Cyber Risk and Compliance News and Alerts, April 2024

Mary Ann Evans (pen name: George Eliot) was an English novelist and poet. She has said: “Blessed is the influence of one true, loving human soul on another.”

Unfortunately, influence is not always that positive. Max Weber has said: “Politics means striving to share power or striving to influence the distribution of power, either among states or among groups within a state.”

I have just read an excellent report that covers countermeasures and capabilities against *information influence operations (IIO).*

It includes scenarios and assists in creating a discussion on *what capabilities* are needed and *how* organisations can develop these capabilities based on available resources.

All parts of society can be affected by IIO and should develop capabilities to counter disinformation. The selected workshops can be adapted to work on a *local, regional, or national* level.

To test the workshop method, three workshops at the local, regional, and national level were planned and conducted together with the Swedish Psychological Defence Agency (MPF). Sweden was the example nation, but the method can of course be applied to other nations. Testing the method at different societal levels contributed to analysing whether the selected method was suited to different actors and could be used to find reasonable levels of capability in countering IIO regarding their responsibilities.

The workshops, called PSYCAP 2023, were held in Sweden and run with a Municipal and a County Administration Board, and a Swedish National agency.

All three organisations were faced with the same challenges, just slightly modified to fit their responsibilities.

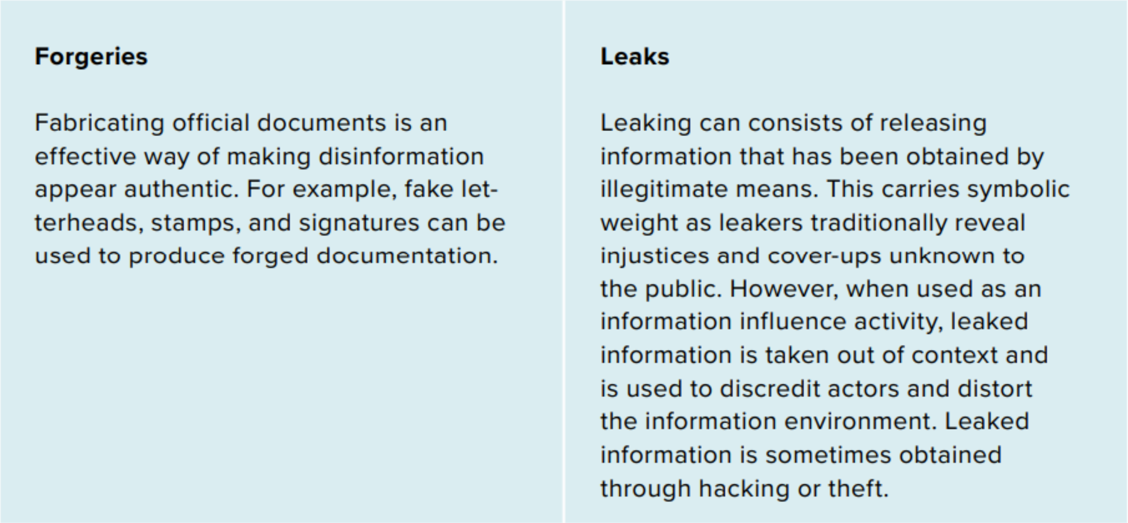
The first challenge described a cyberattack that involved someone infiltrating the organisation’s IT systems and uploading a new copy of the entire digital folder structure, as well as deleting and adding a large number of documents.

Meanwhile, an investigation into the situation was under way, news starts to spread in the traditional media about leaked documents revealing that a manager within the organisation had misused large sums of money or had otherwise been acting corruptly.

Hacking and leaking documents often carry symbolic value as they can expose injustices that are otherwise concealed from the public. The narrative for the challenge was that all levels of society are corrupt, and public institutions cannot be trusted.

The second challenge continued with the same narrative of distrust in public institutions and corruption. This time a deep fake of the prime minister of Sweden was circulated on social media, announcing in a press conference that the organisation was part of a corruption scandal.

Subsequently, there was a surge of hatred and threats towards the organisation and its staff, leading to sabotage against some of the organisation’s facilities.



Forgeries	**Leaks**
Fabricating official documents is an effective way of making disinformation appear authentic. For example, fake letterheads, stamps, and signatures can be used to produce forged documentation.	Leaking can consists of releasing information that has been obtained by illegitimate means. This carries symbolic weight as leakers traditionally reveal injustices and cover-ups unknown to the public. However, when used as an information influence activity, leaked information is taken out of context and is used to discredit actors and distort the information environment. Leaked information is sometimes obtained through hacking or theft.

Challenge three described an international nuclear incident that could potentially spread some radioactivity to northern Europe, but with smaller particles that would not cause significant impact.

False experts disseminated misinformation claiming that the authorities were lying to the public to avoid causing panic.

This created a substantial information demand among the population, who were trying to find factual recommendations and advice, which is challenging when truth is mixed with lies and disinformation.

The report has the title "Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops", a workshop methodology for developing increased capability against information influence operations, prepared and published by the NATO Strategic Communications centre of Excellence (StratCom COE).

Read more at number 10 below.

Friedrich Nietzsche believed that it is impossible to suffer without making someone pay for it; every *complaint* already contains revenge. Unfortunately, Nietzsche had no access to any *complaint center,* for an organized response to threat actors.

Today, the *U. S. Internet Crime Complaint Center (IC3)* provides the public with a reporting mechanism to submit information to the Federal Bureau of Investigation (FBI) concerning suspected Internet-facilitated criminal activity.

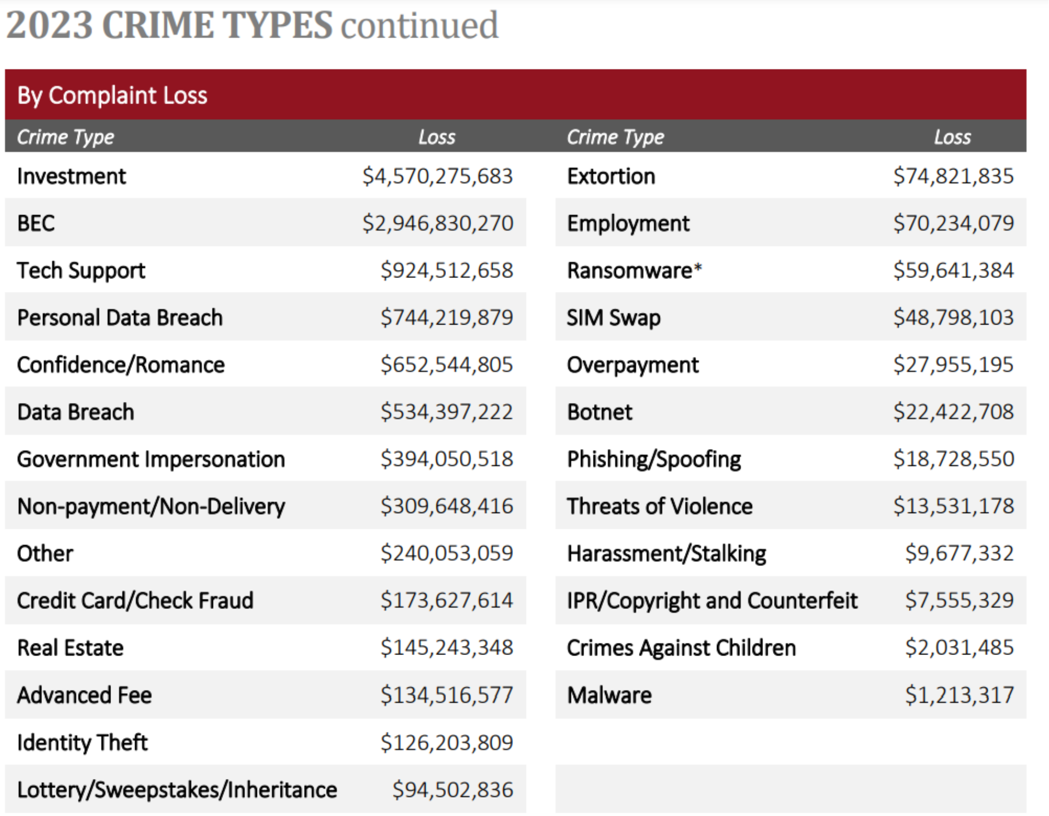
It was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes.

I have just read the very important *Internet Crime Report 2023,* from IC3.
In 2023, the IC3 received 21,489 Business Email Compromise (BEC) complaints with adjusted losses over 2.9 billion.

BEC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques.

Procedures should be put in place to verify payments and purchase requests outside of email communication and can include direct phone calls but to a known verified number and not relying on information or phone numbers included in the email communication.

Other best practices include carefully examining the email address, URL, and spelling used in any correspondence and not clicking on anything in an unsolicited email or text message asking you to update or verify account information.



2023 CRIME TYPES continued

By Complaint Loss

Crime Type	Loss	Crime Type	Loss
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

Read the report carefully. Try to understand the details. T. S. Eliot has asked: *"Where is the life we have lost in living? Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?"*

Read more at number 7 below.

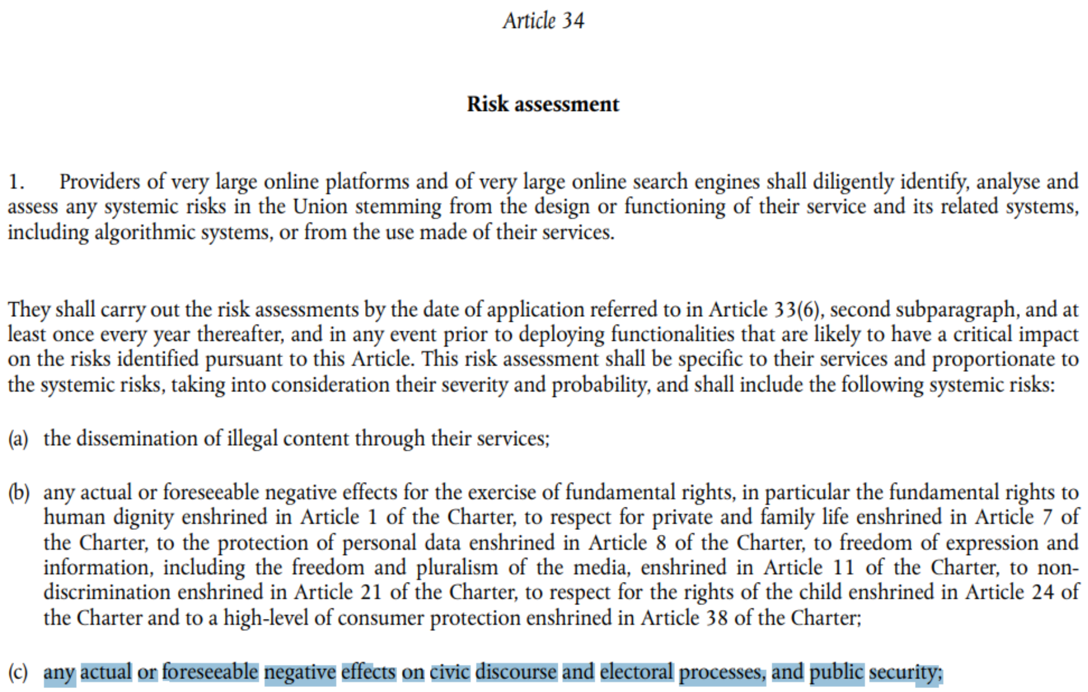
Marcus Aurelius has said: "Look back over the past, with its changing empires that rose and fell, and you can foresee the future, too."

George Orwell believed that people can foresee the future only when it coincides with their own wishes, and the most grossly obvious facts can be ignored when they are unwelcome.

Marcus and George, in regulatory compliance we live in a very difficult and complex world. I must develop a presentation for a client about "any actual or foreseeable negative effects on civic discourse and electoral processes". How can I meet the expectations?

Online platforms and search engines have become important venues for public debate and for shaping public opinion and voter behaviour. Regulation (EU) 2022/2065 (the Digital Services Act) imposes obligations on providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) to carry out specific risk assessments and put in place reasonable, proportionate, and effective risk mitigation measures including for "any actual or foreseeable negative effects on civic discourse and electoral processes".

You can find it at Article 34.1.c of the Digital Services Act.



Article 34

Risk assessment

1. Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.

They shall carry out the risk assessments by the date of application referred to in Article 33(6), second subparagraph, and at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks:

(a) the dissemination of illegal content through their services;

(b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter;

(c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;

Perhaps I should start with Burnt Norton, the first poem of T. S. Eliot's Four Quartets:

“Time present and time past,
Are both perhaps present in time future.”

In risk management language, we can discuss what has happened in the past, the trends in hybrid warfare and cyber security, and then we can make “reasonable assumptions” about the future (or “plausible assumptions”, as it is called in the Basel framework.

Yes, this is a “history repeats itself” approach, but it will do the job. No, it cannot cover all foreseeable negative effects. I secretly call it “mission impossible”, please do not disclose this to the European Commission.

Read more at number 13 and 19 below.

Financial stress tests are very difficult risk and compliance management exercises.

The European Insurance and Occupational Pensions Authority (EIOPA) has just launched its 2024 stress test. Insurers in the European Economic Area must consider a hypothetical scenario of severe but plausible adverse developments in financial and economic conditions.

For many years we discuss the word plausible. Francis Bacon believed that *truth is so hard to tell, it sometimes needs fiction to make it plausible.* No, Francis was not speaking about financial stress testing.

According to EIOPA, the adverse scenario is based on “the uncertainty deriving from the economic consequences of a re-intensification or prolongation of geopolitical tensions. Such an environment would fuel supply chain disruptions and lead to lower growth and higher inflation.

Second-round effects stemming from a wage-price spiral would further exacerbate inflationary pressures, ultimately leading to a re-appraisal of market expectations of interest rates across tenors and currencies.”

We also read: “Households would also experience losses in real income and face higher borrowing costs amid higher unemployment. This would make it challenging for homeowners to service their mortgages, resulting in an increase in mortgage defaults.

The ensuing fall in residential real estate prices is exacerbated by a slowdown in residential property market activity.

At the same time, the large increase in interest rates would fuel a disorderly repricing in the commercial real estate market, in the context of structural changes to demand for office space that had been initiated by the COVID-19 pandemic.

The higher cost of debt-servicing, coupled with the sharp fall in property prices, would trigger a sudden repricing of covered bonds and other asset-backed securities, driving spreads upwards.

Such market reactions would also trigger a sudden revaluation of other financial assets in an uncertain environment characterised by high volatility.

In particular, equity valuations would drop substantially worldwide, while hedge funds, real estate investment trusts and private equity funds would incur in losses. The latter would be largely affected by an amplification of liquidity stress.

Finally, commodity prices would surge in line with the supply-chain driven inflation prospect.”

Is Europe preparing for war? Friedrich Nietzsche believed that the best weapon against an enemy is another enemy, but EIOPA, the European Insurance and Occupational Pensions Authority, follows the regulatory path. Insurance firms will benefit from this stress test, especially when they make proper assumptions.

Albert Einstein has said: You cannot simultaneously prevent and prepare for war. Well, perhaps Albert was wrong this time. I believe that the opposite is true today.

Read more at number 28 below.

Aristotle believed that *the secret to humor is surprise*. I have no excuse, but I am still *surprised* when I read: “this guide is aimed at data protection officers (DPO), chief information security officer (CISO) and computer scientists. Privacy lawyers will also be able to find useful elements.”

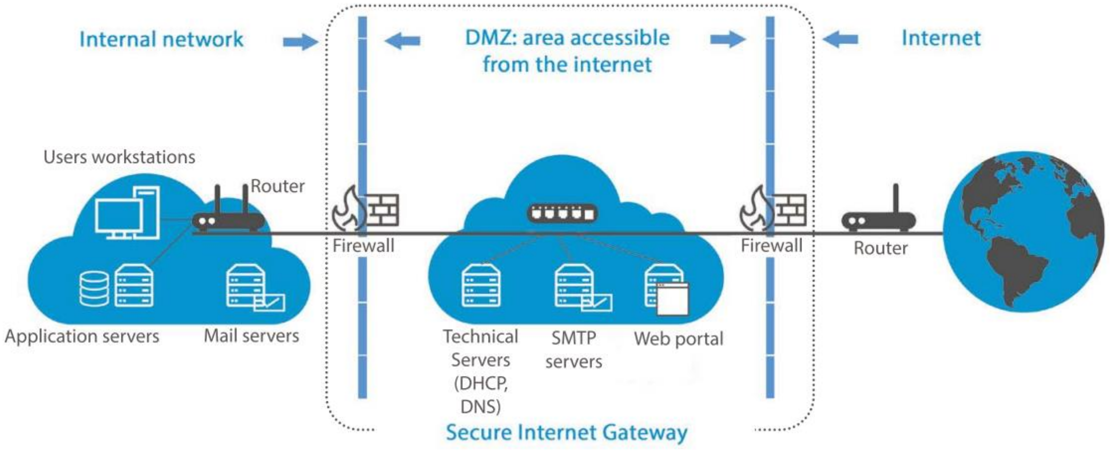
Ten years ago, this would be a joke. There were no papers for privacy lawyers and computer scientists. But this one is not a joke, and I found it very useful. This is a guide from the French data protection authority (CNIL) on the issue of data security, “a living tool that is enriched by state-of-the-art practices and doctrine elements”.

According to the guide, “Only allow access to data that the user really needs. Respecting the principle of least privilege, through the management of the authorisation profiles, allows to limit the consequences of an error of manipulation.”

Well, the Principle of Least Privilege (PoLP), necessary for highly sensitive environments to ensure that access is strictly limited to individuals who absolutely need access to perform their duties, is now used for privacy and personal information protection. Granting a user more privileges than necessary is a privacy issue too.

Ten years ago, we would not find the words privacy protection and demilitarized zone in the same sentence. We read in the guide:

“Partition the network to mitigate potential security breaches impacts. Implement at least two distinguished network areas: an internal network where no Internet connection is allowed and a DMZ (demilitarized zone) accessible from the Internet, separated by gateways.”



After that I will not be surprised if in the next “Guide 2025” we read that for privacy protection, we also need honeypots (as they are used in network security, not espionage).

Honeypots in network security are decoy systems designed to attract cyber attackers, allowing security professionals to study attack methods, identify attackers, and improve defenses.

Honeypots in espionage are men or women used to entice, seduce, or otherwise manipulate targets to extract information or influence their actions. This involves human interaction and psychological manipulation. Well, the guide was produced in France, but it does not cover fields like that.

As Monica Bellucci (note: not a risk and compliance expert) has said: “In France, they call the beauty of youth “the evil beauty.” You don't have it because of you but because you're born with it. The other kind of beauty is your own work, and it takes forever.”

Well, the French guide is talking *about the other kind of beauty, our own work, and I am afraid it really takes forever* to comply with the new privacy regulations and guides. Read more at number 29 below.

In Switzerland, the Swiss National Cyber Security Centre (NCSC) has been monitoring the phenomenon of fake calls from alleged police authorities for nine months now.

In the last three weeks, reports reaching the NCSC about this phenomenon have almost tripled and account for the highest number of reports received since the contact point was founded. However, the high number of incoming reports is not all bad.

Since last summer the NCSC has been receiving an increasing number of fake calls purporting to be from the police.

The scam starts with a phone call supposedly from the police or customs authority claiming, for example, that personal bank details have arisen in connection with a criminal offence.

They try on different stories but what they all have in common is that a computer-generated voice speaking in impeccable English asks the person being called to press 1 to be put through to a ‘police officer’ to obtain further information.

After an initial wave of calls last autumn tailing off over the winter months, the number of reports has exploded in recent weeks. The attackers have obviously intensified their business model.

The trick with getting you to press "1"

The attacks are similar to the calls made in the name of Microsoft that have been observed for some time. Here, the fraudster calls the victim directly and claims that the caller's computer is infected.

As most callers were quick to spot the scam, they either hung up immediately or vented their anger on the scammers. The perpetrators therefore came up with a more effective variant.

With the current variant, it is no longer a person who calls, but a software. The machine randomly tries Swiss phone numbers throughout the day. If the number is invalid, it simply moves on to the next one; if it comes across a valid number, the announcement is played and the victim is asked to press 1.

Only after pressing 1 is the caller connected to the fraudster. And that is why they try to get you to press 1: Only those who believe the story, at least to some extent, are connected to the fraudsters in this way.

The high number of incoming reports is not all bad

By using such a software, the number of calls that can be made is virtually unlimited. It could go through practically all the phone numbers in Switzerland in a day.

The more aware the public are and immediately cancels the calls, the more calls the fraudsters' machine has to make in order to generate enough potential victims who are then connected to the fraudsters. However, the high number of reports made to the NCSC is also positive in that a large proportion of the public are alert, quickly spotting the scam and hanging up straight away.

Don't call back, the number shown is faked

A Swiss mobile phone number almost always appears on the display for these calls. Often those submitting reports state that they missed the call and tried to call back. However, the true owner of the phone number has no idea that their number is being misused is certainly not from the police.

In these cases, the number displayed has been faked. The callers use Internet telephony and can falsify or mask the phone number. Sometimes the number displayed is assigned, in other cases the number is not assigned to anyone.

As the number displayed may belong to someone who has nothing to do with the scam, it cannot simply be blocked. If the number were to be blocked, the connection of someone uninvolved in the scam would be blocked, which would have even more serious consequences for them in addition to the annoyance caused by numerous returned calls from irate members of the public.

Having their mobile phone number misused is also very annoying for the owner. However, the calls do usually stop after a while. If this is not the case, the only option is often to change the phone number.

Recommendations from the Swiss National Cyber Security Centre (NCSC)

- End such calls immediately. Neither the police nor other authorities make calls to gain access to your devices.

- Do not allow anyone to remotely access your computer. If you gave remote access, it is possible that your computer has been infected.

- The first step is to uninstall the remote access program.

- If you suspect an infection, have your device checked immediately by a specialist and cleaned if necessary. The safest option is to completely reinstall the computer. However, do not forget to back up all personal data beforehand.

- If you have suffered a financial loss, report the case to your bank and file a complaint.

More information at the Swiss National Cyber Security Centre (NCSC):
https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/wochenrueckblick_15.html

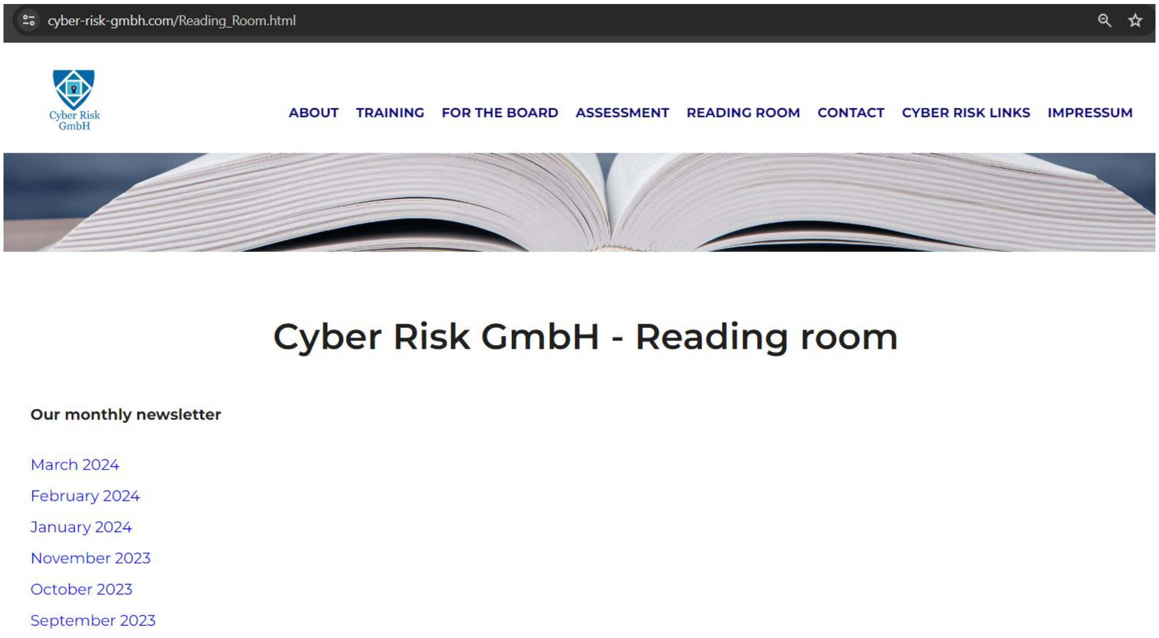
---

We are carefully monitoring the developments and the regulatory compliance obligations in the EU. You may visit: https://www.cyber-risk-gmbh.com/Impressum.html

c. Understanding Cybersecurity in the European Union.

1. The NIS 2 Directive
2. The Digital Operational Resilience Act (DORA)
3. The Critical Entities Resilience Directive (CER)
4. The European Data Act
5. The European Data Governance Act (DGA)
6. The European Cyber Resilience Act (CRA)
7. The Digital Services Act (DSA)
8. The Digital Markets Act (DMA)
9. The European Chips Act
10. The Artificial Intelligence Act
11. The Artificial Intelligence Liability Directive
12. The Framework for Artificial Intelligence Cybersecurity Practices (FAICP)
13. The EU Cyber Solidarity Act
14. The Digital Networks Act (DNA)
15. The European ePrivacy Regulation
16. The European Digital Identity Regulation
17. The European Media Freedom Act (EMFA)
18. The Corporate Sustainability Due Diligence Directive (CSDDD)
19. The Systemic Cyber Incident Coordination Framework (EU-SCICF)
20. The European Health Data Space (EHDS)
21. The European Financial Data Space (EFDS)
22. The Financial Data Access (FiDA) Regulation

Welcome to our monthly newsletter.
Our reading room: https://www.cyber-risk-gmbh.com/Reading_Room.html



Cyber Risk GmbH - Reading room

Our monthly newsletter

- March 2024
- February 2024
- January 2024
- November 2023
- October 2023
- September 2023

Best regards,

George Lekatis

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

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

Number 1 (Page 18)

European Defence Industrial Strategy (EDIS)

EUROPEAN
COMMISSION

Number 2 (Page 23)

Commission Delegated Regulation establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

EUROPEAN
COMMISSION

Number 3 (Page 26)

Compendium on Elections Cybersecurity and Resilience
NIS Cooperation Group Publication, Updated version (2024)

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Number 4 (Page 29)

Making messaging interoperability with third parties safe for users in Europe

Engineering at Meta

Number 5 (Page 34)

According to Advocate General Priit Pikamäe, a database containing personal data may, under certain conditions, be sold in enforcement proceedings, even if the data subjects have not consented to the sale

COURT OF JUSTICE
OF THE EUROPEAN UNION

Number 6 (Page 36)

Commission fines Apple over €1.8 billion over abusive App store rules for music streaming providers

European
Commission

Number 7 (Page 40)

Internet Crime Report 2023

INTERNET CRIME COMPLAINT CENTER

Number 8 (Page 43)

The U.S. Government Accountability Office (GAO)
COMBATING DEEPFAKES

GAO Science, Technology Assessment, and Analytics

Number 9 (Page 45)

SXSW Panel Replay: Real or Not, Defending Authenticity in a Digital World

Experts from DARPA, Google, Graphika, and LinkedIn speak with CNN at SXSW 2024 about how to address the growing threat posed by deepfakes

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 10 (Page 47)

Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops

A workshop methodology for developing increased capability against information influence operations

Number 11 (Page 51)

Browse safely with real-time protection on Chrome

Google

Number 12 (Page 53)

World War II Slogan is Crucial to Preventing Unauthorized Disclosure in 2024 - DITMAC Team Working to Reduce Unauthorized Disclosures, Training DOD Workforce

Story by John Joyce, Defense Counterintelligence and Security Agency

Number 13 (Page 57)

Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act

Number 14 (Page 59)

Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System

Number 15 (Page 62)

FCC Proposes Cybersecurity Labeling Program for Smart Devices

Number 16 (Page 64)

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note

Obligations of foreign-based persons to comply with U.S. sanctions and export control laws

Number 17 (Page 66)

The IC OSINT Strategy 2024-2026

Number 18 (Page 69)

Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats

Number 19 (Page 72)

Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections

Number 20 (Page 74)

Supo identified the cyber espionage operation against the parliament as APT31

Number 21 (Page 76)

Propelling 3D printing into the future - Printing stronger materials five times faster

Number 22 (Page 79)

Johns Hopkins APL and Navy Chart Next Steps to Accelerate 3D-Printing Advancements

Number 23 (Page 82)

Cybersecurity and Infrastructure Security Agency (CISA), DHS
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Number 24 (Page 85)

Amazon’s request to suspend its obligation to make an advertisement repository publicly available is rejected

COURT OF JUSTICE
OF THE EUROPEAN UNION

Number 25 (Page 87)

Gas Pipeline Safety: Better Data and Planning Would Improve Implementation of Regulatory Changes

GAO
U.S. Government Accountability Office

Number 26 (Page 89)

Fighting cookie theft using device bound sessions

Chromium Blog

Number 27 (Page 93)

Protect Yourself: Commercial Surveillance Tools

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
UNITED STATES OF AMERICA

DEPARTMENT OF STATE
UNITED STATES OF AMERICA

Number 28 (Page 95)

EIOPA stress tests European insurers’ resilience with a scenario of escalating geopolitical tensions

eiopa
European Insurance and
Occupational Pensions Authority

Number 29 (Page 97)

CNIL and the application of the EU GDPR to Artificial Intelligence

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Number 30 (Page 100)

Cyber Resilience Act Requirements Standards Mapping

Auswärtiges Amt

European Commission

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Number 31 (Page 102)

Revisiting the Non-Paper

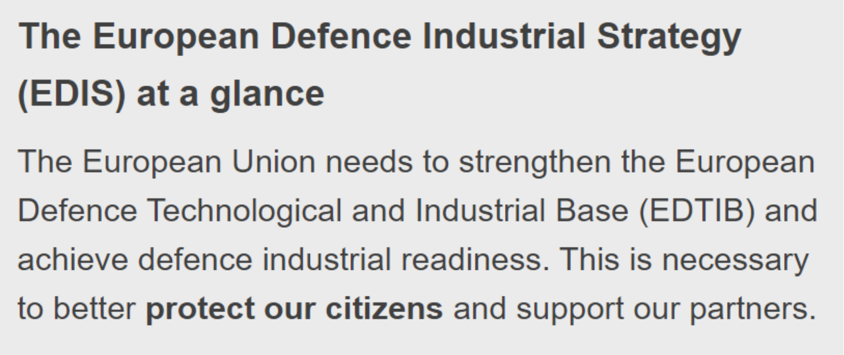
Non-Paper on EU Cyber Diplomacy, by Estonia, France, Germany, Poland, Portugal and Slovenia

Federal Foreign Office

Number I

European Defence Industrial Strategy (EDIS)

The European Commission and the High Representative presented the first-ever European Defence Industrial Strategy at EU level and proposed an ambitious set of new actions to support the competitiveness and readiness of its defence industry.



The European Defence Industrial Strategy (EDIS) at a glance

The European Union needs to strengthen the European Defence Technological and Industrial Base (EDTIB) and achieve defence industrial readiness. This is necessary to better **protect our citizens** and support our partners.

Two years ago, Russia's unjustified, on-going war of aggression against Ukraine marked the return of high-intensity conflict on our continent. The European Defence Industrial Strategy (EDIS) sets a clear, long-term vision to achieve defence industrial readiness in the European Union.

As a first immediate and central means to deliver the Strategy, the European Commission today tables a legislative proposal for a European Defence Industry Programme (EDIP) and a framework of measures to ensure the timely availability and supply of defence products.

The Strategy outlines the challenges currently faced by the European Defence Technological and Industrial Base (EDTIB) but also the opportunity to tap its full potential and sets out a direction for the next decade.

To increase European defence industrial readiness, Member States need to invest more, better, together, and European. To support Member States in achieving these goals, the European Defence Industrial Strategy presents a set of actions aiming at:

- Supporting a more efficient expression of the Member States' collective defence demand. This will be based on existing instruments and initiatives, such as the Capability Development Plan (CDP), the Coordinated Annual Review on Defence (CARD) and the Permanent Structured Cooperation (PESCO). It will be supported by incentivising Member States' cooperation in the procurement phase of defence capabilities;

- Securing the availability of all defence products through a more responsive EDTIB, under any circumstances and time horizon. Investments by Member States and the European defence industry in developing and bringing to market tomorrow's state of the art defence technologies and capabilities will be supported. Measures are also proposed to ensure that the EDTIB has at its disposal what it needs even in crisis periods, thereby increasing the EU's Security of Supply;

- Ensuring that national and EU budgets support with the necessary means the adaptation of the European defence industry to the new security context;

- Mainstreaming a defence readiness culture across policies, notably by calling for a review of the European Investment Bank's lending policy this year;

- Developing closer ties with Ukraine through its participation in Union initiatives in support of defence industry and stimulating cooperation between the EU and Ukrainian defence industries;

- Teaming up with NATO and our strategic, like-minded and international partners, and cooperating more closely with Ukraine.

The Strategy sets indicators, aimed at measuring Member States' progress towards industrial readiness. Member States are invited to:

- Procure at least 40% of defence equipment in a collaborative manner by 2030;

- Ensure that, by 2030, the value of intra-EU defence trade represents at least 35% of the value of the EU defence market;

- Make steady progress towards procuring at least 50% of their defence procurement budget within the EU by 2030 and 60% by 2035.

The European Defence Industry Programme (EDIP) is the new legislative initiative that will bridge from short-term emergency measures, adopted in 2023 and ending in 2025, to a more structural and longer-term approach to achieve defence industrial readiness. This will ensure continuity in the support to the European defence technological and industrial base, to accompany its swift adaptation to the new reality.

EDIP includes both financial and regulatory aspects. EDIP will mobilise €1.5 billion of the EU budget over the period 2025-2027, to continue enhancing the competitiveness of the EDTIB.

EDIP financial support will notably extend the intervention logic of EDIRPA (financial support from EU budget to offset the complexity of cooperation between Member States in the procurement phase) and ASAP (financial support to defence industries increasing their production capacity), to further encourage investments by the EDTIB.

EDIP will also support the industrialisation of products stemming from cooperative R&D actions supported by the European Defence Fund. The EDIP budget may also be used to set up a Fund to Accelerate defence Supply chains Transformation (FAST).

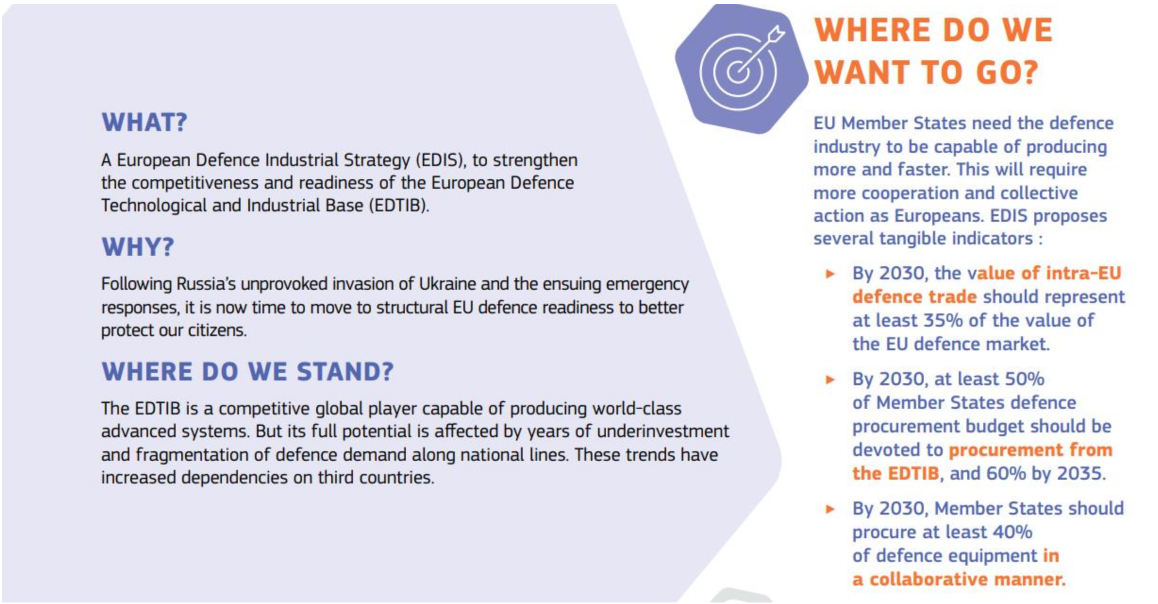
That new fund will aim at facilitating access to debt and/or equity financing for SMEs and small midcaps industrialising defence technologies and/or manufacturing defence products. EDIP budget will also enhance the EU's defence industrial cooperation with Ukraine and support the development of its defence industrial and technological base.

To do so, EDIP could possibly draw additional funding from the windfall profits derived from immobilised Russian sovereign assets (subject to Council decision on a proposal by the High Representative).

On the regulatory aspects, EDIP comes with novel solutions. It will make available a new legal framework, the Structure for European Armament Programme (SEAP), to facilitate and scale up Member States' cooperation on defence equipment, in full complementarity with the PESCO framework.

It also entails an EU-wide regime for security of supply of defence equipment, which will ensure constant access to all necessary defence products in Europe and provide a framework to efficiently react to possible future supply crises of defence products.

In addition, EDIP will allow the launch of European Defence Projects of Common Interest, with potential EU financial support. Finally, EDIP proposes to set up a governance structure, where Member States are fully involved, to ensure overall consistency of EU action in the field of defence industry (the Defence Industrial Readiness Board).



WHAT?

A European Defence Industrial Strategy (EDIS), to strengthen the competitiveness and readiness of the European Defence Technological and Industrial Base (EDTIB).

WHY?

Following Russia's unprovoked invasion of Ukraine and the ensuing emergency responses, it is now time to move to structural EU defence readiness to better protect our citizens.

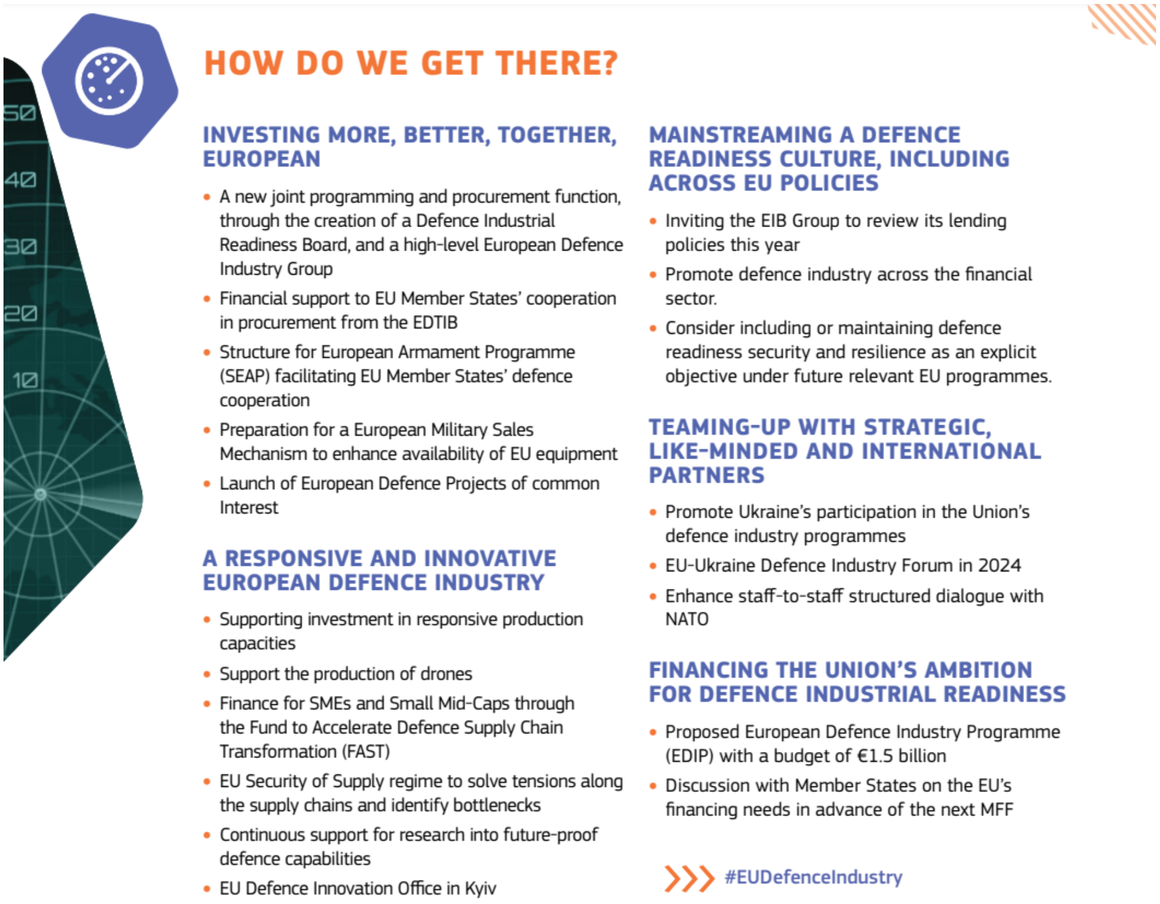
WHERE DO WE STAND?

The EDTIB is a competitive global player capable of producing world-class advanced systems. But its full potential is affected by years of underinvestment and fragmentation of defence demand along national lines. These trends have increased dependencies on third countries.

WHERE DO WE WANT TO GO?

EU Member States need the defence industry to be capable of producing more and faster. This will require more cooperation and collective action as Europeans. EDIS proposes several tangible indicators :

- By 2030, the **value of intra-EU defence trade** should represent at least 35% of the value of the EU defence market.
- By 2030, at least 50% of Member States defence procurement budget should be devoted to **procurement from the EDTIB**, and 60% by 2035.
- By 2030, Member States should procure at least 40% of defence equipment **in a collaborative manner.**



HOW DO WE GET THERE?

INVESTING MORE, BETTER, TOGETHER, EUROPEAN

- A new joint programming and procurement function, through the creation of a Defence Industrial Readiness Board, and a high-level European Defence Industry Group
- Financial support to EU Member States' cooperation in procurement from the EDTIB
- Structure for European Armament Programme (SEAP) facilitating EU Member States' defence cooperation
- Preparation for a European Military Sales Mechanism to enhance availability of EU equipment
- Launch of European Defence Projects of common Interest

A RESPONSIVE AND INNOVATIVE EUROPEAN DEFENCE INDUSTRY

- Supporting investment in responsive production capacities
- Support the production of drones
- Finance for SMEs and Small Mid-Caps through the Fund to Accelerate Defence Supply Chain Transformation (FAST)
- EU Security of Supply regime to solve tensions along the supply chains and identify bottlenecks
- Continuous support for research into future-proof defence capabilities
- EU Defence Innovation Office in Kyiv

MAINSTREAMING A DEFENCE READINESS CULTURE, INCLUDING ACROSS EU POLICIES

- Inviting the EIB Group to review its lending policies this year
- Promote defence industry across the financial sector.
- Consider including or maintaining defence readiness security and resilience as an explicit objective under future relevant EU programmes.

TEAMING-UP WITH STRATEGIC, LIKE-MINDED AND INTERNATIONAL PARTNERS

- Promote Ukraine's participation in the Union's defence industry programmes
- EU-Ukraine Defence Industry Forum in 2024
- Enhance staff-to-staff structured dialogue with NATO

FINANCING THE UNION'S AMBITION FOR DEFENCE INDUSTRIAL READINESS

- Proposed European Defence Industry Programme (EDIP) with a budget of €1.5 billion
- Discussion with Member States on the EU's financing needs in advance of the next MFF

››› #EUDefenceIndustry

A stronger and more responsive European defence industry will benefit the Member States and ultimately EU citizens. It will also benefit the EU's key partners, including NATO and Ukraine.

The EDIP proposal is the first operational measure of the European Defence Industrial Strategy.

To read more: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-strategy_en

Number 2

Commission Delegated Regulation establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

EUROPEAN COMMISSION

This initiative was identified as an important measure to improve the resilience of critical energy infrastructure and services in Commission communications on energy system integration, the Security Union Strategy and the Cybersecurity Strategy.

It is based on the powers that the European Parliament and the Council conferred on the Commission in the Regulation (EU) 2019/9434 (Electricity Regulation) to develop sector-specific rules ('network code') that address the cybersecurity aspects of cross-border electricity flows.

This includes rules on common minimum requirements, planning, monitoring, reporting and crisis management.

The network code aims to establish a recurrent process of cybersecurity risk assessments in the electricity sector. The assessments will aim to systematically identify the entities that perform digitalised processes with a critical or high impact in cross-border electricity flows, their cybersecurity risks and the necessary mitigating measures that they need to implement.

Multiple methodologies and standards exist today in the cybersecurity industry. Moreover, it is a fast-evolving knowledge field. With the objective of harmonising and ensuring a common baseline while respecting existing practices and investments as much as possible, the network code therefore establishes a governance model to develop, follow and regularly review the methodologies of different stakeholders.

This governance and stakeholder contribution model takes into account the current mandates of different bodies in both the cybersecurity and electricity regulatory systems.

As technology is constantly evolving and the electricity sector is undergoing rapid digitalisation, the network code therefore strives not to be detrimental to innovation and not to constitute a barrier to new entities accessing the electricity market and the subsequent use of innovative solutions that help make the electricity system more efficient.

As part of this objective, all new systems, processes and procedures must respect cybersecurity requirements. In order to identify new trends and possible future risks in cybersecurity, regular reporting will occur with the comprehensive cross-border electricity cybersecurity risk assessment report, provided for in the network code and carried out at least every 3 years.

The measures envisaged in the network code are important for improving the security of electricity supply in the EU.

This delegated Regulation will lay down harmonised rules applicable to all relevant operators in all Member States. It will aim to reach the objectives, while ensuring a level playing field. It will further help integrate the EU electricity market in a non-discriminatory manner and ensure effective competition.

The objectives of this initiative cannot be achieved at national level as it focuses on crossborder electricity flows and refers to interconnected energy networks across Europe.

This Regulation aims at:

- establishing rules concerning the governance of cybersecurity aspects of cross-border electricity flows to ensure the reliability of the electricity system and the close collaboration with existing governance structures for cybersecurity;

- determining common criteria for performing cybersecurity risk assessments for the operational reliability of the electricity system with regard to cross-border electricity flows;

- promoting a common electricity cybersecurity framework and by that fostering a common minimum electricity cybersecurity level across the Union;

- providing for mechanisms in order to assess the application of the minimum and advanced cybersecurity controls on systems that can affect cross-border electricity flows;

- establishing information flows by establishing rules for the collection and sharing of information in relation to cross-border electricity flows, compatible with other national and EU legislation;

- establishing effective processes to identify, classify and respond to cyber-attacks impacting the cross-border flows of electricity;

- setting up effective processes for the management of cross-border electricity crises related to cyber-attacks;

- defining common principles for electricity cybersecurity exercises to increase resilience and improve the risk preparedness of the electricity sector;

- protecting the information exchanged under this Regulation;

- determining a process for monitoring the implementation of this Regulation, to assess the effectiveness of investments in cybersecurity protection and to report on the progress of cybersecurity protection across the Union; and

- ensuring that the recommendations on the cybersecurity procurement specifications with relevance for cross-border electricity flows are not detrimental to innovation, new systems, processes and procedures.

To read more: https://energy.ec.europa.eu/document/download/c7580561-4ced-4011-b63e-e1482a83c7b1_en?filename=Delegated%20Act%20on%20the%20new%20Network%20Code%20on%20Cybersecurity_draft.pdf

Number 3

Compendium on Elections Cybersecurity and Resilience

NIS Cooperation Group Publication, Updated version (2024)

This document has been drafted and endorsed by the NIS Cooperation Group.

The NIS Cooperation Group, composed of representatives of EU Member States, the European Commission, and the European Union Agency for Cybersecurity ('ENISA'), has been established by Article 14 of the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). The NIS Cooperation Group supports and facilitates strategic cooperation and the exchange of information among Member States, as well as strengthens trust and confidence between the EU Member States regarding cybersecurity issues.

Introduction

During the last decade, elections across the globe have become a frequent target of cyberattacks. Cyber threat activity targeting elections has increased worldwide. These cyberattacks are often combined with information operations and other hybrid threats.

Even when the actual vote is often carried out with pen and paper, electoral processes increasingly depend on network and information systems, and it is therefore important to take cybersecurity measures to protect the integrity of elections.

Cyber-attacks against the core functions of our democratic processes could undermine the safeguards in place to protect them, the participants in this best moment of the democratic process and the very legitimacy of democratic institutions.

In the case of the elections for the European Parliament, a successful campaign of cyberattacks against one EU Member State could threaten to compromise the entire parliamentary election.

For instance, the disruption of the network and information systems underpinning the elections in one Member State, or even the perception of it, could impact vote counting and tabulation processes at the national level and cause a delay in Member States notification of the names of the elected Members to the Parliament resulting in affecting the proper functioning of the European Parliament or even its democratic legitimacy.

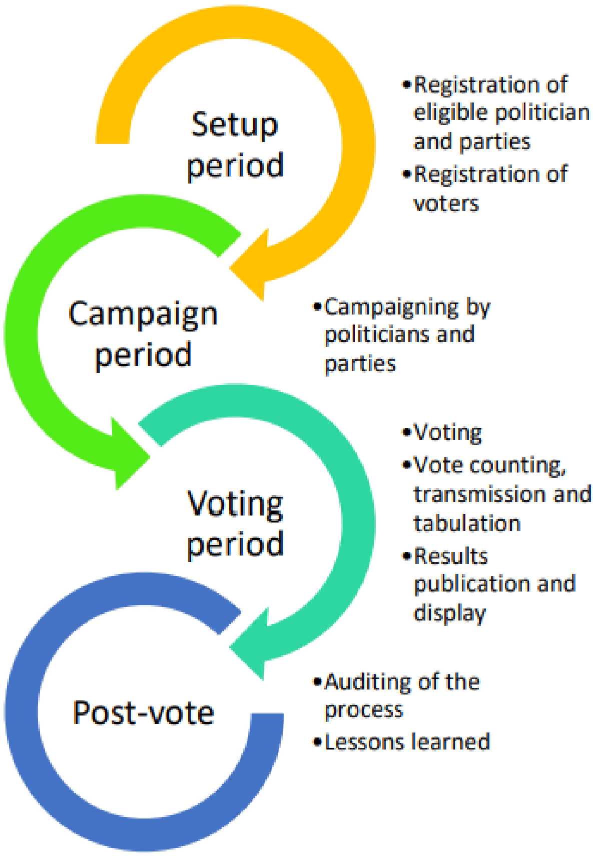
This compendium aims to support elections management bodies, national electoral authorities and cybersecurity bodies involved in cybersecurity and resilience of elections in the EU Member States. The present document is an updated version of the document published by the NIS Cooperation Group in March 2018.

This living document provides guidelines and practical measures based on relevant experiences and best practices identified by its contributors. Contributions have been made by most EU Member States as well as the European Commission and the European Union Agency for Cybersecurity (ENISA).

The European External Action Service (EEAS) as well as the European Cooperation Network on Elections (ECNE) also assisted in drafting this document. However, the organization and security of elections is ensured at national level, with significant variation across EU Member States.

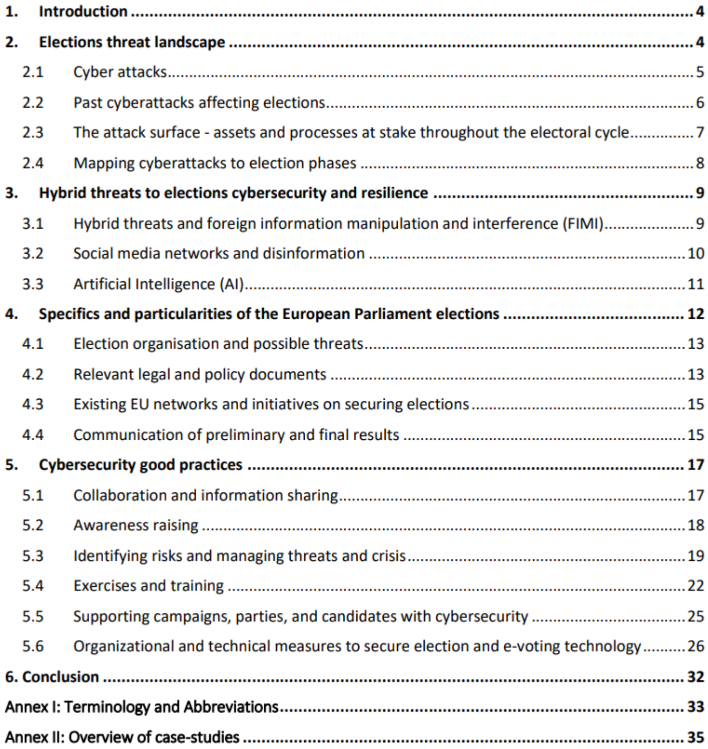
Therefore, this compendium has been designed to allow EU Member States select approaches and measures they consider appropriate for their national context and provide them with good practices identified through the sharing of experiences by the EU Member States.

In addition, a number of checklists and case studies are included to offer further practical guidance.


Setup period
•Registration of eligible politician and parties
•Registration of voters
Campaign period
•Campaigning by politicians and parties
Voting period
•Voting
•Vote counting, transmission and tabulation
•Results publication and display
Post-vote
•Auditing of the process
•Lessons learned

Elections threat landscape

It is important to take an **all-hazard approach** and to take into account all potential cybersecurity threats and incidents, which could impact election technology, including cyber-attacks, system failures (such as software bugs, hardware failures, etc.), human errors (such as software misconfigurations, mistakes with maintenance or software updates), natural disasters and similar contingencies such as power cuts and network outages.



To read more: https://www.enisa.europa.eu/news/safeguarding-eu-elections-amidst-cybersecurity-challenges

Number 4

Making messaging interoperability with third parties safe for users in Europe

Engineering at Meta

- To comply with a new EU law, the Digital Markets Act (DMA), which comes into force on March 7th, we've made major changes to WhatsApp and Messenger to enable interoperability with third-party messaging services.

- We're sharing how we enabled third-party interoperability (interop) while maintaining end-to-end encryption (E2EE) and other privacy guarantees in our services as far as possible.

On March 7th, a new EU law, the Digital Markets Act (DMA), comes into force. One of its requirements is that designated messaging services must let third-party messaging services become interoperable, provided the third-party meets a series of eligibility, including technical and security requirements.

This allows users of third-party providers who choose to enable interoperability (interop) to send and receive messages with opted-in users of either Messenger or WhatsApp – both designated by the European Commission (EC) as being required to independently provide interoperability to third-party messaging services.

For nearly two years our team has been working with the EC to implement interop in a way that meets the requirements of the law and maximizes the security, privacy and safety of users. Interoperability is a technical challenge – even when focused on the basic functionalities as required by the DMA.

In year one, the requirement is for 1:1 text messaging between individual users and the sharing of images, voice messages, videos, and other attached files between individual end users. In the future, requirements expand to group functionality and calling.

To interoperate, third-party providers will sign an agreement with Messenger and/or WhatsApp and we'll work together to enable interoperability.

Today we'll publish the WhatsApp Reference Offer for third-party providers which will outline what will be required to interoperate with the service. The Reference Offer for Messenger will follow in due course.

While Meta must be ready to enable interoperability with other services within three months of receiving a request, it may take longer before the functionality is ready for public use. We wanted to take this opportunity to set out the technical infrastructure and thinking that sits behind our interop solution.

A privacy-centric approach to building interoperable messaging services

Our approach to compliance with the DMA is centered around preserving privacy and security for users as far as is possible. The DMA quite rightly makes it a legal requirement that we should not weaken security provided to Meta's own users.

The approach we have taken in terms of implementing interoperability is the best way of meeting DMA requirements, whilst also creating a viable approach for the third-party providers interested in becoming interoperable with Meta and maximizing user security and privacy.

Implementing an end-to-end encrypted protocol

First, we need to protect the underlying security that keeps communication on Meta E2EE messaging apps secure: the encryption protocol. WhatsApp and Messenger both use the tried and tested Signal Protocol as a foundational piece for their encryption.

Messenger is still rolling out E2EE by default for personal communication, but on WhatsApp, this default has been the case since 2016. In both cases, we are using the Signal Protocol as the foundation for these E2EE communications, as it represents the current gold standard for E2EE chats.

In order to maximize user security, we would prefer third-party providers to use the Signal Protocol. Since this has to work for everyone however, we will allow third-party providers to use a compatible protocol if they are able to demonstrate it offers the same security guarantees as Signal.

To send messages, the third-party providers have to construct message protobuf structures which are then encrypted using the Signal Protocol and then packaged into message stanzas in eXtensible Markup Language (XML).

Meta servers push messages to connected clients over a persistent connection. Third-party servers are responsible for hosting any media files their client applications send to Meta clients (such as image or video files).

After receiving a media message, Meta clients will subsequently download the encrypted media from the third-party messaging servers using a Meta proxy service.

It's important to note that the E2EE promise Meta provides to users of our messaging services requires us to control both the sending and receiving clients. This allows us to ensure that only the sender and the intended recipient(s) can see what has been sent, and that no one can listen to your conversation without both parties knowing.

While we have built a secure solution for interop that uses the Signal Protocol encryption to protect messages in transit, without ownership of both clients (endpoints) we cannot guarantee what a third-party provider does with sent or received messages, and we therefore cannot make the same promise.

Our technical solution builds on Meta's existing client / server architecture

We think the best way to deliver interoperability is through a solution which builds on Meta's existing client / server architecture [Figure 1].

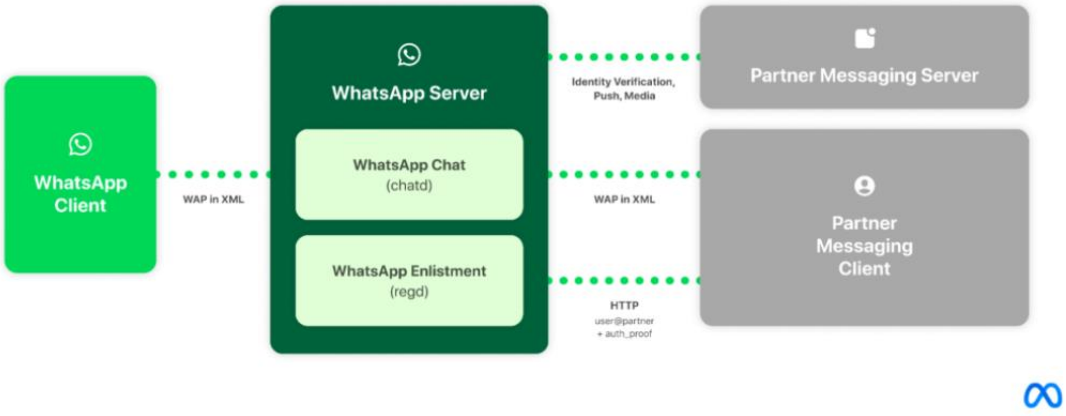


Figure 1: A simplified illustration of WhatsApp's technical architecture.

In particular, the requirement that clients connect to Meta infrastructure has the following benefits, it:

- Enables Meta to maximize the level of security and safety for all users by carrying out many of the same integrity checks as it does for existing Meta users

- Constitutes a "plug-and-play" model for third-party providers, lowering the barriers for potential new entrants and costs for third-party providers

- Helps maximize protection of user privacy by limiting the exposure of their personal data to Meta servers only

- Improves overall reliability of the interoperable service as it benefits from Meta's infrastructure, which is already globally scaled to handle over 100 billion messages each day

Taking the example of WhatsApp, third-party clients will connect to WhatsApp servers using our protocol (based on the Extensible Messaging and Presence Protocol – XMPP). The WhatsApp server will interface with a third-party server over HTTP in order to facilitate a variety of things including authenticating third-party users and push notifications.

WhatsApp exposes an Enlistment API that third-party clients must execute when opting in to the WhatsApp network. When a third-party user registers on WhatsApp or Messenger, they keep their existing user-visible identifier, and are also assigned a unique, WhatsApp-internal identifier that is used at the infrastructure level (for protocols, data storage, etc.)

WhatsApp requires third-party clients to provide "proof" of their ownership of the third-party user-visible identifier when connecting or enlisting.

The proof is constructed by the third-party service cryptographically signing an authentication token. WhatsApp uses the standard OpenID protocol (with some minor modifications) alongside a JSON Web Token (JWT Token) to verify the user-visible identifier through public keys periodically fetched from the third-party server.

WhatsApp uses the Noise Protocol Framework to encrypt all data traveling between the client and the WhatsApp server. As part of the Noise Protocol, the third-party client must perform a "Noise Handshake" every time the client connects to the WhatsApp server. Part of this Handshake is providing a payload to the server which also contains the JWT Token.

Once the client has successfully connected to the WhatsApp server, the client must use WhatsApp's chat protocol to communicate with the WhatsApp server. WhatsApp's chat protocol uses optimized XML stanzas to communicate with our servers.

As we continue to discuss this architecture with third-party providers, we think there is also an approach to implementing interop where we could give third-party providers the option to add a proxy or an "intermediary" between their client and the WhatsApp server.

A proxy could potentially give third-party providers more flexibility and control over what their client can receive from the WhatsApp server and also removes the requirement that third-party clients must implement WhatsApp's client-to-server protocol, i.e. maintain their existing "chat channel" on their clients.

The challenge here is that WhatsApp would no longer have direct connection to both clients and, as a result, would lose connection level signals that are important for keeping users safe from spam and scams such as TCP fingerprints.

We would therefore anticipate implementing additional requirements for third-party providers who take up this option under our Reference Offer. This approach also exposes all the chat metadata to the proxy server, which increases the likelihood that this data could be accidentally or intentionally leaked.

Clearly explaining how interop works to users

We believe it is essential that we give users transparent information about how interop works and how it differs from their chats with other WhatsApp or Messenger users. This will be the first time that users have been part of an interoperable network on our services, so giving them clear and straightforward information about what to expect will be paramount.
For example, users need to know that our security and privacy promise, as well as the feature set, won't exactly match what we offer in WhatsApp chats.

Privacy and security is a shared responsibility

As is hopefully clear from this post, preserving privacy and security in an interoperable system is a shared responsibility, and not something that Meta is able to do on its own.

We will therefore need to continue collaborating with third-party providers in order to provide the safest and best experience for our users.

To read more: https://engineering.fb.com/2024/03/06/security/whatsapp-messenger-messaging-interoperability-eu/

Number 5

According to Advocate General Priit Pikamäe, a database containing personal data may, under certain conditions, be sold in enforcement proceedings, even if the data subjects have not consented to the sale

COURT OF JUSTICE
OF THE EUROPEAN UNION

A Polish court is ruling on a dispute between a company and a member of the board of directors of another company that specialises in online sales and against which the first company has a debt claim.

That member may be personally liable where the debtor company does not have assets to satisfy the creditor company's claim. However, that member is of the opinion that this is not the case because the debtor company has, among other assets, two databases of users of the online platform it had created.

They contain personal data of hundreds of thousands of people who have not consented to the processing of their data in the form of making those data available to third parties outside that platform.

The Polish court has doubts as to whether the General Data Protection Regulation (GDPR) allows a court enforcement officer to sell those databases, in the context of enforcement proceedings, without the consent of the data subjects and has referred the matter to the Court of Justice.

In his Opinion, Advocate General Priit Pikamäe proposes that the Court should answer in the affirmative.

In his view, the operations carried out by the court enforcement officer for the purposes of estimating the value of the databases concerned and selling them by public auction come within the scope of the GDPR.

They include, at the very least, the retrieval, consultation, use and making available to the purchaser of those personal data and, consequently, must be regarded as a 'processing' of those data within the meaning of that regulation.

Furthermore, the Advocate General takes the view that the court enforcement officer must be regarded as the controller of the personal data.

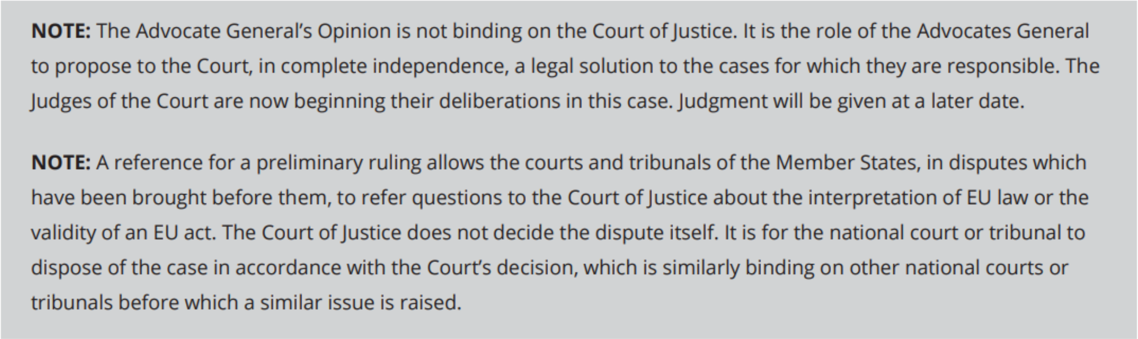
Furthermore, the Advocate General concludes that the processing in question is lawful where it is necessary for the performance of a task carried out in the exercise of official authority vested in the court enforcement officer.

Lastly, the Advocate General notes that the purpose of the processing carried out by the court enforcement officer differs from the initial purpose of enabling the use of the online sales platform concerned.

In order for such further processing to be regarded as being compatible with the GDPR, it must constitute a necessary and proportionate measure in a democratic society to achieve one of the objectives of general interest pursued by that regulation.

According to the Advocate General, of those objectives, the objective of ensuring the enforcement of civil law claims may, in principle, justify the processing of the data at issue in the present case.

He also states that the assessment of whether a measure is proportionate, which the Polish court must carry out, involves balancing the creditor company’s right to property and the right to protection of personal data of the users of the online platform concerned.



NOTE: The Advocate General’s Opinion is not binding on the Court of Justice. It is the role of the Advocates General to propose to the Court, in complete independence, a legal solution to the cases for which they are responsible. The Judges of the Court are now beginning their deliberations in this case. Judgment will be given at a later date.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of EU law or the validity of an EU act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court’s decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Unofficial document for media use, not binding on the Court of Justice.

To read more: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-02/cp240035en.pdf

https://curia.europa.eu/juris/documents.jsf?num=C-693/22

Number 6

Commission fines Apple over €1.8 billion over abusive App store rules for music streaming providers

The European Commission has fined Apple over €1.8 billion for abusing its dominant position on the market for the distribution of music streaming apps to iPhone and iPad users (‘iOS users') through its App Store.

In particular, the Commission found that Apple applied restrictions on app developers preventing them from informing iOS users about alternative and cheaper music subscription services available outside of the app (‘anti-steering provisions'). This is illegal under EU antitrust rules.

The infringement

Apple is currently the sole provider of an App Store where developers can distribute their apps to iOS users throughout the European Economic Area (‘EEA'). Apple controls every aspect of the iOS user experience and sets the terms and conditions that developers need to abide by to be present on the App Store and be able to reach iOS users in the EEA.

The Commission's investigation found that Apple bans music streaming app developers from fully informing iOS users about alternative and cheaper music subscription services available outside of the app and from providing any instructions about how to subscribe to such offers. In particular, the anti-steering provisions ban app developers from:

- Informing iOS users within their apps about the prices of subscription offers available on the internet outside of the app.

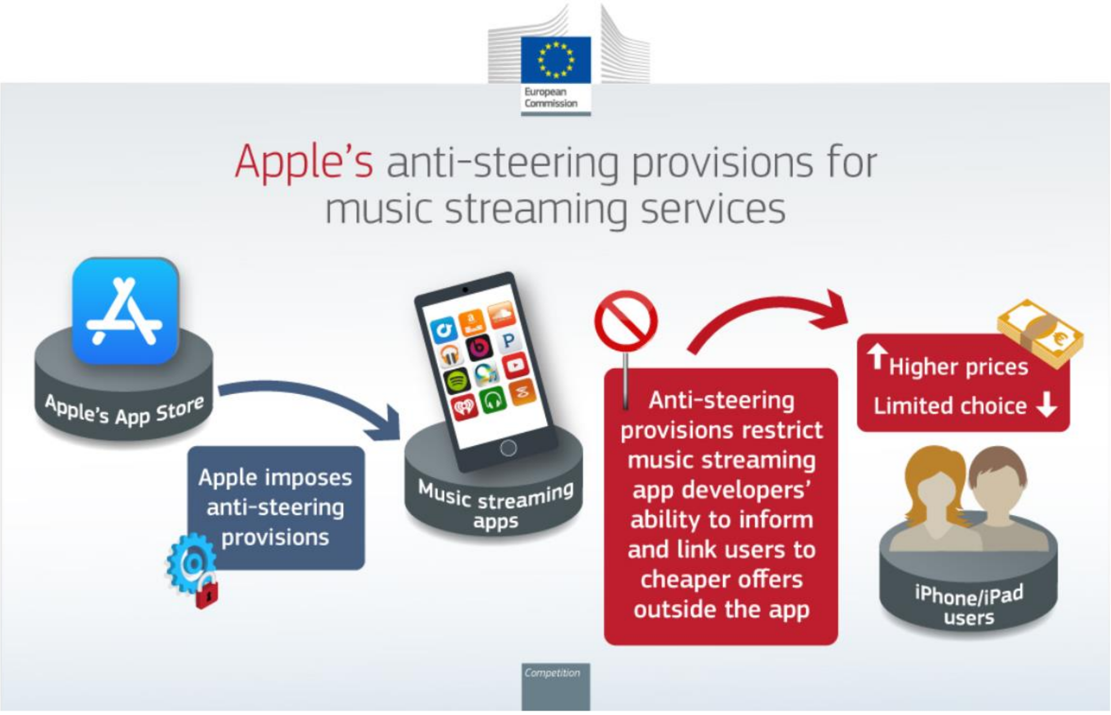
- Informing iOS users within their apps about the price differences between in-app subscriptions sold through Apple's in-app purchase mechanism and those available elsewhere.

- Including links in their apps leading iOS users to the app developer's website on which alternative subscriptions can be bought. App developers were also prevented from contacting their own newly acquired users, for instance by email, to inform them about alternative pricing options after they set up an account.

Today's decision concludes that Apple's anti-steering provisions amount to unfair trading conditions, in breach of Article 102(a) of the Treaty on the Functioning of the European Union (‘TFEU'). These anti-steering provisions are neither necessary nor proportionate for the protection of Apple's commercial interests in relation to the App Store on Apple's smart mobile devices and negatively affect the interests of iOS users, who cannot make informed and effective decisions on where and how to purchase music streaming subscriptions for use on their device.

Apple's conduct, which lasted for almost ten years, may have led many iOS users to pay significantly higher prices for music streaming subscriptions because of the high commission fee imposed by Apple on developers and passed on to consumers in the form of higher subscription prices for the same service on the Apple App Store.

Moreover, Apple's anti-steering provisions led to non-monetary harm in the form of a degraded user experience: iOS users either had to engage in a cumbersome search before they found their way to relevant offers outside the app, or they never subscribed to any service because they did not find the right one on their own.



Apple’s anti-steering provisions for music streaming services

Apple’s App Store

Apple imposes anti-steering provisions

Music streaming apps

Anti-steering provisions restrict music streaming app developers’ ability to inform and link users to cheaper offers outside the app

↑Higher prices

Limited choice ↓

iPhone/iPad users

Fine

The fine was set on the basis of the Commission's 2006 Guidelines on fines. In setting the level of the fine, the Commission took into account the duration and gravity of the infringement as well as Apple's total turnover and market capitalization. It also factored in that Apple submitted incorrect information in the framework of the administrative procedure.

In addition, the Commission decided to add to the basic amount of the fine an additional lump sum of €1.8 billion to ensure that the overall fine imposed on Apple is sufficiently deterrent.

Such lump sum fine was necessary in this case because a significant part of the harm caused by the infringement consists of non-monetary harm, which cannot be properly accounted for under the revenue-based methodology as set out in the Commission's 2006 Guidelines on Fines. In addition, the fine must be sufficient to deter Apple from repeating the present or a similar infringement; and to deter other companies of a similar size and with similar resources from committing the same or a similar infringement.

The Commission has concluded that the total amount of the fine of over €1.8 billion is proportionate to Apple's global revenues and is necessary to achieve deterrence.

The Commission has also ordered Apple to remove the anti-steering provisions and to refrain from repeating the infringement or from adopting practices with an equivalent object or effect in the future.

Background to the investigation

In June 2020, the Commission opened formal proceedings into Apple's rules for app developers on the distribution of apps via the App Store. In April 2021, the Commission sent Apple a Statement of Objections, to which Apple responded in September 2021.

In February 2023 the Commission replaced the 2021 Statement of Objections by another Statement of Objections clarifying the Commission's objections, to which Apple responded in May 2023.

Procedural background

Article 102 of the TFEU and Article 54 of the European Economic Area Agreement prohibit the abuse of a dominant position.

Market dominance is, as such, not illegal under EU antitrust rules. However, dominant companies have a special responsibility not to abuse their powerful market position by restricting competition, either in the market where they are dominant or in separate markets.

Fines imposed on companies found in breach of EU antitrust rules are paid into the general EU budget. These proceeds are not earmarked for particular expenses, but Member States' contributions to the EU budget for the following year are reduced accordingly. The fines therefore help to finance the EU and reduce the burden for taxpayers.

In accordance with the EU-UK Withdrawal Agreement, the EU continues to be competent for this case, which was initiated before the end of the transition period (“continued competence case”) for the UK. The EU will reimburse the UK for its share of the amount of the fine collected by the EU once the fine has become definitive.

More information on this case will be available under the case number AT.40437 in the public case register on the Commission's competition website, once confidentiality issues have been dealt with.

Action for damages

Any person or company affected by anti-competitive behaviour as described in this case may bring the matter before the courts of the Member States and seek damages.

The case law of the Court of Justice of the European Union and Regulation 1/2003 both confirm that in cases before national courts, a Commission decision constitutes binding proof that the behaviour took place and was illegal.

Even though the Commission has fined the company concerned, damages may be awarded by national courts without being reduced on account of the Commission fine.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161

Number 7

Internet Crime Report 2023

THE IC3

Today’s FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities.

We are focused on protecting the American people from terrorism, espionage, cyber-attacks, and major criminal threats which are increasingly emanating from our digitally connected world.

To do that, the FBI leverages the IC3 as a mechanism to gather intelligence on internet crime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes.

As of December 31, 2023, the IC3 has received over eight million complaints.

The IC3’s mission is to provide the public and our partners with a reliable and convenient reporting mechanism to submit information concerning suspected cyber enabled criminal activity and to develop effective alliances with law enforcement and industry partners to help those who report.

Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and public awareness.

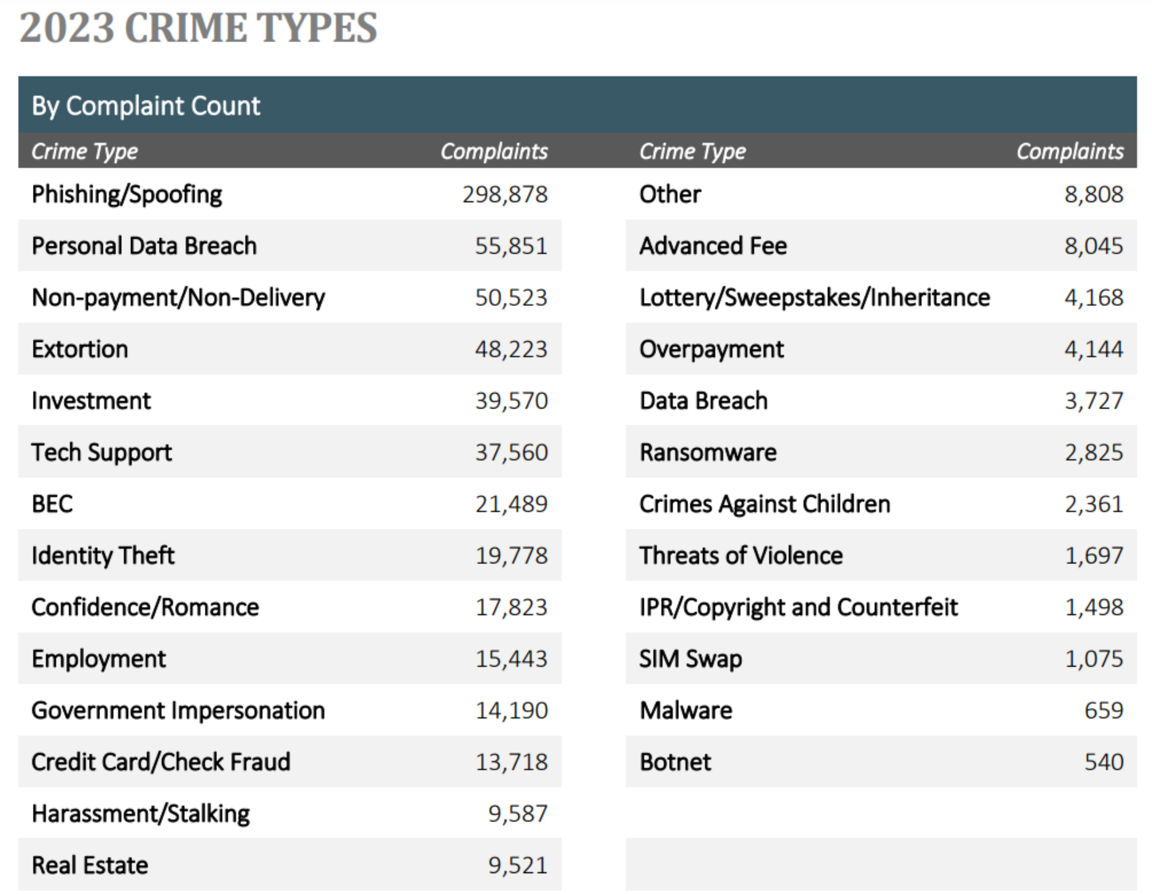
The information submitted to the IC3 can be impactful in the individual complaints, but it is most impactful in the aggregate.

That is, when the individual complaints are combined with other data, it allows the FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds.

Just as importantly, the IC3 shares reports of crime throughout its vast network of FBI field offices and law enforcement partners, strengthening our nation’s collective response both locally and nationally.

To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends.

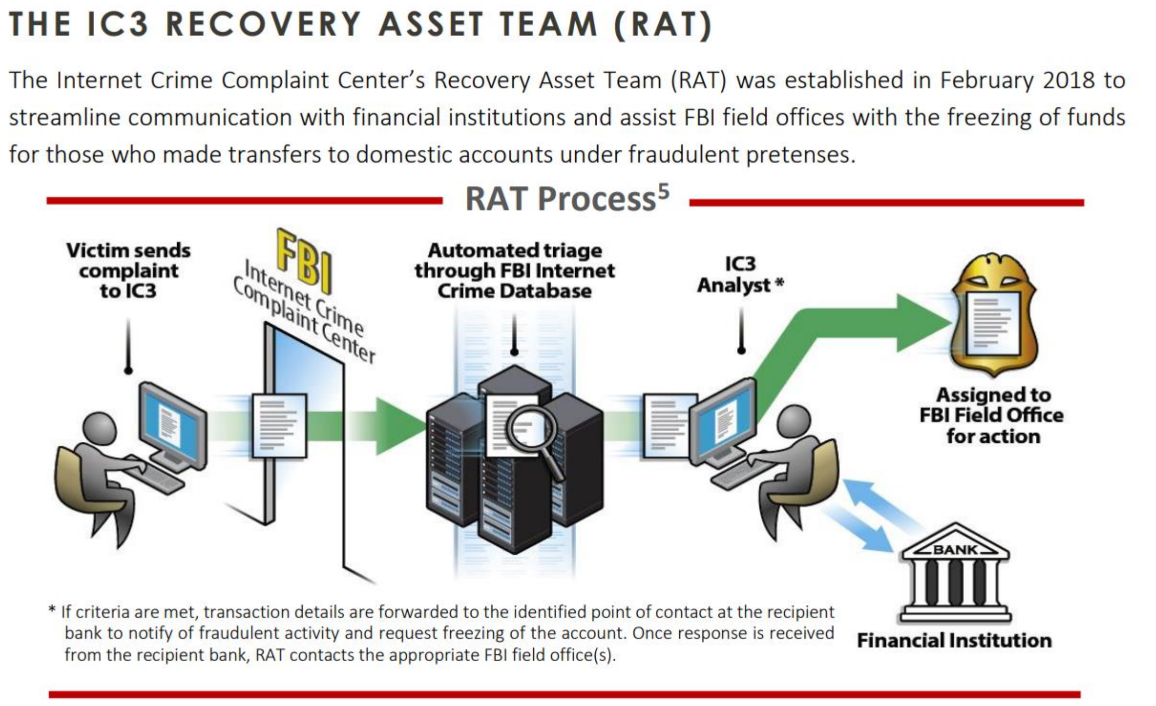
The success of these efforts is directly related to the quality of the data submitted by the public through the www.ic3.gov interface. Their efforts help the IC3, and the FBI better protect their fellow citizens.



2023 CRIME TYPES

By Complaint Count

Crime Type	*Complaints*	*Crime Type*	*Complaints*
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		



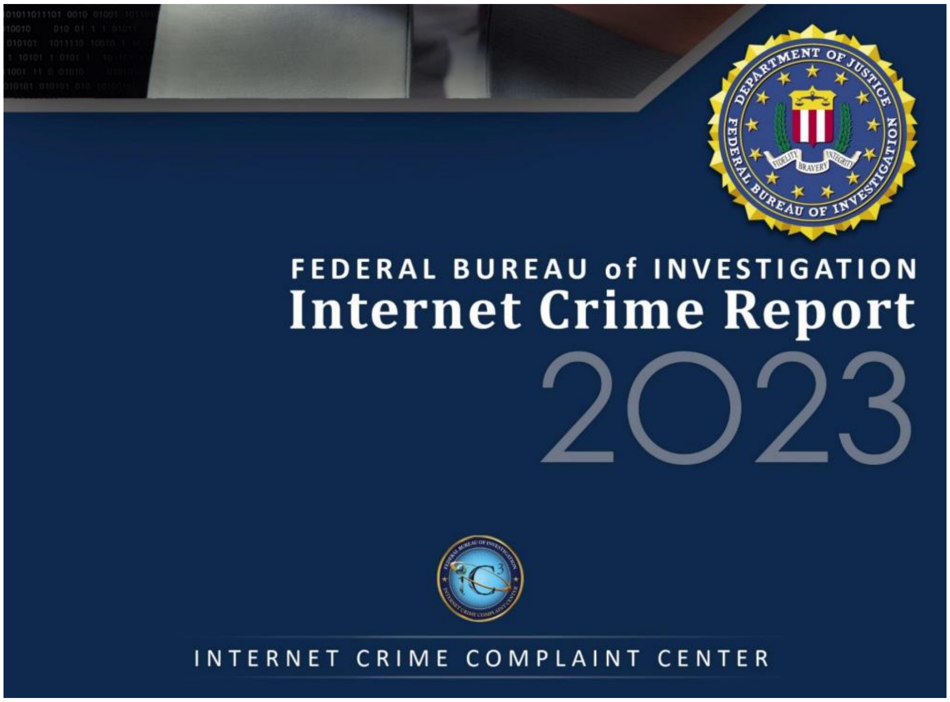
THE IC3 RECOVERY ASSET TEAM (RAT)

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for those who made transfers to domestic accounts under fraudulent pretenses.

RAT Process5
Victim sends complaint to IC3
FBI
Internet Crime Complaint Center
Automated triage through FBI Internet Crime Database
IC3 Analyst *
Assigned to FBI Field Office for action
BANK
Financial Institution

* If criteria are met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

To read more:
https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf



FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2023

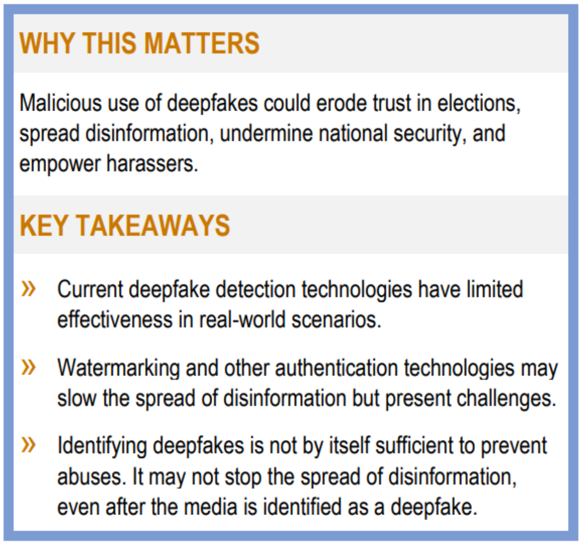
INTERNET CRIME COMPLAINT CENTER

Number 8

The U.S. Government Accountability Office (GAO)

COMBATING DEEPFAKES

GAO Science, Technology Assessment, and Analytics



WHY THIS MATTERS

Malicious use of deepfakes could erode trust in elections, spread disinformation, undermine national security, and empower harassers.

KEY TAKEAWAYS

» Current deepfake detection technologies have limited effectiveness in real-world scenarios.

» Watermarking and other authentication technologies may slow the spread of disinformation but present challenges.

» Identifying deepfakes is not by itself sufficient to prevent abuses. It may not stop the spread of disinformation, even after the media is identified as a deepfake.

Deepfakes are videos, audio, or images that have been manipulated using artificial intelligence (AI), often to create, replace, or alter faces or synthesize speech. They can seem authentic to the human eye and ear.

They have been maliciously used, for example, to try to influence elections and to create non-consensual pornography.

To combat such abuses, technologies can be used to detect deepfakes or enable authentication of genuine media.

Detection technologies aim to identify fake media without needing to compare it to the original, unaltered media.

These technologies typically use a form of AI known as machine learning.

The models are trained on data from known real and fake media.

Methods include looking for:

(1) facial or vocal inconsistencies,

(2) evidence of the deepfake generation process, or

(3) color abnormalities.

Authentication technologies are designed to be embedded during the creation of a piece of media. These technologies aim to either prove authenticity or prove that a specific original piece of media has been altered.

They include:

- Digital watermarks. They can be embedded in a piece of media, which can help detect subsequent deepfakes. One form of watermarking adds pixel or audio patterns that are detectable by a computer but are imperceptible to humans.

  The patterns disappear in any areas that are modified, enabling the owner to prove that the media is an altered version of the original. Another form of watermarking adds features that cause any deepfake made using the media to look or sound unrealistic.

- Metadata—which describe the characteristics of data in a piece of media—can be embedded in a way that is cryptographically secure. Missing or incomplete metadata may indicate that a piece of media has been altered.

- Blockchain. Uploading media and metadata to a public blockchain creates a relatively secure version that cannot be altered without the change being obvious to other users. Anyone could then compare a file and its metadata to the blockchain version to prove or disprove authenticity.

To read more: https://www.gao.gov/assets/d24107292.pdf

Number 9

SXSW Panel Replay: Real or Not, Defending Authenticity in a Digital World

Experts from DARPA, Google, Graphika, and LinkedIn speak with CNN at SXSW 2024 about how to address the growing threat posed by deepfakes

Have you ever wondered if that video you're watching, the photo you're looking at, or even that person on the other line is the real deal?

Deepfakes aren't just Hollywood magic anymore—they're part of our everyday lives, found in everything from the news we consume to the memes we share.

During this panel, experts dive into the world of deepfakes to break down the impacts of digital deception and what we can do about it.

Industry, government, and academic leaders discussed how new analytical tools — including those developed by DARPA's Semantic Forensics program — can help organizations and individuals protect themselves against manipulated media.

Speakers included:

- Donie O'Sullivan (moderator), Politics and Technology Correspondent, CNN
- Wil Corvey, Semantic Forensics Program Manager, DARPA
- Matt Turek, Deputy Director, Information Innovation Office, DARPA
- Nick Dufour, Misinformation Mitigation Researcher, Google
- Amruta Deshpande, Senior Research Scientist, Graphika
- James Verbus, Senior Staff Machine Learning Engineer, LinkedIn

DARPA recently announced its analytic catalog of open-source resources developed under SemaFor for use by researchers and industry. As capabilities mature and become available, they will be added to this repository.

The agency also launched the AI Forensics Open Research Challenge Evaluation (AI FORCE). This open community research effort invites participants to contribute their expertise in developing innovative and robust machine learning, or deep learning, models that can accurately detect synthetic AI-generated images.

Through a series of mini challenges, AI FORCE asks participants to build models that can discern between authentic images, including ones that may have been manipulated or edited using non-AI methods, and fully synthetic AI-generated images.

To read more: https://www.darpa.mil/news-events/2024-03-26

https://www.youtube.com/watch?v=8zniAjqWI2A

Number 10

Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops

A workshop methodology for developing increased capability against information influence operations

The purpose of the report is to present a method for exploring an actor's possibilities for countermeasures and capabilities against information influence operations (IIO).

Using specific scenario conditions, the method assists in creating a discussion on what capabilities are needed and how organisations can develop these capabilities based on available resources.

The method involves conducting workshops using a red team versus blue team exercise which has been adapted to generate a gap analysis for countermeasures in countering IIO.

The report provides guidance on preparing for a workshop aimed at identifying vulnerabilities in an organisation's information environment and developing effective strategies to mitigate the consequences of IIO.

The workshops create a common problem understanding from a scenario and challenges chosen beforehand.

The end result is an analysis that includes existing capabilities in the organisation, a reflection on how to develop capability activities and functions further, and prioritising between these.

The report concludes that the workshop method is a useful tool for risk assessment and preparedness planning, and can be used for decision-making and operational development.

While countering IIO is often a national-level responsibility, we argue that all parts of society can be affected by IIO and should develop capabilities to counter disinformation. Therefore, the selected workshop method can be adapted to work on a local, regional, or national level.

Anticipating disinformation requires proactive capabilities and activities such as risk and threat assessments, forecasting, contingency planning, and policy development to increase preparedness.

Recognising disinformation requires both proactive and reactive functions, including monitoring capabilities and documentation to create indications for recognition.

Reactive functions include impact assessment and investigation into negative impacts on public discourse.

To recognise disinformation campaigns, organisations can monitor social media and set up systems for reporting suspicious activity.

Adapting includes both proactive and reactive functions. Proactively, organisations can prevent and mitigate disinformation by increasing media literacy, creating public awareness, and developing partnerships.

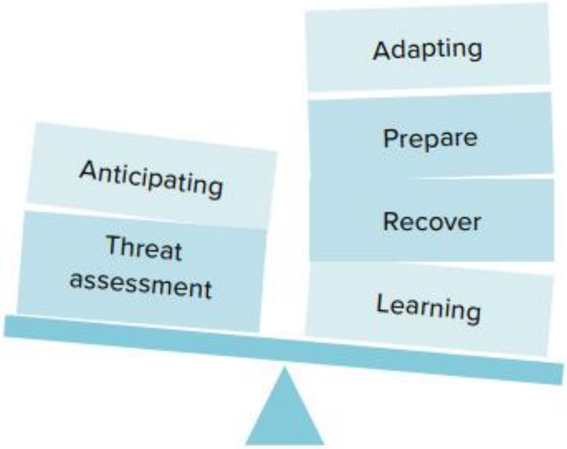
They can also prepare for potential threats by establishing partnerships and publishing relevant analysis.

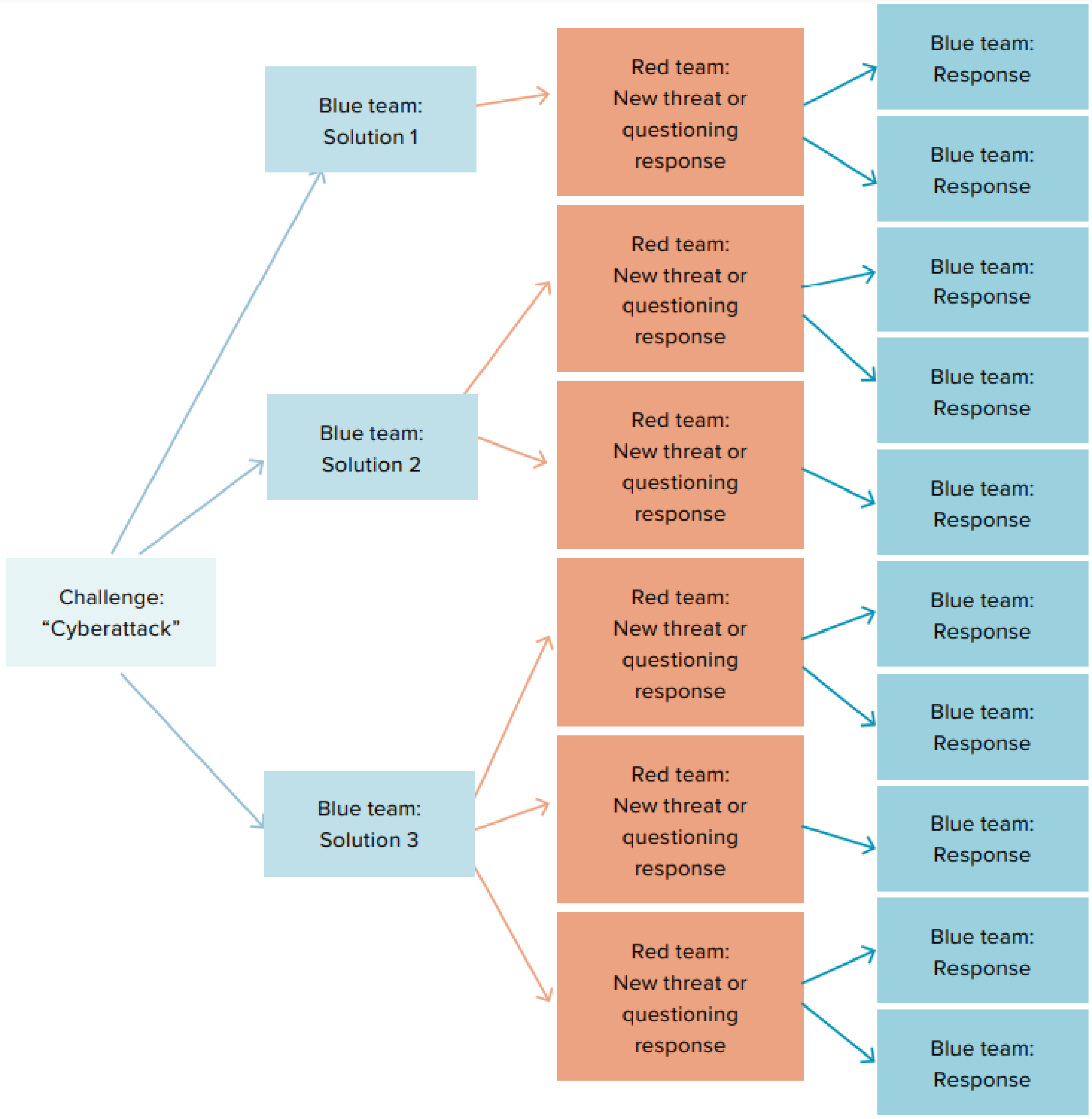
Reactively, organisations can respond to disinformation by using counter-branding, fact checking, debunking, and counter-messaging.

Recovery may involve publishing analysis, conducting post-incident reviews, and developing strategies to rebuild trust and repair damage to reputation or public trust.

Learning is mainly a reactive function done over time in response to events or specific activities.

To improve continuously, organisations can conduct regular research and analysis, implement training programmes, create evaluation structures, and share best practices with others, feeding back into the cycle, leading back to "Anticipation".





1

1. Introduce the challenge: The facilitator presents a scenario that the blue team needs to respond to.

2

2. Blue team response: The blue team discusses and proposes several solutions to the scenario, based on the team members’ existing capabilities within the organisation. The focus should be on anticipation, recognition, adapting, and learning capabilities.

3

3. Red team response: The red team challenges the blue team’s proposed solutions, providing feedback on why they may not work in the current organisational structure, or creates new threats that the blue team has not considered.

4

4. Blue team revision: The blue team responds to the red team’s feedback and questions by revising its proposed solutions or creating new solutions to address the new threats.

Figure 3. This flowchart demonstrates the team discussions and how they typically progress. Additionally, it serves as a method for organising discussions on a whiteboard to facilitate documentation and analysis.

Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops

A workshop methodology for developing increased capability against information influence operations

PREPARED AND PUBLISHED BY THE
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

To read more: https://stratcomcoe.org/publications/enhancing-organisational-capability-a-tailored-approach-with-red-team-vs-blue-team-adapted-workshops/299

Number 11

Browse safely with real-time protection on Chrome

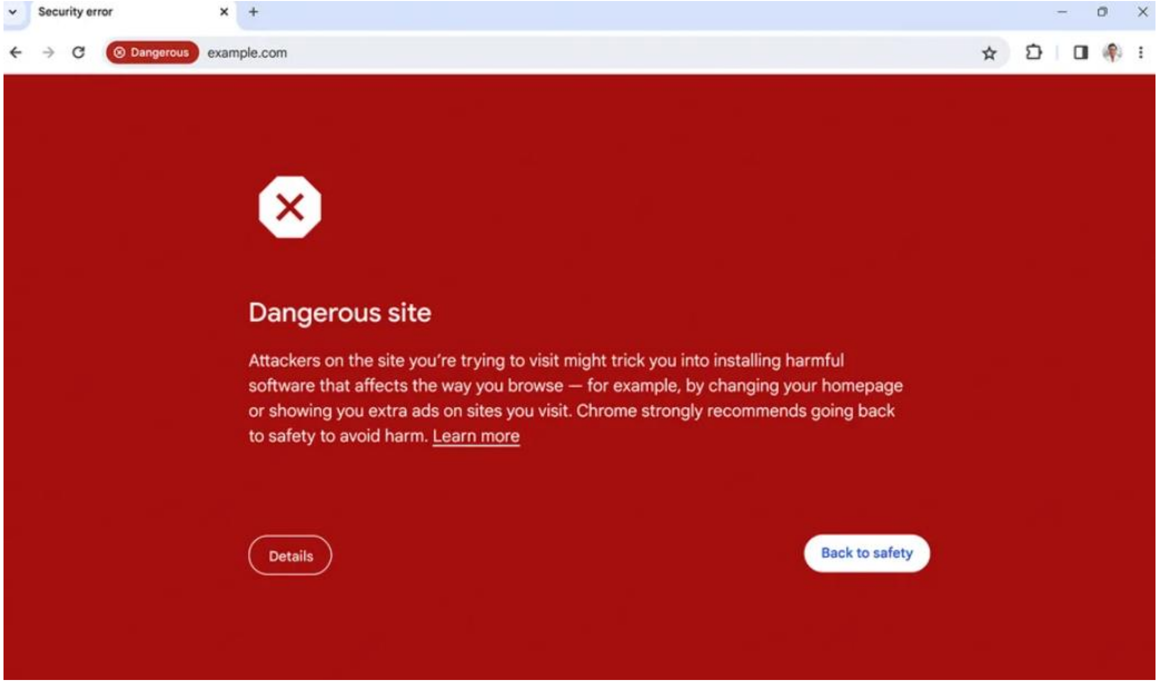
Google

Cybersecurity attacks are constantly evolving, and sometimes the difference between successfully detecting a threat or not is a matter of minutes. To keep up with the increasing pace of hackers, we're bringing real-time, privacy-preserving URL protection to Google Safe Browsing for anyone using Chrome on desktop or iOS. Plus we're introducing new password protections on Chrome for iOS as another way to help you safely navigate the web.

Real-time protection through Safe Browsing

Safe Browsing already protects more than 5 billion devices worldwide, defending against phishing, malware, unwanted software and more. In fact, Safe Browsing assesses more than 10 billion URLs and files every day, showing more than 3 million user warnings for potential threats.

Previously, the Standard protection mode of Safe Browsing used a list stored on your device to check if a site or file was known to be potentially dangerous. That list is updated every 30 to 60 minutes — but we've found that the average malicious site actually exists for less than 10 minutes.



Dangerous site

Attackers on the site you're trying to visit might trick you into installing harmful software that affects the way you browse — for example, by changing your homepage or showing you extra ads on sites you visit. Chrome strongly recommends going back to safety to avoid harm. Learn more

So now, the Standard protection mode for Chrome on desktop and iOS will check sites against Google's server-side list of known bad sites in real time. If we suspect a site poses a risk to you or your device, you'll see a warning with more information. By checking sites in real time, we expect to block 25% more phishing attempts.

The new capability — also rolling out to Android later this month — uses encryption and other privacy-enhancing techniques to ensure that no one, including Google, knows what website you're visiting. While this does require some additional horsepower from the browser, we've worked to make sure your experience remains smooth and speedy.

If you want even more protection, you can always turn on Safe Browsing's Enhanced Protection mode, which uses AI to block attacks, provides deep file scans and offers extra protection from malicious Chrome extensions.

To read more: https://blog.google/products/chrome/google-chrome-safe-browsing-real-time/

Number 12

World War II Slogan is Crucial to Preventing Unauthorized Disclosure in 2024 - DITMAC Team Working to Reduce Unauthorized Disclosures, Training DOD Workforce

Story by John Joyce, Defense Counterintelligence and Security Agency

dvids
DEFENSE VISUAL INFORMATION DISTRIBUTION SERVICE

It was World War II and the "loose lips sink ships" slogan sprang up throughout the United States from billboards and posters to Hollywood productions advising Americans in the military, government, industry and the public to prevent inadvertent disclosure of important information to the enemy.

"It's just as true and crucial today as it was throughout World War II," said Andy Rovnak, DOD Unauthorized Disclosure Program Management Office (UDPMO) chief.

Rovnak was reflecting on how the U.S. Office of War Information's campaign to protect critical information focused on specific rules of conduct established to protect strategic military plans, national security, the American people, and warfighters deployed on two fronts and around the globe.

"Deterring, detecting and mitigating unauthorized disclosure is everyone's responsibility – it's our military, government and civic duty," said Rovnak in a February 2024 interview with DCSA Gatekeeper magazine.

"We've got to be very careful in what we say and do. We're not just talking on the phone – we're on cyber while people are trying to compromise the integrity of our networks and our cyber capability. It's where we are right now in the state of the world, and we must avoid any release of classified or secure information which could damage our national security."

Rovnak leads the UDPMO team – one of several DCSA counter insider threat teams comprising the DOD Insider Threat Management and Analysis Center (DITMAC) – in their efforts to help prevent unauthorized disclosure or leaks of non-public information, crucial to maintaining the nation's security, personnel safety and public trust.

"The 'loose lips sink ships' campaign also applies to the unauthorized disclosure of sensitive unclassified information," he said. "Although unclassified, this sensitive material could enable our adversaries and any potential adversaries to identify and exploit vulnerabilities. It would allow them to steal and use our intellectual property and technology against us, leading to an increased risk of mission failure and potential loss of life."

An unauthorized disclosure occurs when trusted individuals inside an organization communicates or physically transfers classified national security information or controlled unclassified information — including Operations Security critical information and indicators — to an unauthorized recipient.

“There are multiple threats out there and we’re losing intellectual property to unauthorized recipients,” said Rovnak, pointing out that recipients span external threats such as nation state actors to criminal entities who target the federal government, defense industrial base and American citizens.

“If information in the care of government on behalf of its citizens to protect the nation is exposed – someone will take advantage of it. The same is true with personal information. The technological revolution and transformation into a digital society since the World War II era resulted in a fragility in how we operate from an information standpoint that didn't exist back then. Someone without nation-state capabilities can interfere and cause a significant amount of damage. They're able to get the information quicker now and turn it around faster against us. If someone knows about a vulnerability, that person can use ChatGPT and write code that may go out to exploit that vulnerability.”

This knowledge released through an unauthorized disclosure of classified information or controlled unclassified information (CUI) can happen in various ways.

It could be disclosed intentionally, negligently or inadvertently through leaks, data spills, espionage and improper safeguarding of national security information.

When classified information is involved, unauthorized disclosure can be categorized as a type of threat or security incident, characterized as an infraction or violation depending on the seriousness of the incident.

“My UDPMO team coordinates the reporting of unauthorized disclosures within the Department of Defense to ensure prompt and complete delivery of case referrals to the Department of Justice and DOD senior officials for administrative action, civil remedies or criminal prosecution,” Rovnak explained.

“We are also charged with promoting collaboration and information sharing of unauthorized disclosure information across DOD and the intelligence community.”

Since April 2023 when he arrived at DCSA, Rovnak carried out his UDPMO vision to provide continuous workforce engagement activities that reinforce the importance of protecting DOD information from unauthorized access or disclosure while providing it to those who need it, plus gaining efficiencies to deter, detect and mitigate instances of unauthorized disclosure.

“This requires a deliberate enterprise-wide effort to ensure everyone understands the importance of appropriate information sharing and safeguarding across the department and the role they have in providing protection of classified national security Information and CUI from those who don’t have an appropriate need to know,” said Rovnak.

"Our goal for this year is to provide a measurable reduction of DOD unauthorized disclosures through focused security awareness training activities that change human behavior toward the direction of prevention. We are planning to increase collaboration and engagement with the workforce as key elements to improve the identification, investigation, tracking and reporting of unauthorized disclosures in 2024."

The Unauthorized Disclosure of Classified Information and CUI course – available on the Center for Development of Security Excellence (CDSE) Security Awareness Hub – provides an overview of unauthorized disclosure, including specific types of unauthorized disclosure and some common misconceptions about unauthorized disclosure.

The course also discusses the types of damage caused by unauthorized disclosure and the various sanctions one could face if caught engaging in unauthorized disclosure. CDSE also provides resources to bring security expertise straight to any organization, including those for unauthorized disclosure.

In support of the January 2024 OPSEC Awareness Month, the Unauthorized Disclosure Program Management Office held three 'Unauthorized Disclosure 101' briefs to the DOD workforce, attended by over 350 individuals.

The UDPMO team is immediately notified of all incidents involving the release of classified national security information and CUI in the public domain.

Notifications to UDPMO include the release or enabled theft of information relating to any defense operation, system or technology determined to be classified national security information or CUI.

The team is also alerted to incidents of classified information or CUI disclosed to an unauthorized person or persons resulting in an individual's administrative action, referral for criminal or counterintelligence investigation, or the suspension or revocation of a security clearance.

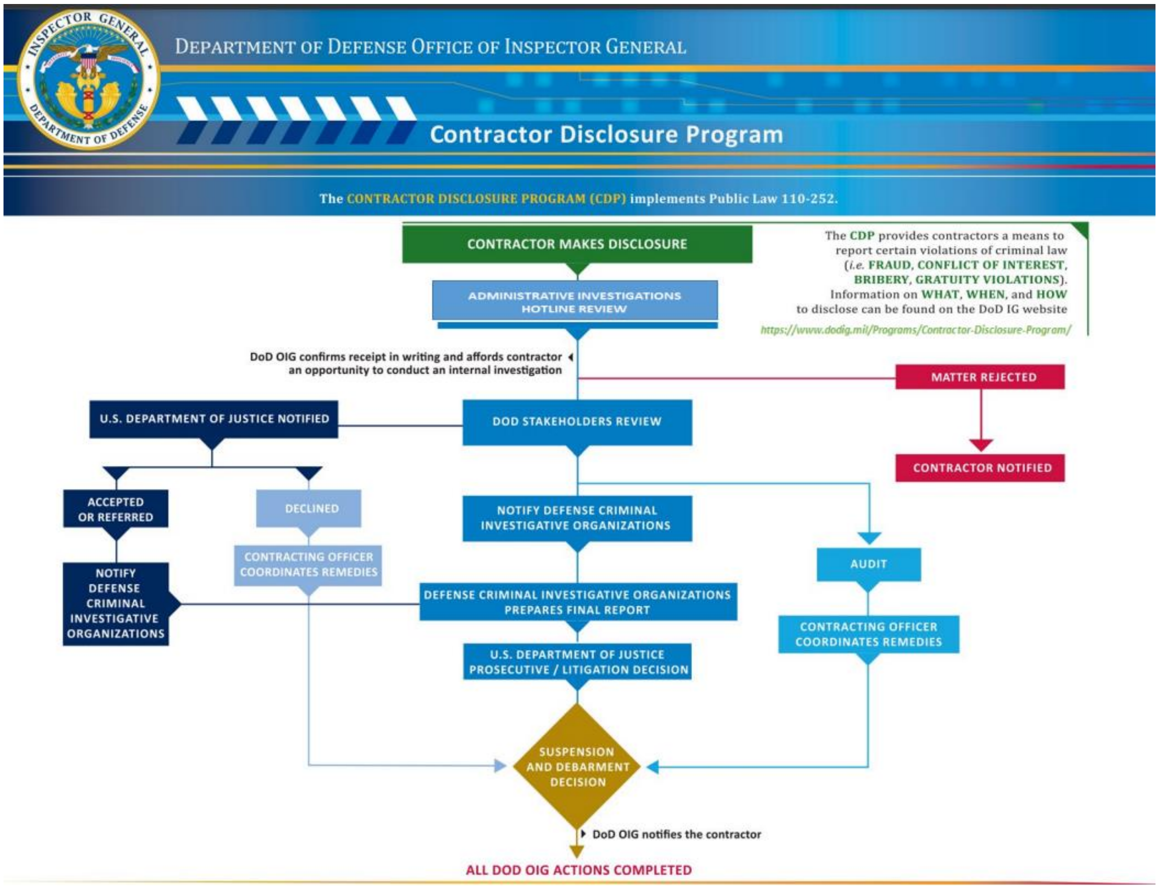
"Everyone has a civic duty to say something if they see an unauthorized disclosure," said Rovnak. "If they report it to us, we can work to mitigate it, but I need to be informed. It's crucial to report a potential unauthorized disclosure to the appropriate authorities."

When UDPMO receives a confirmed report of unauthorized disclosure in the public domain, the team submits a crime report to the Department of Justice. Included in the report are findings from a preliminary inquiry conducted by the affected component; a damage and impact assessment; and a media leaks questionnaire for the unauthorized disclosures appearing in the media.

In terms of reporting unauthorized disclosures, the DOD Whistleblower Protection allows individuals to report information they reasonably believe provides evidence of a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, abuse of authority, or a substantial danger to public health and safety to designated officials via specific channels.

Additional information regarding DoD Whistleblower Protection is available on the DoD Inspector General website at www.dodig.mil

Those making contractor disclosures in response to Federal Acquisition Regulation clause 52.203-13 – Contractor Business Ethics Compliance Program and Disclosure Requirements – can find relevant instructions at www.dodig.mil/Programs/Contractor-Disclosure-Program.


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
CONTRACTOR MAKES DISCLOSURE
ADMINISTRATIVE INVESTIGATIONS HOTLINE REVIEW
MATTER REJECTED
CONTRACTOR NOTIFIED
U.S. DEPARTMENT OF JUSTICE NOTIFIED
DOD STAKEHOLDERS REVIEW
ACCEPTED OR REFERRED
DECLINED
NOTIFY DEFENSE CRIMINAL INVESTIGATIVE ORGANIZATIONS
CONTRACTING OFFICER COORDINATES REMEDIES
NOTIFY DEFENSE CRIMINAL INVESTIGATIVE ORGANIZATIONS
AUDIT
DEFENSE CRIMINAL INVESTIGATIVE ORGANIZATIONS PREPARES FINAL REPORT
CONTRACTING OFFICER COORDINATES REMEDIES
U.S. DEPARTMENT OF JUSTICE PROSECUTIVE / LITIGATION DECISION
SUSPENSION AND DEBARMENT DECISION
ALL DOD OIG ACTIONS COMPLETED

Department of Defense Office of Inspector General

Contractor Disclosure Program

The CONTRACTOR DISCLOSURE PROGRAM (CDP) implements Public Law 110-252.

The CDP provides contractors a means to report certain violations of criminal law (*i.e.* FRAUD, CONFLICT OF INTEREST, BRIBERY, GRATUITY VIOLATIONS). Information on WHAT, WHEN, and HOW to disclose can be found on the DoD IG website *https://www.dodig.mil/Programs/Contractor-Disclosure-Program/*

DoD OIG confirms receipt in writing and affords contractor an opportunity to conduct an internal investigation

DoD OIG notifies the contractor

The differences between unauthorized disclosure and protected whistleblowing are further clarified at: https://www.cdse.edu/Training/Toolkits/Unauthorized-Disclosure-Toolkit

To read more: https://www.dvidshub.net/news/466044/world-war-ii-slogan-crucial-preventing-unauthorized-disclosure-2024-ditmac-team-working-reduce-unauthorized-disclosures-training

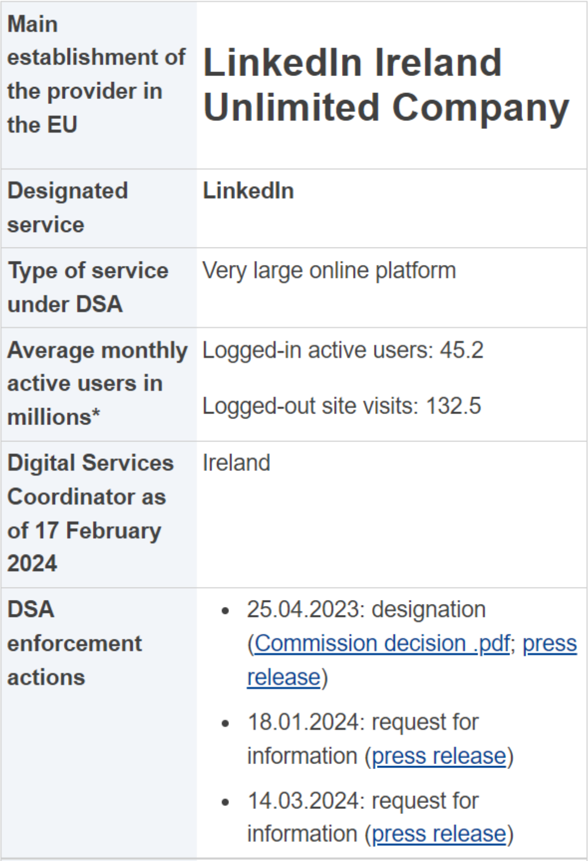
Number 13

Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act

The European Commission has formally sent LinkedIn a request for information under the Digital Services Act (DSA), asking for more details on how their service complies with the prohibition of presenting advertisements based on profiling using special categories of personal data.

LinkedIn must provide the requested information by 5 April 2024. Based on the assessment of LinkedIn's reply, the Commission will assess next steps.

A request for information is an investigatory act that does not prejudge potential further steps the Commission may or may not decide to take. However, pursuant to Article 74 (2) of the DSA, the Commission can impose fines for incorrect, incomplete, or misleading information in response to a request for information.



Main establishment of the provider in the EU	**LinkedIn Ireland Unlimited Company**
Designated service	**LinkedIn**
Type of service under DSA	Very large online platform
Average monthly active users in millions*	Logged-in active users: 45.2 Logged-out site visits: 132.5
Digital Services Coordinator as of 17 February 2024	Ireland
DSA enforcement actions	• 25.04.2023: designation (Commission decision .pdf; press release) • 18.01.2024: request for information (press release) • 14.03.2024: request for information (press release)

Following the designation as a very large online platform in April 2023, LinkedIn is required to comply with the full set of provisions introduced by the DSA, including the obligation to enable users to identify basic information about the nature and origins of an advertisement and the ban on presenting advertisements based on profiling using special categories of personal data, such as sexual orientation, political opinions, or race.

This enforcement action is based on a complaint submitted to the Commission by civil society organisations: https://edri.org/our-work/civil-society-complaint-raises-concern-that-linkedin-is-violating-dsa-ad-targeting-restrictions/

To read more: https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data#:~:text=The%20European%20Commission%20has%20formally,special%20categories%20of%20personal%20data.

Number 14

Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System

GAO

United States Government Accountability Office

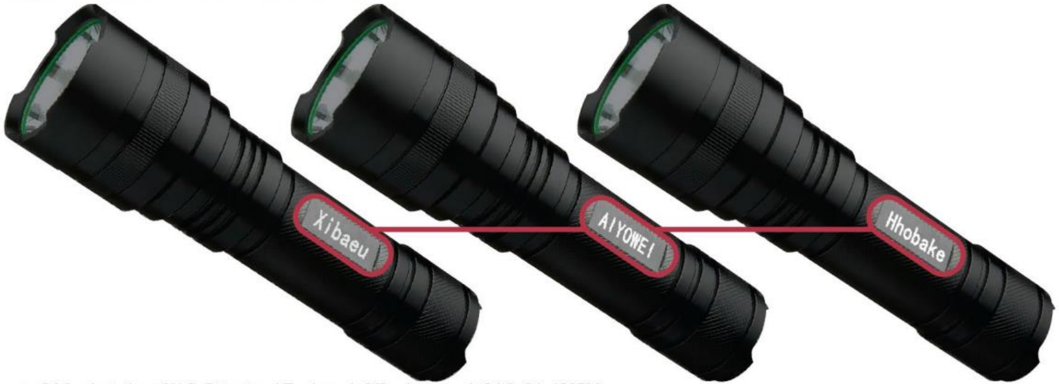
Report to Congressional Committees

What GAO Found

The Trademark Modernization Act of 2020 (TMA) established two new procedures—expungement and reexamination—that allow individuals and businesses to challenge a registered trademark on the basis that it was not used in commerce, as is normally required. A successful challenge results in the trademark being removed from the register, thus making it available for potential use for the challenger or other applicants.

GAO found that from December 2021 through June 2023 the U.S. Patent and Trademark Office (USPTO) and attorneys representing trademark owners filed nearly 500 petitions under the new procedures.

Fraudulent Images of the Same Flashlight with Different Logos Included in Trademark Applications Submitted to USPTO



Source: GAO adaptation of U.S. Patent and Trademark Office images. | GAO-24-106533

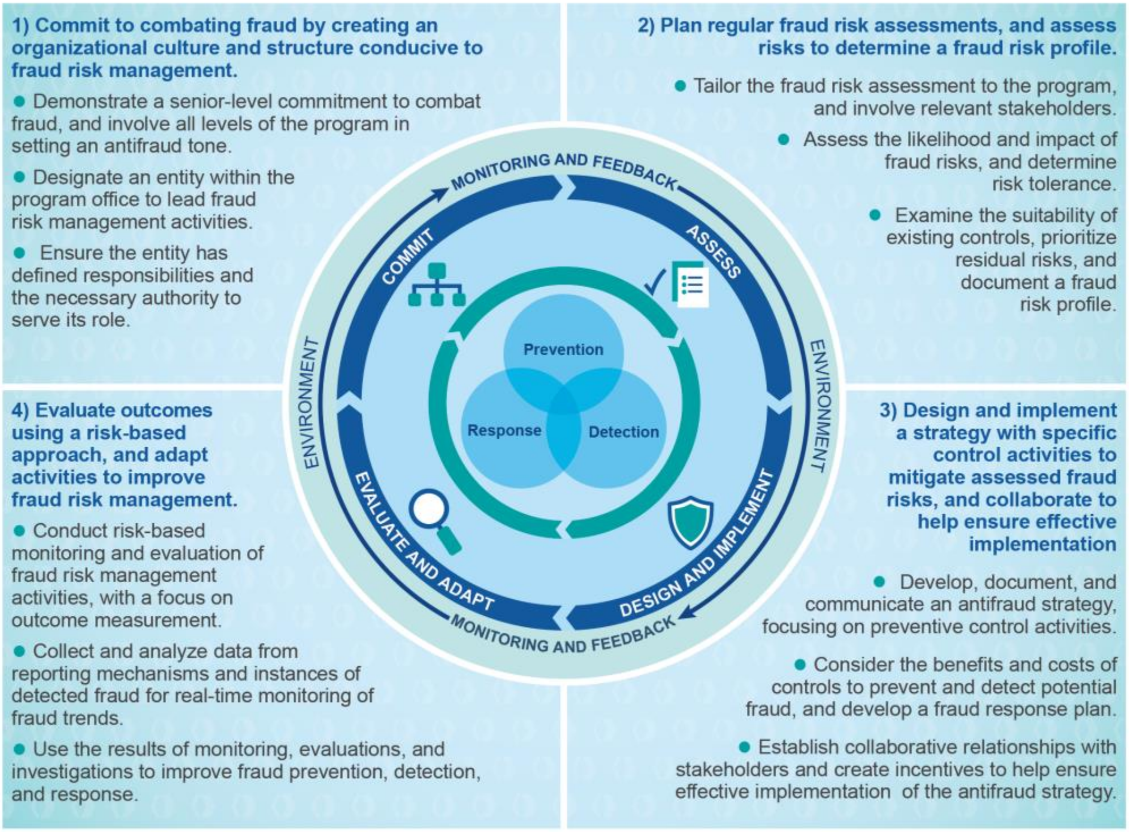
Collectively, these petitions resulted in the removal of more than 2,500 falsely claimed goods and services from the trademark register. Trademark attorneys told GAO that the new procedures can be cost-effective and low-risk.

Existing USPTO programs have also addressed inaccurate or false trademark applications and registrations. The agency's post registration audit program removed trademarked goods and services in about half of its randomly selected audits each year from the start of the program in 2017. This suggests that there may be more than 1 million false and inaccurate registrations out of about 2.8 million overall due to an influx of applications, among other factors.

The USPTO has taken steps to limit fraud risks, such as establishing a culture conducive to fraud risk management. However, the USPTO has not conducted a comprehensive fraud risk assessment of the trademark register or designed a fraud risk strategy. Implementing leading practices from GAO's Fraud Risk

Framework would allow the USPTO to comprehensively consider fraud risks, establish more effective controls, and fully articulate a tolerable level of fraud risk while considering the costs and benefits of potential control activities.

Figure 3: GAO Fraud Risk Management Framework



1) Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

- Demonstrate a senior-level commitment to combat fraud, and involve all levels of the program in setting an antifraud tone.
- Designate an entity within the program office to lead fraud risk management activities.
- Ensure the entity has defined responsibilities and the necessary authority to serve its role.

2) Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile.

- Tailor the fraud risk assessment to the program, and involve relevant stakeholders.
- Assess the likelihood and impact of fraud risks, and determine risk tolerance.
- Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.

3) Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation

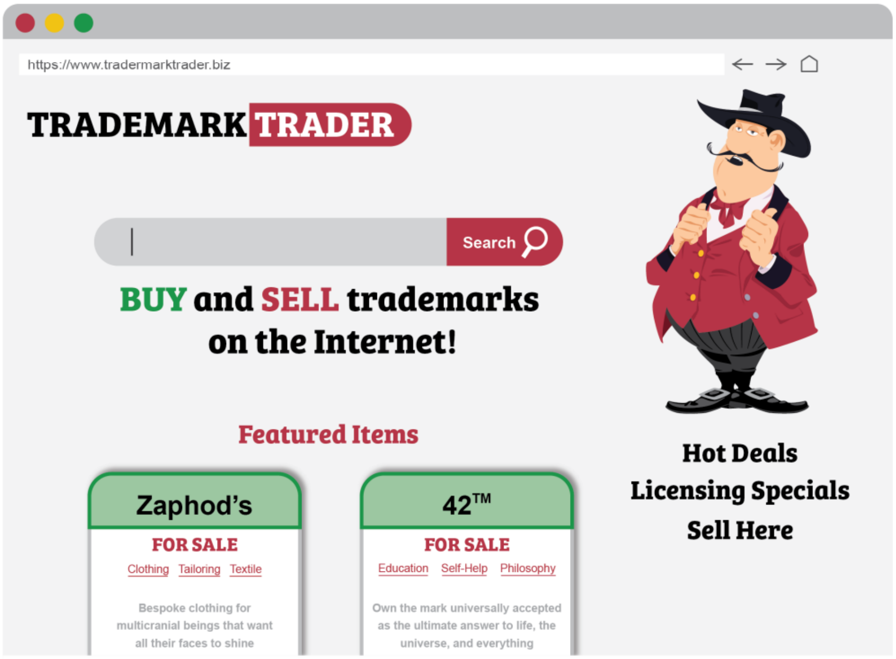
- Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.
- Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
- Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy.

4) Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management.

- Conduct risk-based monitoring and evaluation of fraud risk management activities, with a focus on outcome measurement.
- Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.
- Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.

Source: GAO (information and icons). | GAO-24-106533

Figure 8: Illustrative Example of a Fictitious Trademark Auction Site



https://www.tradermarktrader.biz

TRADEMARK TRADER

BUY and SELL trademarks on the Internet!

Featured Items

Zaphod's

FOR SALE

Clothing Tailoring Textile

Bespoke clothing for multicranial beings that want all their faces to shine

42™

FOR SALE

Education Self-Help Philosophy

Own the mark universally accepted as the ultimate answer to life, the universe, and everything

Hot Deals
Licensing Specials
Sell Here

Source: GAO (data); Alexandr Sidorov/stock.adobe.com (images). | GAO-24-106533

GAO also found that the USPTO's current data systems do not allow the agency to:

(1) assess the effectiveness of current trademark fraud prevention programs and

(2) implement new technologies for identifying fraud.

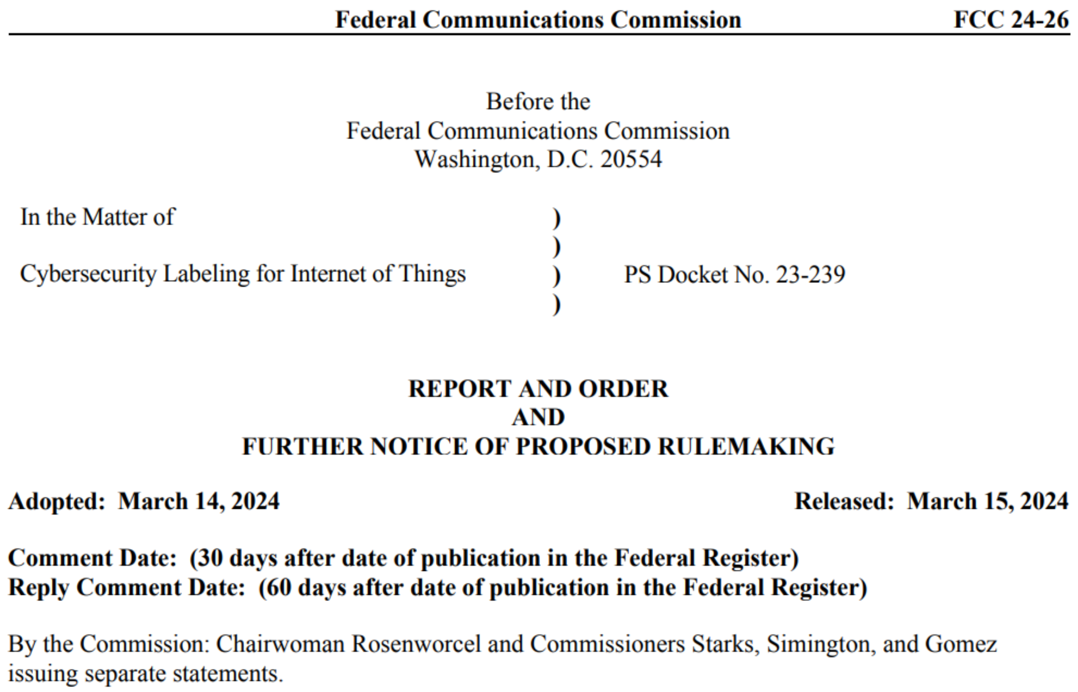
Academics told GAO that computational tools such as predictive analytics could help the USPTO identify trademark applications with false or inaccurate information more effectively.

To read more: https://www.gao.gov/assets/d24106533.pdf

Number 15

FCC Proposes Cybersecurity Labeling Program for Smart Devices

A voluntary cybersecurity labeling program providing consumers with clear information about the security of their internet-enabled devices, commonly called "Internet of Things" (IoT) or "smart" devices.



Federal Communications Commission **FCC 24-26**

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Cybersecurity Labeling for Internet of Things) PS Docket No. 23-239
)

REPORT AND ORDER
AND
FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: March 14, 2024 **Released: March 15, 2024**

Comment Date: (30 days after date of publication in the Federal Register)
Reply Comment Date: (60 days after date of publication in the Federal Register)

By the Commission: Chairwoman Rosenworcel and Commissioners Starks, Simington, and Gomez issuing separate statements.

Consumers rely heavily on Internet-connected products to help them manage many aspects of day-to-day life, including home safety, health, recreation, and personal convenience.

With this convenience, however, comes risk. Internet of Things (IoT) products are susceptible to a wide range of relatively common security vulnerabilities that are increasingly exploited by cybercriminals who are invading people's privacy and threatening national security.

With this Report and Order (Order), the Commission takes prompt and decisive measures to strengthen the nation's cybersecurity posture by adopting a voluntary cybersecurity labeling program for wireless Internet of Things products.

The Commission's IoT Labeling Program will provide consumers with an easy-to-understand and quickly recognizable FCC IoT Label that includes the U.S. government certification mark (referred to as the Cyber Trust Mark) that provides assurances regarding the baseline cybersecurity of an IoT product, together with a QR code that directs consumers to a registry with specific information about the product.

Consumers who purchase an IoT product that bears the FCC IoT Label can be assured that their product meets the minimum cybersecurity standards of the IoT Labeling Program, which in turn will strengthen the chain of connected IoT products in their own homes and as part of a larger national IoT ecosystem.

Today's Order will help consumers make better purchasing decisions, raise consumer confidence with regard to the cybersecurity of the IoT products they buy to use in their homes and their lives, and encourage manufacturers of IoT products to develop products with security-by-design principles in mind.

In the following Order, we set forth the framework by which the IoT Labeling Program will operate. We focus the IoT Labeling Program initially on IoT "products," which we define to include one or more IoT devices and additional product components necessary to use the IoT device beyond basic operational features.

Recognizing that a successful voluntary IoT Labeling Program will require close partnership and collaboration between industry, the federal government, and other stakeholders, we adopt an administrative framework for the IoT Labeling Program that capitalizes on the existing public, private, and academic sector work in this space, while ensuring the integrity of the IoT Labeling Program through oversight by the Commission.

To read more: https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device

https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf

Number 16

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note

Obligations of foreign-based persons to comply with U.S. sanctions and export control laws

Today's increasingly interconnected global marketplace offers unprecedented opportunities for companies around the world to trade with the United States and one another, contributing to economic growth.

At the same time, malign regimes and other bad actors may attempt to misuse the commercial and financial channels that facilitate foreign trade to acquire goods, technology, and services that risk undermining U.S. national security and foreign policy and that challenge global peace and prosperity.

In response to such risks, the United States has put in place robust sanctions and export controls to restrict the ability of sanctioned actors to misuse the U.S. financial and commercial system in advance of malign activities.

These measures can create legal exposure not only for U.S. persons, but also for non-U.S. companies who continue to engage with sanctioned jurisdictions or persons in violation of applicable laws.

To mitigate the risks of non-compliance, companies outside of the United States should be aware of how their activities may implicate U.S. sanctions and export control laws.

This Note highlights the applicability of U.S. sanctions and export control laws to persons and entities located abroad, as well as the enforcement mechanisms that are available for the U.S. government to hold non-U.S. persons accountable for violations of such laws, including criminal prosecution.

It further provides an overview of compliance considerations for non-U.S. companies and compliance measures to help mitigate their risk.

COMPLIANCE CONSIDERATIONS FOR FOREIGN-BASED PERSONS

As with any company participating in the global marketplace, foreign-based persons must ensure that they have robust compliance measures in place to avoid violating U.S. sanctions or export control laws.

In particular, companies should take care to do the following:

- Employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program.

- Establish strong internal controls and procedures to govern payments and the movement of goods involving affiliates, subsidiaries, agents, or other counterparties. Such controls can help detect linkages to sanctioned persons or jurisdictions that may otherwise be obscured by complex payment and invoicing arrangements.

- Ensure that know-your-customer information (such as passports, phone numbers, nationalities, countries of residence, incorporation, and operations, and addresses) and geolocation data are appropriately integrated into compliance screening protocols and information is updated on an ongoing basis based on its overall risk assessment and specific customer risk rating.

- Ensure that subsidiaries and affiliates are trained on U.S. sanctions and export controls requirements, can effectively identify red flags, and are empowered to escalate and report prohibited conduct to management.

- Take immediate and effective action when compliance issues are identified, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

- Identify and implement measures to mitigate sanctions and export control risks prior to merging with or acquiring other enterprises, especially where a company is expanding rapidly and/or disparate information technology systems and databases are being integrated across multiple entities.

- Parties who believe that they may have violated sanctions or export control laws should voluntarily self-disclose the conduct to the relevant agency. Please review the Compliance Note: Voluntary Self-Disclosure of Potential Violations.

To read more: https://ofac.treasury.gov/media/932746/download?inline

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note:

Obligations of foreign-based persons to comply with U.S. sanctions and export control laws

Number 17

The IC OSINT Strategy 2024-2026

OSINT Definition: OSINT is intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps

Mission: IC professionals collect, create, and deliver timely, relevant, and insightful open source intelligence to inform national security decisions and protect our Nation and its interests.

Vision: A professionalized, integrated, and agile IC OSINT enterprise providing decision advantage for U.S. policymakers and warfighters and driving innovation with partners.

Strategic Focus Areas

This IC OSINT Strategy comprises four strategic focus areas that, taken together, will strengthen OSINT as a core intelligence discipline and position the IC to capitalize on the full potential of open-source data and information to enhance the intelligence mission in a manner consistent with our nation's principles and values.

- Coordinate Open-Source Data Acquisition and Expand Sharing
- Establish Integrated Open-Source Collection Management
- Drive OSINT Innovation To Deliver New Capabilities
- Develop the Next-Generation OSINT Workforce and Tradecraft

In addition to the four focus areas, this strategy recognizes that effective and supportive governance and robust partnerships with industry, academia, and foreign counterparts will be essential for success in the OSINT mission and key enablers of the IC OSINT Strategy.

The OSINT Functional Manager, in partnership with the IC OSINT Executive and the Defense Intelligence Enterprise Manager for OSINT, will lead implementation of this strategy, including identifying concrete actions the IC will take to achieve the strategy's objectives and measure outcomes.

Given the fast pace of change in the open source environment, the OSINT

Community will review the strategy on an annual basis and develop an iterative action plan each year to guide implementation efforts.

Introduction

OSINT is vital to the Intelligence Community's Mission. OSINT both enables other intelligence collection disciplines and delivers unique intelligence value of its own, allowing the IC to more efficiently and effectively leverage its exquisite collection capabilities.

As the open source environment continues to expand and evolve at breakneck speed, the ability to extract actionable insights from vast amounts of open source data will only increase in importance.

Rapid advances in artificial intelligence and machine learning present significant opportunities to capitalize on the value of OSINT.

At the same time, the IC must be attuned to the risks in the open source domain, including the provenance and validity of information it obtains.

To maintain an intelligence advantage in the open source environment, we must embrace new technologies and tradecraft to collect and evaluate open source data.

At the same time, the IC must reimagine its relationships with industry and academia to leverage cutting-edge capabilities being developed and applied in the private sector.

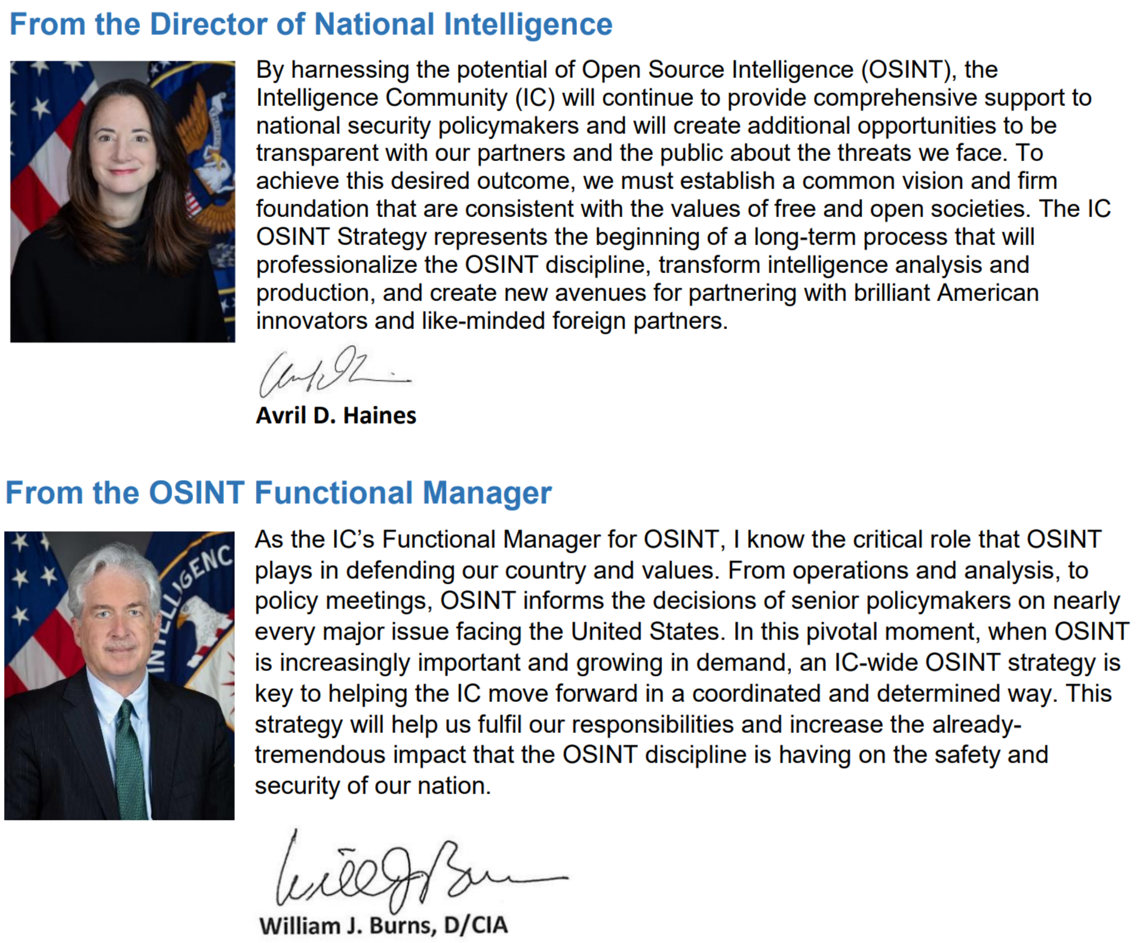
Because of the unclassified nature of open source information, OSINT presents a unique opportunity among collection disciplines to explore new partnership models to speed the adoption of new tools and tradecraft.

For the IC to surpass nation-state competitors that are making significant investments in the open source domain, we must build an integrated and agile OSINT community that can rapidly innovate as the open source environment evolves.

The IC OSINT Strategy provides the framework for integrating OSINT more fully into IC workflows, tradecraft, and all-source analysis, while ensuring appropriate protections for privacy and civil liberties.

To advance the OSINT discipline, the IC will streamline data acquisition, develop innovative technologies to collect and derive insight from open source data, strengthen the coordination of open source collection activities across the community, update and standardize OSINT tradecraft, and develop a highly skilled OSINT workforce.

Through these efforts, we will work together to leverage the full power of OSINT to support IC analysts and operators and ensure the IC is poised to provide decision advantage for warfighters and national security policymakers.



From the Director of National Intelligence

By harnessing the potential of Open Source Intelligence (OSINT), the Intelligence Community (IC) will continue to provide comprehensive support to national security policymakers and will create additional opportunities to be transparent with our partners and the public about the threats we face. To achieve this desired outcome, we must establish a common vision and firm foundation that are consistent with the values of free and open societies. The IC OSINT Strategy represents the beginning of a long-term process that will professionalize the OSINT discipline, transform intelligence analysis and production, and create new avenues for partnering with brilliant American innovators and like-minded foreign partners.

Avril D. Haines

From the OSINT Functional Manager

As the IC's Functional Manager for OSINT, I know the critical role that OSINT plays in defending our country and values. From operations and analysis, to policy meetings, OSINT informs the decisions of senior policymakers on nearly every major issue facing the United States. In this pivotal moment, when OSINT is increasingly important and growing in demand, an IC-wide OSINT strategy is key to helping the IC move forward in a coordinated and determined way. This strategy will help us fulfil our responsibilities and increase the already-tremendous impact that the OSINT discipline is having on the safety and security of our nation.

William J. Burns, D/CIA

To read more:
https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

Number 18

Skills shortage and unpatched systems soar to high-ranking 2030 cyber threats

The European Union Agency for Cybersecurity (ENISA) publishes the executive summary of this year's 'Foresight Cybersecurity Threats for 2030' presenting an overview of key findings in the top 10 ranking.

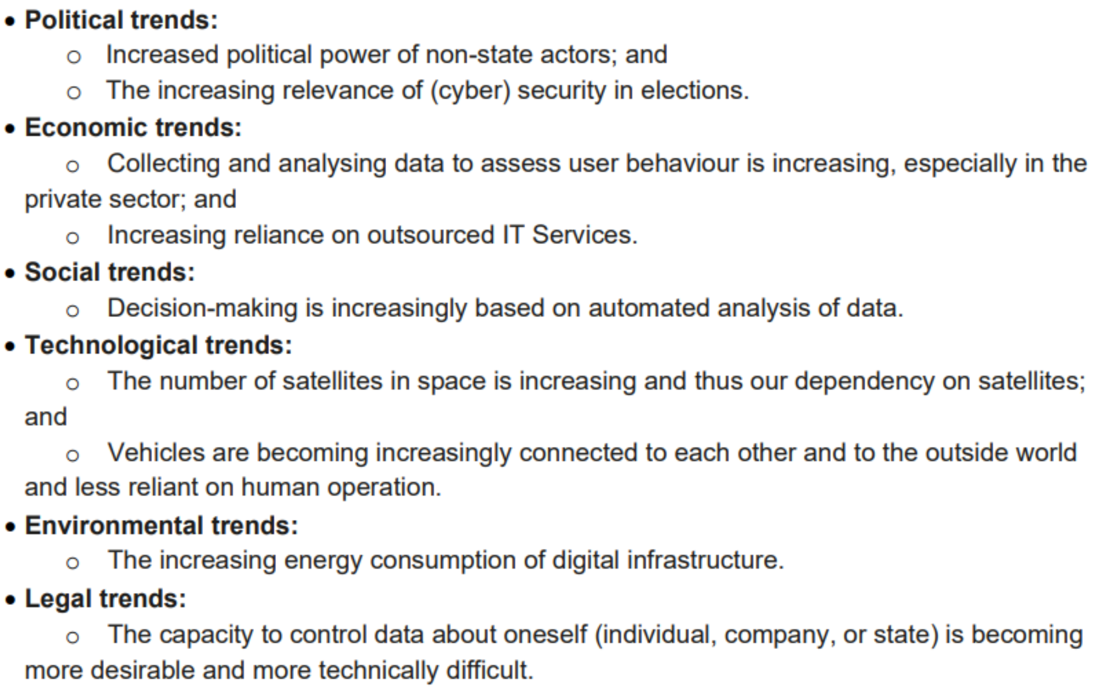
The following top ten list includes a revised line-up of the emerging cybersecurity threats to have an impact by 2030:

1. Supply Chain Compromise of Software Dependencies
2. Skill Shortage
3. Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems
4. Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [New in Top Ten]
5. Rise of Digital Surveillance Authoritarianism / Loss of Privacy
6. Cross-border ICT Service Providers as a Single Point of Failure
7. Advanced Disinformation / Influence Operations (IO) Campaigns
8. Rise of Advanced Hybrid Threats
9. Abuse of AI
10. Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [New in Top Ten]

Despite a slight decline compared to past years' results in the overall score of impact and likelihood, 'Supply Chain Compromise of Software Dependencies' still remains the highest-ranking threat. This is considered as an after-effect of the expanding integration of third-party suppliers and partners in the supply chain, leading to new vulnerabilities and opportunities for attacks.

'Cross-border ICT Service Providers as a Single Point of Failure' threats have significantly moved up due to growing concerns that can emanate from the growing ICT interconnectedness in critical infrastructure between Member States.

It is also notable that ‘Skill Shortage’ threats have significantly moved up the ladder to the top threats, moving from the end of the list to the second place.



- **Political trends:**
    - Increased political power of non-state actors; and
    - The increasing relevance of (cyber) security in elections.
- **Economic trends:**
    - Collecting and analysing data to assess user behaviour is increasing, especially in the private sector; and
    - Increasing reliance on outsourced IT Services.
- **Social trends:**
    - Decision-making is increasingly based on automated analysis of data.
- **Technological trends:**
    - The number of satellites in space is increasing and thus our dependency on satellites; and
    - Vehicles are becoming increasingly connected to each other and to the outside world and less reliant on human operation.
- **Environmental trends:**
    - The increasing energy consumption of digital infrastructure.
- **Legal trends:**
    - The capacity to control data about oneself (individual, company, or state) is becoming more desirable and more technically difficult.

While efforts have been focused on fulfilling the skills shortage challenge, organisational willingness to develop talent and bridge the educational gap still remain a concern in cybersecurity.

This appears to be closely connected to threats related to unpatched systems, as it interferes with the familiarisation of staff with the multitude of tools at hand to update unpatched services that are vulnerable to exploitation.

Other key takeaways of the threats review are the addition of the ‘Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem’ and the ‘Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure’, as a result of a shift in perceived impact and likelihood score.

Likewise, the rise of the ‘Abuse of AI’ threat can be considered an expected outcome of the widespread emergence of AI models in our lives and the relevant concerns regarding the growing reliance on AI.

This led to the exclusion of the ‘Lack of Analysis and Control of Space-based Infrastructure and Objects’, and ‘Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data’ threats from the top ten list.

In line with ENISA’s strategic objective to provide expertise and insights on future cybersecurity challenges, the foresight report can work as a tool that facilitates a comprehensive understanding of the current cybersecurity threat landscape.

The participation of designated experts and stakeholders in the study is an added value that enables better informed actions and improves preparedness. Overall, this study is a step along the way of our efforts to build strong cybersecurity frameworks and best practices that remain up-to-date and adaptable to the ever-changing ecosystem.

To read more: https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

Number 19

Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections

The European Commission has published guidelines on recommended measures to Very Large Online Platforms and Search Engines to mitigate systemic risks online that may impact the integrity of elections, with specific guidance for the upcoming European Parliament elections in June.

Under the Digital Services Act (DSA), designated services with more than 45 million active users in the EU have the obligation to mitigate the risks related to electoral processes, while safeguarding fundamental rights, including the right to freedom of expression.

These guidelines recommend mitigation measures and best practices to be undertaken by Very Large Online Platforms and Search Engines before, during, and after electoral events, such as to:

1. Reinforce their internal processes, including by setting up internal teams with adequate resources, using available analysis and information on local context-specific risks and on the use of their services by users to search and obtain information before, during and after elections, to improve their mitigation measures.

2. Implement election-specific risk mitigation measures tailored to each individual electoral period and local context. Among the mitigation measures included in the guidelines, Very Large Online Platforms and Search Engines should promote official information on electoral processes, implement media literacy initiatives, and adapt their recommender systems to empower users and reduce the monetisation and virality of content that threatens the integrity of electoral processes. Moreover, political advertising should be clearly labelled as such, in anticipation of the new regulation on the transparency and targeting of political advertising.

3. Adopt specific mitigation measures linked to generative AI: Very Large Online Platforms and Search Engines whose services could be used to create and/or disseminate generative AI content should assess and mitigate specific risks linked to AI, for example by clearly labelling content generated by AI (such as deepfakes), adapting their terms and conditions accordingly and enforcing them adequately.

4. Cooperate with EU level and national authorities, independent experts, and civil society organisations to foster an efficient exchange of information before, during and after the election and facilitate the use of adequate mitigation measures, including in the areas of Foreign Information Manipulation and Interference (FIMI), disinformation and cybersecurity. Adopt specific measures, including an incident response mechanism, during an electoral period to reduce

the impact of incidents that could have a significant effect on the election outcome or turnout.

5. Assess the effectiveness of the measures through post-election reviews. Very Large Online Platforms and Search Engines should publish a non-confidential version of such post-election review documents, providing opportunity for public feedback on the risk mitigation measures put in place.

The guidelines include specific measures ahead of the upcoming European elections. Given their unique cross-border and European dimension, Very Large Online Platforms and Search Engines should ensure that sufficient resources and risk mitigation measures are available and distributed in a way that is proportionate to the risk assessments. The guidelines also encourage close cooperation with the European Digital Media Observatory (EDMO) Task Force on the 2024 European elections.

Next Steps

The specific mitigation measures that a Very Large Online Platform or Search Engine should take depend on the specificities of their service and on their risk profile. The guidelines represent best practices for mitigating risks related to electoral processes at this moment in time.

As such, Very Large Online Platforms and Search Engines which do not follow these guidelines must prove to the Commission that the measures undertaken are equally effective in mitigating the risks. Should the Commission receive information casting doubt on the suitability of such measures, it can request further information or start formal proceedings under the Digital Services Act.

To add an additional element of readiness, the Commission plans a stress test with relevant stakeholders at the end of April to exercise the most effective use of the instruments and the cooperative mechanisms that have been put in place.

Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes: https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes

Number 20

Supo identified the cyber espionage operation against the parliament as APT31

SUPO
FINNISH SECURITY AND
INTELLIGENCE SERVICE

Supo identified a cyber espionage operation targeted in 2020 against the Parliament with the aim of intruding into the Parliament's IT systems.

The Parliament improved its information security after receiving instructions from Supo.

2020, the year of the pandemic, was also a year of exceptionally intensive cyber espionage operations both in Finland and elsewhere in Europe. Supo identified a state-run cyber espionage operation targeted last year against the Parliament with the aim of intruding into its IT systems. According to Supo intelligence, APT31 was responsible for the attack.

Supo provided the Parliament with information that enabled the Parliament to identify possible further break-in attempts. The Parliament followed the instructions it had received and further strengthened its information security.

Besides warning the Parliament, Supo also provided information to the National Cyber Security Centre Finland (NCSC-FI), which is the national cyber security authority, to improve NCSC-FI monitoring capabilities.

As the Parliament's own technical investigation revealed that its IT systems had been compromised, Supo assessed that the constituent elements of an aggravated offence were fulfilled and advised the National Bureau of Investigation (NBI) of the case.

The case in question is the same of which the Parliament announced in the end of December 2020. The NBI is responsible for the pre-trial investigation of the case and for providing information on it.

To read more: https://supo.fi/en/-/supo-identified-the-cyber-espionage-operation-against-the-parliament-as-apt31

Investigation into hacking of Parliament's information systems has been ongoing (26.3.2024)

POLIISI
POLICE OF FINLAND

On 18 March 2021, the National Bureau of Investigation published a press release on a criminal investigation into the hacking of Parliament's information systems in 2020–2021. The suspected offences under investigation have been aggravated espionage, aggravated unlawful access to an information system, and aggravated violation of the secrecy of communications.

The police recorded a report of the incident in 2020. It is suspected that the offences were committed between autumn 2020 and early 2021. The police have previously informed that they investigate the hacking group APT31's connections with the incident. These connections have now been confirmed by the investigation, and the police have also identified one suspect.

– The criminal investigation has been demanding and time-consuming because it has involved challenging investigations into a complex criminal infrastructure, says Head of Investigation, Detective Chief Inspector Aku Limnéll of the National Bureau of Investigation.

The criminal investigation has involved demanding investigations and analyses, and international exchange of information. The National Bureau of Investigation has worked in close cooperation with international actors and the Finnish Security and Intelligence Service.

The criminal investigation is ongoing.

To read more: https://poliisi.fi/en/-/investigation-into-hacking-of-parliament-s-information-systems-has-been-ongoing

Number 21

Propelling 3D printing into the future - Printing stronger materials five times faster

3D printing has changed the world.

It's allowed the aerospace, medical, automotive, manufacturing and many other industries to customize parts and prototypes in ways they never could before. It has drastically increased flexibility and cost effectiveness while reducing waste and production time. But many 3D-printed materials aren't the strongest.

A team of chemists and materials scientists at Sandia hopes to change that.

They've developed a new printing process that prints stronger nonmetallic materials in record time, five times faster than traditional 3D printing.

"It opens up a whole new world of what you can build and what 3D materials can be used for," materials scientist Samuel Leguizamon said.

He led the team that developed SWOMP, which stands for Selective Dual-Wavelength Olefin Metathesis 3D-Printing. As indicated by its name, it uses dual-wavelength light, unlike the traditional printing process.

How 3D printing works

Traditionally, vat 3D printing is accomplished by irradiating a vat of photosensitive liquid resin in a desired pattern.

As the resin is exposed to light from beneath the vat, the resin cures and hardens into a polymer layer. The cured polymer is then lifted, and a new pattern is projected beneath to cure subsequent layers.

One challenge: As the polymer cures, it adheres to the previous layer and to the bottom of the vat. After each layer, the cured polymer must be slowly peeled from the vat to prevent damage, significantly slowing down the 3D printing process.

Fellow creator Leah Appelhans said it's kind of like baking cookies. "After you bake the cookies, you have to let them cool. If you were to try to peel the warm cookie off the cookie sheet, it's squishy and it breaks apart. The same thing would happen with a 3D printer if you tried to quickly print each layer. Your work would get deformed."

Samuel, Leah, former Sandian Jeff Foster and polymer scientist Alex Commisso came up with a way to cool the "cookies" quicker.

UV and blue light

The key is combining two lights. In this case, ultraviolet and blue light.

The team took inspiration from a technique known as continuous liquid interface printing along with a printing approach using dual-wavelength light for acrylic-based polymerizations.

With it, they created SWOMP.

“You are still printing layer by layer, but you are using a second wavelength of light to prevent polymerization at the bottom of the vat. So it doesn’t adhere to the bottom,” Samuel said. “That means you can lift the cured polymer part more quickly and speed up the printing process significantly.”

Making 3D materials stronger

But this new process isn’t just about efficiency. It’s about making 3D-printed materials stronger and more versatile. Most vat-polymerization-printed materials are acrylic-based, not the strongest material.

“It’s really hard to use these materials in things like aircraft and space and aerospace and automotive. They are very harsh environments,” Sandia licensing executive Bob Sleeper said.

This team turned to the material dicyclopentadiene, which is commonly used in the production of paints, varnishes and flame retardants for plastics. They were able to develop a way to polymerize it more rapidly with light so that it can be used more efficiently in 3D printing.

“We changed building blocks of the materials from acrylic-based to olefin-based,” Samuel said. “Which lets us print materials that are a lot tougher.”

“That is the beauty of what they are doing,” Bob said. “You have very high-quality plastic parts that are made very precisely by using some light in a very novel way.”

Opening a new world of 3D printing

This team hopes their new printing process will open the world of 3D printing.

While the project was initially funded through a rapid three-month Exploratory Express program, it’s now funded by a Sandia technology maturation program.

“What we are trying to do is build the toolbox of materials available,” Leah said. “We want designers, researchers, engineers to be able to select the type of material they want to use.”

One day, they hope to see these 3D-printed parts in rockets, engines, batteries, maybe even in fusion applications. Samuel said they’re already talking with researchers at Lawrence Livermore National Laboratory to explore applications. “It turns out that monomers are already used in fusion components. You don’t usually think of a polymer used in fusion, but it’s really cool and exciting potential.”

The team also sees a world where 3D printing can be done more easily in remote areas. “We’re looking at locations where machinery and parts are not readily available; like in space, on the moon or in the Middle East at a U.S. military base,” Bob said. “You can bring with you some lightweight materials and make whatever you need on the spot.”

Samuel, who grew up in the small town of Wagener, South Carolina, is also thinking of applications that could help closer to home.

“I have horses. I grew up in a rural area, my dad was a farrier, so I’m thinking of ways to make horseshoes for racehorses. They have to be impact-resistant, but by changing the material properties, stress can be better spread out, and impact in the right space on the hoof. You could think of it as insoles for horses.”

The possibilities are endless.

“I think what attracted me to chemistry in the first place is the potential to make something that has never existed before,” Leah said. “The fun thing about 3D printing is that you apply that chemical knowledge to something that has a very concrete outcome. Something you can see and hold in your hands.”

To read more: https://www.sandia.gov/labnews/2024/03/07/propelling-3d-printing-into-the-future/

Number 22

Johns Hopkins APL and Navy Chart Next Steps to Accelerate 3D-Printing Advancements

Ever made a mistake while sketching or writing in permanent ink and wanted to adjust your work — or scrap the whole thing altogether and start again? If so, you've utilized in situ monitoring.

It's a technique used in a variety of industries to monitor the production of something in real time and ensure defect-free items. It's also become increasingly important in the field of additive manufacturing.

"In traditional manufacturing, such as welding, a real person is operating the equipment, and the welder can adapt as they go," explained Michael Presley, a manufacturing engineer and project manager at the Johns Hopkins Applied Physics Laboratory (APL) in Laurel, Maryland.

"In additive manufacturing, we currently have open-loop systems in which we set parameters and the machine begins manufacturing on its own. The machine can lay miles of welds without ever knowing if something goes wrong. By utilizing in situ monitoring technologies, we can spot those errors earlier if they arise and develop more efficient and accurate processes."

These monitoring technologies cover a range of sensing modalities: systems ranging from cameras to pyrometers and thermocouples (devices that measure temperatures); spectrometers (that measure wavelengths of light to identify chemicals and materials) tuned across the infrared, visible, ultraviolet and X-ray spectrums; displacement sensors; profilometers (that measure the roughness of a surface's finish); ultrasonic transducers (that generate or sense energy, often vibration); and even microphones — just to name a few.

This wide scope arises from the complexity of the additive manufacturing process. Engineers need systems that concurrently measure the temperature and surface behavior of a molten metal drop moving at meters per second across a build plate, the quality of the bulk material it leaves behind, and the system health of all the lasers, pumps, actuators and feedback controls used by the machine.

Anticipating an Urgent Need

Integrating the wide range of technologies at the heart of in situ monitoring is a large systems-engineering challenge — and one of increasing importance to the Navy's manufacturing base. While speaking on a panel in London, U.S. Air Forces in Europe Commander Gen. James Hecker said the U.S. stockpile of weapons and munitions is getting "dangerously low."

And to further support the Department of Defense's deterrence plans, the Navy plans to invest roughly $132 billion to acquire 12 Columbia-class submarines — the largest and most complex submarines in Navy history. But a recent Government Accountability Office report noted there could be trouble delivering those ships on time.

To address these manufacturing challenges, the Navy is prioritizing the development and fielding of additive manufacturing systems, often called 3D printers, to supplement traditional casting methods and accelerate submarine production. To support this effort, APL hosted a working group in July to discuss the current state of in situ monitoring in additive manufacturing, identify opportunities for advancement, and develop a path forward for future Navy implementation of such technology.

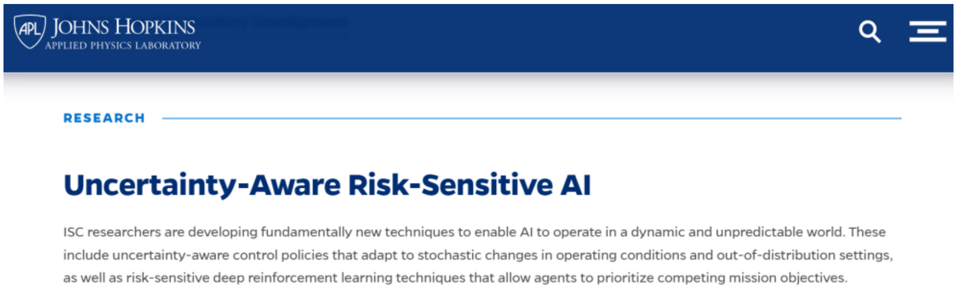
"Collaboration is going to be key in addressing both logistics and sustainment challenges in the current fleet and force and the manufacturing challenges of our future fleet and its weapon systems," said James Borghardt, APL's Maritime Expeditionary Logistics program manager. "We're looking forward to our continued work with the Navy, Department of Defense and partner organizations to keep the field moving forward."

The event was managed by team members from APL's Force Projection Sector, Air and Missile Defense Sector, and Research and Exploratory Development Department with support from the Naval Sea Systems Command (NAVSEA 05T) and the Program Executive Office, Strategic Submarines.

Among the 32 participating organizations were the Applied Research Laboratory at Penn State University, Virginia's Commonwealth Center for Advanced Manufacturing, America Makes, the Army Research Laboratory, Naval Air Systems Command, the Office of Naval Research, Oak Ridge National Laboratory, the Defense Logistics Agency, the Nuclear Regulatory Commission and a range of Naval Surface Warfare Centers.

"We went from having a few dozen people in the Navy studying and monitoring additive manufacturing capabilities to now having hundreds," said Presley. "And we're trying to bring everyone up to speed and move as fast as possible because these are real, near-term needs. In situ monitoring will play a vital role here because it can speed up and improve inspection of additive manufactured parts."

To read more: https://www.jhuapl.edu/news/news-releases/240319b-apl-navy-chart-next-steps-for-3d-printing-advancements



RESEARCH

Uncertainty-Aware Risk-Sensitive AI

ISC researchers are developing fundamentally new techniques to enable AI to operate in a dynamic and unpredictable world. These include uncertainty-aware control policies that adapt to stochastic changes in operating conditions and out-of-distribution settings, as well as risk-sensitive deep reinforcement learning techniques that allow agents to prioritize competing mission objectives.

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY
80
YEARS

Number 23

Cybersecurity and Infrastructure Security Agency (CISA), DHS
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

AGENCY:
Cybersecurity and Infrastructure Security Agency, DHS

ACTION:
Proposed rule.

SUMMARY:
The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities.

CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements.

DATES:
Comments and related material must be submitted on or before June 3, 2024.

Executive Summary

A. Purpose and Summary of the Regulatory Action

On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law.

CIRCIA requires covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report.

CIRCIA further requires the Director of CISA to implement these new reporting requirements through rulemaking, by issuing an NPRM no later than March 15, 2024, and a final rule within 18 months of publication of the NPRM. CISA is issuing this NPRM to solicit public comment on proposed regulations that would codify these reporting requirements.

This NPRM is divided into six sections.

Section I—Public Participation describes the process for members of the public to submit comments on the proposed regulations and lists specific topics on which CISA is particularly interested in receiving public comment.

Section II—Executive Summary contains a summary of the proposed regulatory action and the anticipated costs and benefits of the proposed regulations.

Section III—Background and Purpose contains a summary of the legal authority for this proposed regulatory action; an overview of the current regulatory cyber incident reporting landscape; a description of the purpose of the proposed regulations; a discussion of efforts CISA has taken to harmonize these proposed regulations with other Federal cyber incident reporting regulations; a discussion of information sharing activities related to the proposed regulations; and a summary of the comments CISA received in response to an RFI issued by CISA on approaches to the proposed regulations and during listening sessions hosted by CISA on the same topic.

Section IV—Discussion of Proposed Rule includes a detailed discussion of the proposed rule, the justification for CISA's specific proposals, and the alternatives considered by CISA.

Section V—Statutory and Regulatory Analyses contains the analyses that CISA is required by statute or Executive Order to perform as part of the rulemaking process prior to issuance of the final rule, such as the Initial Regulatory Flexibility Analysis and Unfunded Mandates Reform Act analysis.

Section VI contains the proposed regulatory text.

The proposed rule is comprised of 20 sections, §§ 226.1 through 226.20, beginning with a section containing definitions for a number of key terms used throughout the proposed regulation. Among other definitions, § 226.1 includes proposed definitions for the terms used to describe and ultimately scope what types of incidents must be reported to CISA (cyber incident, covered cyber incident, ransom payment, and substantial cyber incident) and the term used to describe the different types of reports that must be submitted (CIRCIA Reports).

The next section of the proposed rule, § 226.2, describes the applicability of the proposed rule to certain entities in a critical infrastructure sector, those entities that are considered covered entities and to whom the operative provisions of the rule would apply.

The next section of the proposed rule, § 226.3, describes the circumstances under which a covered entity must submit a CIRCIA Report to CISA. This includes when a covered entity experiences a covered cyber incident, makes a ransom payment, has another entity make a ransom payment on its behalf, or acquires substantial new or different information after submitting a previous CIRCIA Report.

CISA is proposing three exceptions to these reporting requirements for covered entities, which are in § 226.4 of the proposed regulation and described in Section IV.D in this document.

These exceptions include when a covered entity reports substantially similar information in a substantially similar timeframe to another Federal agency pursuant to an existing law, regulation, or contract when a CIRCIA Agreement is in place between CISA and the other Federal agency; when an incident impacts certain covered entities related to the Domain Name System (DNS); and when Federal agencies are required by the Federal Information Security Modernization Act of 2014 (FISMA) to report incidents to CISA. See § 226.4 of the proposed regulation and Section IV.D of this document.

Section 226.5 of the proposed regulation contains the submission deadlines for the four different types of CIRCIA Reports (Covered Cyber Incident Reports; Ransom Payment Reports; Joint Covered Cyber Incident and Ransom Payment Reports; Supplemental Reports).

These deadlines, including how to calculate them, are discussed further in Section IV.E.iv in this document. Section 226.6 of the proposed regulation sets forth the proposed manner and form of reporting, which CISA proposes to be through a web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner and form of reporting approved by the Director.

To read more: https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

Number 24

Amazon's request to suspend its obligation to make an advertisement repository publicly available is rejected

COURT OF JUSTICE
OF THE EUROPEAN UNION

Order of the Vice-President of the Court in Case C-639/23 P(R) | Commission v Amazon Services Europe

Amazon Services Europe belongs to the Amazon group. Its business activities comprise online retail and other services such as cloud computing and digital streaming. It provides marketplace services to third-party sellers enabling them to offer products for sale via Amazon Store.

By a decision of 23 April 2023, adopted under the Regulation on a Single Market for Digital Services, the Commission designated Amazon Store as a very large online platform. That means, in particular, that Amazon Store is obliged to make publicly available a repository containing detailed information 3 on its online advertising.

Amazon sought the annulment of that decision before the General Court of the European Union. It had also made an application for interim measures. By order of 27 September 2023, the President of the General Court ordered suspension of the operation of that decision in so far as Amazon Store will be required to make the advertisement repository publicly available. The Commission lodged an appeal before the Court of Justice against that order.

In his order today, *the Vice-President of the Court of Justice sets aside the part of the order of the President of the General Court suspending the Commission's decision in so far as it concerns the advertisement repository.*

He finds that the Commission was denied, in breach of the principle that the parties should be heard, the opportunity to comment on the arguments put forward by Amazon during the proceedings before the General Court. Since the Commission presented to the Court of Justice the arguments that it intended to make against the elements put forward by Amazon before the General Court, *the Vice-President of the Court of Justice gives final judgment in the dispute and dismisses the application for interim measures.*

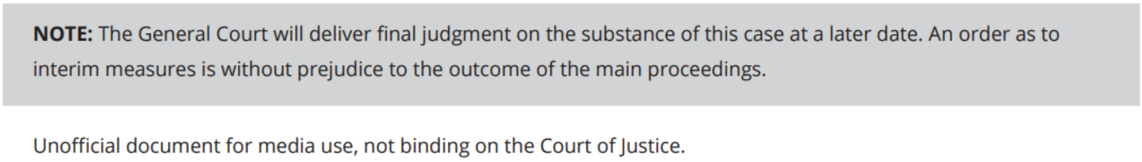
The Vice-President of the Court considers that Amazon's argument that the obligation introduced by the EU legislature to make an advertisement repository publicly available unlawfully limits its fundamental rights to respect for private life and the freedom to conduct a business, cannot be regarded, prima facie, as irrelevant and, moreover, as lacking in seriousness.

Furthermore, in the absence of a suspension, it is likely that Amazon would suffer serious and irreparable harm before the intervention of any judgment annulling the Commission's decision.

Those findings are not however decisive in themselves. It is necessary to assess whether the balancing of all the interests involved may justify refusing suspension. In that regard, the Vice-President of the Court finds that, in the event that suspension is not granted, the annulment of the Commission's decision would retain an interest for Amazon.

In addition, it has not been demonstrated that, in such a situation, Amazon's existence or long-term development would be jeopardised. Moreover, suspension would lead to a delay, potentially for several years, in the full achievement of the objectives of the Regulation on a Single Market for Digital Services and therefore potentially allow an online environment threatening fundamental rights to persist or develop, whereas the EU legislature considered that very large platforms play an important role in that environment.

The interests defended by the EU legislature prevail, in the present case, over Amazon's material interests, with the result that the balancing of interests weighs in favour of rejecting the request for suspension.



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.

Unofficial document for media use, not binding on the Court of Justice.

To read more: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-03/cp240060en.pdf

Full text: https://curia.europa.eu/juris/documents.jsf?num=C-639/23%20P(R)

Number 25

Gas Pipeline Safety: Better Data and Planning Would Improve Implementation of Regulatory Changes

About 300,000 miles of natural gas transmission pipelines across the United States carry products from processing facilities to communities and other large volume customers.

Pipelines are a relatively safe mode for transporting natural gas, but incidents can still occur that result in death, injury, and property and environmental damage. The Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) sets the federal minimum safety standards for these pipelines.

In 2003, PHMSA established integrity management—a risk-based approach to managing certain gas transmission pipelines—as an addition to its existing pipeline safety regulations.

Under this approach, operators are required to assess pipelines in high consequence areas (HCA)—generally, areas where an incident could have the greatest impact to public safety or property—to identify threats and mitigate risks.

In October 2019 and August 2022, PHMSA issued final rules that both strengthened its gas transmission pipeline safety regulations and expanded some integrity assessment requirements beyond HCAs, including to newly defined moderate consequence areas (MCA).

The Protecting our Infrastructure of Pipelines and Enhancing Safety Act of 2016 includes a provision for us to examine gas transmission integrity management programs following PHMSA's completion of a specific pipeline safety rulemaking.

We are providing information on potential changes to the methods operators use to identify HCAs; how selected stakeholders, including pipeline operators and state inspectors, view the regulatory changes to gas transmission pipeline safety; and how PHMSA is overseeing the implementation of the 2019 and 2022 final rules stemming from the rulemaking.

What are gas transmission pipelines?

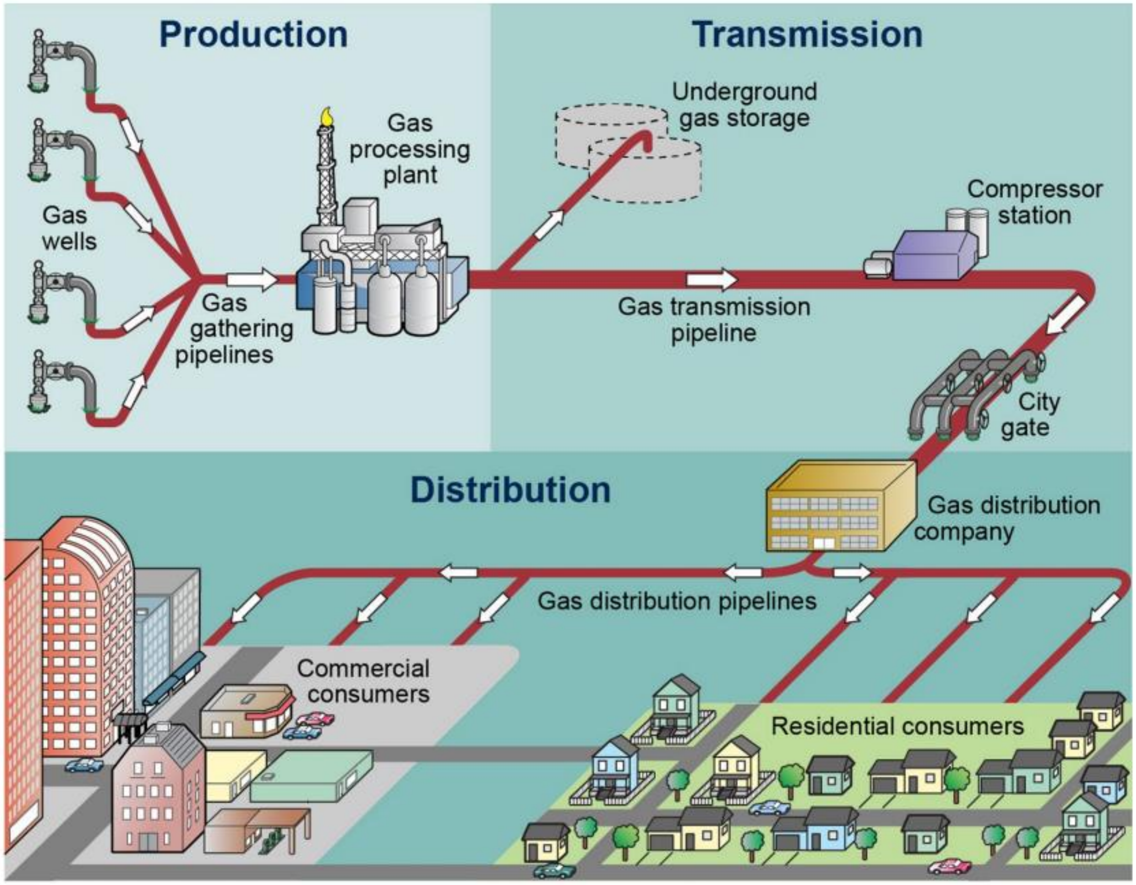
Natural gas transmission pipelines carry gas, sometimes over hundreds of miles, to communities and large-volume users (e.g., factories).

In 2023, PHMSA
officials estimated that the United States has over 300,000 miles of onshore gas transmission pipelines. Roughly two-thirds of these miles were interstate

pipelines, or pipelines that generally cross state boundaries.
The remaining third were intrastate pipelines, or pipelines that tend to operate within a single state.

Transmission pipelines tend to have larger diameters and operate at higher pressures than other types of pipelines (see fig.1).

Figure 1: Transmission Pipelines within a Natural Gas Pipeline System



Source: GAO analysis of Energy Information Administration and Natural Gas Council documents; GAO (illustration). | GAO-24-106690

To read more: https://www.gao.gov/products/gao-24-106690

Number 26

Fighting cookie theft using device bound sessions

Chromium Blog

Note: The Chromium projects include Chromium and ChromiumOS, the open-source projects behind the Google Chrome browser and Google ChromeOS.

Cookies – small files created by sites you visit – are fundamental to the modern web. They make your online experience easier by saving browsing information, so that sites can do things like keep you signed in and remember your site preferences. Due to their powerful utility, cookies are also a lucrative target for attackers.

Many users across the web are victimized by cookie theft malware that gives attackers access to their web accounts.

Operators of Malware-as-a-Service (MaaS) frequently use social engineering to spread cookie theft malware. These operators even convince users to bypass multiple warnings in order to land the malware on their device.

The malware then typically exfiltrates all authentication cookies from browsers on the device to remote servers, enabling the attackers to curate and sell the compromised accounts.

Cookie theft like this happens after login, so it bypasses two-factor authentication and any other login-time reputation checks. It's also difficult to mitigate via anti-virus software since the stolen cookies continue to work even after the malware is detected and removed.

And because of the way cookies and operating systems interact, primarily on desktop operating systems, Chrome and other browsers cannot protect them against malware that has the same level of access as the browser itself.

To address this problem, we're prototyping a new web capability called Device Bound Session Credentials (DBSC) that will help keep users more secure against cookie theft.

The project is being developed in the open at github.com/WICG/dbsc with the goal of becoming an open web standard.

By binding authentication sessions to the device, DBSC aims to disrupt the cookie theft industry since exfiltrating these cookies will no longer have any value.

We think this will substantially reduce the success rate of cookie theft malware.

Attackers would be forced to act locally on the device, which makes on-device detection and cleanup more effective, both for anti-virus software as well as for enterprise managed devices.

Learning from prior work, our goal is to build a technical solution that's practical to deploy to all sites large and small, to foster industry support to ensure broad adoption, and to maintain user privacy.

Technical solution

At a high level, the DBSC API lets a server start a new session with a specific browser on a device.

When the browser starts a new session, it creates a new public/private key pair locally on the device, and uses the operating system to safely store the private key in a way that makes it hard to export.

Chrome will use facilities such as Trusted Platform Modules (TPMs) for key protection, which are becoming more commonplace and are required for Windows 11, and we are looking at supporting software-isolated solutions as well.

The API allows a server to associate a session with this public key, as a replacement or an augmentation to existing cookies, and verify proof-of-possession of the private key throughout the session lifetime.

To make this feasible from a latency standpoint and to aid migrations of existing cookie-based solutions, DBSC uses these keys to maintain the freshness of short-lived cookies through a dedicated DBSC-defined endpoint on the website.

This happens out-of-band from regular web traffic, reducing the changes needed to legacy websites and apps.

This ensures the session is still on the same device, enforcing it at regular intervals set by the server. For current implementation details please see the public explainer.

Preserving user privacy

Each session is backed by a unique key and DBSC does not enable sites to correlate keys from different sessions on the same device, to ensure there's no persistent user tracking added.

The user can delete the created keys at any time by deleting site data in Chrome settings. The out-of-band refresh of short-term cookies is only performed if a user is actively using the session (e.g. browsing the website).

DBSC doesn't leak any meaningful information about the device beyond the fact that the browser thinks it can offer some type of secure storage.

The only information sent to the server is the per-session public key which the server uses to certify proof of key possession later.

We expect Chrome will initially support DBSC for roughly half of desktop users, based on the current hardware capabilities of users' machines.

We are committed to developing this standard in a way that ensures it will not be abused to segment users based on client hardware.

For example, we may consider supporting software keys for all users regardless of hardware capabilities. This would ensure that DBSC will not let servers differentiate between users based on hardware features or device state (i.e. if a device is Play Protect certified or not).

DBSC will be fully aligned with the phase-out of third-party cookies in Chrome. In third-party contexts, DBSC will have the same availability and/or segmentation that third-party cookies will, as set by user preferences and other factors.

This is to make sure that DBSC does not become a new tracking vector once third-party cookies are phased out, while also ensuring that such cookies can be fully protected in the meantime.

If the user completely opts out of cookies, third-party cookies, or cookies for a specific site, this will disable DBSC in those scenarios as well.

Improving user protection

We are currently experimenting with a DBSC prototype to protect some Google Account users running Chrome Beta. This is an early initiative to gauge the reliability, feasibility, and the latency of the protocol on a complex site, while also providing meaningful protection to our users.

When it’s deployed fully, consumers and enterprise users will get upgraded security for their Google accounts under the hood automatically. We are also working to enable this technology for our Google Workspace and Google Cloud customers to provide another layer of account security.

This prototype is integrated with the way Chrome and Google Accounts work together, but is validating and informing all aspects of the public API we want to build.

Interest outside Google

Many server providers, identity providers (IdPs) such as Okta, and browsers such as Microsoft Edge have expressed interest in DBSC as they want to secure their users against cookie theft.

We are engaging with all interested parties to make sure we can present a standard that works for different kinds of websites in a privacy preserving way.

Where to follow the progress

Development happens on GitHub and we have published an estimated timeline. This is where we will post announcements and updates to the expected timelines as needed.

Our goal is to allow origin trials for all interested websites by the end of 2024. Please reach out if you'd like to get involved.

We welcome feedback from all sources, either by opening a new issue or starting a discussion on GitHub.

To read more: https://blog.chromium.org/2024/04/fighting-cookie-theft-using-device.html

Number 27

Protect Yourself: Commercial Surveillance Tools

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes.

Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections.

In some cases, malign actors can infect a targeted device with no action from the device owner.

In others, they can use an infected link to gain access to a device.

These surveillance tools can:

- Record audio, including phone calls.

- Track phone's location.

- Access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history.

Below are common cybersecurity practices that may mitigate some risks:

- Regularly update device operating systems and mobile applications.

- Be suspicious of content from unfamiliar senders, especially those which contain links or attachments.

- Don't click on suspicious links or suspicious emails and attachments.

- Check URLs before clicking links, or go to websites directly.

- Regularly restart mobile devices, which may help damage or remove malware implants.

- Encrypt and password protect your device.

- Maintain physical control of your device when possible.

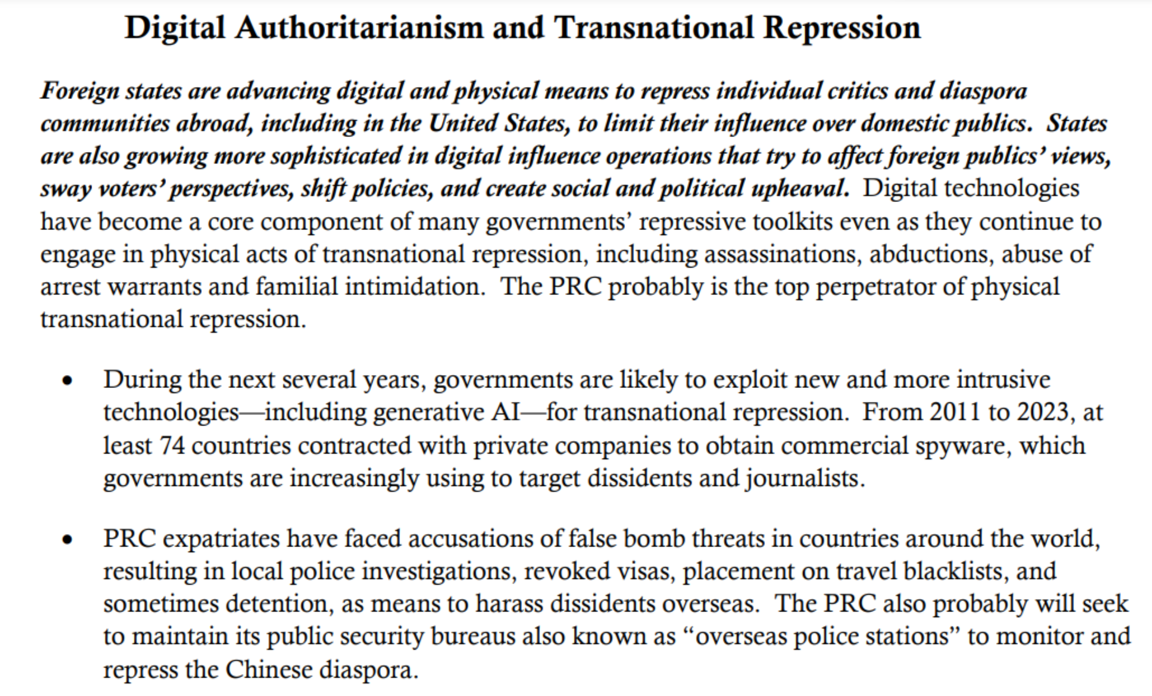
- Use trusted Virtual Private Networks.

• Disable geo-location options and cover camera on devices.

• While these steps mitigate risks, they don't eliminate them. It's always safest to behave as if the device is compromised, so be mindful of sensitive content.

From 2011 to 2023, at least 74 countries contracted with private companies to obtain commercial spyware, which governments are increasingly using to target dissidents and journalists," per the 2024 IC Annual Threat Assessment.

ANNUAL THREAT ASSESSMENT
OF THE U.S. INTELLIGENCE COMMUNITY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA



Digital Authoritarianism and Transnational Repression

Foreign states are advancing digital and physical means to repress individual critics and diaspora communities abroad, including in the United States, to limit their influence over domestic publics. States are also growing more sophisticated in digital influence operations that try to affect foreign publics' views, sway voters' perspectives, shift policies, and create social and political upheaval. Digital technologies have become a core component of many governments' repressive toolkits even as they continue to engage in physical acts of transnational repression, including assassinations, abductions, abuse of arrest warrants and familial intimidation. The PRC probably is the top perpetrator of physical transnational repression.

- During the next several years, governments are likely to exploit new and more intrusive technologies—including generative AI—for transnational repression. From 2011 to 2023, at least 74 countries contracted with private companies to obtain commercial spyware, which governments are increasingly using to target dissidents and journalists.

- PRC expatriates have faced accusations of false bomb threats in countries around the world, resulting in local police investigations, revoked visas, placement on travel blacklists, and sometimes detention, as means to harass dissidents overseas. The PRC also probably will seek to maintain its public security bureaus also known as "overseas police stations" to monitor and repress the Chinese diaspora.

To read more:
https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_Jan-7-2022_Protect_Yourself_Commercial_Surveillance_Tools.pdf

Number 28

EIOPA stress tests European insurers' resilience with a scenario of escalating geopolitical tensions

The European Insurance and Occupational Pensions Authority (EIOPA) is launching its 2024 stress test in which it subjects insurers in the European Economic Area to a hypothetical scenario of severe but plausible adverse developments in financial and economic conditions.

This year's exercise envisions a re-intensification or prolongation of geopolitical tensions and assesses how European insurers would cope with the wide-ranging economic and financial market consequences of such an event.

Objective

While EIOPA's 2024 stress test is not a pass or fail exercise, it has a mostly microprudential orientation.

The goal is primarily to assess the resilience of the participants to the adverse scenario whose shocks go beyond the regular resilience required under Solvency II and provide supervisors with information on whether these insurers are able to withstand severe shocks. EIOPA will also analyze aggregate results to assess potential sector-wide vulnerabilities.

This microprudential approach will enable European and national supervisors to issue recommendations to the industry as a whole, and, where relevant, to discuss potential follow-up actions with individual insurers, to improve their resilience.

The microprudential assessment is complemented by the estimation of potential spillover from the insurance sector to other parts of the financial system, triggered by reactions to the prescribed shocks.

Scenario

The 2024 scenario, developed by EIOPA in close cooperation with the European Systemic Risk Board, presumes a renewed build-up or continuation of geopolitical tensions together with a broad range of knock-on effects.

As a result of high tensions, the narrative envisages a resurgence of widespread supply-chain disruptions, leading to sluggish growth and reigniting inflationary pressures.

The ripple effects include a re-evaluation of interest rate expectations marked by a surge in short-term market rates and more muted increases in longer term yields, further steepening an already inverted yield curve.

The resulting tightening of financing conditions, coupled with subdued growth, is poised to dampen corporate profitability, widen credit spreads, and adversely affect asset classes across the board.

The high level of government bond yields, also driven by sustained high risk-free rates, would tighten financing conditions for public spending.

The pandemic-induced elevated level of government debt and the need for mitigating measures to support the real economy in a downturn would fuel concerns about sovereign debt sustainability, leading to a further heterogenous increase in government bond rates.

Approach and scope

EIOPA has translated the above narrative into a set of market and insurance-specific shocks to assess the insurance industry's resilience to them from a capital as well as from a liquidity perspective.

The sample for the stress test will include 48 undertakings from 20 member states and cover over 75% of the EEA market in terms of total assets.

Timeline

Following the launch, participating undertakings will have until mid-August 2024 to calculate their results based on the prescribed scenario and submit them to the relevant national supervisor.

Once the results are submitted, EIOPA will undertake a quality assurance process to validate the results, which is expected to last until end of October 2024.

Communication of the results

The outcome of the 2024 Stress Test will be published in December in two forms:

- Report based on aggregated data;

- Publication of individual results relating to a subset of capital-based indicators (subject to the consent of the relevant entity).

For more information, go to the dedicated page of the exercise:
https://www.eiopa.europa.eu/insurance-stress-test-2024_en

To read more: https://www.eiopa.europa.eu/eiopa-stress-tests-european-insurers-resilience-scenario-escalating-geopolitical-tensions-2024-04-02_en

Number 29

CNIL and the application of the EU GDPR to Artificial Intelligence

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Note: CNIL is the French National Commission on Information Technology and Liberties. It was created in January 1978.

The objective of this guide is to support organisations in the implementation of security measures in order to ensure the protection of personal data. It is aimed in particular at data protection officers (DPO), chief information security officer (CISO) and computer scientists. Privacy lawyers will also be able to find useful elements.

This guide is a living tool that is enriched by state-of-the-art practices and doctrine elements of the French data protection authority (CNIL) on the issue of data security. A changelog is available on the CNIL website to help actors identify the evolutions that need to be taken into account in order to adapt their level of security.

PRACTICE
GUIDE
GDPR

SECURITY OF
PERSONAL DATA
Version 2024

Security is an essential part of the protection of personal data. It is binding on any data controller and data processor through Article 32 of the General Data Protection Regulation (GDPR).

In principle, each processing operation must be subjected to a set of security measures decided according to the context, namely “useful precautions, having regard to the nature of the data and the risks presented by the processing” (Article 121 of the French Data Protection Act).

The GDPR specifies that the protection of personal data requires taking “appropriate technical and organisational measures to ensure a level of security appropriate to the risk” for the rights and freedoms of natural persons, including their privacy.

To assess the measures to be put in place, two complementary approaches are to be deployed:

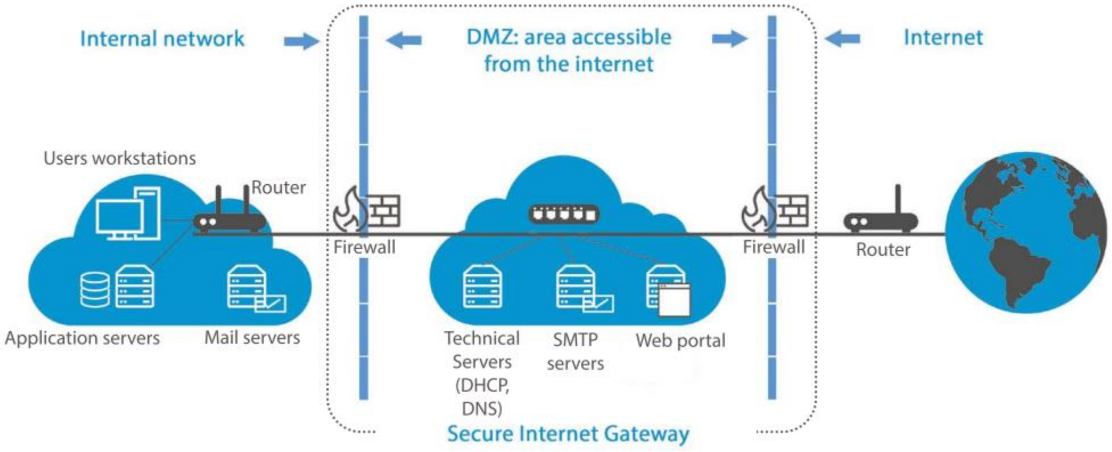
– the establishment of a security base incorporating good practices resulting from years of capitalising on hygiene and IT security (e.g.: regulations, standards, guides). This base aims to address the most common risks;

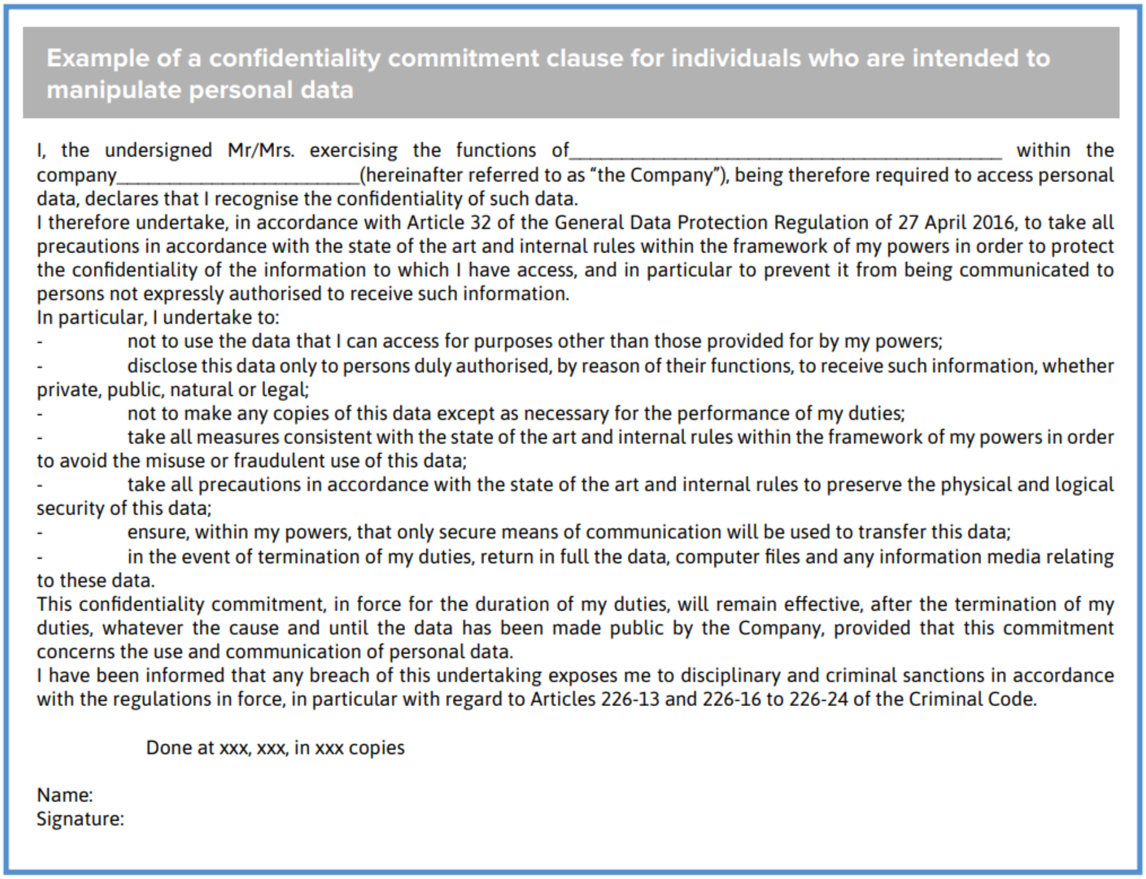
– the risk analysis for the persons concerned by the processing, which aims to identify and assess the risks specific to the treatment. Such an analysis supports objective decision-making on the treatment of these risks and the identification of necessary and context-appropriate measures. However, it is difficult for non-specialists in IT security to implement such an approach and to ensure that the level of security of the processing for which they are responsible is sufficient.

To help with compliance, this guide presents a set of recommendations grouped by thematic factsheets. Each factsheet is structured in three sections:

– basic precautions, which incorporate essential good practices;
– bad trend practices, which should be avoided;
– additional measures, to go further.

Each factsheet can be read separately from the others: references are given when another factsheet.





Example of a confidentiality commitment clause for individuals who are intended to manipulate personal data

I, the undersigned Mr/Mrs. exercising the functions of____ within the company____________________________(hereinafter referred to as "the Company"), being therefore required to access personal data, declares that I recognise the confidentiality of such data.

I therefore undertake, in accordance with Article 32 of the General Data Protection Regulation of 27 April 2016, to take all precautions in accordance with the state of the art and internal rules within the framework of my powers in order to protect the confidentiality of the information to which I have access, and in particular to prevent it from being communicated to persons not expressly authorised to receive such information.

In particular, I undertake to:

- not to use the data that I can access for purposes other than those provided for by my powers;
- disclose this data only to persons duly authorised, by reason of their functions, to receive such information, whether private, public, natural or legal;
- not to make any copies of this data except as necessary for the performance of my duties;
- take all measures consistent with the state of the art and internal rules within the framework of my powers in order to avoid the misuse or fraudulent use of this data;
- take all precautions in accordance with the state of the art and internal rules to preserve the physical and logical security of this data;
- ensure, within my powers, that only secure means of communication will be used to transfer this data;
- in the event of termination of my duties, return in full the data, computer files and any information media relating to these data.

This confidentiality commitment, in force for the duration of my duties, will remain effective, after the termination of my duties, whatever the cause and until the data has been made public by the Company, provided that this commitment concerns the use and communication of personal data.

I have been informed that any breach of this undertaking exposes me to disciplinary and criminal sanctions in accordance with the regulations in force, in particular with regard to Articles 226-13 and 226-16 to 226-24 of the Criminal Code.

Done at xxx, xxx, in xxx copies

Name:
Signature:

To read more: https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_ven_0.pdf

Number 30

Cyber Resilience Act Requirements Standards Mapping

The increasing number of cyberattacks affecting digital products, coupled with widespread vulnerabilities and insufficient timely security updates, creates heavy financial burdens on society.

In response, the European Commission has drafted the Cyber Resilience Act (CRA), a new proposal for regulation to define the legislative framework of essential cybersecurity requirements that manufacturers must meet when placing any product with digital elements on the internal market.

To facilitate adoption of the CRA provisions, these requirements need to be translated into the form of harmonised standards, with which manufacturers can comply.

In support of the standardisation effort, this study attempt to identify the most relevant existing cybersecurity standards for each CRA requirement, analyses the coverage already offered on the intended scope of the requirement and highlights possible gaps to be addressed.

Introduction

On 15 September 2022, the European Commission published the proposal for the Cyber Resilience Act (CRA), a proposal for a first ever EU-wide legislation of its kind, aimed at introducing mandatory cybersecurity requirements for products with digital elements throughout their lifecycle.

The CRA proposal covers all products with digital elements put on the market which can be connected to a device or a network, including their building blocks (i.e., hardware and software) and encompassing also solutions provided in a Software as a Service (SaaS) fashion if they qualify as remote data processing solutions, as defined by Article 3(2) of the CRA proposal.

The CRA proposal provides two sets of essential requirements:

— Product cybersecurity requirements in Annex I, Section 1 of the CRA proposal

— Vulnerability handling process requirements in Annex I, Section 2 of the CRA proposal

These requirements should be the subject of a standardisation process by the European Standardisation Organizations (ESOs) to express them in the form of specifications in harmonised standards.

The general principle is that for the products on the market, a self-assessment of compliance with the requirements specified in Annex I will be sufficient.

For certain categories of more critical products, the application of harmonised standards will be required.

For even more critical products, a third-party assessment will be mandatory.

This report details the available standardisation outputs on the cybersecurity of products (hardware and software products, including hardware and software components of more complex products) carried out mainly by ESOs and international Standards Development Organizations (SDOs).

Specifically, the study aim at presenting a mapping of the existing cybersecurity standards against the essential requirements listed in Annex I of the CRA proposal, along with a gap analysis between the mapped standards and the requirements.

In view of the development of harmonised standards, this analysis offers a possible overview about the current coverage of the requirements by existing specifications, highlighting possible lacks that may be compensated by further standardisation work.

Upon request of DG CNECT, this study has been developed jointly by the Joint Research Centre (JRC) and the European Union Agency for Cybersecurity (ENISA).

This was also in line with the expectations of the proposal of regulation, in which it is stated that synergies on standardisation aspects should be considered between the Commission and ENISA.

In Section 2, the methodology adopted to carry out this study is summarised.

Section 3 is devoted to the presentation of the mapping between requirements and standards, giving an analysis of the coverage offered by the standards and possible gaps.

In Section 4, a summary of all identified standards and their respective mapping is offered along with some overall remarks, while Section 5 is for conclusions.

To read more: https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

Number 31

Revisiting the Non-Paper

Non-Paper on EU Cyber Diplomacy, by Estonia, France, Germany, Poland, Portugal and Slovenia

Federal Foreign Office

Auswärtiges Amt

Note: The German Federal Foreign Office (Auswärtige Amt) represents Germany’s interests to the world. It promotes international exchange and offers protection and assistance to Germans abroad.

The Context: Changing Circumstances

Since the adoption of the Council Conclusions on Cyber Diplomacy in February 2015, several interlinked developments in the political, economic, societal and technological spheres have increased the importance of cyberspace and highlight the need for a renewed strategic reference document at EU level for cyber diplomacy:

Due to the inexorable progress of digitalisation in almost all areas of life, including in the global economy and the private lives of citizens, the need to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with regard to the processing of personal data, and the need to protect critical infrastructure in the EU and its Member States against malicious cyber-attacks are of ever-increasing importance.

Cyberspace is continuously generating novel attack targets and vectors and cyber-attacks are growing in terms of scope, frequency and sophistication as well as the damage they inflict, and state and non-state actors, including proxies, are increasingly willing to pursue their objectives by conducting malicious cyber activities varying in scope, scale, duration, intensity, complexity, sophistication and impact.

Malicious cyber activities can serve several purposes and take various forms, including attacks against infrastructure, cyber-espionage, intellectual property theft, cybercrime, and possibly also attacks in the context of hybrid threats.

The COVID-19 pandemic has demonstrated the increasing dependence on fast and stable connectivity and that a functioning, stable and secure cyberspace is an important condition for this.

Cyberspace has increasingly become an area of strategic competition between states which reflects the dynamic geopolitical environment in recent years, and technological innovations have increasingly become points of contention between states due to their growing significance for economic and military competitiveness, which has also resulted in a technological confrontation between major actors.

More confrontational approaches in the technological realm may lead to certain decoupling effects and to a further severing of global supply chains and cooperation with regard to research and innovation, including in the area of cyber security, as well as to a potential fracturing of the global internet, which is noted with concern.

The EU and its Member States have to clearly define their role in the context of growing competition between major actors that are increasingly willing to shape the digital environment and the discussion surrounding it, meaning that the EU and its Member States have to assert themselves in international cyberspace norm-setting and technological standard-setting bodies.

States with an authoritarian outlook are increasingly trying to enforce their interests in cyberspace and in the technological realm and the EU and its Member States have to react by promoting their values and interests, which include human rights, prosperity, security and Europe´s digital sovereignty.

The use and deployment of technologies to track, surveil, anticipate or even grade the behaviour of citizens in a repressive and unprecedented way, and the use of digital tools by authoritarian states that is contrary to the idea of a free, open and global internet and international human rights law as well as plans by some countries to build an alternative internet regulated by the State are noted with concern.

Protection of its Citizens and Modern Societies

Recent EU cyber-related initiatives aimed at protecting its citizens and the resilience of its modern societies and the related data and critical infrastructure against malicious activities in cyberspace, such as the renewed Cyber Security Strategy, Review of the NIS Directive and the EU 5G Toolbox with its objective of establishing a coordinated European approach aimed at mitigating the main cyber security risks of 5G networks, are welcomed and the importance of maintaining and strengthening coherence among the EU cyber and digital initiatives is noted.

With the advent of innovative technologies such as artificial intelligence, the Internet of Things or 5G, new possible targets and vectors are emerging in cyberspace, which also have to be reflected in global debates concerning norms of behaviour in cyberspace.

Furthermore, cybercrime actors are steadily developing new forms of malicious activities to exploit vulnerabilities in cyberspace.

While digital technologies and increased connectivity are key components of modern societies and bring major benefits in terms of growth and prosperity, at the same time citizens, companies and governments are, especially in the context of the COVID-19 pandemic, more and more exposed to offenses in the field of cybercrime, which are steadily increasing in number and sophistication.

Thus, the EU and its Member States reiterate the need for a coordinated and determined fight against cybercrime and continue to promote the Council of Europe Convention on Cybercrime, also known as the Budapest Convention, and the negotiations on the Second Additional Protocol to the Budapest Convention, as an important framework for international cooperation in the fight against cybercrime.

Regarding access to digital evidence, the EU and its Member States first recognize encryption as an important tool for the protection of cybersecurity and fundamental rights, such as privacy, including the confidentiality of communications, and personal data.

The EU and its Member States are invited to find solutions that allow law enforcement and other competent authorities to gain lawful access to digital evidence concerning malicious cyber activities, without prohibiting or generally weakening encryption, and in full respect of privacy and fair trial guarantees consistent with applicable law.

The EU and its Member States acknowledge in that context the work done by EUROPOL and similar European and international institutions with a view to supporting and coordinating investigations of cyber-attacks and cybercrime among the Member States.

The EU, for instance in the context of the Horizon Europe framework programme, and its Member States are encouraged to further invest in cyber security research, including in the areas of digital forensics analysis, threat intelligence and incident response in the face of malicious activities in cyberspace.

Cyberspace as a Key Area for the EU's Foreign Policy and Digital Sovereignty

Due to the increasing importance of cyberspace for several areas of life and the growing significance of digital technologies for power projection on the international stage, cyber diplomacy should be considered an important tool for fulfilling the objectives and interests of the EU.

The protection and reinforcement of Europe's digital sovereignty in the EU stands in direct connection with cyber security, as it ensures trust in digital technologies and the digital transformation process.

Thus, a coherent international cyberspace policy must be considered a key component of the determined engagement of the EU and its Member States with a view to reinforcing their digital sovereignty by having the ability and the will to shape global debates, which reflects the EU's values as well as its strategic and economic interests, and the capacity to act self assertively in cyberspace, which should not be confused with isolating itself or striving for digital or technological autarky.

Through its engagement – within the EU and beyond – with regard to setting norms of behaviour and establishing regulations concerning cyberspace and its self-conception as a preventive actor in contributing to a secure, stable and open cyberspace, the EU serves as an international point of reference, especially for states which want to avoid confrontational approaches internationally and adhere to international law in cyberspace, and the EU positions itself as a champion of and force for peaceful relations, conflict prevention and greater stability in cyberspace.

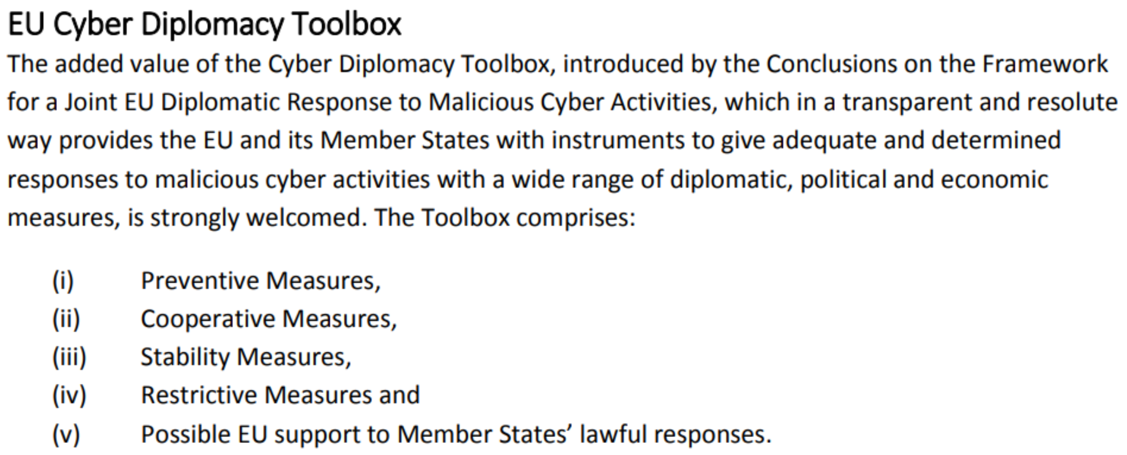
The EU with its human-centred approach is in an excellent position to set sophisticated cyber-related and technology standards, such as the General Data Protection Regulation (GDPR) or the ethical and legal framework proposed by the AI White Paper concerning high-risk applications, which serves as a model for other regions.

Such a coherent international cyberspace policy of the EU – especially in the context of the previously mentioned numerous and interlinked developments in the political, economic, societal and technological spheres – should serve:

- the EU's foreign and security policy objectives and broader values, as stated in the EU Global Strategy, with cyber diplomacy being an integral part of the pursuit of these goals in the context of the Common Foreign and Security Policy (CFSP), and with activities in cyberspace being conceived jointly and in line with contextual developments at international level;

- the purpose of protection of its citizens and modern societies, and of the related data and critical infrastructures, against malicious activities in cyberspace, as well as the integrity and security of the EU and

- the purpose of promotion and protection of the fundamental EU values of democracy, human rights, gender and digital equality and the rule of law in cyberspace, including the right of expression and equal access to and secure use of information and communication technology (ICT) and the internet, on the global stage, especially in light of the increasing misuse of new technologies that leads to human rights and privacy violations.



EU Cyber Diplomacy Toolbox

The added value of the Cyber Diplomacy Toolbox, introduced by the Conclusions on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, which in a transparent and resolute way provides the EU and its Member States with instruments to give adequate and determined responses to malicious cyber activities with a wide range of diplomatic, political and economic measures, is strongly welcomed. The Toolbox comprises:

(i) Preventive Measures,
(ii) Cooperative Measures,
(iii) Stability Measures,
(iv) Restrictive Measures and
(v) Possible EU support to Member States' lawful responses.

To read more: https://www.auswaertiges-amt.de/blob/2418160/206b3bf9aa4ef45a2887399231840d23/201119-non-paper-pdf-data.pdf

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 prejudge 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 prejudge 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

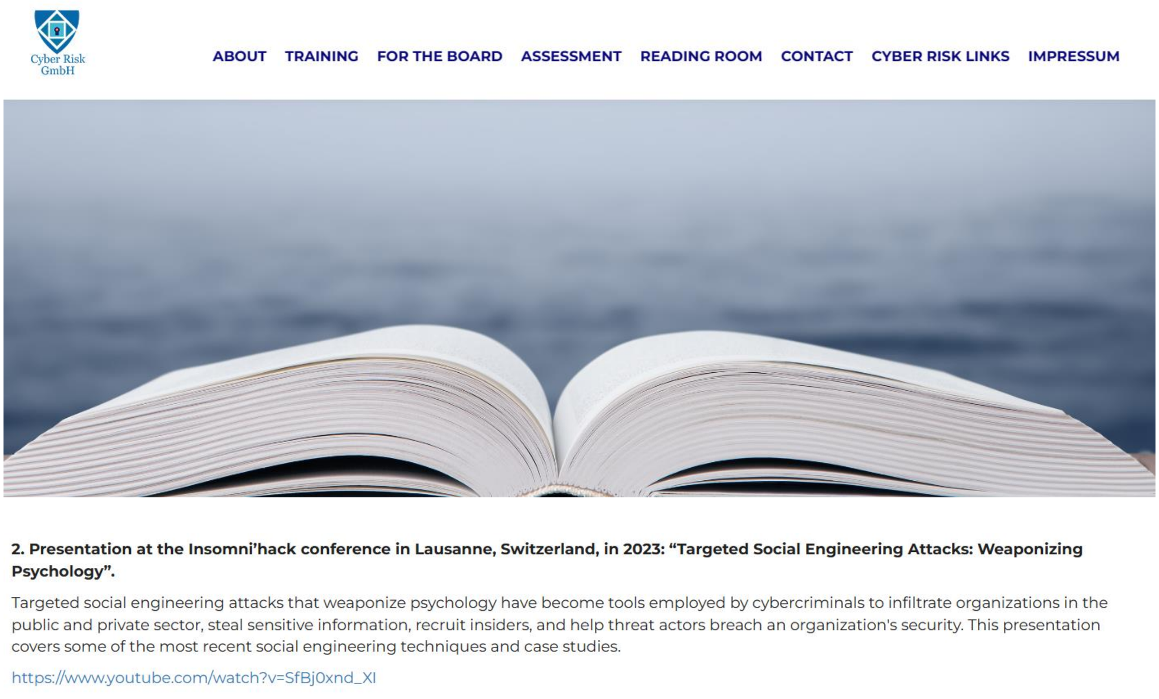
- Great training, exceptional venues.
- Presentations for the Board and the C-Suite.

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



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=SfBj0xnd_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

8. Electricity Cybersecurity - https://www.electricity-cybersecurity.com

9. Gas Cybersecurity - https://www.gas-cybersecurity.com

10. Hydrogen Cybersecurity - https://www.hydrogen-cybersecurity.com

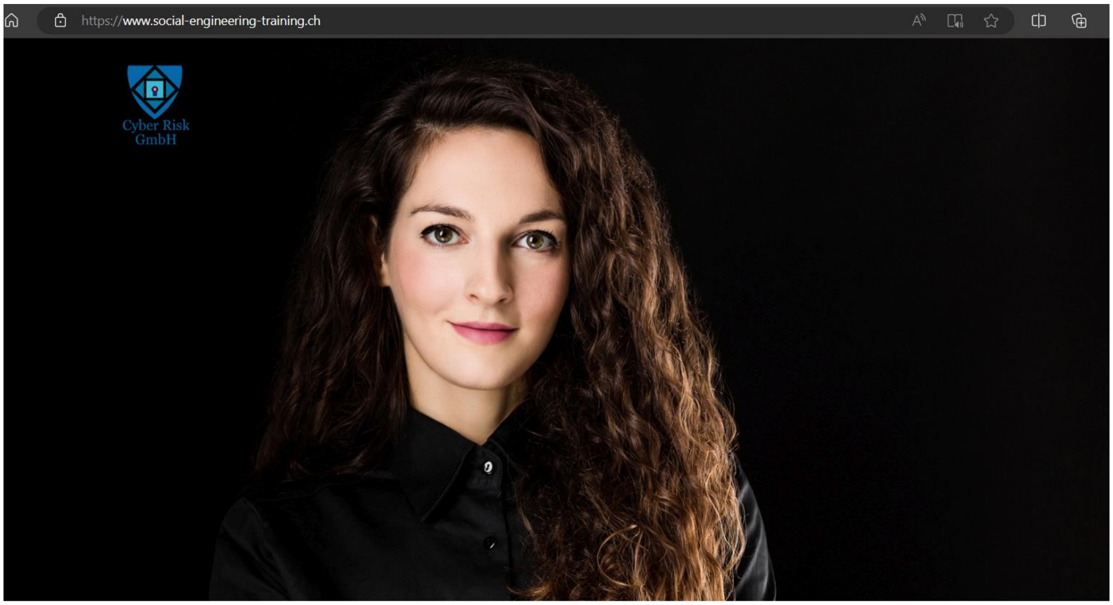
11. Transport Cybersecurity - https://www.transport-cybersecurity.com

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

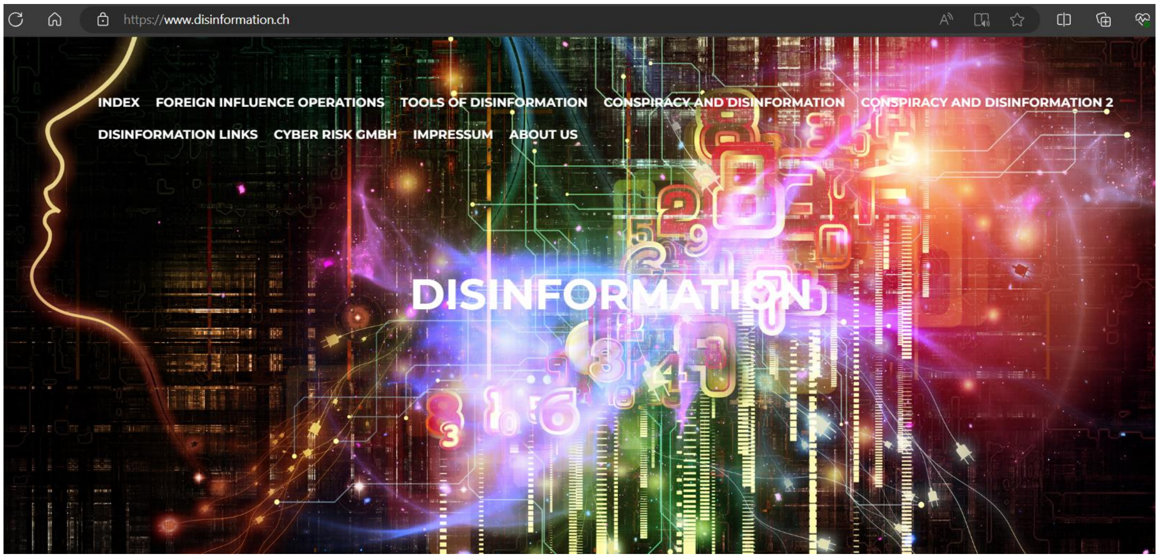
4. What is Synthetic Identity Fraud? - https://www.synthetic-identity-fraud.com

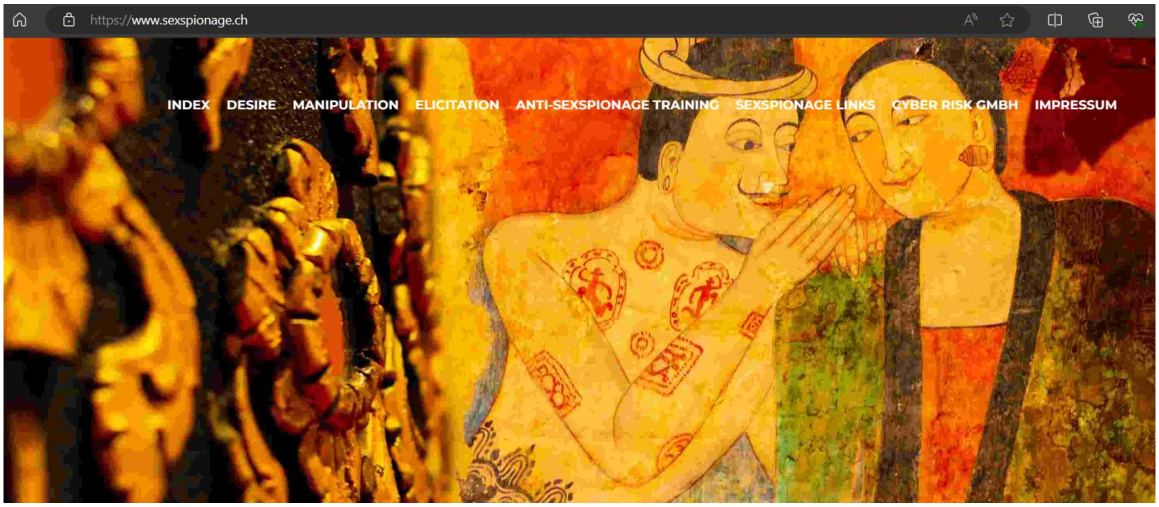
5. What is a Romance Scam? - https://www.romance-scams.ch

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


https://www.disinformation.ch
INDEX
FOREIGN INFLUENCE OPERATIONS
TOOLS OF DISINFORMATION
CONSPIRACY AND DISINFORMATION
CONSPIRACY AND DISINFORMATION 2
DISINFORMATION LINKS
CYBER RISK GMBH
IMPRESSUM
ABOUT US
DISINFORMATION



c. Understanding Cybersecurity in the European Union.

1. The NIS 2 Directive - https://www.nis-2-directive.com

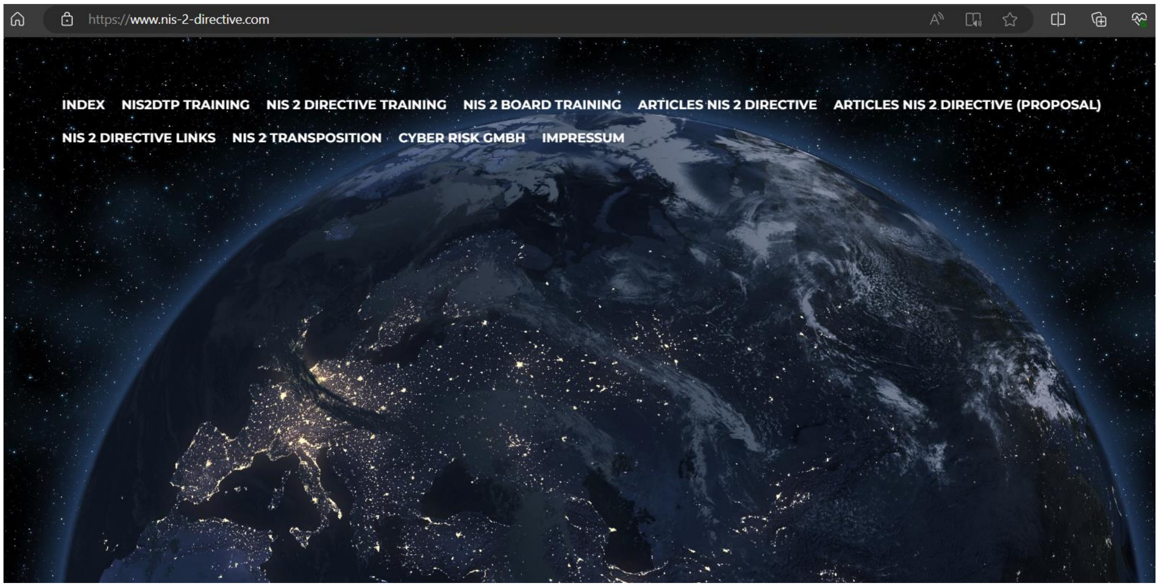
2. The European Cyber Resilience Act - https://www.european-cyber-resilience-act.com

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

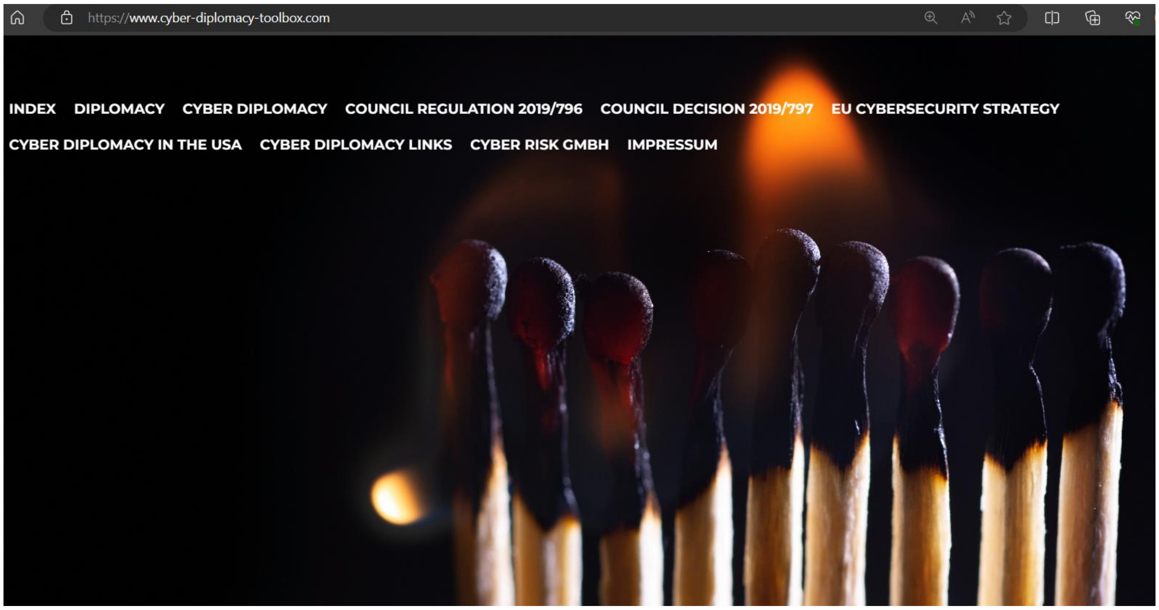
17. The European Digital Identity Regulation - https://www.european-digital-identity-regulation.com

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

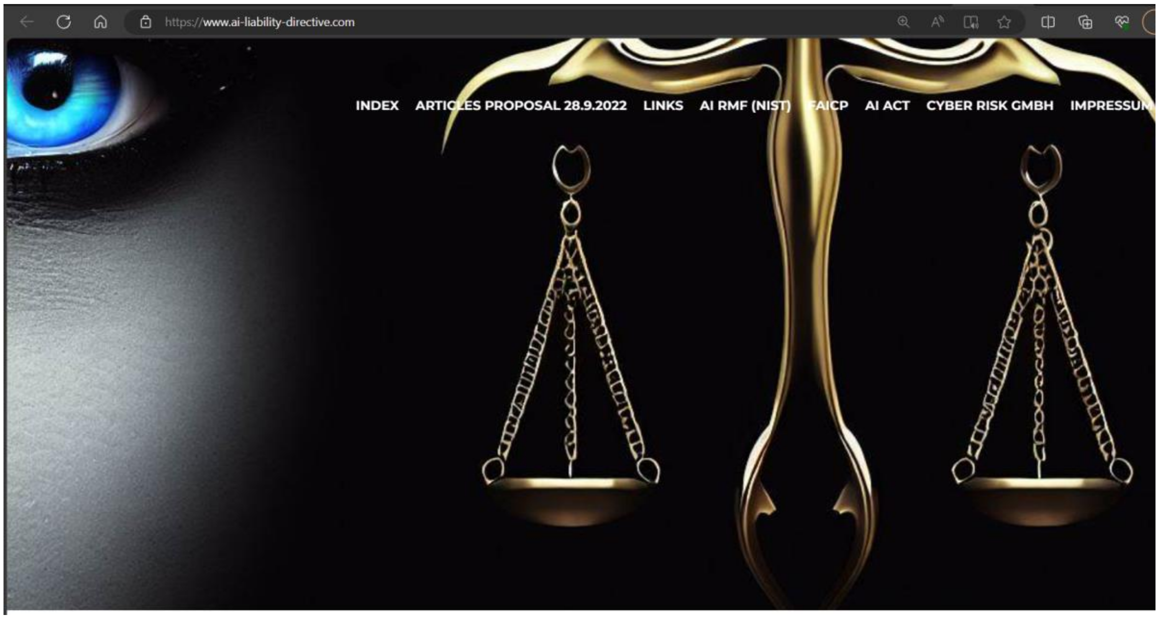
20. The Strategic Compass of the European Union https://www.strategic-compass-european-union.com

21. The EU Cyber Diplomacy Toolbox - https://www.cyber-diplomacy-toolbox.com


https://www.cyber-diplomacy-toolbox.com
INDEX
DIPLOMACY
CYBER DIPLOMACY
COUNCIL REGULATION 2019/796
COUNCIL DECISION 2019/797
EU CYBERSECURITY STRATEGY
CYBER DIPLOMACY IN THE USA
CYBER DIPLOMACY LINKS
CYBER RISK GMBH
IMPRESSUM

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


https://www.ai-liability-directive.com
INDEX
ARTICLES PROPOSAL 28.9.2022
LINKS
AI RMF (NIST)
AICP
AI ACT
CYBER RISK GMBH
IMPRESSU