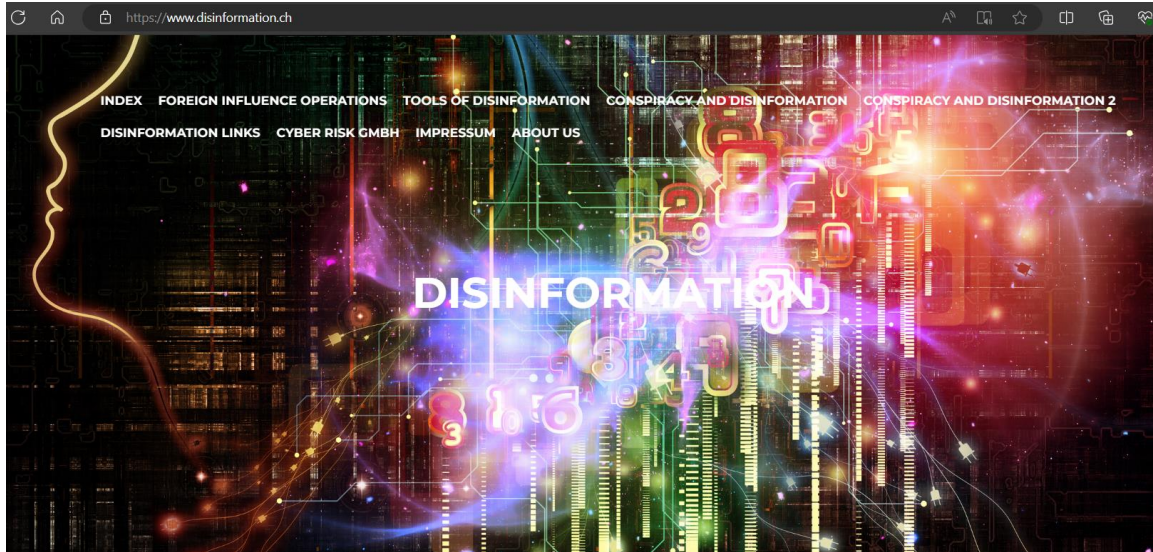
8. Electricity Cybersecurity - <https://www.electricity-cybersecurity.com>
9. Gas Cybersecurity - <https://www.gas-cybersecurity.com>
10. Hydrogen Cybersecurity - <https://www.hydrogen-cybersecurity.com>
11. Transport Cybersecurity - <https://www.transport-cybersecurity.com>
12. Transport Cybersecurity 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.

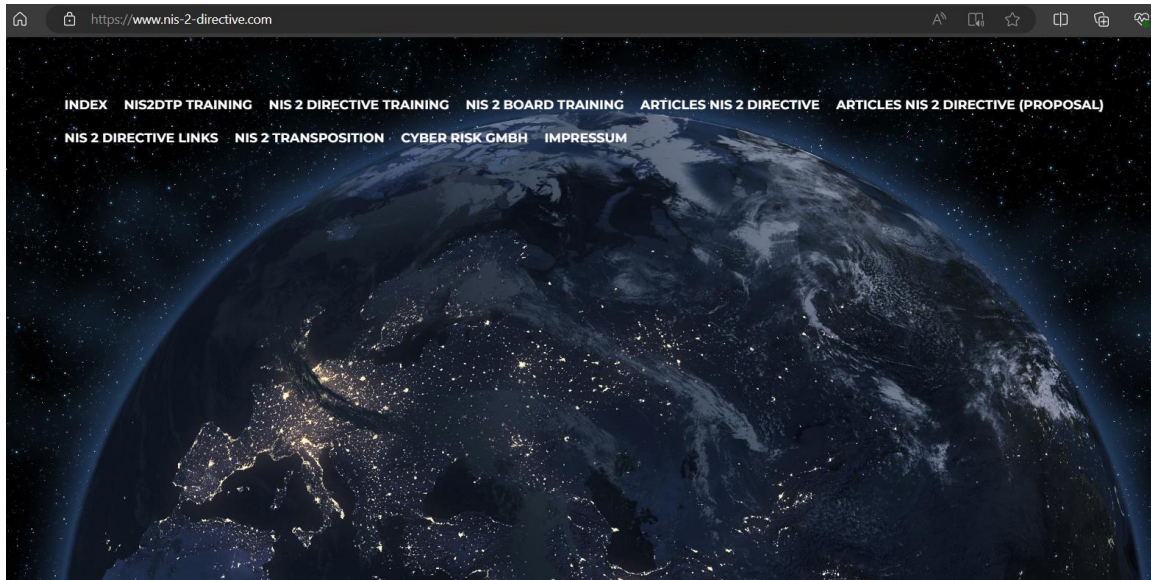
1. What is Disinformation? - <https://www.disinformation.ch>
2. What is Steganography? - <https://www.steganography.ch>
3. What is Cyberbiosecurity? - <https://www.cyberbiosecurity.ch>
4. What is Synthetic Identity Fraud? - <https://www.synthetic-identity-fraud.com>
5. What is a Romance Scam? - <https://www.romance-scams.ch>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

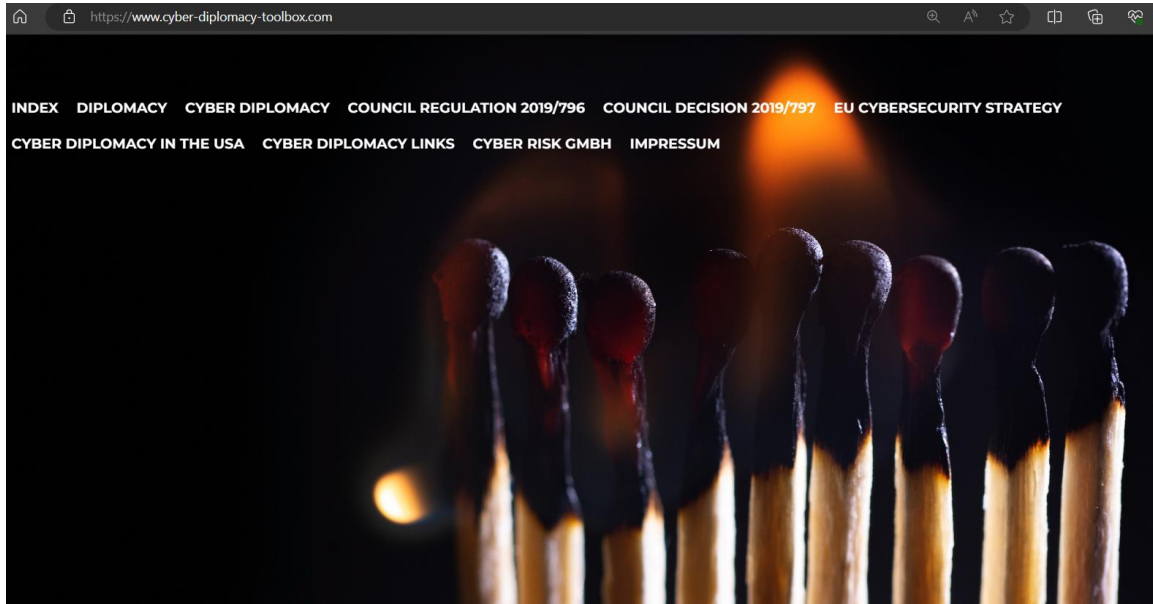
1. The NIS 2 Directive - <https://www.nis-2-directive.com>
2. The European Cyber Resilience Act - <https://www.european-cyber-resilience-act.com>
3. The Digital Operational Resilience Act (DORA) - <https://www.digital-operational-resilience-act.com>
4. The Critical Entities Resilience Directive (CER) - <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

