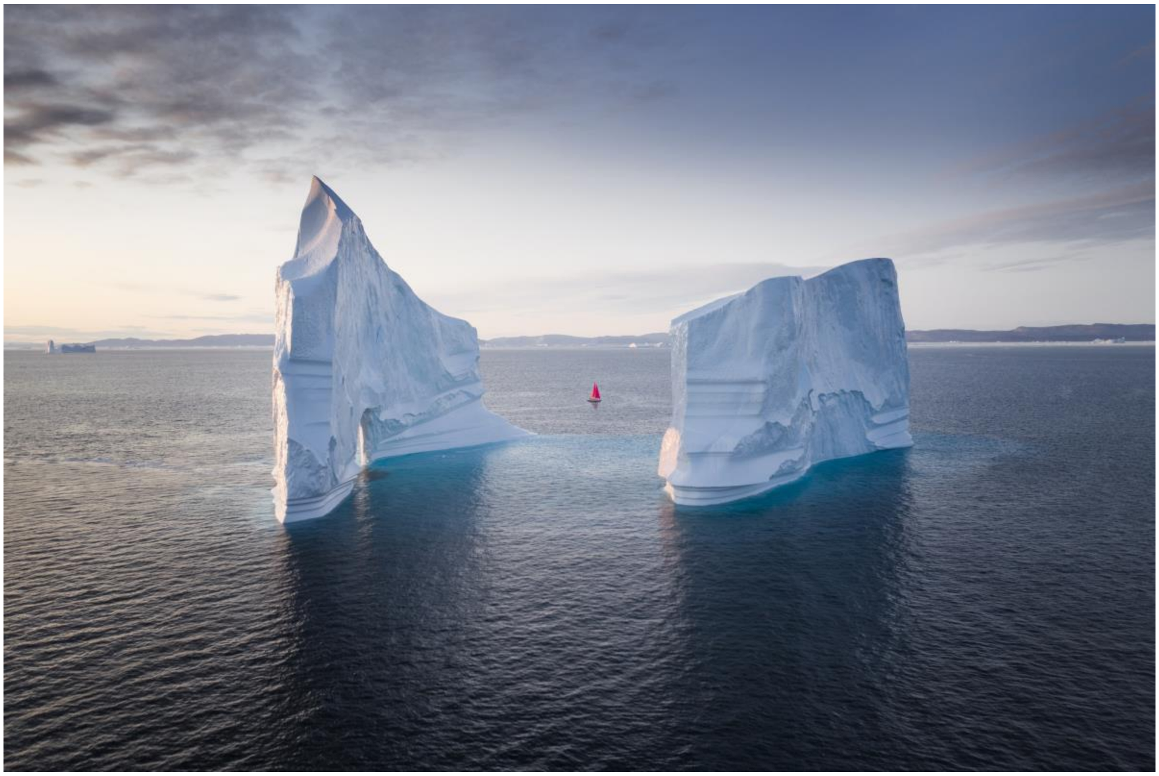
Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341
Dammstrasse 16, 8810 Horgen, Switzerland
Tel: +41 79 505 89 60 Web: https://www.cyber-risk-gmbh.com



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

Dear readers,

The law is (and always has been) made by humans for humans, but this is going to change. The rise of Artificial Intelligence (AI) and robots leads to the emergence of *'robot law'*. This is not a joke.

AI is changing the way we live and work. Routine tasks, not only manual but also cognitive, are becoming increasingly automated, and "embodied AI" (robots that use AI to interact with the physical world and to learn from their interactions) take more and more jobs month after month.

Embodied AI is not recognized by law as a natural person, but corporations are not natural persons too. Corporations are legal persons, and have the ability to transact and follow rules, they have obligations, and are liable for certain behaviour. Will robots have a legal personality, like corporations? Will humans that incorporate elements of machine intelligence into their brains and bodies still be considered as natural persons?

Scientists from areas as diverse as law, engineering, philosophy, psychology, sociology, computer science, biology, neuroscience, biomechanics, material science, and linguistics have to work hard to understand the benefits of AI, and to reduce the negative consequences.

A picture may sometimes be worth a thousand words, but a thousand pictures cannot represent what we may mean using a single word. The road is not going to be easy.

Read more about AI developments in Numbers 14, 15, 16 below.

I have just read for the second time the EU Artificial Intelligence Act (AI Act, Council Proposal 25.11.2022) of the European Union. I am particularly interested in the definition and regulation of the *"subliminal components"* of AI systems, and how it affects Psychological operations (PSYOP) in the increasingly important field of information confrontation.

In Latin, *"sub"* means below, and *"limen"* is the threshold. Subliminal is something that exists just below the threshold of conscious awareness.

We read in the AI Act: "AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices. The placing on the market, putting into service or use of certain AI systems materially distorting human behaviour, whereby physical or psychological harms are likely to occur, are particularly dangerous and should therefore be forbidden."

"Such AI systems deploy *subliminal components* such as audio, image, video stimuli that persons cannot perceive as those stimuli are beyond human perception or other subliminal techniques that subvert or impair person's autonomy, decision-making or free choices in ways that people are not consciously aware of, or even if aware not able to control or resist, for example in cases of machine-brain interfaces or virtual reality."

In Article 2 of the AI Act, we read that the regulation applies to:

- providers placing on the market or putting into service AI systems in the EU, irrespective of whether those providers are physically present or established within the Union or in a third country;

- users of AI systems who are physically present or established within the EU;

- providers and users of AI systems who are physically present or established in a third country, where the output produced by the system is used in the Union;

- importers and distributors of AI systems;

- product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark;

- authorised representatives of providers, which are established in the Union;"

Obviously we have interesting extraterritorial application of EU law. But how it affects Psychological Operations?

Psychological operations are planned political, economic, military, and ideological activities directed towards foreign countries, organizations, and individuals in order to create emotions, attitudes, understanding, beliefs, and behavior favourable to the achievement of political and military objectives. *No matter if we like it or not,* this is an important part or the new hybrid warfare.

In Article 2, paragraph 3 of the AI Act, we read: "This Regulation shall not apply to AI systems if and insofar placed on the market, put into service, or used with or without modification of such systems for the purpose of activities which fall outside the scope of Union law, and in any event activities concerning military, defence or national security, regardless of the type of entity carrying out those activities."

The exclusion for military and defence purposes is justified both by Article 4(2) of the Treaty on European Union (TEU), and by the common EU defence policy covered by Chapter 2 of Title V of the TEU.

The exclusion for national security purposes is justified by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) of the TEU.

Read more at number 5 below.

We expect a surprise for *auditors* from the European Commission. I was reading the final text of the EU Digital Operational Resilience Act (DORA) - (EU) 2022/2554. In Article 58 we read that by 17 January 2026, the European Commission shall carry out a review and submit a report to the European Parliament and the Council, accompanied, where appropriate, by a legislative proposal.

Which is the scope of the review? The appropriateness of *strengthened requirements for statutory auditors and audit firms as regards digital operational resilience,* by means of the *inclusion* of statutory auditors and audit firms into the scope of this Regulation, or by means of amendments to Directive 2006/43/EC of the European Parliament and of the Council.

Directive 2006/43/EC is the 8th Company Law Directive, it is also called ESOX, the European Sarbanes-Oxley.

The Digital Operational Resilience Act (DORA) is a very interesting regulation. Before DORA, financial institutions managed the main categories of financial risk (credit risk, market risk, liquidity risk etc.) using the traditional quantitative approach (setting a capital requirement), but they did not manage all components of operational resilience.

After the Russia's invasion of Ukraine that, according to Ursula von der Leyen, president of the European Commission, has brought death, devastation and unspeakable suffering, and after DORA, financial institutions must also follow qualitative rules for the protection, detection, containment, recovery and repair after ICT-related incidents.

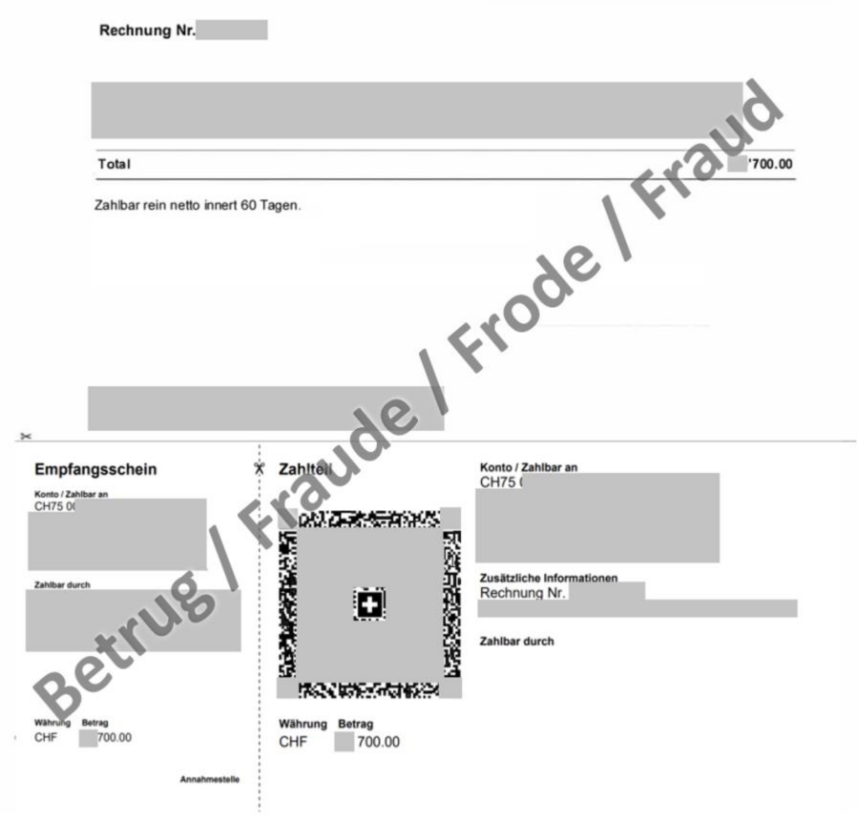
DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the financial system, even if there is “adequate” capital for the traditional risk categories in individual institutions.

Read more at number 2 below.

According to the Swiss National Cyber Security Centre (NCSC), QR codes are becoming increasingly popular in Switzerland, and are used for various purposes. They are used not only to provide links to websites, but also to organise entire logistics processes. QR codes have also found their way into invoices. Effective since 1 October 2022, only invoices with QR codes are accepted in Switzerland. Clearly, QR codes can also be misused, as illustrated by two examples reported to the NCSC last week.

Attackers are increasingly scouring hacked email accounts for sent invoices or payment instructions. If they find them, they copy and manipulate the invoice. The fraudsters change the IBAN indicated on the invoice to which the amount is to be paid and re-send it to the victim in the name of the actual invoice issuer on the spurious grounds that the beneficiary account has changed. The recipient is now supposed to pay the amount into the new account, which is actually the fraudsters'.

Until recently, the attackers in this sort of invoice manipulation scam, also called business email compromise, confined themselves to changing the IBAN in the invoice or simply indicated to the invoice recipient that the amount should be transferred to another account. However, a case reported to the NCSC last week was different. The invoice was manipulated and looked remarkably authentic. Not only was the IBAN changed, but the QR code was also adapted accordingly. In addition, the amount was supposed to be paid into a Swiss account, which made it difficult for the victim to spot the fraud attempt.



Rechnung Nr. [redacted]

[redacted]

Total	[redacted]'700.00

Zahlbar rein netto innert 60 Tagen.

[redacted]

Empfangsschein

Konto / Zahlbar an
CH75 [redacted]

Zahlbar durch
[redacted]

Währung	Betrag
CHF	[redacted]700.00

Annahmestelle

Zahlteil

Währung	Betrag
CHF	[redacted] 700.00

Konto / Zahlbar an
CH75 [redacted]

Zusätzliche Informationen
Rechnung Nr. [redacted]
[redacted]

Zahlbar durch

- Raise the awareness of all employees, especially those in finance divisions and key positions, about these possible methods of attack.

- Ignore unusual payment requests.

- In the case of unusual requests within the company, check by telephone that the request is genuine.

- All processes which concern payment transactions should be clearly defined internally and complied with by employees in all cases (e.g. dual control principle, joint signature by two people).

NCSC - When the QR code suddenly takes you to the wrong page

Last week, the NCSC also received reports about an information letter from a company that was sent by post.

To make it easier for recipients to respond, the letters contained a QR code enabling them to go directly to the correct feedback page without the hassle of typing it.

However, some recipients complained to the sender of the letters that they were taken to a dubious site that required credit card details.

The underlying reason was unclear at first. Manipulation of the QR code itself was quickly ruled out.

The QR code was identical in all of the letters, including those sent to the people who had noticed the suspicious behaviour.

Consequently, the QR scanner came under suspicion, especially since all of those affected had always used the same QR scanner.

The NCSC then took a closer look at the QR code scanner, but there were no irregularities in the scanning process and the link was reproduced correctly.

However, it was conspicuous that an advertisement was displayed in the lower part of the screen whenever the link was accessed. Some of these advertisements were designed to confuse the user and suggested that the advertisement was an official part of the app.

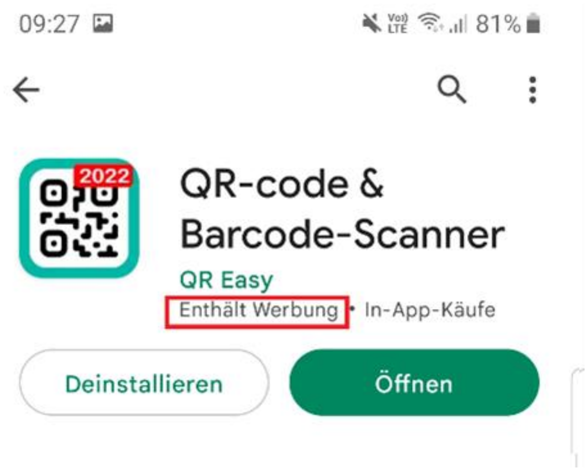
Specifically, in addition to the genuine "Open connection" link, which is outlined in an inconspicuous light blue, a "Start" button is displayed at the very bottom in vivid green.

If people are stressed and do not look closely at the page, they inevitably press the button that is the most conspicuous. This is precisely what the people who place these advertisements are after.

They buy advertising space with the intention of confusing users and thus tricking them into clicking on the dubious link – in this case, a subscription scam.

The providers, who make their space available for advertising and thereby finance the app, can do very little about this, as they commission the advertising through third-party companies. They have no influence on the content.

The advertisements placed are always very small and are therefore hardly noticed.



QR-code & Barcode-Scanner

QR Easy

Enthält Werbung • In-App-Käufe

- Use a reliable app that is recognised as secure to scan QR codes. The advantage of this is that your device will ask you to confirm the action before the code contained in the QR is executed. Both Apple and Android also allow the camera to recognise QR codes.

- After scanning and before execution, most scanners will display the action to be performed or the page to be accessed. Check this information.

- Never enter login credentials on a website that you accessed via a QR code.

- Before scanning a QR code, take a close look at it or touch it to see if it is not just a sticker that has been affixed to the original.

- If you scan a QR code that contains something malicious, immediately notify the owner of the place (magazine, website, etc.) where you discovered it.

Further information can be found at:
https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-private/aktuelle-themen/qr-code-anwendungen-und-risiken.html

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Dammstrasse 16, 8810 Horgen

Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

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

Number 1 (Page 13)

Public responses to consultation on achieving greater convergence in cyber incident reporting

Number 2 (Page 15)

The EU Digital Operational Resilience Act (DORA)

Number 3 (Page 18)

Preparing the economy and financial system for hybrid war - Finland's experience

Olli Rehn, Governor of the Bank of Finland, at the Peterson Institute for International Economics (PIIE) Financial Statements web event series

Number 4 (Page 20)

Interoperable EU Risk Management Framework

Number 5 (Page 22)

Council of the European Union

Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

Number 6 (Page 26)

XLLing in Excel - threat actors using malicious add-ins

By Vanja Svajcer, Cisco Talos Intelligence Blog

Number 7 (Page 28)

CISA Releases Four Industrial Control Systems Advisories

Number 8 (Page 29)

Ransomware-as-a-service (RaaS) - Cybercriminals stung as HIVE infrastructure shut down

Europol supported German, Dutch and US authorities to shut down the servers and provide decryption tools to victims

Number 9 (Page 33)

U.S. Department of Justice Disrupts Hive Ransomware Variant

FBI Covertly Infiltrated Hive Network, Thwarting Over $130 Million in Ransom Demands

Number 10 (Page 37)

Daring to know in times of uncertainty and structural shifts

Klaas Knot, President of the Netherlands Bank and Chair of the Financial Stability Board, at the 11th ILF Conference on the Future of the Financial Sector "The Next Systemic Financial Crisis – Where Might it Come From?": Financial Stability in a Polycrisis World, at the Goethe University's Law and Finance Institute, Frankfurt am Main.

Number 11 (Page 45)

Information Laundering via Baltnews on Telegram

Number 12 (Page 48)

Achieving Foundational Security for Food Systems

New DARPA effort seeks advanced threat-detection and warning capabilities for crop defense

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 13 (Page 51)

Wi-Fi Could Help Identify When You're Struggling to Breathe

NIST National Institute of Standards and Technology U.S. Department of Commerce

Number 14 (Page 54)

NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence

New guidance seeks to cultivate trust in AI technologies and promote AI innovation while mitigating risk.

NIST National Institute of Standards and Technology U.S. Department of Commerce

Number 15 (Page 58)

VIDEO: A New Generation of AI Assistants

Perceptually-enabled Task Guidance prototypes demonstrated ability to help people complete recipes as a proxy to unfamiliar tasks

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 16 (Page 60)

Some paragraphs from the EU Artificial Intelligence Act

Not the final text – It is the proposal from the Council of the European Union for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Council of the
European Union

Number 1

Public responses to consultation on achieving greater convergence in cyber incident reporting

FSB FINANCIAL STABILITY BOARD

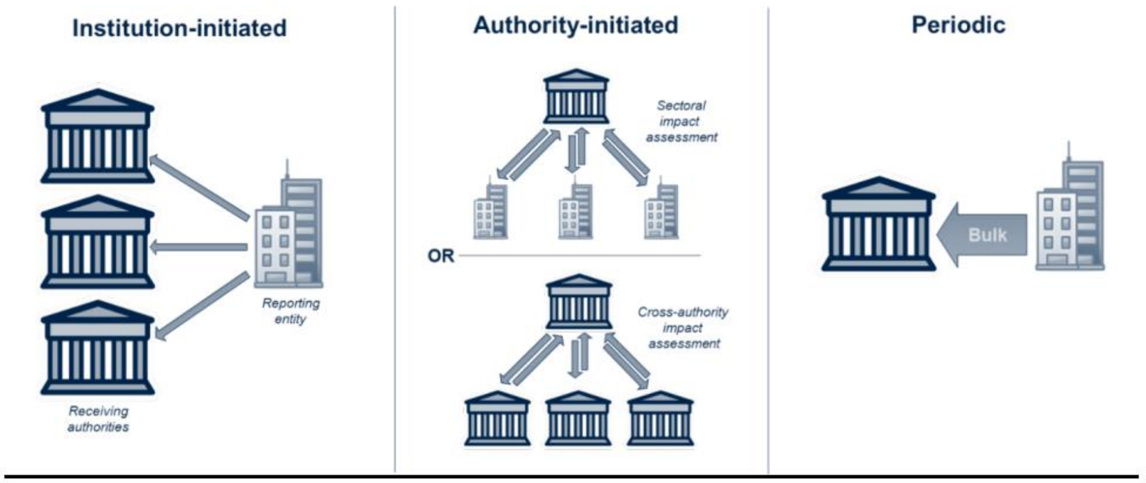
On 17 October 2022, the FSB published Achieving Greater Convergence in Cyber Incident Reporting – Consultative document. You may visit: https://www.fsb.org/2022/10/achieving-greater-convergence-in-cyber-incident-reporting-consultative-document/

FSB FINANCIAL STABILITY BOARD

Achieving Greater Convergence in Cyber Incident Reporting

Consultative Document

Illustration of reporting types **Figure 6**

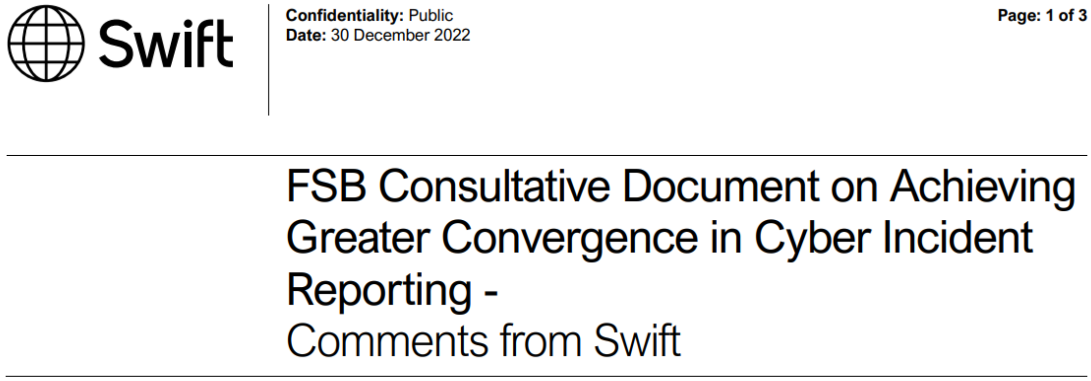


Interested parties were invited to provide written comments by 31 December 2022. The public comments received are available below.

The FSB thanks those who took the time and effort to express their views. The FSB expects to publish the final report in April 2023.

We have very interesting responses from:

- Banking Association of South Africa
- EBA Clearing
- European Banking Federation
- Financial Services Sector Coordinating Council
- German Banking Industry Committee
- Global Financial Markets Association
- Global Legal Entity Identifier Foundation
- Google Cloud
- Institute of International Finance
- Insurance Europe
- Intesa Sanpaolo
- NASDAQ
- SWIFT
- Swiss Insurance Association
- UK Finance
- Unipol
- World Council
- World Federation of Exchanges



Swift

Confidentiality: Public
Date: 30 December 2022

Page: 1 of 3

FSB Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting -
Comments from Swift

To read more: https://www.fsb.org/2023/01/public-responses-to-consultation-on-achieving-greater-convergence-in-cyber-incident-reporting/

Number 2

The EU Digital Operational Resilience Act (DORA)

EUR-Lex
Access to European Union law

Article 1, Subject matter

1. In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:

(a) requirements applicable to financial entities in relation to:

(i) information and communication technology (ICT) risk management;

(ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;

(iii) reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d);

(iv) digital operational resilience testing;

(v) information and intelligence sharing in relation to cyber threats and vulnerabilities;

(vi) measures for the sound management of ICT third-party risk;

(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

(c) rules for the establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities;

(d) rules on cooperation among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

2. In relation to financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive.

3. This Regulation is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.

Article 2, Scope

1. Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities:

(a) credit institutions;

(b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;

(c) account information service providers;

(d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;

(e) investment firms;

(f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens;

(g) central securities depositories;

(h) central counterparties;

(i) trading venues;

(j) trade repositories;

(k) managers of alternative investment funds;

(l) management companies;

(m) data reporting service providers;

(n) insurance and reinsurance undertakings;

(o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;

(p) institutions for occupational retirement provision;

(q) credit rating agencies;

(r) administrators of critical benchmarks;

(s) crowdfunding service providers;

(t) securitisation repositories;

(u) ICT third-party service providers.

2. For the purposes of this Regulation, entities referred to in paragraph 1, points (a) to (t), shall collectively be referred to as 'financial entities'.

3. This Regulation does not apply to:

(a) managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU;

(b) insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC;

(c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;

(d) natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU;

(e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises;

(f) post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

4. Member States may exclude from the scope of this Regulation entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU that are located within their respective territories. Where a Member State makes use of such option, it shall inform the Commission thereof as well as of any subsequent changes thereto. The Commission shall make that information publicly available on its website or other easily accessible means.

To read more: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Number 3

Preparing the economy and financial system for hybrid war - Finland's experience

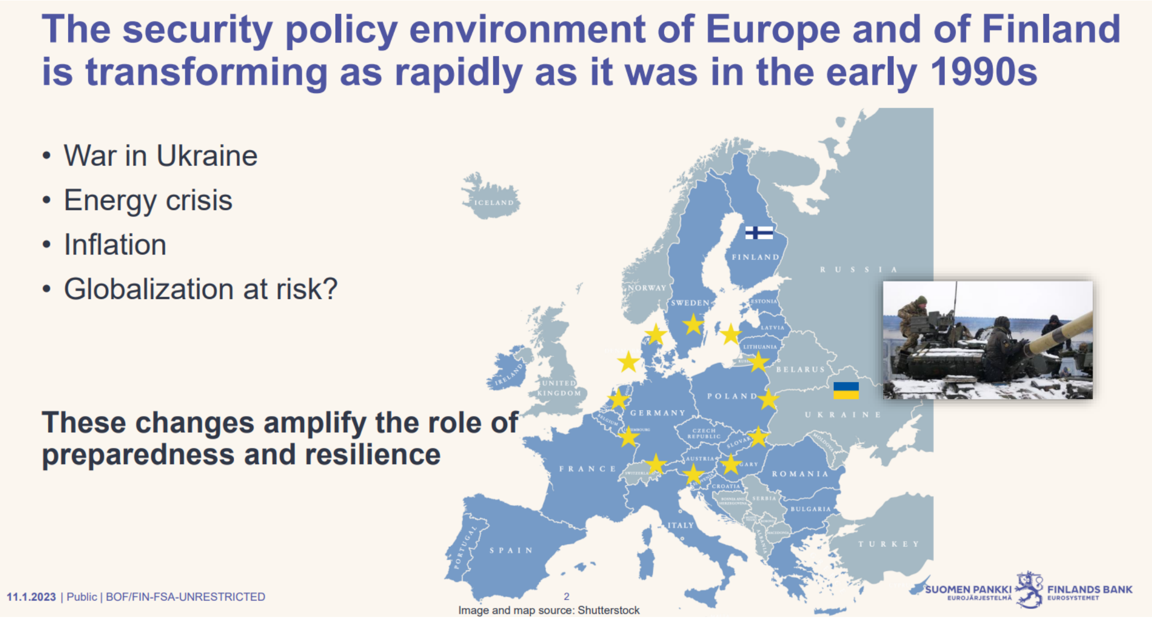
Olli Rehn, Governor of the Bank of Finland, at the Peterson Institute for International Economics (PIIE) Financial Statements web event series

Ladies and Gentlemen,

Greetings from a snowy Helsinki – and thank you very much for this opportunity to exchange views with you at this event today. The topic of my talk is Finland's experience in building up resilience and preparing the economy and financial system to cope with hybrid warfare.

Around a year ago, a rapid recovery from the COVID-19 pandemic was well under way in Europe. Those positive prospects were crushed last February by Russia's illegal and brutal attack against Ukraine.

The horrific bombardment of critical Ukrainian infrastructure has left millions of Ukrainians at the mercy of winter conditions, and no end to the war is in sight.



The security policy environment of Europe and of Finland is transforming as rapidly as it was in the early 1990s

- War in Ukraine
- Energy crisis
- Inflation
- Globalization at risk?

These changes amplify the role of preparedness and resilience

11.1.2023 | Public | BOF/FIN-FSA-UNRESTRICTED

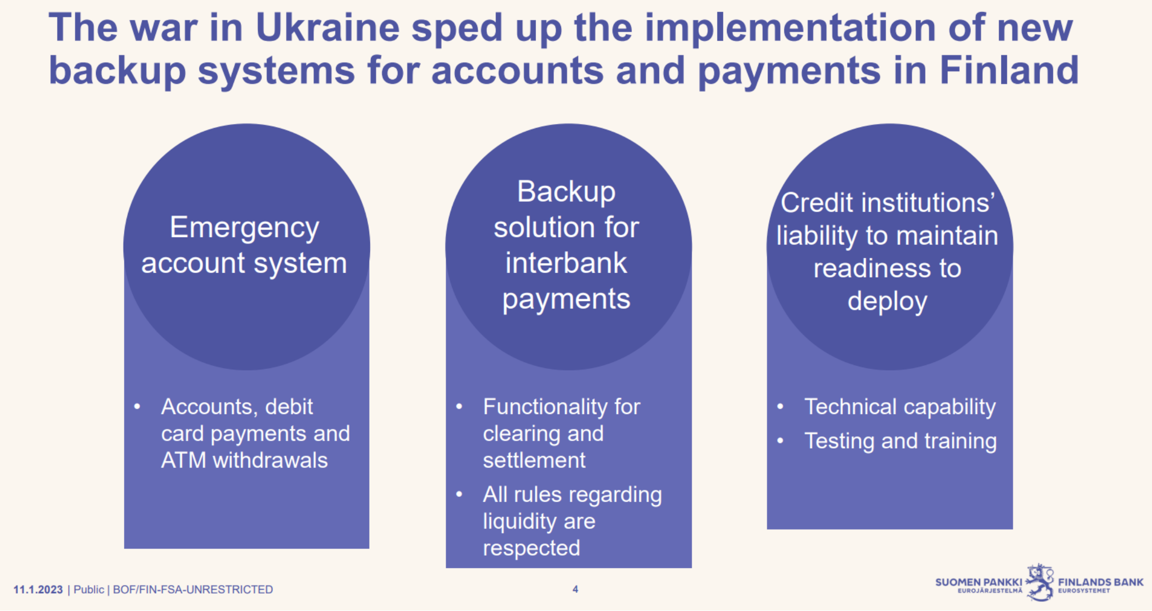
2

Image and map source: Shutterstock

We need to be prepared for a long confrontation between Putin's Russia and the liberal West, or more broadly between authoritarian governments and liberal democracies.

Russia's war has been a litmus test of European unity. Supporting Ukraine in its fight for freedom remains a policy priority. For Finns, this is really close to our hearts, also by our own experience.

After all, we ourselves were attacked by the Soviet Union in the Second World War, and we still have Europe's longest border with Russia: 832 miles, or 1340 kilometres.



The war in Ukraine sped up the implementation of new backup systems for accounts and payments in Finland

Emergency account system

- Accounts, debit card payments and ATM withdrawals

Backup solution for interbank payments

- Functionality for clearing and settlement
- All rules regarding liquidity are respected

Credit institutions' liability to maintain readiness to deploy

- Technical capability
- Testing and training

11.1.2023 | Public | BOF/FIN-FSA-UNRESTRICTED 4

SUOMEN PANKKI EUROJÄRJESTELMÄ FINLANDS BANK EUROSYSTEMET

To read more: https://www.suomenpankki.fi/en/media-and-publications/speeches-and-interviews/2023/governor-olli-rehn-preparing-the-economy-and-financial-system-for-hybrid-war-finlands-experience/

SUOMEN PANKKI
EUROJÄRJESTELMÄ

FINLANDS BANK
EUROSYSTEMET

Number 4

Interoperable EU Risk Management Framework

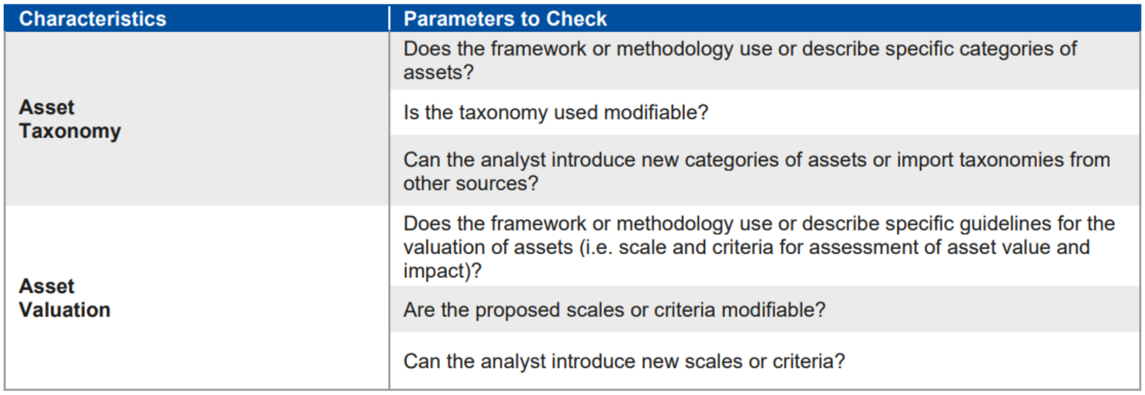
This report is an update of the report “Interoperable EU Risk Management Framework” published by ENISA in January 2022.

The “Interoperable EU Risk Management Framework” proposes a methodology for assessing the potential interoperability of risk management (RM) frameworks and methods and presents related results.

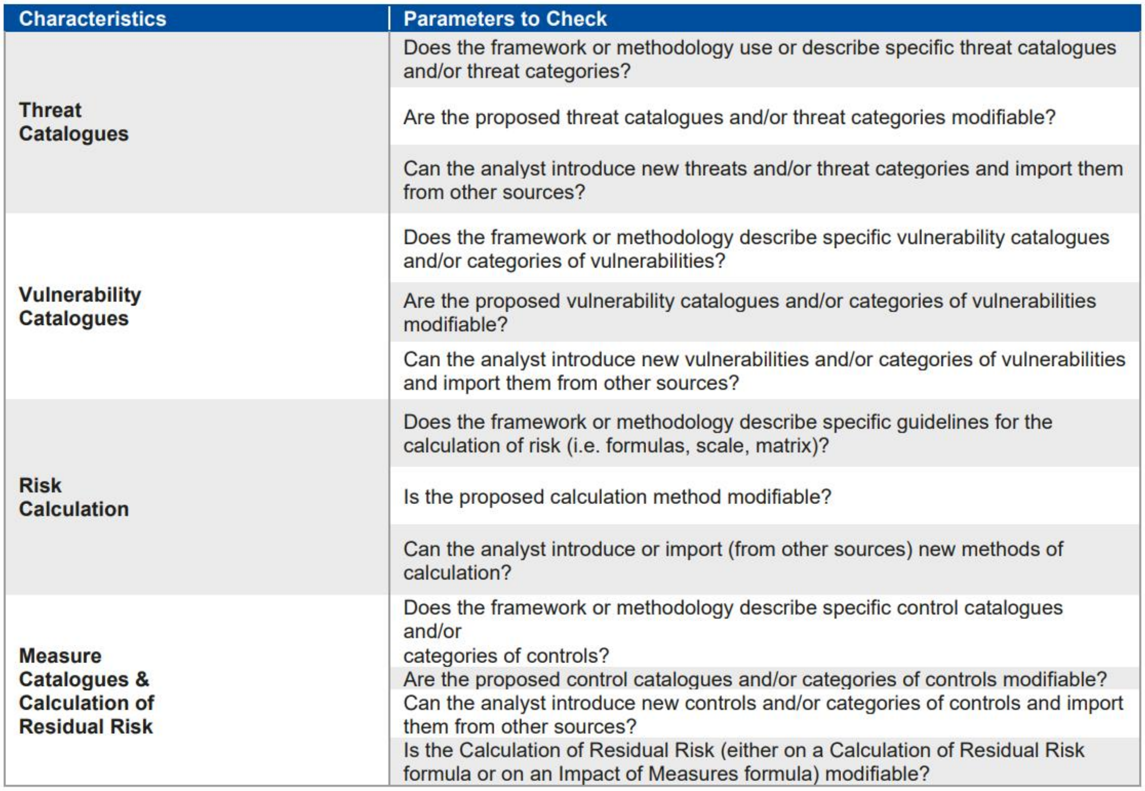
The methods included in this report have been selected as prominent, based on their interoperability features, after evaluating an extended list of risk management frameworks and methods (included in the Compendium of Risk Management Frameworks with Potential Interoperability, ENISA, January 2002) which has been published as Supplement to the Interoperable EU Risk Management.

The “Interoperable EU Risk Management Framework” describes and evaluates the interoperability features for prominent risk management frameworks and methods, by employing a four-level scale to evaluate their interoperability level.

The features assessed to evaluate the interoperability level include the approach used by the RM method (i.e. to whether it is assetbased or scenario-based), whether risk assessment is quantitative or qualitative, as well as other characteristics such as the use of asset taxonomies, valuation methods, the cataloguing of threats and vulnerabilities, the method of risk calculation etc. It also provides an overview of possible collaborative combinations between them.



Characteristics	Parameters to Check
Asset Taxonomy	Does the framework or methodology use or describe specific categories of assets?
	Is the taxonomy used modifiable?
	Can the analyst introduce new categories of assets or import taxonomies from other sources?
Asset Valuation	Does the framework or methodology use or describe specific guidelines for the valuation of assets (i.e. scale and criteria for assessment of asset value and impact)?
	Are the proposed scales or criteria modifiable?
	Can the analyst introduce new scales or criteria?



Characteristics	Parameters to Check
Threat Catalogues	Does the framework or methodology use or describe specific threat catalogues and/or threat categories?
	Are the proposed threat catalogues and/or threat categories modifiable?
	Can the analyst introduce new threats and/or threat categories and import them from other sources?
Vulnerability Catalogues	Does the framework or methodology describe specific vulnerability catalogues and/or categories of vulnerabilities?
	Are the proposed vulnerability catalogues and/or categories of vulnerabilities modifiable?
	Can the analyst introduce new vulnerabilities and/or categories of vulnerabilities and import them from other sources?
Risk Calculation	Does the framework or methodology describe specific guidelines for the calculation of risk (i.e. formulas, scale, matrix)?
	Is the proposed calculation method modifiable?
	Can the analyst introduce or import (from other sources) new methods of calculation?
Measure Catalogues & Calculation of Residual Risk	Does the framework or methodology describe specific control catalogues and/or categories of controls?
	Are the proposed control catalogues and/or categories of controls modifiable?
	Can the analyst introduce new controls and/or categories of controls and import them from other sources?
	Is the Calculation of Residual Risk (either on a Calculation of Residual Risk formula or on an Impact of Measures formula) modifiable?

To read more: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

Number 5

Council of the European Union

Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values.

This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it ensures the free movement of AI-based goods and services crossborder, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

Artificial intelligence systems (AI systems) can be easily deployed in multiple sectors of the economy and society, including cross border, and circulate throughout the Union.

Certain Member States have already explored the adoption of national rules to ensure that artificial intelligence is safe and is developed and used in compliance with fundamental rights obligations.

Differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop, import or use AI systems.

A consistent and high level of protection throughout the Union should therefore be ensured, while divergences hampering the free circulation of AI systems and related products and services within the internal market should be prevented, by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market based on Article 114 of the Treaty on the Functioning of the European Union (TFEU).

To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

Artificial intelligence is a fast evolving family of technologies that can contribute to a wide array of economic and societal benefits across the entire spectrum of industries and social activities.

By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, education and training, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, and climate change mitigation and adaptation.

At the same time, depending on the circumstances regarding its specific application and use, artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial.

A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law.

To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services.

By laying down those rules and building on the work of the High-level Expert Group on Artificial Intelligence as reflecetd in the Guidelines for Trustworthy Artificial Intelligence in the EU, this Regulation supports the objective of the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence as stated by the European Council , and it ensures the protection of ethical principles, as specifically requested by the European Parliament.

Aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices.

Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child.

AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices.

The placing on the market, putting into service or use of certain AI systems materially distorting human behaviour, whereby physical or psychological harms are likely to occur, are particularly dangerous and should therefore be forbidden.

Such AI systems deploy subliminal components such as audio, image, video stimuli that persons cannot perceive as those stimuli are beyond human perception or other subliminal techniques that subvert or impair person's autonomy, decision-making or free choices in ways that people are not consciously aware of, or even if aware not able to control or resist, for example in cases of machine-brain interfaces or virtual reality.

In addition, AI systems may also otherwise exploit vulnerabilities of a specific group of persons due to their age, disability within the meaning of Directive (EU) 2019/882, or a specific social or economic situation that is likely to make those persons more vulnerable to exploitation such as persons living in extreme poverty, ethnic or religious minorities.

Such AI systems can be placed on the market, put into service or used with the objective to or the effect of materially distorting the behaviour of a person and in a manner that causes or is reasonably likely to cause physical or phycological harm to that or another person or groups of persons, including harms that may be accumulated over time.

The intention to distort the behaviour may not be presumed if the distortion results from factors external to the AI system which are outside of the control of the provider or the user, meaning factors that may not be reasonably foreseen and mitigated by the provider or the user of the AI system.

In any case, it is not necessary for the provider or the user to have the intention to cause the physical or psychological harm, as long as such harm results from the manipulative or exploitative AI-enabled practices.

The prohibitions for such AI practices are complementary to the provisions contained in Directive 2005/29/EC, notably that unfair commercial practices leading to economic or financial harms to consumers are prohibited under all circumstances, irrespective of whether they are put in place through AI systems or otherwise.

The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychological treatment of a mental disease or physical rehabilitation, when those practices are carried out in accordance with the applicable medical standards and legislation.

In addition, common and legitimate commercial practices that are in compliance with the applicable law should not in themselves be regarded as constituting harmful manipulative AI practices.

To read more: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf

Number 6

XLLing in Excel - threat actors using malicious add-ins

By Vanja Svajcer, Cisco Talos Intelligence Blog

- Microsoft is phasing out support for executing VBA macros in downloaded Office documents.

- Cisco Talos investigates another vector for introduction of malicious code to Microsoft Excel—malicious add-ins, specifically XLL files.

- Although XLL files were supported since early versions of Excel, including Excel 97, malicious actors started using it relatively recently.

- Currently, a significant number of advanced persistent threat actors and commodity malware families are using XLLs as an infection vector and this number continues to grow.

For decades, Microsoft Office applications have served as one of the most significant entry points for malicious code. Malicious actors have continued to utilize Visual Basic for Applications (VBA) macros, despite automatic warnings to users after opening Office documents containing code.

In addition to VBA macros, malicious actors, from cybercrime actors to state-sponsored groups, also exploited vulnerabilities in Office applications in order to launch malicious code without user intervention.

Over the years, ever since the first VBA malware was discovered at the end of the century, the cybersecurity community have been vocal in calling on Microsoft to introduce default behavior that will block execution of VBA macros if a document was downloaded or received from the internet.

Finally, this year in July, Microsoft started rolling out versions of Office applications which will block execution of any VBA macros by default.

The Office applications now go through a decision making process that is much stricter than before and do not even offer the user a possibility to run macros when a document has a so called Mark Of The Web (MOTW) tag, an alternate data stream that indicates a file has been downloaded from the internet.

Microsoft Office is the most popular office application package used by a large number of corporate and home users with many versions, licensed and unlicensed, still in use worldwide.

Although the change to block macros and not allow their execution through the Office application user interface will be a significant factor in the future, it will take a long time until old versions of Office–still capable of executing macros–are phased out.

Even if malicious actors continue targeting VBA macros in older Office versions, more and more high profile targets will start using new versions which will prevent attacks using documents containing VBA code.

Unfortunately, it would be naive to assume that Office will stop being targeted, now that VBA macros have been blocked. The purpose of this research is to identify other means of introducing third party code into Office applications which, perhaps, are already being used by malware authors.

To read more: https://blog.talosintelligence.com/xlling-in-excel-malicious-add-ins/

Number 7

CISA Releases Four Industrial Control Systems Advisories

There are 4 very important Industrial Control Systems (ICS) advisories from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) for security flaws affecting products from Siemens, GE Digital, and Contec.

1. Vendor: GE Digital.
Equipment: Proficy Historian.
Exploitable remotely/low attack complexity.
Vulnerabilities: Authentication Bypass using an Alternate Path or Channel, Unrestricted Upload of File with Dangerous Type, Improper Access Control, Weak Encoding for Password.

2. Vendor: Mitsubishi Electric.
Equipment: MELSEC iQ-F and iQ-R Series products.
Exploitable remotely.
Vulnerability: Predictable Seed in Pseudo-Random Number Generator (PRNG).

3. Vendor: Siemens.
Equipment: SINEC INS.
Exploitable remotely/low attack complexity.
Vulnerabilities: OS Command Injection, Inadequate Encryption Strength, Out-of-bounds Write, HTTP Request Smuggling, Inadequate Encryption Strength, Use of Insufficiently Random Values, Authentication Bypass by Spoofing, Path Traversal, Command Injection

4. Vendor: Contec
Equipment: CONPROSYS HMI System (CHS)
Exploitable remotely/low attack complexity.
Vulnerability: OS Command Injection, Use of Default Credentials, Use of Password Hash Instead of Password for Authentication, Cross-site Scripting, Improper Access Control.

To read more: https://www.cisa.gov/uscert/ncas/current-activity/2023/01/17/cisa-releases-four-industrial-control-systems-advisories

Number 8

Ransomware-as-a-service (RaaS) - Cybercriminals stung as HIVE infrastructure shut down

Europol supported German, Dutch and US authorities to shut down the servers and provide decryption tools to victims

Europol supported the German, Dutch and US authorities in taking down the infrastructure of the prolific HIVE ransomware. This international operation involved authorities from 13 countries* in total. Law enforcement identified the decryption keys and shared them with many of the victims, helping them regain access to their data without paying the cybercriminals.

* Canada – Royal Canadian Mounted Police (RCMP) & Peel Regional Police
France: National Police (Police Nationale)
Germany: Federal Criminal Police Office (Bundeskriminalamt) and Police Headquarters Reutlingen – CID Esslingen (Polizei BW)
Ireland: National Police (An Garda Síochána)
Lithuania: Criminal Police Bureau (Kriminalinės Policijos Biuras)
Netherlands – National Police (Politie)
Norway: National Police (Politiet)
Portugal: Judicial Police (Polícia Judiciária)
Romania: Romanian Police (Poliţia Română – DCCO)
Spain: Spanish Police (Policía Nacional)
Sweden: Swedish Police (Polisen)
United Kingdom – National Crime Agency
USA – United States Secret Service, Federal Bureau of Investigations

In the last year, HIVE ransomware has been identified as a major threat as it has been used to compromise and encrypt the data and computer systems of large IT and oil multinationals in the EU and the USA. Since June 2021, over 1 500 companies from over 80 countries worldwide have fallen victim to HIVE associates and lost almost EUR 100 million in ransom payments.

Affiliates executed the cyberattacks, but the HIVE ransomware was created, maintained and updated by developers. Affiliates used the double extortion model of ‘ransomware-as-a-service’; first, they copied data and then encrypted the files.

Then, they asked for a ransom to both decrypt the files and to not publish the stolen data on the Hive Leak Site. When the victims paid, the ransom was then split between affiliates (who received 80 %) and developers (who received 20 %).

Other dangerous ransomware groups have also used this so-called ransomware-as-a-service (RaaS) model to perpetrate high-level attacks in the last few years. This has included asking for millions of euros in ransoms to decrypt affected systems, often in companies maintaining critical infrastructures.

Since June 2021, criminals have used HIVE ransomware to target a wide range of businesses and critical infrastructure sectors, including government facilities, telecommunication companies, manufacturing, information technology, and healthcare and public health.

In one major attack, HIVE affiliates targeted a hospital, which led to severe repercussions about how the hospital could deal with the COVID-19 pandemic. Due to the attack, this hospital had to resort to analogue methods to treat existing patients, and was unable to accept new ones.

The affiliates attacked companies in different ways. Some HIVE actors gained access to victim's networks by using single factor logins via Remote Desktop Protocol, virtual private networks, and other remote network connection protocols.

In other cases, HIVE actors bypassed multifactor authentication and gained access by exploiting vulnerabilities. This enabled malicious cybercriminals to log in without a prompt for the user's second authentication factor by changing the case of the username.

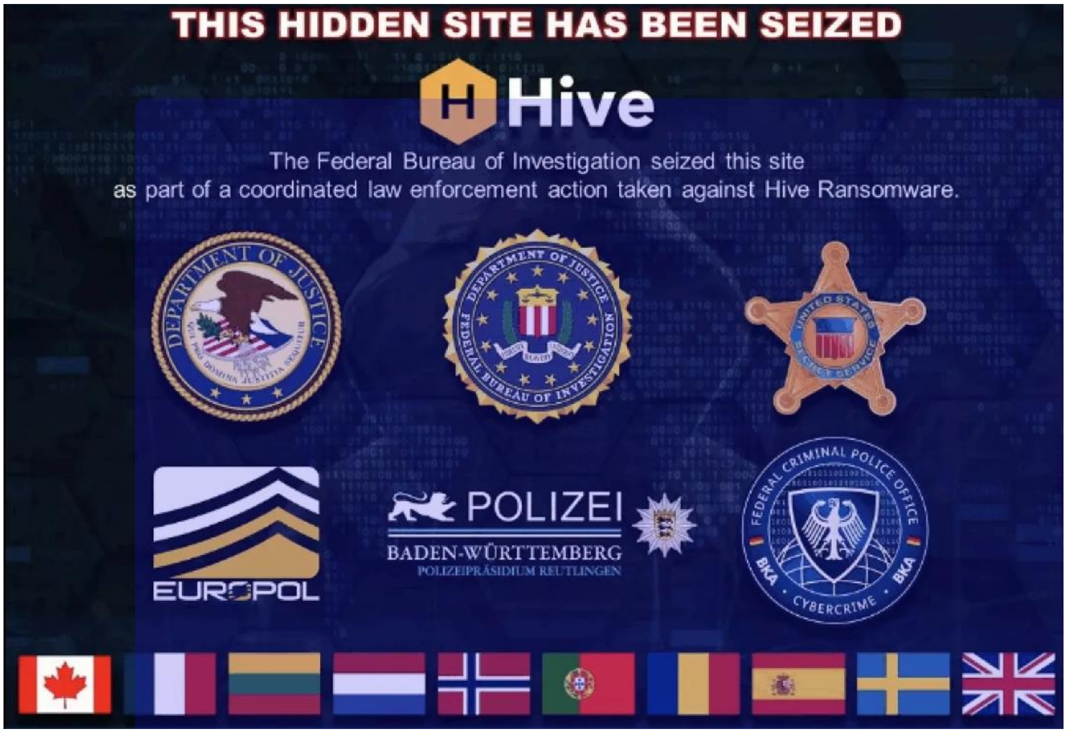
Some HIVE actors also gained initial access to victim's networks by distributing phishing emails with malicious attachments and by exploiting the vulnerabilities of the operating systems of the attacked devices.

About EUR 120 million saved thanks to mitigation efforts

Europol streamlined victim mitigation efforts with other EU countries, which prevented private companies from falling victim to HIVE ransomware.

Law enforcement provided the decryption key to companies which had been compromised in order to help them decrypt their data without paying the ransom. This effort has prevented the payment of more than USD 130 million or the equivalent of about EUR 120 million of ransom payments.

Europol facilitated the information exchange, supported the coordination of the operation and funded operational meetings in Portugal and the Netherlands. Europol also provided analytical support linking available data to various criminal cases within and outside the EU, and supported the investigation through cryptocurrency, malware, decryption and forensic analysis.



THIS HIDDEN SITE HAS BEEN SEIZED

Hive

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

DEPARTMENT OF JUSTICE
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
EUROPOL
POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM REUTLINGEN
FEDERAL CRIMINAL POLICE OFFICE
BKA
CYBERCRIME

On the action days, Europol deployed four experts to help coordinate the activities on the ground.

Europol supported the law enforcement authorities involved by coordinating the cryptocurrency and malware analysis, cross-checking operational information against Europol's databases, and further operational analysis and forensic support.

Analysis of this data and other related cases is expected to trigger further investigative activities.

The Joint Cybercrime Action Taskforce (J-CAT) at Europol also supported the operation.

This standing operational team consists of cybercrime liaison officers from different countries who work on high-profile cybercrime investigations.

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime, and other serious and organized crime forms.

Europol also works with many non-EU partner states and international organisations.

From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

The European Multidisciplinary Platform Against Criminal Threats (EMPACT) tackles the most important threats posed by organised and serious international crime affecting the EU. EMPACT strengthens intelligence, strategic and operational cooperation between national authorities, EU institutions and bodies, and international partners. EMPACT runs in four-year cycles focusing on common EU crime priorities.

To read more: https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down#empact

Number 9

U.S. Department of Justice Disrupts Hive Ransomware Variant

FBI Covertly Infiltrated Hive Network, Thwarting Over $130 Million in Ransom Demands

The Justice Department announced its months-long disruption campaign against the Hive ransomware group that has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure.

Since late July 2022, the FBI has penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay $130 million in ransom demanded.

Since infiltrating Hive's network in July 2022, the FBI has provided over 300 decryption keys to Hive victims who were under attack. In addition, the FBI distributed over 1,000 additional decryption keys to previous Hive victims.

Finally, the department announced today that, in coordination with German law enforcement (the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen) and the Netherlands National High Tech Crime Unit, it has seized control of the servers and websites that Hive uses to communicate with its members, disrupting Hive's ability to attack and extort victims.

"Last night, the Justice Department dismantled an international ransomware network responsible for extorting and attempting to extort hundreds of millions of dollars from victims in the United States and around the world," said Attorney General Merrick B. Garland. "Cybercrime is a constantly evolving threat. But as I have said before, the Justice Department will spare no resource to identify and bring to justice, anyone, anywhere, who targets the United States with a ransomware attack. We will continue to work both to prevent these attacks and to provide support to victims who have been targeted. And together with our international partners, we will continue to disrupt the criminal networks that deploy these attacks."

"The Department of Justice's disruption of the Hive ransomware group should speak as clearly to victims of cybercrime as it does to perpetrators," said Deputy Attorney General Lisa O. Monaco. "In a 21st century cyber stakeout, our investigative team turned the tables on Hive, swiping their decryption keys, passing them to victims, and ultimately averting more than $130 million dollars in ransomware payments. We will continue to strike back against cybercrime using any means possible and place victims at the center of our efforts to mitigate the cyber threat."

"The coordinated disruption of Hive's computer networks, following months of decrypting victims around the world, shows what we can accomplish by combining a relentless search for useful technical information to share with victims with investigation aimed at developing operations that hit our adversaries hard," said FBI Director Christopher Wray. "The FBI will continue to leverage our intelligence and law enforcement tools, global presence, and partnerships to counter cybercriminals who target American business and organizations."

"Our efforts in this case saved victims over a hundred million dollars in ransom payments and likely more in remediation costs," said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department's Criminal Division. "This action demonstrates the Department of Justice's commitment to protecting our communities from malicious hackers and to ensuring that victims of crime are made whole. Moreover, we will continue our investigation and pursue the actors behind Hive until they are brought to justice."

"Cybercriminals utilize sophisticated technologies to prey upon innocent victims worldwide," said U.S. Attorney Roger Handberg for the Middle District of Florida. "Thanks to the exceptional investigative work and coordination by our domestic and international law enforcement partners, further extortion by HIVE has been thwarted, critical business operations can resume without interruption, and millions of dollars in ransom payments were averted."

Since June 2021, the Hive ransomware group has targeted more than 1,500 victims around the world and received over $100 million in ransom payments.

Hive ransomware attacks have caused major disruptions in victim daily operations around the world and affected responses to the COVID-19 pandemic. In one case, a hospital attacked by Hive ransomware had to resort to analog methods to treat existing patients and was unable to accept new patients immediately following the attack.

Hive used a ransomware-as-a-service (RaaS) model featuring administrators, sometimes called developers, and affiliates.
RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with

which to operate it and then recruit affiliates to deploy the ransomware against victims. Affiliates identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment.

Hive actors employed a double-extortion model of attack. Before encrypting the victim system, the affiliate would exfiltrate or steal sensitive data. The affiliate then sought a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data. Hive actors frequently targeted the most sensitive data in a victim's system to increase the pressure to pay. After a victim pays, affiliates and administrators split the ransom 80/20. Hive published the data of victims who do not pay on the Hive Leak Site.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Hive affiliates have gained initial access to victim networks through a number of methods, including: single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols; exploiting FortiToken vulnerabilities; and sending phishing emails with malicious attachments.

For more information about the malware, including technical information for organizations about how to mitigate its effects, is available from CISA, visit https://www.cisa.gov/uscert/ncas/alerts/aa22-321a

Victims of Hive ransomware should contact their local FBI field office for further information.

The FBI Tampa Field Office, Orlando Resident Agency is investigating the case.

Trial Attorneys Christen Gallagher and Alison Zitron of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Chauncey Bratt for the Middle District of Florida are prosecuting the case.

The Justice Department also recognizes the critical cooperation of the German Reutlingen Police Headquarters-CID Esslingen, the German Federal Criminal Police, Europol, and the Netherlands Politie, and significant assistance was provided by the U.S. Secret Service, U.S. Attorney's Office for the Eastern District of Virginia, and U.S. Attorney's Office for the Central District of California. The Justice Department's Office of International Affairs and the Cyber Operations International Liaison also provided significant assistance. Additionally, the following foreign law enforcement authorities provided substantial assistance and support: the Canadian Peel Regional Police and Royal Canadian Mounted

Police, French Direction Centrale de la Police Judiciaire, Lithuanian Criminal Police Bureau, Norwegian National Criminal Investigation Service in collaboration with the Oslo Police District, Portuguese Polícia Judiciária, Romanian Directorate of Countering Organized Crime, Spanish Policia Nacional, Swedish Police Authority, and the United Kingdom's National Crime Agency.

Number 10

Daring to know in times of uncertainty and structural shifts

Klaas Knot, President of the Netherlands Bank and Chair of the Financial Stability Board, at the 11th ILF Conference on the Future of the Financial Sector "The Next Systemic Financial Crisis – Where Might it Come From?": Financial Stability in a Polycrisis World, at the Goethe University's Law and Finance Institute, Frankfurt am Main.

Hello everyone.

This beautiful wood engraving (Note 1) depicts a scene in 1794. You can see four well-dressed men, sitting in a flourishing garden in Jena – a city a few hours east from Frankfurt.

Note 1 "Schiller, Wilhelm and Alexander von Humboldt and Goethe in Jena"(Refers to an external site) (Event date: 1794, image date: 1860). Wood engraving after drawing by Andreas Müller (1831-1901).

The four men are sitting around a table, filled with wine and grapes– and they appear to be engaged in a civilized discussion. The four men on the drawing are the brothers Wilhelm and Alexander von Humboldt, respectively statesman and explorer, the poet Friedrich von Schiller and, of course, scientist, writer and poet, Johan Wolfgang von Goethe.

The four of them were the intellectual fab four of late 18th century Germany. They strongly believed in the powers of reason – as opposed to royal decrees or religious dogmas. They strongly believed that individuals were to be enlightened – through science, art, and literature. They strongly believed in "sapere aude" – in daring to know.

I was asked to talk about systemic risks today. More precisely, about where the next systemic financial crisis might come from. And truth be told – this is hard to say. We can't predict that with any reliability. One only needs to recall the way that the covid pandemic hit us to know that a crisis can emerge unexpectedly. This is exactly why predicting the next crisis is not what we aim to do at the Financial Stability Board (FSB).

Instead of predicting, our aim is to approach financial stability with a different way of thinking. Financial stability is the capacity of the global financial system to withstand shocks, by containing the risk of disruptions in the financial intermediation process that would be severe enough to adversely impact the real economy.

In short: our work is about enhancing the resilience of the global financial system. So that, when the next crisis materialises, the system as a whole can cope with it.

In order to increase that resilience, we try to know as much as possible about the vulnerabilities in our financial system. And we do this by relying on the powers of reason, logic, cooperation and data. In other words, by following the brothers von Humboldt, Friedrich von Schiller, and Johan Wolfgang von Goethe in sapere aude.

So how do we go about that?

To increase the resilience of the global financial system and to enhance financial stability, we rely on the FSB's financial stability surveillance framework. Let me start by walking you through this framework, and then I will illustrate how we apply it.

The FSB's financial stability framework is based on four guiding principles.

First, we need to identify the vulnerabilities that may threaten global financial stability. I say 'vulnerabilities' instead of 'shocks' or 'risks'. That is intentional.

The pandemic is a shock. The war in Ukraine is a shock. A rapid shift in financial market conditions would be a shock. Shocks are by definition unpredictable – so they don't offer a solid starting point for financial stability policy. Risk – that is the risk of a shock large enough to have a financial stability impact – is similarly very difficult to assess.

Vulnerabilities, on the other hand, can usually be measured, at least to a certain extent. Think for instance about the build-up of imbalances, like a rise in leverage during a credit boom. And so, they do offer a starting point for financial stability policy – policy that is aimed at reducing these vulnerabilities. Through this approach we can mitigate potential systemic disruption, once a shock hits our global, highly interconnected financial system.

And so, in the spirit of Alexander von Humboldt, who measured and mapped large parts of the world, we, in turn, try to map and measure global vulnerabilities – rather than the shocks that may or may not materialise.

Second, once mapped and measured, we monitor these vulnerabilities, taking into account the potential interactions between them. We also deploy a forward-looking perspective, by considering emerging vulnerabilities in addition to current ones. It is better to prevent vulnerabilities from growing in the first place, rather than having to reduce them once they already pose a global threat.

Our third guiding principle is that we recognise the differences among countries. The FSB's membership reflects the diversity of our global financial system, with members from both emerging market and advanced economies. And these differences are reflected in our assessment of vulnerabilities. We fully recognise that some vulnerabilities may be more relevant for emerging market economies, and others for advanced economies, or for different sets of jurisdictions.

For example, the urgency policymakers ascribe to some of the risks relating to crypto-assets and crypto-markets differs across countries. In some economies, the most pressing concern is the potential loss of monetary sovereignty. In other economies, the risks of money laundering and fraud are perceived to be more urgent.

The fourth and final guiding principle, is that the FSB leverages on this diversity of its membership. There lies tremendous strength in that diversity. FSB members not only come from different kinds of economies, but they are also represented by different kinds of authorities: ministries of finance, central banks, and securities and market authorities. Our members also include global standard-setting bodies and international organisations. Many of those members carry out and publish financial stability assessments. The FSB's vulnerabilities assessment therefore builds on those analyses.

With these four guiding principles, I have given you a brief and mainly theoretical outline of the FSB's financial stability surveillance framework. I hope that this approach, this way of thinking about how to enhance the resilience of the global financial system, provides you with some stimulus for today's discussions.

But what does it look like when we actually apply this framework? To illustrate this, allow me to touch on several of the key FSB priorities that are also on your agenda today.

First, I will focus on the cyclical vulnerabilities that emerge from the current outlook. The combination of rising inflation, tightening financial conditions and the fallout from Russia's invasion of Ukraine has led to a synchronised slowdown in global economic activity.

This is occurring against a backdrop of high levels of debt of households, non-financial corporates and sovereigns. The latter implies that some governments have limited fiscal space to provide additional targeted policy support. And given the increases in inflation, central banks also have less policy space to react to financial stability shocks.

Although this outlook is challenging, so far the global banking system has shown itself to be resilient. Global financial markets have largely coped in an orderly manner, with limited and temporary support when necessary. And systemic financial institutions have shown resilience to market strains – in large part due to the financial reforms, following the 2008 Global Financial Crisis, that were coordinated through the FSB.

However, there is no room for complacency. Financial institutions and market participants have not experienced sharply rising interest rates for a long time. Very low interest rates may have become embedded in business models, making the adjustment to a world of higher rates challenging. Companies and households that have borrowed money will also need to adjust to higher interest payments, and problems may materialise only with a lag.

So, we need to remain vigilant. A deterioration of banks' asset quality may still occur, and other vulnerabilities, like the ones on today's agenda, need to be monitored closely. Some of these vulnerabilities may have been previously prevented from materialising by authorities' COVID-19 support measures. But now these measures are being lifted. So it is important to address debt overhang issues of non-financial corporates, and to respond to potential issues of underinvestment due to excessive indebtedness or misallocation of resources to unviable companies.

All of these are what I would call cyclical vulnerabilities.

But, more fundamentally, we also need to be wary of vulnerabilities that stem from structural shifts in the global financial system.

So allow me to say a few words on three structural shifts that the FSB is currently focusing on, and the associated vulnerabilities. It is, of course, no coincidence that the topics of today's panels overlap with many of the FSB's priorities.

First – the structural shift in the provision of finance from banks to non-banks.

In our Global Monitoring Report on non-bank financial intermediation, from December 2022, we highlighted that the NBFI sector reached 239 trillion US dollars in 2021. If a number on that scale is hard to put into context, a more telling figure is perhaps that the NBFI sector increased its relative share of total global financial assets to 49% in 2021, compared with 42% in 2008. Almost half of all global financial assets are now being intermediated by non-banks.

While diversifying the sources of credit can make the global economy more resilient, the growth in NBFI has exposed important vulnerabilities in the non-bank sector.

We have seen the problems that these vulnerabilities can cause several times in recent years: for instance, the 'dash for cash' episode during the onset of the pandemic, the strains in commodity markets last year, and more recently the challenges faced by UK pension funds.

Thankfully, these strains have proved temporary, but only after massive official sector interventions were deployed. These examples therefore serve as a warning to remain vigilant on the recurring themes of leverage, including hidden leverage, liquidity mismatches, and data gaps.

The FSB's NBFI work programme and policy proposals aim to address these vulnerabilities. In 2023, we will continue to focus on some key vulnerabilities within the sector. Apart from monitoring systemic risk in NBFI, we will review the effectiveness of our money market funds policy proposals from 2021; revise our recommendations from 2017 on liquidity mismatches in open-ended funds; and conduct follow-up work on margining practices and hidden leverage in NBFI.

A second structural shift we have witnessed, is the digitalisation of finance. This comes in many shapes and forms, but I will focus on the rapidly developing crypto-asset ecosystem. Crypto-asset markets and activities bear a multitude of risks and vulnerabilities. While the technology behind crypto-assets is often being promoted as game-changing, the vulnerabilities associated with them are in fact quite similar to those we know from traditional finance.

Liquidity mismatches, hidden leverage, and counterparty credit risk are all examples of well-known financial risks that have also materialised in crypto-asset markets in the past year. National regulatory authorities have recognized that these activities are in essence financial activities and have begun regulating them. This is challenging for national authorities, however, because crypto-asset markets are inherently global in reach.

So, in the presence of structural vulnerabilities and in the absence of globally consistent regulation, the FSB is concerned crypto-asset markets may soon pose a challenge to global financial stability.

The FSB therefore concluded that crypto-asset activities and markets must be subject to effective regulation and oversight commensurate to the risks they pose, both at the domestic and international levels.

To this end, the FSB proposed a comprehensive global framework for the effective regulation of crypto-asset activities, including stablecoins, in October last year. This framework embeds the principle of 'same activity, same risk, same regulation'. Finalising these recommendations and monitoring their effective implementation across all jurisdictions will be a priority for the FSB in 2023.

Of course, the FSB does not operate alone. Just like in the traditional financial sector, there is a myriad of functions that the crypto asset ecosystem covers or otherwise touches. So it is key to have solid cooperation between the different standard setting bodies, all with their different mandates.

Third – it is impossible to talk about systemic risk without mentioning one of the most fundamental challenges of our time: climate change.

This third structural shift is not on the agenda today, but the events of the past year have again emphasised the importance of addressing these vulnerabilities. The volatility in energy markets, exposures to hard-to-predict physical risks and the challenges of the transition to net zero are all examples of vulnerabilities that have an impact on the financial sector.

So addressing the financial risks stemming from climate change is, and will remain, high on the FSB agenda. One way we are working on this, is with our roadmap. With that roadmap, we are coordinating the international efforts to address climate-related financial vulnerabilities. It consists of four key elements: disclosure, data, vulnerability analysis and supervisory and regulatory tools.

One of the main priorities is the reliability and consistency of data, because that is what good risk management starts with. A key priority for this year is the finalisation and implementation of a global climate-related disclosure standard. Other priorities are analysing the use of transition planning and the improvement of our framework for monitoring climate-related vulnerabilities.

Let me wrap up.

NBFI, crypto and climate-related financial risks – these are just three priorities for the FSB and the global financial system I wanted to touch on today.

But for every risk or vulnerability we focus on, be it cyclical or structural, the same principle applies: the FSB diligently maps, measures and monitors all threats to the stability of our global financial system.

We provide a global, cross-border, cross-sectoral and forward-looking perspective on the vulnerabilities we identify. And we do this by drawing on the collective perspective of the broad membership of the FSB.

And this way of working, fearless and in the spirit of “sapere aude”, does not allow me to predict where the next systemic crisis might come from, but it does allow us to enhance the resilience of the global financial system, to whatever may come its way.

In that spirit, the FSB decides where coordinated action is required, monitors the effects of its actions, and assesses where further adjustments are needed. Or, as Goethe said: "Knowing is not enough; we must apply. Willing is not enough; we must do.”

The four men in the wood engraving I talked about at the beginning continue to be an inspiration today. Each with their own merits – and together, as an example of how reason advances humankind.
After Friedrich von Schiller’s death, and as an introduction to the correspondence between the two men, Wilhelm von Humboldt wrote an essay on his close association with the famous poet. And in that essay, he stresses the importance Schiller attached to conversation – to how conversation, expressing ideas, exchanging views, ultimately leads to deeper understanding.

To how conversation, you could say, embodies “sapere aude”. Or in Schiller’s words: "Erkühne dich, weise zu sein".

And this is just the kind of conversation I hope you will have today.

Thank you.

To read more: https://www.dnb.nl/en/general-news/speech-2023/speech-klaas-knot-daring-to-know-in-times-of-uncertainty-and-structural-shifts/

Number 11

Information Laundering via Baltnews on Telegram

Information has long been used as a foreign policy tool by the Kremlin. Most recently the Russian attack on Ukraine has prompted a new wave of research into the way pro-Kremlin messaging is spread in Western countries and to what effect.

This study examines a specific form of information influence campaigns (IICs): information laundering (IL). IL is a compilation of deception techniques and thus has the potential to change readers' beliefs and attitudes.

Overall, the study presents a refined, systematic, and reproducible way to identify which current IL attempts target the audience of a specific Telegram channel, and which networks of websites are behind these attempts. It also asks which potential framing biases the audience could be influenced by and with what strategic aim.

More specifically the Baltnews Telegram channel serves as a gateway systematically leading to IL attempts that are geared to reach a Russian-speaking audience in the Baltic States.

A distinction was drawn between the overt amplification of content stemming from Kremlin-official sources and the covert distortion of content from Western news outlets via a network of intermediary websites.

In total, 355 posts were screened for cases of IL, of which at least 39 showed signs of taking part in IL processes. These 39 cases alone are linked to the activity of 444 Russian-domain or Kremlin-official websites which were engaged in distorting information by Western news outlets.

First, the techniques used to manipulate information during IL processes were uncovered and the network of interacting websites behind selected IL attempts were mapped.

Second, the themes of the 39 IL attempts tied to Western media were compared to the way Kremlin-official sources were treated by the Baltnews Telegram channel in 66 cases.

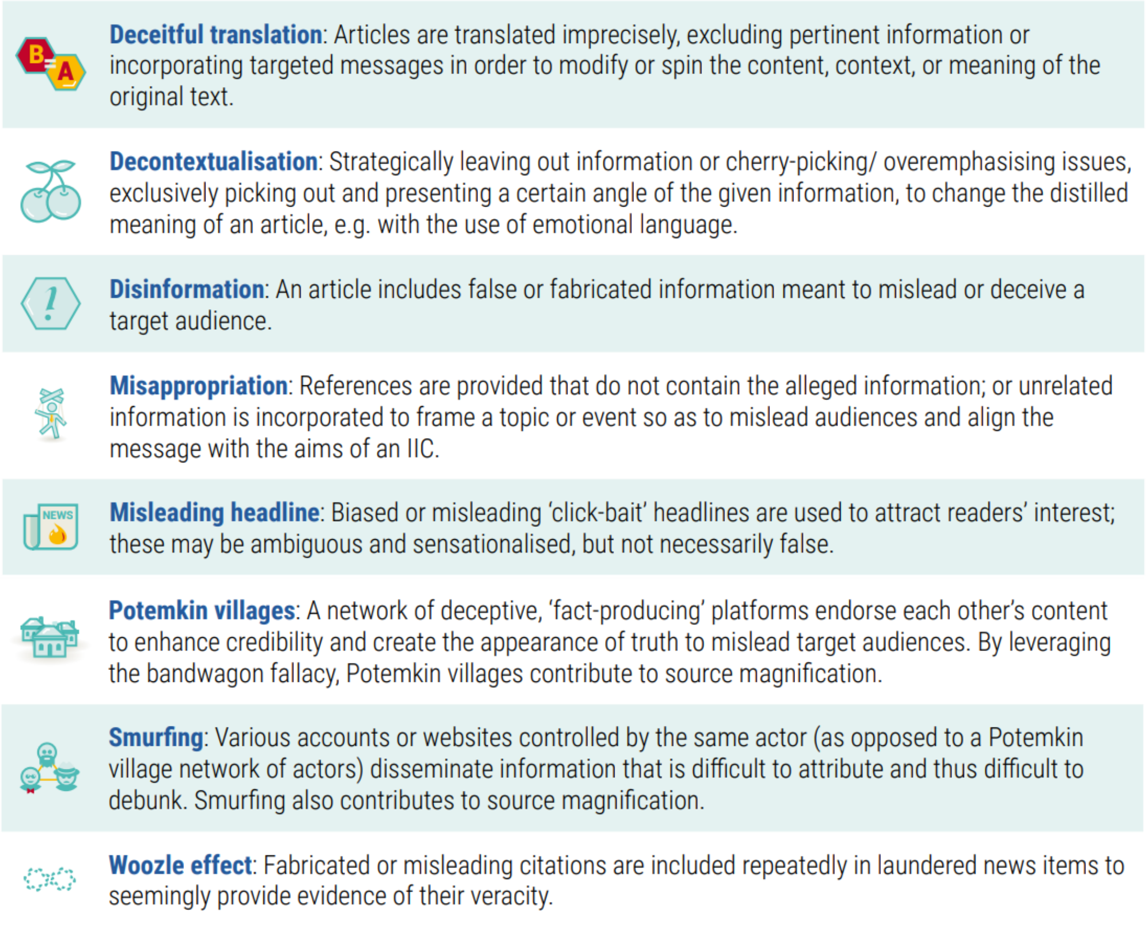
Coverage and framing biases as well as their potential strategic aims were identified. The study thereby demonstrates ways to analyse the different biases that IICs make use of, as well as their intended influence.

The investigation reveals that, apart from increasingly amplifying Kremlin-official media since February 2022, like Sputnik, RT, or RIA Novosti, the Baltnews Telegram channel has also increasingly spread cases of IL, by nature a more covert technique of audience manipulation.

In the process of IL, information of Western news articles was manipulated and spread on Russian-domain websites, later reaching NordicBaltic websites and the Baltnews Telegram channel.

The study thus demonstrates how Russian-domain and Kremlin-official media systematically draw from and amplify content published in the Western press that can be made to align with their own messaging as part of IICs.

Spreading IL attempts via Telegram might constitute a mechanism of Russian state-sponsored media to evade sanctions.



Deceitful translation: Articles are translated imprecisely, excluding pertinent information or incorporating targeted messages in order to modify or spin the content, context, or meaning of the original text.

Decontextualisation: Strategically leaving out information or cherry-picking/ overemphasising issues, exclusively picking out and presenting a certain angle of the given information, to change the distilled meaning of an article, e.g. with the use of emotional language.

Disinformation: An article includes false or fabricated information meant to mislead or deceive a target audience.

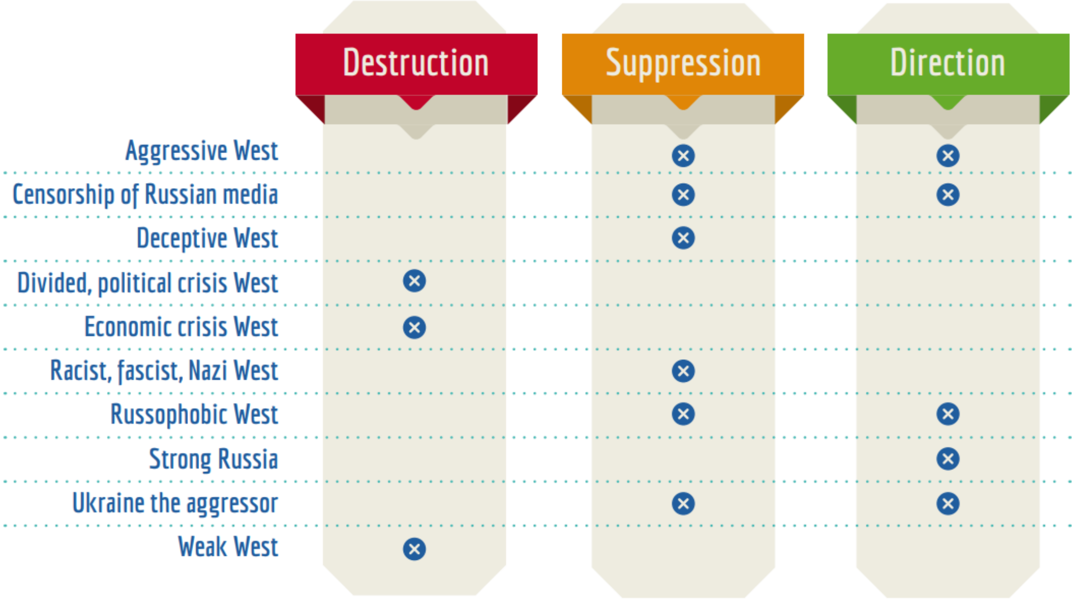
Misappropriation: References are provided that do not contain the alleged information; or unrelated information is incorporated to frame a topic or event so as to mislead audiences and align the message with the aims of an IIC.

Misleading headline: Biased or misleading 'click-bait' headlines are used to attract readers' interest; these may be ambiguous and sensationalised, but not necessarily false.

Potemkin villages: A network of deceptive, 'fact-producing' platforms endorse each other's content to enhance credibility and create the appearance of truth to mislead target audiences. By leveraging the bandwagon fallacy, Potemkin villages contribute to source magnification.

Smurfing: Various accounts or websites controlled by the same actor (as opposed to a Potemkin village network of actors) disseminate information that is difficult to attribute and thus difficult to debunk. Smurfing also contributes to source magnification.

Woozle effect: Fabricated or misleading citations are included repeatedly in laundered news items to seemingly provide evidence of their veracity.



	Destruction	Suppression	Direction
Aggressive West		⊗	⊗
Censorship of Russian media		⊗	⊗
Deceptive West		⊗	
Divided, political crisis West	⊗		
Economic crisis West	⊗		
Racist, fascist, Nazi West		⊗	
Russophobic West		⊗	⊗
Strong Russia			⊗
Ukraine the aggressor		⊗	⊗
Weak West	⊗		

To read more: https://stratcomcoe.org/publications/information-laundering-via-baltnews-on-telegram-how-russian-state-sponsored-media-evade-sanctions-and-narrate-the-war/257

INFORMATION LAUNDERING VIA BALTNEWS ON TELEGRAM:
How Russian State-Sponsored Media Evade Sanctions and Narrate the War

Number 12

Achieving Foundational Security for Food Systems

New DARPA effort seeks advanced threat-detection and warning capabilities for crop defense

U.S. cereal crops such as corn, rice, and wheat feed hundreds of millions of Americans and millions more around the world. Ensuring active defense of these and other staple food grasses is a critical national security priority.

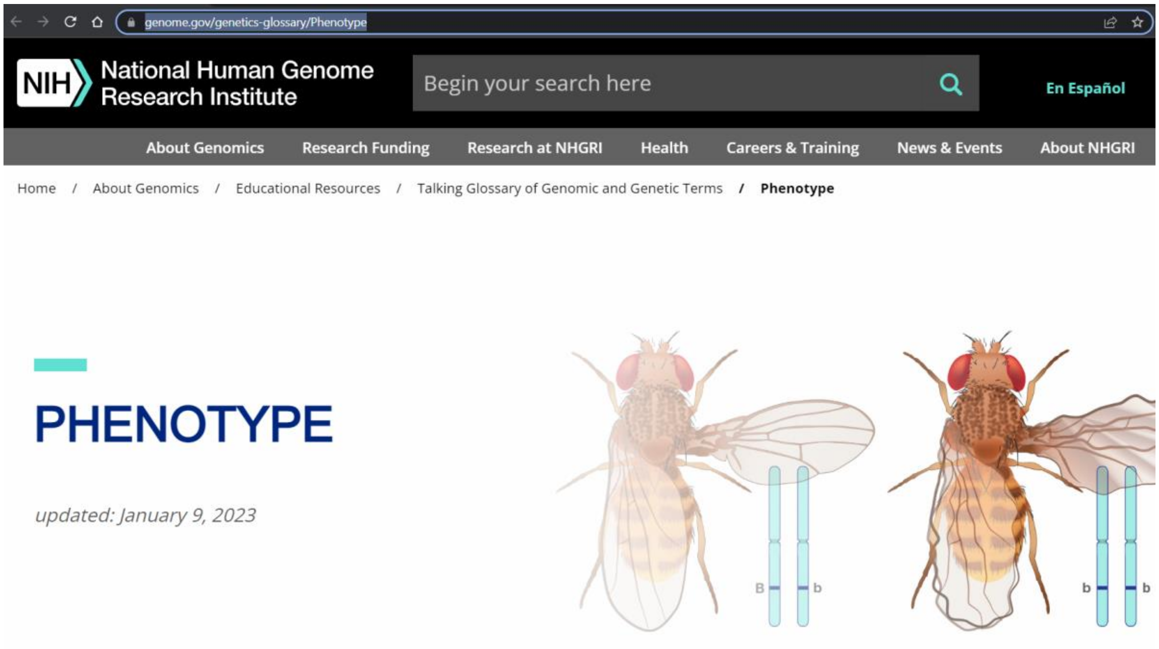
DARPA’s Foundational Security for Food Systems (FS2) program will explore a pathway-based approach to provide advanced threat detection and warning of crop damage irrespective of the triggering agent. FS2 will conduct research to test the feasibility of applying this approach for defense of cereal crops, specifically rice and corn.

“The FS2 program will test the idea that there may be only very few pathways in cereal crops that, when activated, are capable of resulting in sufficient damage to be of major concern,” said Molly Jahn, FS2 program manager in DARPA’s Defense Sciences Office.

“Similar to how a person can have any one of thousands of viruses long before certain common symptoms present, we're interested in finding the earliest signs those pathways are active before symptoms show up in cereal crops. FS2 will investigate the ability to create detection and warning protocols based on pathways with observable plant-level effects including signatures that are detectable remotely. Our vision with FS2 is to shift from agent-focused defenses to agent-agnostic signatures that reveal if damage of major concern is underway.”

FS2 will use rust fungi as a program test case. Rice is not susceptible to fungal rust pathogens; however, many other important cereal crops are, including corn. Despite this type of phenotypic variation between cereal species, many key genetic and biochemical pathways are widely conserved across members of the grass family. Because of their economic impact, cereal rust diseases are monitored using plant and field-level data during the growing season through snapshot Agriculture Department surveys, and are scouted via cultivation and harvest equipment, drones, smartphones, and other devices with cameras or sensors. FS2 aims to develop validated models to systematically identify earliest observable features of key damage pathways irrespective of the activating agent.

You may also visit: https://www.genome.gov/genetics-glossary/Phenotype



Home / About Genomics / Educational Resources / Talking Glossary of Genomic and Genetic Terms / **Phenotype**

PHENOTYPE

updated: January 9, 2023

FS2 is part of DARPA's Disruptioneering effort designed to rapidly explore bold and risky ideas with the goal of accelerating scientific discovery. The 18-month FS2 program comprises two phases. You may visit: https://www.darpa.mil/work-with-us/disruptioneering

The 10-month first phase addresses genetic modeling with the goal of demonstrating that it is possible to link plant-level observable variation via actual and inferred pathways in corn.

A second, eight-month phase aims to demonstrate whether it is possible to build a candidate explanatory pathways model that can link adverse plant-level observations of unknown origin in corn to candidate explanatory pathways. Maximum award value for each phase is $500,000 for total maximum award value of $1,000,000.

The FS2 program does not involve genetic modification of any organism. All research will be conducted in compliance with approved regulatory standards.
Interested proposers may learn more by attending the FS2 Information Session webcast on Jan. 17, 2023, from 3-4 p.m. ET. Registration details

are available here:
https://sam.gov/opp/046ffd42d3264b64b02d84e7c8eadea2/view

A program announcement for FS2 with full program details and instructions for submitting a proposal is expected to appear on SAM.gov prior to the information session.

To read more: https://www.darpa.mil/news-events/2023-01-03

Number 13

Wi-Fi Could Help Identify When You're Struggling to Breathe

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Wi-Fi routers continuously broadcast radio frequencies that your phones, tablets and computers pick up and use to get you online. As the invisible frequencies travel, they bounce off or pass through everything around them — the walls, the furniture and even you. Your movements, even breathing, slightly alter the signal's path from the router to your device.

Those interactions don't interrupt your internet connection, but they could signal when someone is in trouble. NIST has developed a deep learning algorithm, called BreatheSmart, that can analyze those minuscule changes to help determine whether someone in the room is struggling to breathe. And it can do so with already available Wi-Fi routers and devices. This work was recently published in IEEE Access.

In 2020 NIST scientists wanted to help doctors fight the COVID-19 pandemic. Patients were isolated; ventilators were scarce. Previous research had explored using Wi-Fi signals to sense people or movement, but these setups often required custom sensing devices, and data from these studies were very limited.

"As everybody's world was turned upside down, several of us at NIST were thinking about what we could do to help out," says Jason Coder, who leads NIST's research in shared spectrum metrology. "We didn't have time to develop a new device, so how can we use what we already have?"

Working with colleagues at the Office of Science and Engineering Labs (OSEL) in the FDA's Center for Devices and Radiological Health, Coder and research associate Susanna Mosleh advanced a new way to use existing Wi-Fi routers to measure the breathing rate of a person in the room.

In Wi-Fi, the "channel state information," or CSI, is a set of signals sent from the client (such as a cellphone or laptop) to the access point (such as the router).

The CSI signal sent by the client device is always the same, and the access point receiving the CSI signals knows what it should look like. But as the CSI signals travel through the environment, they get distorted as they bounce off things or lose strength. The access point analyzes the amount of distortion to adjust and optimize the link.

These CSI streams are small, less than a kilobyte, so it doesn't interfere with the flow of data over the channel. The team modified the firmware on the router to ask for these CSI streams more frequently, up to 10 times per second, to get a detailed picture of how the signal was changing.

They set up a manikin used to train medical professionals in an anechoic chamber with a commercial off-the-shelf Wi-Fi router and receiver.

This manikin is designed to replicate several breathing conditions, from normal respiration to abnormally slow breathing (called bradypnea), abnormally rapid breathing (tachypnea), asthma, pneumonia and chronic obstructive pulmonary diseases, or COPD.

What alters the Wi-Fi signal is the way the body moves as we breathe. Think of how your chest moves differently when you are wheezing or coughing, compared with breathing normally.

As the manikin "breathed," the movement of its chest altered the path traveled by the Wi-Fi signal. The team members recorded the data provided by the CSI streams. Although they collected a wealth of data, they still needed help to make sense of what they had gathered.

"This is where we can leverage deep learning," Coder said.

Deep learning is a subset of artificial intelligence, a type of machine learning that mimics humans' ability to learn from their past actions and improves the machine's ability to recognize patterns and analyze new data.

Mosleh worked on a deep learning algorithm to comb through the CSI data, understand it, and recognize patterns that indicated different breathing problems. The algorithm, which they named BreatheSmart, successfully classified a variety of respiratory patterns simulated with the manikin 99.54% of the time.

"Most of the work that's been done before was working with very limited data," Mosleh says. "We were able to collect data with a lot of simulated respiratory scenarios, which contributes to the diversity of the training set that was available to the algorithm."

There has been a lot of interest in using Wi-Fi signals for sensing applications, Coder says. He and Mosleh hope that app and software developers can use the process presented in the work as a framework to create programs to remotely monitor breathing.

"All the ways we're gathering the data is done on software on the access point (in this case, the router), which could be done by an app on a phone," Coder says. “This work tries to lay out how somebody can develop and test their own algorithm. This is a framework to help them get relevant information.”

To read more: https://www.nist.gov/news-events/news/2022/12/wi-fi-could-help-identify-when-youre-struggling-breathe

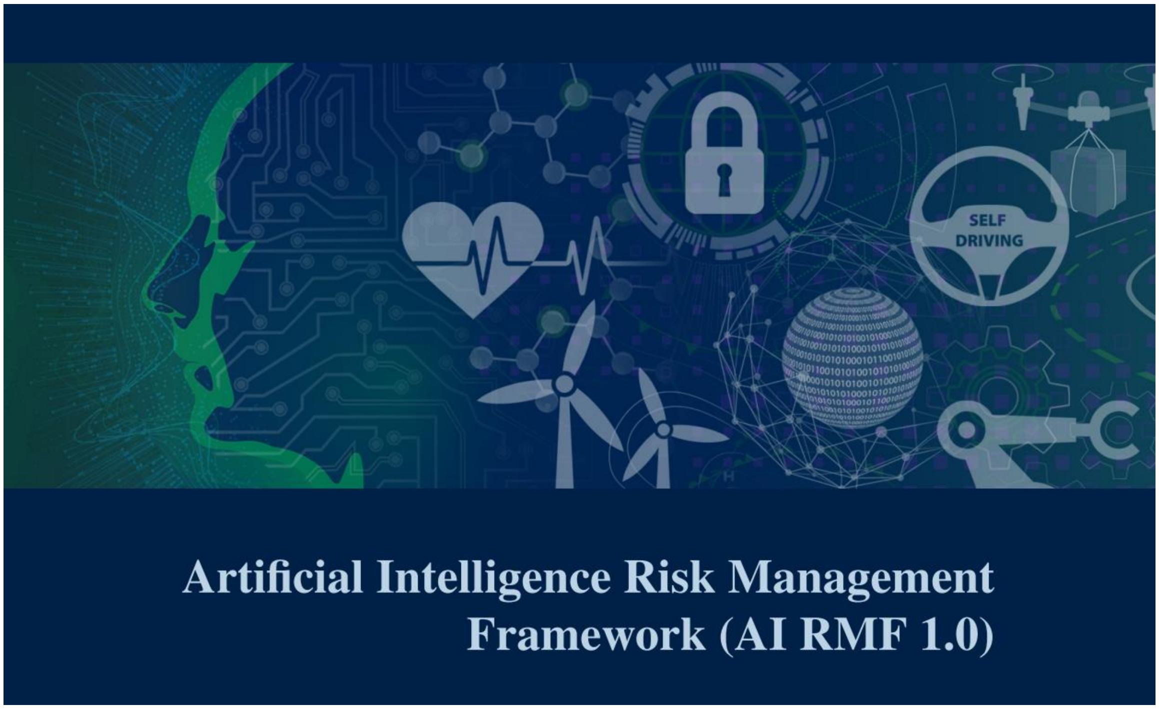
Number 14

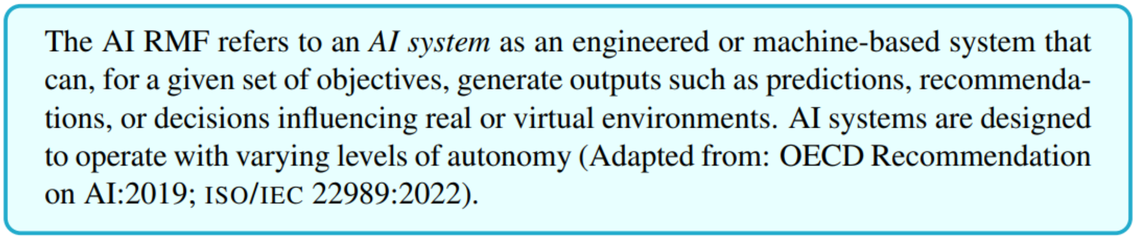
NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence

New guidance seeks to cultivate trust in AI technologies and promote AI innovation while mitigating risk.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has released its Artificial Intelligence Risk Management Framework (AI RMF 1.0), a guidance document for voluntary use by organizations designing, developing, deploying or using AI systems to help manage the many risks of AI technologies.




The AI RMF refers to an *AI system* as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy (Adapted from: OECD Recommendation on AI:2019; ISO/IEC 22989:2022).

The AI RMF follows a direction from Congress for NIST to develop the framework and was produced in close collaboration with the private and public sectors. It is intended to adapt to the AI landscape as technologies continue to develop, and to be used by organizations in varying degrees and capacities so that society can benefit from AI technologies while also being protected from its potential harms.

"This voluntary framework will help develop and deploy AI technologies in ways that enable the United States, other nations and organizations to enhance AI trustworthiness while managing risks based on our democratic values," said Deputy Commerce Secretary Don Graves. "It should accelerate AI innovation and growth while advancing — rather than restricting or damaging — civil rights, civil liberties and equity for all."

Compared with traditional software, AI poses a number of different risks. AI systems are trained on data that can change over time, sometimes significantly and unexpectedly, affecting the systems in ways that can be difficult to understand.

These systems are also "socio-technical" in nature, meaning they are influenced by societal dynamics and human behavior. AI risks can emerge from the complex interplay of these technical and societal factors, affecting people's lives in situations ranging from their experiences with online chatbots to the results of job and loan applications.

The framework equips organizations to think about AI and risk differently. It promotes a change in institutional culture, encouraging organizations to approach AI with a new perspective — including how to think about, communicate, measure and monitor AI risks and its potential positive and negative impacts.

The AI RMF provides a flexible, structured and measurable process that will enable organizations to address AI risks. Following this process for managing AI risks can maximize the benefits of AI technologies while reducing the likelihood of negative impacts to individuals, groups, communities, organizations and society.

The framework is part of NIST's larger effort to cultivate trust in AI technologies — necessary if the technology is to be accepted widely by society, according to Under Secretary for Standards and Technology and NIST Director Laurie E. Locascio.

"The AI Risk Management Framework can help companies and other organizations in any sector and any size to jump-start or enhance their AI risk management approaches," Locascio said. "It offers a new way to integrate responsible practices and actionable guidance to operationalize trustworthy and responsible AI. We expect the AI RMF to help drive development of best practices and standards."
The AI RMF is divided into two parts. The first part discusses how organizations can frame the risks related to AI and outlines the

characteristics of trustworthy AI systems. The second part, the core of the framework, describes four specific functions — govern, map, measure and manage — to help organizations address the risks of AI systems in practice. These functions can be applied in context-specific use cases and at any stages of the AI life cycle.

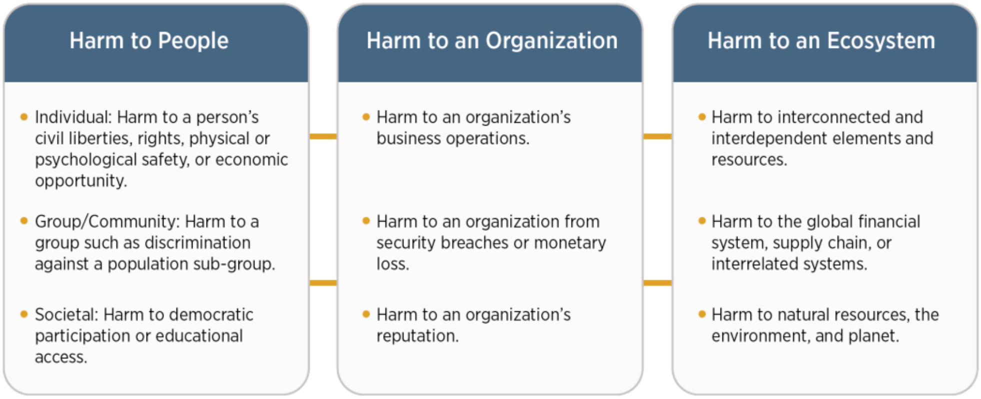
Working closely with the private and public sectors, NIST has been developing the AI RMF for 18 months. The document reflects about 400 sets of formal comments NIST received from more than 240 different organizations on draft versions of the framework. NIST today released statements from some of the organizations that have already committed to use or promote the framework.

The agency also today released a companion voluntary AI RMF Playbook, which suggests ways to navigate and use the framework.

NIST plans to work with the AI community to update the framework periodically and welcomes suggestions for additions and improvements to the playbook at any time. Comments received by the end of February 2023 will be included in an updated version of the playbook to be released in spring 2023.

To read more: https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve-trustworthiness-artificial

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf



Harm to People

- Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.
- Group/Community: Harm to a group such as discrimination against a population sub-group.
- Societal: Harm to democratic participation or educational access.

Harm to an Organization

- Harm to an organization's business operations.
- Harm to an organization from security breaches or monetary loss.
- Harm to an organization's reputation.

Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources.
- Harm to the global financial system, supply chain, or interrelated systems.
- Harm to natural resources, the environment, and planet.

Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.

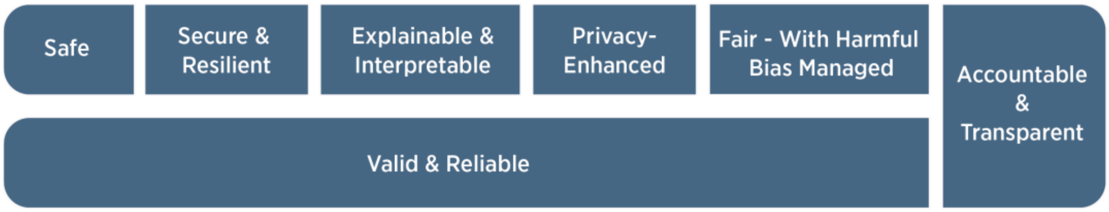

Safe
Secure & Resilient
Explainable & Interpretable
Privacy-Enhanced
Fair - With Harmful Bias Managed
Accountable & Transparent
Valid & Reliable

Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.

Number 15

VIDEO: A New Generation of AI Assistants

Perceptually-enabled Task Guidance prototypes demonstrated ability to help people complete recipes as a proxy to unfamiliar tasks

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In this video, DARPA program manager Dr. Bruce Draper describes the technology he thinks could usher in the next "do-it-yourself" revolution.

The Perceptually-enabled Task Guidance (PTG) program aims to develop virtual "task guidance" assistants that can work with different sensor platforms to help military personnel perform complex physical tasks and expand their skillsets.

Unlike today's AI assistants, PTG technology would be able to see what the user sees and hears what they hear by integrating with a microphone, a head-mounted camera, and displays like augmented reality (AR) headsets, to deliver accurate instructions.

The video: https://www.youtube.com/watch?v=pEM8gcRkA7M

PTG performers* recently demonstrated early successes of their prototypes by using the task of cooking recipes as a proxy for unfamiliar, more complex tasks, such as battlefield medical procedures, military equipment sustainment, and co-piloting aircraft.

*PTG Performers: Kitware (Columbia University; University of California, Berkeley; University of Texas at Austin); PARC (University of California, Santa Barbara; University of Rostock); Northeastern University (University of California, Santa Barbara; Stony Brook University); New York University; University of Texas at Dallas (University of California, Irvine; University of Florida); Stevens Institute of Technology (Purdue University; University of Michigan; University of Rochester); University of Florida (Northeastern University; Topos Institute; Texas A&M University; University of Arizona); Raytheon Technologies (Valkyries Austere Medical Solutions); Northrop Grumman (University of Central Florida); Red Shred (Third Insight); MIT Lincoln Laboratory

“Today the commercial sector is pursuing new, useful ways to present data to the user but it doesn’t go far enough,” said Draper. “The gamechanger with PTG would be having perceptually-driven AI interfaces that can make sense of the real world, react to whatever the user is doing and provide advice. I'm really impressed at how quickly performing teams are making progress toward the goals.”

To read more: https://www.darpa.mil/news-events/2023-01-25

Number 16

Some paragraphs from the EU Artificial Intelligence Act

Not the final text – It is the proposal from the Council of the European Union for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Council of the
European Union

(8) The notion of remote biometric identification system as used in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons typically at a distance, without their active involvement, through the comparison of a person's biometric data with the biometric data contained in a reference data repository, irrespectively of the particular technology, processes or types of biometric data used.

Such remote biometric identification systems are typically used to perceive (scan) multiple persons or their behaviour simultaneously in order to facilitate significantly the identification of a number of persons without their active involvement.

Such a definition excludes verification / authentication systems whose sole purpose would be to confirm that a specific natural person is the person he or she claims to be, as well as systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises.

This exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons.

In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays.

'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

(11) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union.

This is the case for example of an operator established in the Union that contracts certain services to an operator established outside the Union in relation to an activity to be performed by an AI system that would qualify as high-risk. In those circumstances, the AI system used by the operator outside the Union could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union.

To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and users of AI systems that are established in a **third country,** to the extent the output produced by those systems is used in the Union.

Nonetheless, to take into account existing arrangements and special needs for future cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and judicial cooperation with the Union or with its Member States.

Such agreements have been concluded bilaterally between Member States and third countries or between the European Union, Europol and other EU agencies and third countries and international organisations. Recipient Member States authorities and Union institutions, offices, bodies and bodies making use of such outputs in the Union remain accountable to ensure their use comply with Union law.

When those international agreements are revised or new ones are concluded in the future, the contracting parties should undertake the utmost effort to align those agreements with the requirements of this Regulation.

(18) The use of AI systems for ‘real-time’ remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of

a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights.

In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities.

(37) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living.

In particular, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services.

AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts.

Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by micro or small entreprises, as defined in the Annex of Commission Recommendation 2003/361/EC for their own use.

Natural persons applying for or receiving essential public assistance benefits and services from public authorities are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities.

If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, including whether beneficiaries are legitimately entitled to such benefits or services, those systems may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy.

Those systems should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons.

Finally, AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

AI systems are also increasingly used for risk assessment in relation to natural persons and pricing in the case of life and health insurance which, if not duly designed, developed and used, can lead to serious consequences for people's life and health, including financial exclusion and discrimination.

To ensure a consistent approach within the financial services sector, the above mentioned exception for micro or small enterprises for their own use should apply, insofar as they themselves provide and put into service an AI system for the purpose of selling their own insurance products.

38) Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter.

In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner.

Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented.

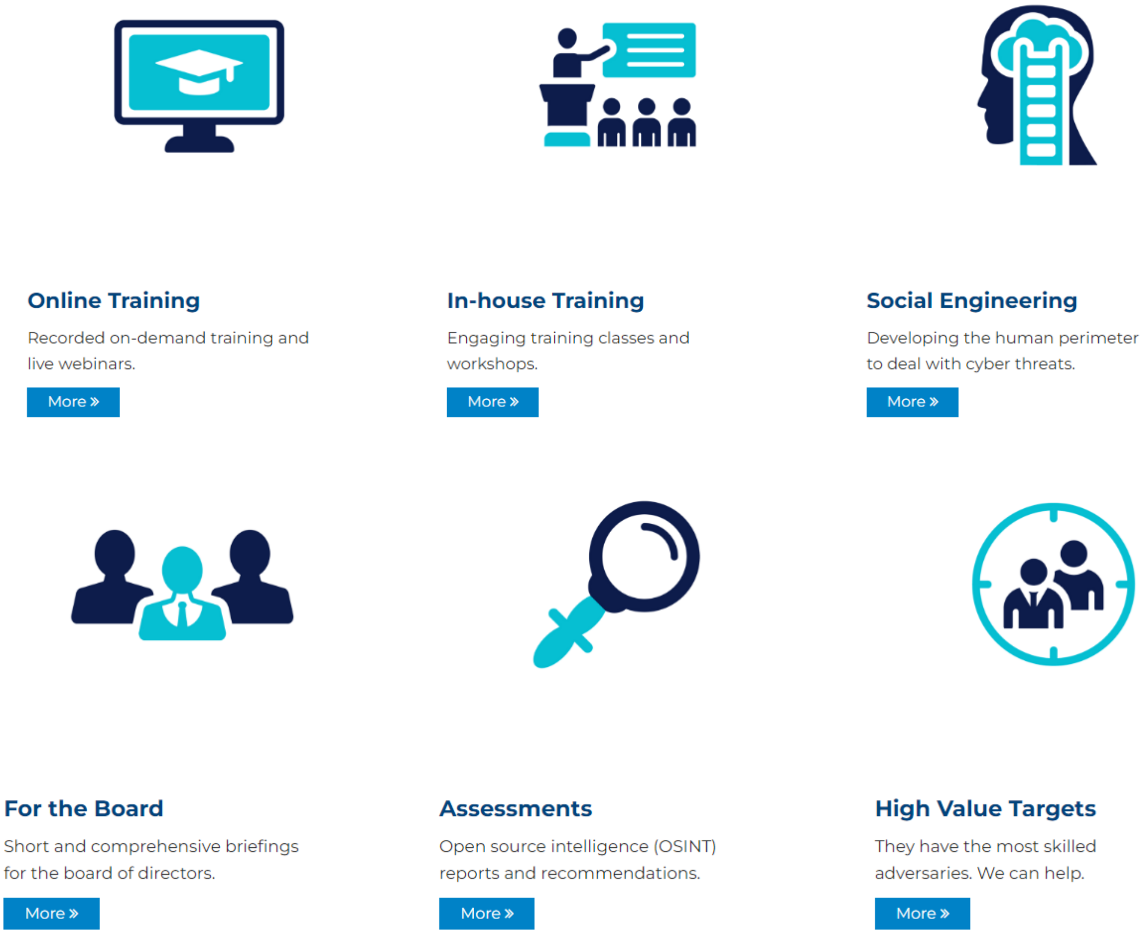
It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress.

In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by law enforcement authorities for individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person, for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences.

AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out adminstrative tasks analysing information pursuant to Union anti-money laundering legislation should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.

Cyber Risk GmbH

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



Online Training

Recorded on-demand training and live webinars.

More »

In-house Training

Engaging training classes and workshops.

More »

Social Engineering

Developing the human perimeter to deal with cyber threats.

More »

For the Board

Short and comprehensive briefings for the board of directors.

More »

Assessments

Open source intelligence (OSINT) reports and recommendations.

More »

High Value Targets

They have the most skilled adversaries. We can help.

More »

Cyber security training

Overview

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

Our training programs have the objective to help managers and employees not only understand the cyber security threats, but also their responsibility towards protecting the assets they handle. We explain how to proactively apply good cyber security practices, how to identify threats and attacks, and what to do to protect themselves and their organizations. Cyber security is a shared responsibility.

Duration

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

Our Education Method

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

Our Instructors

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

Our websites include:

a. Sectors and Industries.

1. Cyber Risk GmbH - https://www.cyber-risk-gmbh.com

2. Social Engineering Training - https://www.social-engineering-training.ch

3. Healthcare Cybersecurity - https://www.healthcare-cybersecurity.ch

4. Airline Cybersecurity - https://www.airline-cybersecurity.ch

5. Railway Cybersecurity - https://www.railway-cybersecurity.com

6. Maritime Cybersecurity - https://www.maritime-cybersecurity.com

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

8. Transport Cybersecurity Toolkit - https://www.transport-cybersecurity-toolkit.com

9. Hotel Cybersecurity - https://www.hotel-cybersecurity.ch

10. Sanctions Risk - https://www.sanctions-risk.com

11. Travel Security - https://www.travel-security.ch

b. Understanding Cybersecurity.

1. What is Disinformation? - https://www.disinformation.ch

2. What is Steganography? - https://www.steganography.ch

3. What is Cyberbiosecurity? - https://www.cyberbiosecurity.ch

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

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

6. What is Cyber Espionage? - https://www.cyber-espionage.ch

7. What is Sexspionage? - https://www.sexspionage.ch

c. Understanding Cybersecurity in the European Union.

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

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

3. The Digital Operational Resilience Act (DORA) - https://www.digital-operational-resilience-act.com

4. The Critical Entities Resilience Directive (CER) - https://www.critical-entities-resilience-directive.com

5. The Digital Services Act (DSA) - https://www.eu-digital-services-act.com

6. The Digital Markets Act (DMA) - https://www.eu-digital-markets-act.com

7. The European Health Data Space (EHDS) - https://www.european-health-data-space.com

8. The European Chips Act - https://www.european-chips-act.com

9. The European Data Act - https://www.eu-data-act.com

10. European Data Governance Act (DGA) - https://www.european-data-governance-act.com

11. The Artificial Intelligence Act - https://www.artificial-intelligence-act.com

12. The European ePrivacy Regulation - https://www.european-eprivacy-regulation.com

13. The European Cyber Defence Policy - https://www.european-cyber-defence-policy.com

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

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

You may contact:

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

Disclaimer

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

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

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

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

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of interpretative;

- does not 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 (hereinafter "GTC"):
https://www.cyber-risk-gmbh.com/Impressum.html