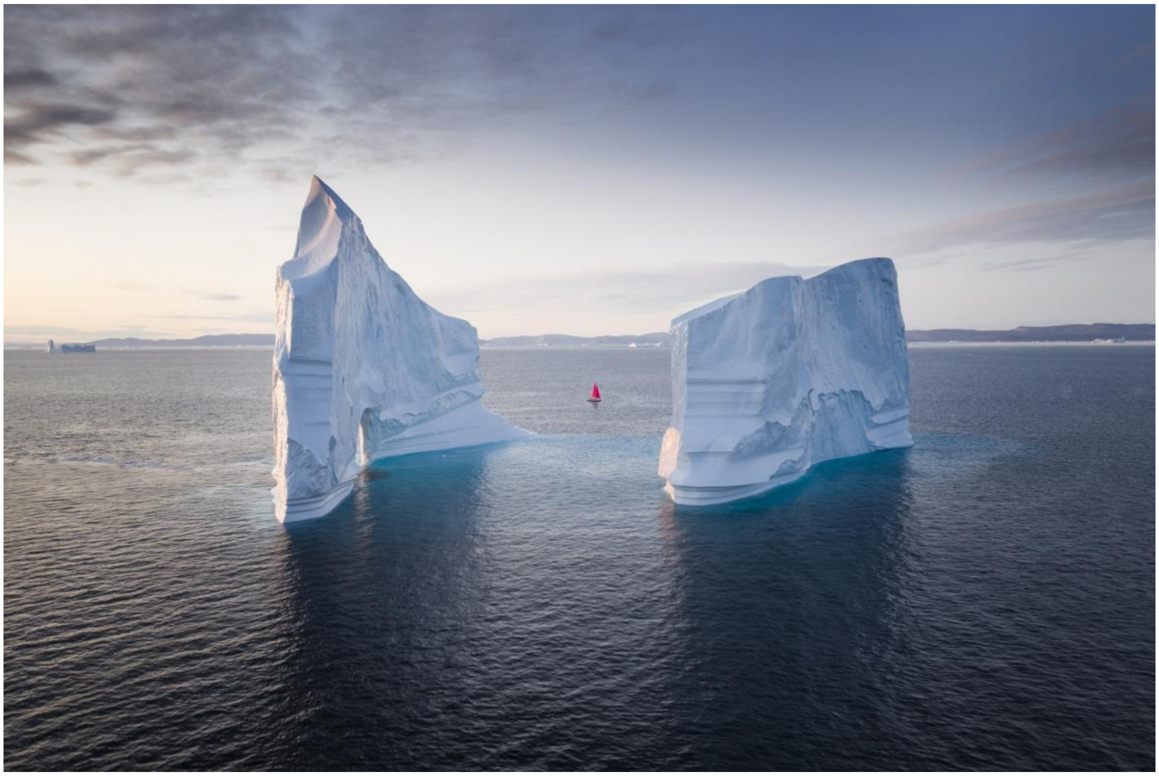


Cyber Risk and Compliance News and Alerts, October 2023

This was one of the most difficult meetings in my professional life. It was about Article 11 of the proposed European Cyber Resilience Act.

I do understand that Article 11 is good for cybersecurity. But I also know that *all foreign intelligence agencies* will attack persons and systems to obtain extremely valuable information and the single key to the kingdom. Do I agree with Article 11, or not? I would say no, I do not agree.

Let's start at the very beginning. The proposed European Cyber Resilience Act (CRA) describes the cybersecurity requirements for hardware and software products placed on the market of the European Union.

Before the European Cyber Resilience Act, the various acts and initiatives taken at EU and national levels only partially addressed the cybersecurity related problems and risks, creating a legislative patchwork. It increased legal uncertainty for both manufacturers and users of those products.

After the European Cyber Resilience Act, two major problems are addressed:

1. *The low level of cybersecurity of products with digital elements*, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them.
2. *The insufficient understanding and access to information by users*, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered as less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or move laterally across systems.

It is time to understand Article 11 - Reporting obligations of manufacturers:

1. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any actively exploited vulnerability contained in the product with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with the NIS 2 Directive of Member States concerned upon receipt, and inform the market surveillance authority about the notified vulnerability.

2. The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify to ENISA any incident having impact on the security of the product with digital elements. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with the NIS 2 Directive of the Member States concerned and inform the market surveillance authority about the notified incidents. The incident notification shall include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact.

3. ENISA shall submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established by the NIS 2 Directive information notified pursuant to paragraphs 1 and 2 if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.

4. The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident.

.....

7. Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component.

This is part of Article 11 (Reporting obligations of manufacturers) of the proposed European Cyber Resilience Act (CRA).

On the positive side, the exchange of information and the coordinated management of large-scale cybersecurity incidents and crises at an operational level is an important step forward.

On the negative side, manufacturers must disclose to EU institutions all product vulnerabilities within 24 hours of becoming aware of them (before fixing them). This involves persons and systems in 27 Member States and in EU institutions. How can we ensure the security of this network of disclosures? How can we avoid the risk of bribery, blackmail, and errors in the human firewall, and the technical issues in the infrastructure?

Let's get in the shoes of a foreign intelligence service. Compromising the security of this network gives the single key to the kingdom of all vulnerabilities that are not fixed yet, and can be easily exploited.

In April 2023, we had an interesting proposal from the European Commission for *another* cyber related Act, this time the *EU Cyber Solidarity Act*.

The Cyber Solidarity Act is a step forward after the Joint Cyber Defence Communication (JOIN(2022) 49), for an EU Cyber Solidarity Initiative with the following objectives:

1. To strengthen common EU detection, situational awareness, and response capabilities,
2. To gradually build an EU-level cybersecurity reserve with services from trusted private providers, and
3. To support testing of critical entities.

According to the European Commission: “Cyber operations are increasingly integrated in hybrid and warfare strategies, with significant effects on the target. In particular, Russia’s military aggression against Ukraine was preceded and is being accompanied by a strategy of hostile cyber operations, which is a game changer for the perception and assessment of the EU’s collective cybersecurity crisis management preparedness and a call for urgent action.”

“The threat of a possible large-scale incident causing significant disruption and damage to critical infrastructures demands heightened preparedness at all levels of the EU’s cybersecurity ecosystem. That threat goes beyond Russia’s military aggression on Ukraine and includes continuous cyber threats from state and non-state actors, which are likely to persist, given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions.”

The objectives of the EU Cyber Solidarity Act will be implemented through the following actions:

1. The deployment of a pan-European infrastructure of Security Operations Centres *(European Cyber Shield)* to build and enhance common detection and situational awareness capabilities.

2. The creation of a *Cyber Emergency Mechanism* to support Member States in preparing for, responding to and immediate recovery from significant and large-scale cybersecurity incidents. Support for incident response shall also be made available to European institutions, bodies, offices and agencies of the Union (EUIBAs).

3. The establishment of a *European Cybersecurity Incident Review Mechanism* to review and assess specific significant or large-scale incidents.

Unfortunately, in April 2023, there was no impact assessment in the proposal for the EU Cyber Solidarity Act, due to the “urgent nature of the proposal”!

In my opinion, the urgent nature of the proposal is a direct result of Russia's unprovoked and unjustified attack on Ukraine. Ursula von der Leyen, president of the European Commission after 2019, has said: "This war changes everything. After this war, you cannot be in between anymore."

According to the proposed EU Cyber Solidarity Act (April 18, 2023):

"Due to the urgent nature of the proposal, no impact assessment was carried out. The actions of this Regulation will be supported by the Digital Europe Programme (DEP), and are in line with those set in the DEP Regulation, which was subject to a dedicated impact assessment.

This Regulation will not entail any significant administrative or environmental impacts beyond those already assessed in the impact assessment of the DEP Regulation.

Furthermore, it builds on first actions developed in closed collaboration with the main stakeholders, as set out above, and follow up on Member States’ call for the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity by the end of Q3 2022.

Specifically, regarding situational awareness and detection under the European Cyber Shield, a Call for Expression of Interest to jointly procure tools and infrastructure to establish Crossborder SOCs, and a call for grants to enable capacity building of SOCs serving public and private organisations, were held under DEP cybersecurity work programme 2021-2022.

In the area of preparedness and incident response, as mentioned above the Commission has set up a short-term programme to support Member States from DEP, being implemented by ENISA. Services covered include preparedness actions, such as penetration testing of critical entities in order to identify vulnerabilities.

It also strengthens possibilities to assist Member States in case of a major incident affecting critical entities. The implementation by ENISA of this short-term programme is under way and has already provided relevant insights that have been taken into account in the preparation of this Regulation."

You can find the above (page 8/58) at:

https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act

In my opinion, this urgency is justified. Unfortunately, this would be challenged by the European Court of Auditors (ECA), as even in the "Better Regulation Guidelines" from the European Commission, the phrase "impact assessment" is repeated 119 times in 43 pages. "Stakeholder consultation" is repeated 28 times.

October 5, 2023 - Warnings (in Opinion 02/2023) from the European Court of Auditors (ECA) about the Cyber Solidarity Act.

According to the European Court of Auditors (ECA):

"Our opinion highlights some *risks* that we have identified and how the measures laid down in the proposal might be implemented. In particular, we highlight the risks that the operation of the European Cyber Shield and its sustainability become dependent on EU financing; that its functioning is impeded by a lack of information sharing; and that the measures introduced by the proposal make the whole EU cybersecurity galaxy more complex."

"The Commission's better regulation guidelines suggest using impact assessments and stakeholder consultations as part of a comprehensive analysis of policy design and implementation options. We consider comprehensive impact assessments as an essential tool to consider whether EU action is needed and analyse the potential impacts of available solutions before any proposal is adopted.

This proposed Regulation was not subject to an impact assessment. In section 3 of the accompanying explanatory memorandum, the Commission explained that it had opted not to carry out such an assessment due to the "urgent nature of the proposal".

It also said that the measures introduced by the proposed Regulation would be supported by the Digital Europe Programme (DEP), and were in line with the DEP Regulation, which had undergone a specific impact assessment in 2018.

Additionally, the Commission explained that the proposed measures were built upon previous actions prepared in close coordination with the main stakeholders and member states, integrating lessons learned.

However, we note that the DEP impact assessment does not cover the new measures introduced by the proposed Regulation. There is thus limited information on available policy options and the costs related to the proposal."

"As a result of our review of the legislative proposal, we suggest that the Commission and legislators should consider:

— making the cost estimates related to establishing and implementing the proposed measures available to enhance transparency (see paragraph 10);

— clarifying how national SOCs, cross-border SOCs, CSIRTs, and the CSIRTs network should interact by laying down clear governance arrangements and responsibilities in order to ensure effective coordination and achieve synergies (paragraph 20);

— ensuring that that the timelapse between the request to receive support services from the EU Cybersecurity Reserve and the response by the Commission is not delayed by the timing of the request (paragraph 29);

— limiting the derogation to the annuality principle to response actions and mutual assistance and clarifying that the automatic carry-over of unused commitments should be limited to the following year (paragraphs 32-34);

— specifying a maximum deadline for the delivery of ENISA's report after any incident, in order to ensure that feedback is provided in good time (paragraph 36);

— advancing the timing for submission by the Commission of a report on the evaluation and review of the Regulation (paragraph 40)."

You can find the above at:
https://www.eca.europa.eu/ECAPublications/OP-2023-02/OP-2023-02_EN.pdf

According to Heraclitus "War is father of all, and king of all. He renders some gods, others men; he makes some slaves, others free."

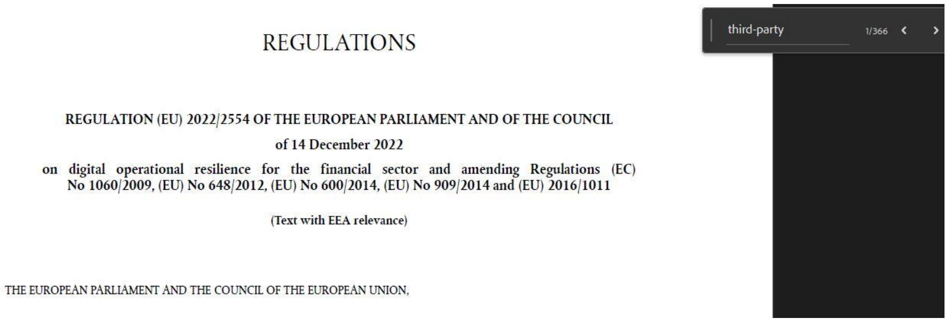
The EU emerged from the idea of ensuring peace in Europe after the second world war, and preventing future military conflicts.

Now, in war mode, the EU has to establish a proper emergency process, adapting to the new challenges.

Read more at number 19 below.

I was reading carefully (again) the DORA regulation of the EU (Regulation 2022/2554 on digital operational resilience for the financial sector). After reading a document, I always try to "feel" what is important. Frequency analysis is a good approach for that.

Well, in 80 pages, the term "third-party" is repeated 366 times.



REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

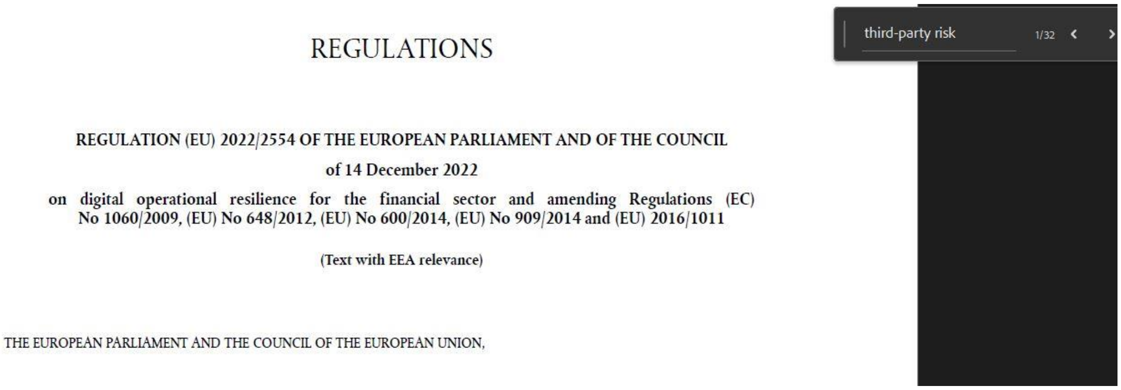
of 14 December 2022

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

The term “third-party risk” is repeated 32 times.



REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

According to DORA, *‘ICT third-party risk’* means an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.

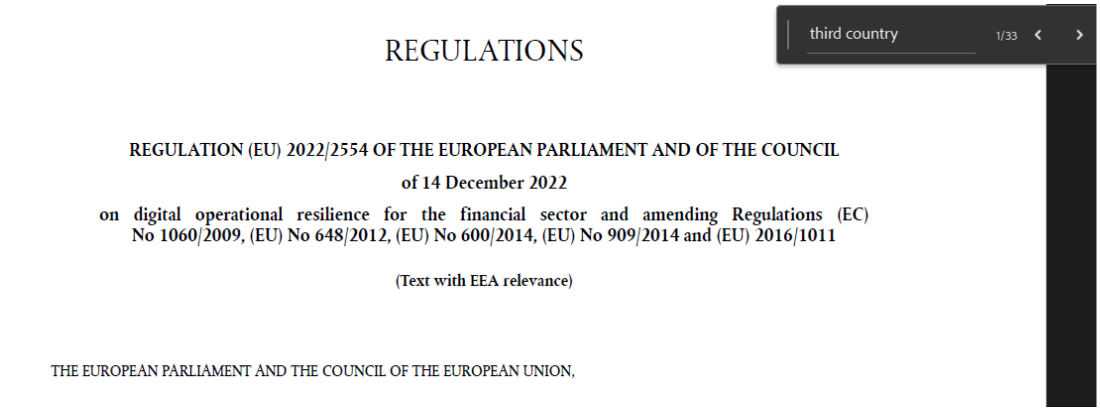
According to Article 28, financial entities must manage ICT *third-party risk* as an integral component of ICT risk within their ICT risk management framework.

We have some surprises for third parties. According to Article 31, the European Supervisory Authorities (ESAs) - the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA) – shall designate the ICT third-party service providers that are critical for financial entities, and appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible.

You can easily guess that service providers will have a difficult time, as we have an Oversight Framework (Article 32-35), and the exercise of the powers of the Lead Overseer outside the European Union (Article 36).

The Lead Overseer may exercise the powers referred to in DORA on any premises located in a third-country which is owned, or used in any way, for the purposes of providing services to Union financial entities, by a critical ICT third-party service provider, in connection with its business operations, functions or services, including any administrative, business or operational offices, premises, lands, buildings or other properties.

An ICT third-party service provider established in a third country which has been designated as critical in accordance with DORA, must undertake, within 12 months of such designation, “all necessary arrangements to ensure its incorporation within the Union, by means of establishing a subsidiary”.
The term “third country” is repeated 33 times in the regulation.



third country 1/33

REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

You can find more about DORA at: https://www.digital-operational-resilience-act.com

DORA will apply from 17 January 2025.

___

In December 2022, Decision (EU) 2022/2481 of the European Parliament and the Council established the “Digital Decade Policy Programme 2030”. Risk and compliance professionals must read the program, to understand the challenges and opportunities that come after that, and the recent developments, like the *first State of the Digital Decade* report.

In Article 1 of decision 2022/2481, we read:

“1. This Decision establishes the Digital Decade Policy Programme 2030 and sets out a monitoring and cooperation mechanism for that programme designated to:

(a) creating an environment favourable to innovation and investment by setting a clear direction for the digital transformation of the Union and for the delivery of digital targets at Union level by 2030, on the basis of measurable indicators;

(b) structuring and stimulating cooperation between the European Parliament, the Council, the Commission and the Member States;

(c) fostering the consistency, comparability, transparency and completeness of monitoring and reporting by the Union.

2. This Decision establishes a framework for multi-country projects.”

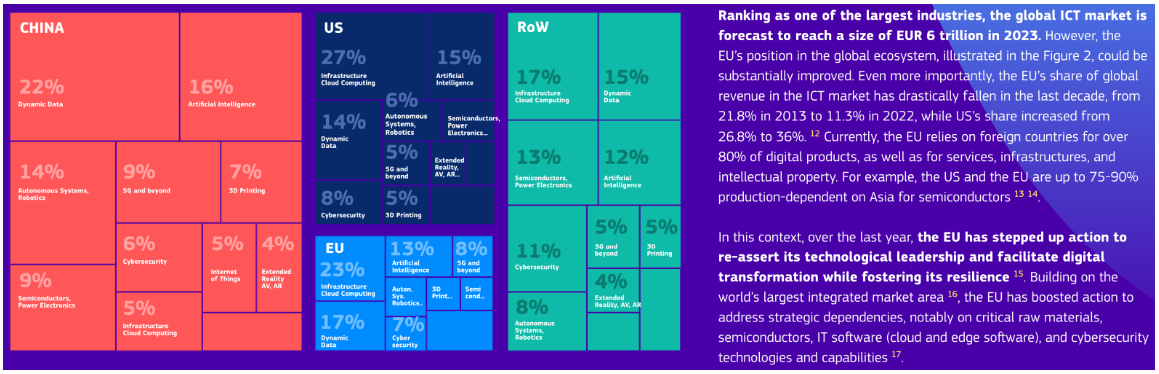
You can find Decision (EU) 2022/2481 at number 6 of our list below.
What is new?

27 September 2023 - The first State of the Digital Decade report takes stock of the EU's progress towards a successful digital transformation as set out in the Digital Decade Policy Programme 2030.

This report highlights the need to accelerate and deepen the collective efforts, including through policy measures and investment in digital technologies, skills and infrastructures.

On this basis, the report includes concrete recommendations to Member States ahead of the adoption of their national strategic roadmaps and for their future adjustments.

This report also includes the monitoring of the European Declaration on Digital Rights and Principles for the Digital Decade, which translates the EU's vision of digital transformation into principles and commitments.



Ranking as one of the largest industries, the global ICT market is forecast to reach a size of EUR 6 trillion in 2023. However, the EU's position in the global ecosystem, illustrated in the Figure 2, could be substantially improved. Even more importantly, the EU's share of global revenue in the ICT market has drastically fallen in the last decade, from 21.8% in 2013 to 11.3% in 2022, while US's share increased from 26.8% to 36%. [12] Currently, the EU relies on foreign countries for over 80% of digital products, as well as for services, infrastructures, and intellectual property. For example, the US and the EU are up to 75-90% production-dependent on Asia for semiconductors [13] [14].

In this context, over the last year, **the EU has stepped up action to re-assert its technological leadership and facilitate digital transformation while fostering its resilience** [15]. Building on the world's largest integrated market area [16], the EU has boosted action to address strategic dependencies, notably on critical raw materials, semiconductors, IT software (cloud and edge software), and cybersecurity technologies and capabilities [17].

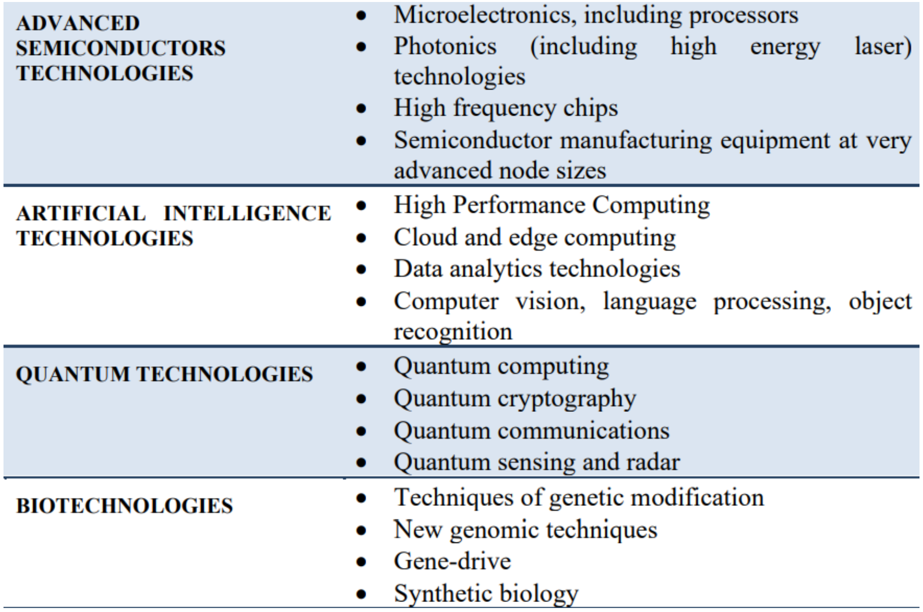
Read more at number 9 below.

The European Union has (another) surprise for risk and compliance professionals.

The European Commission recommends carrying out risk assessments on four critical technology areas:

- Advanced semiconductors,
- Artificial intelligence,
- Quantum, and
- Biotechnologies.

It starts with the new risks in Europe: "The Commission and the High Representative have recognised that with rising geopolitical tensions, deeper economic integration and the acceleration of technological development, certain economic flows and activities can present a risk to
our economic security."



ADVANCED SEMICONDUCTORS TECHNOLOGIES	• Microelectronics, including processors • Photonics (including high energy laser) technologies • High frequency chips • Semiconductor manufacturing equipment at very advanced node sizes
ARTIFICIAL INTELLIGENCE TECHNOLOGIES	• High Performance Computing • Cloud and edge computing • Data analytics technologies • Computer vision, language processing, object recognition
QUANTUM TECHNOLOGIES	• Quantum computing • Quantum cryptography • Quantum communications • Quantum sensing and radar
BIOTECHNOLOGIES	• Techniques of genetic modification • New genomic techniques • Gene-drive • Synthetic biology

The Recommendation identifies 4 technology areas, which are considered highly likely to present the most sensitive and immediate risks related to technology security and technology leakage.

According to the European Commission, "these technology areas should, as a matter of highest priority, be subject to a collective risk assessment with Member States by the end of the year".

"(a) Advanced semiconductors technologies

Semiconductors, microelectronics and photonics are essential components of electronic devices in critical areas such as communications, computing, energy, health, transportation and defence and space systems and applications.

Due to their huge enabling and transformative nature and their use for civil and military purposes, remaining at the forefront of building and further developing these technologies is crucial for economic security.

(b) Artificial intelligence technologies.

AI (software), high-performance computing, cloud and edge computing, and data analytics have a wide range of dual-use applications and are crucial in particular for processing large amounts of data and making decisions or predictions based on this data-driven analysis.

These technologies have huge transformative potential in this regard.

(c) Quantum technologies

Quantum technologies have a vast potential to transform multiple sectors, civil and military, by enabling new technologies and systems that make use of the properties of the quantum mechanics.

The full impact of quantum technologies that are being/will be developed cannot yet be fully qualified.

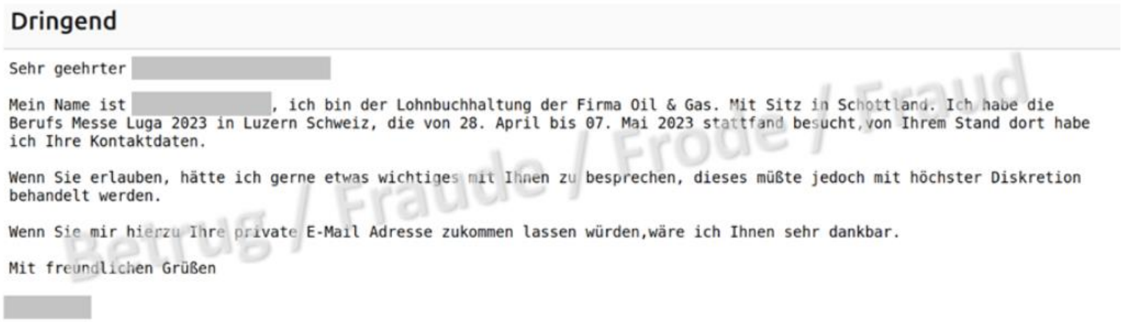
(d) Biotechnologies

Biotechnologies have a major enabling and transformative nature in areas such as agriculture, environment, healthcare, life science, food chains or biomanufacturing.

Some biotechnologies, such as genetic engineering applied to pathogens or harmful compounds produced by genetic modification of microorganisms, can have a security/military dimension, in particular when being misused."

Read more at number 1 below.

According to the Swiss National Cyber Security Centre (NCSC), autumn is the trade fair season. In order to optimise trade fair planning for visitors, many organisers provide information about exhibitors and their products online. Such information is helpful for visitors, but it can also be misused by fraudsters, as illustrated by an example reported to the NCSC.



Dringend

Sehr geehrter [redacted]

Mein Name ist [redacted], ich bin der Lohnbuchhaltung der Firma Oil & Gas. Mit Sitz in Schottland. Ich habe die Berufs Messe Luga 2023 in Luzern Schweiz, die von 28. April bis 07. Mai 2023 stattfand besucht,von Ihrem Stand dort habe ich Ihre Kontaktdaten.

Wenn Sie erlauben, hätte ich gerne etwas wichtiges mit Ihnen zu besprechen, dieses müßte jedoch mit höchster Diskretion behandelt werden.

Wenn Sie mir hierzu Ihre private E-Mail Adresse zukommen lassen würden,wäre ich Ihnen sehr dankbar.

Mit freundlichen Grüßen

[redacted]

The NCSC regularly receives reports from Swiss businesses that are contacted by supposed foreign companies in connection with their presence at a trade fair.

The sender claims to have visited the company's stand at the trade fair and to have received the contact details there.

This also happened in a recent case reported to the NCSC. The attacker posed as a company based in Scotland, referred to a supposed trade fair visit in April 2023 and stated that he wanted to discuss something.

The email mentions an important matter that needs to be handled with the utmost discretion and states that a personal email address should be provided in order to discuss it. However, this trade fair visit never actually took place.

The email recipient was sceptical and did not engage with the sender. Had he gone along with the proposal, it would probably have resulted in some advance payment under the pretext of a lucrative deal.

As with CEO fraud, the attackers in this case use data from public sources. While CEO fraud primarily uses data that can be found on company websites, especially pages that list the functions and contact details of employees, this type of fraud uses trade fair exhibitor lists.

To help visitors find their way around trade fairs, the list of exhibitors can often be consulted online. In addition to this, information such as a brief description of the company or contact details are also provided. While this is practical for visitors, it is a goldmine for fraudsters looking to carry out targeted attacks.

By mentioning the trade fair, the attackers try to create an atmosphere of trust and suggest that they have already met in person at the trade fair stand. This form of personal contact is considered more trustworthy than an anonymous request via email. In most cases, these attacks involve some sort of deal where money has to be transferred.

Recommendations from the Swiss National Cyber Security Centre (NCSC):

- Raise awareness among your employees. Especially employees in finance divisions and in key positions must be informed about these possible methods of attack.

- Ignore unusual payment requests.

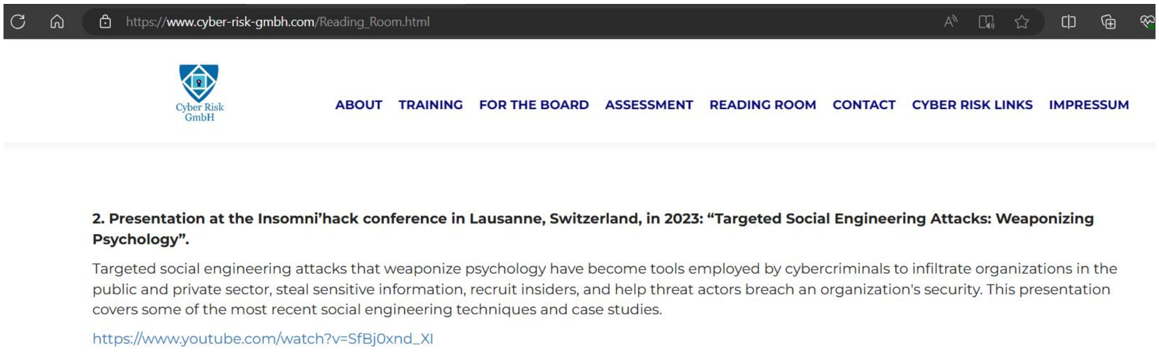
- All processes which concern payment transactions should be clearly defined internally and complied with by employees in all cases (e.g. dual control principle, joint signature by two people).

- In the case of unusual requests, phone the head of the company / authority / association to verify that the order is correct.

- If you made a payment, immediately contact the bank through which you made the payment. They may still be able to stop it. We additionally recommend that you contact the cantonal police responsible for your place of business and file a criminal complaint.

Welcome to our monthly newsletter.

You can find our newsletters at our “Reading Room”. You may visit:
https://www.cyber-risk-gmbh.com/Reading_Room.html



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

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

https://www.youtube.com/watch?v=SfBj0xnd_XI

Best regards,

George Lekatis

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

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

Number 1 (Page 18)

The European Commission recommends carrying out risk assessments on four critical technology areas

Advanced semiconductors, artificial intelligence, quantum, biotechnologies

European Commission

Number 2 (Page 25)

The U.S. Federal Bureau of Investigation (FBI) about dual ransomware attacks targeting the same victims.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

Number 3 (Page 27)

BLUE OLEX 2023: Getting Ready for the Next Cybersecurity Crisis in the EU

enisa
European Network and Information Security Agency

Number 4 (Page 30)

Crypto-assets regulation: from patchwork to framework

DeNederlandscheBank
EUROSYSTEEM

Number 5 (Page 36)

Dive into the Deep Sea: A View of the Subsea Cable Ecosystem

enisa
European Network and Information Security Agency

Number 6 (Page 41)

The Ethics of Outsourcing Information Conflict

Outlining the Responsibilities of Government Funders to their Civil Society Partners

Number 7 (Page 45)

The Commission sends request for information to X under the Digital Services Act

European Commission

Number 8 (Page 47)

NIST Interagency Report - NIST IR 8473

Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Number 9 (Page 49)

27 September 2023 - The first State of the Digital Decade report

European Commission

Number 10 (Page 51)

Project Mariana: BIS and central banks of France, Singapore and Switzerland successfully test cross-border wholesale CBDCs

BIS Innovation Hub

Number 11 (Page 54)

ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA in response to the European Commission's call for advice

EBA EUROPEAN BANKING AUTHORITY eiopa ESMA European Securities and Markets Authority

Number 18 (Page 75)

GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT

Number 19 (Page 78)

Opinion 02/2023

concerning the proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents of 18 April 2023

Number 20 (Page 82)

Mastering your supply chain

A new collection of resources from the NCSC can help take your supply chain knowledge to the next level

Number 21 (Page 84)

Wearable sensor to monitor 'last line of defense' antibiotic

Sandia sensor system can track antibiotic levels in real time

Number 22 (Page 86)

A New Take on Modeling & Simulation for Improved Autonomy

DARPA seeks proposals to rapidly repurpose or transfer autonomy to new and different missions

Number 1

The European Commission recommends carrying out risk assessments on four critical technology areas

Advanced semiconductors, artificial intelligence, quantum, biotechnologies

The European Commission adopted a Recommendation on critical technology areas for the EU's economic security, for further risk assessment with Member States.

This Recommendation stems from the Joint Communication on a European Economic Security Strategy that put in place a comprehensive strategic approach to economic security in the EU.

This Recommendation relates to the assessment of one of four types of risks in that comprehensive approach, namely technology risk and technology leakage.

The risk assessment will be objective in character, and neither its results nor any follow-up measures can be anticipated at this stage. In the Recommendation, the Commission puts forward a list of ten critical technology areas.

These technology areas were selected based on the following criteria:

- Enabling and transformative nature of the technology: the technologies' potential and relevance for driving significant increases of performance and efficiency and/or radical changes for sectors, capabilities, etc.;

- The risk of civil and military fusion: the technologies' relevance for both the civil and military sectors and its potential to advance both domains, as well as risk of uses of certain technologies to undermine peace and security;

- The risk the technology could be used in violation of human rights: the technologies' potential misuse in violation of human rights, including restricting fundamental freedoms.

Collective risk assessments with Member States

Out of the ten critical technology areas, the Recommendations identifies four technology areas that are considered highly likely to present the most sensitive and immediate risks related to technology security and technology leakage:

- Advanced Semiconductors technologies (microelectronics, photonics, high frequency chips, semiconductor manufacturing equipment);

- Artificial Intelligence technologies (high performance computing, cloud and edge computing, data analytics, computer vision, language processing, object recognition);

- Quantum technologies (quantum computing, quantum cryptography, quantum communications, quantum sensing and radar);

- Biotechnologies (techniques of genetic modification, new genomic techniques, gene-drive, synthetic biology).

The Commission recommends that Member States, together with the Commission, initially conduct collective risk assessments of these four areas by the end of this year. The Recommendation includes some guiding principles to structure the collective risk assessments, including consultation of the private sector and protection of confidentiality.

In deciding on proposals for further collective risk assessments with Member States on one or more of the listed additional technology areas, or subsets thereof, the Commission will take into account ongoing or planned actions to promote or partner in the technology area under consideration.

More generally, the Commission will bear in mind that measures taken to enhance the competitiveness of the EU in the relevant areas can contribute to reducing certain technology risks.

Next Steps

The Commission will engage with Member States, through the appropriate expert fora, to initiate the collective risk assessments for the four abovementioned technology areas.

In addition, the Commission will engage in an open dialogue with Member States on the appropriate calendar and scope of further risk assessments, having regard inter alia to the contribution of the time factor to the evolution of risks.

The Commission may present further initiatives in this respect by Spring 2024, in light of such dialogue and of the first experience with the initial collective risk assessments, as well as of further inputs that may be received on the listed technology areas.

The Recommendation will not prejudge the outcome of the risk assessment. Only the outcome of the detailed collective assessment of the level and nature of the risks presented can serve as the basis for a further discussion on the need for any precise and proportionate measures to promote, partner or protect on any of these technology areas, or any subset thereof.

Background

On 20 June 2023, the Commission and the High Representative adopted the Joint Communication on European Economic Security Strategy.

The European Economic Security Strategy is based on a three-pillar approach: promotion of the EU's economic base and competitiveness; protection against risks; and partnership with the broadest possible range of countries to address shared concerns and interests.

It sets out a number of actions to be taken to address risks to the resilience of supply chains, risks to the physical and cyber security of critical infrastructures, risks related to technology security and technology leakage, and risks of weaponization of economic dependencies or economic coercion. The list put forward in the Recommendation is part of the third category of these actions.

Understanding the Recommendation

(1) The Commission and the High Representative have recognised that with rising geopolitical tensions, deeper economic integration and the acceleration of technological development, certain economic flows and activities can present a risk to our economic security and adopted a Joint Communication on European Economic Security Strategy to put in place a comprehensive strategic approach to economic security.

(2) The European Economic Security Strategy is based on a three-pillar approach: promotion of the EU's economic base and competitiveness; protection against risks; and partnership with the broadest possible range of countries to address shared concerns and interests.

(3) As part of this framework and in light of the risks that certain economic dependencies and technical evolutions can present, the EU needs a clear-eyed view of the risks to its economic security and their evolution over time.

(4) These risks should be identified and assessed together with EU Member States, with inputs from private stakeholders in a dynamic and continuous process.

(5) The European Economic Security Strategy identified the following four broad and non-exhaustive categories of risks for further assessment: resilience of supply chains, including energy security; physical and cyber-security of critical infrastructure; technology security and leakage; weaponisation of economic dependencies and economic coercion.

(6) The Commission committed in the Joint Communication to assess the risks of technology security and leakage on the basis of a list of strategic technologies critical for economic security and, as regards the most sensitive risks, to propose a list of critical technologies in view of a risk assessment to be pursued collectively with Member States by the end of 2023.

(7) The Joint Communication identified the following three narrowly defined and forward-looking criteria for the selection of technologies presenting the most sensitive risks, for further assessment: the enabling and transformative nature of the technology; the risk of civil and military fusion; and the risk of misuse of the technology for human rights violations.

(8) The enabling and transformative nature of the technology criterion looks at the technology's potential and relevance for driving significant increases of performance and efficiency and/or radical changes for sectors, capabilities, etc.

(9) The risk of civil and military fusion criterion looks at the technology's relevance for both the civil and military sectors and its potential to advance both domains, as well as risk of uses of certain technologies to undermine peace and security.

(10) The risk of misuse of the technology for human rights violation criterion looks at the technology's potential misuse in violation of human rights, including restricting fundamental freedoms.

(11) Following a first internal analysis, the Commission has identified a list of 10 critical technology areas for the EU's economic security. This list of technology areas takes into account work done pursuant to the Action Plan on synergies between civil, defence and space industries.

It is a living document and could be subject to further amendments reflecting technological developments as part of an ongoing exercise.

(12) On the basis of the three narrowly defined and forward-looking criteria for the selection of technologies for further assessment, out of this list, the present Recommendation identifies 4 technology areas, which it considers highly likely to present the most sensitive and immediate risks related to technology security and technology leakage, namely Advanced Semiconductors, Artificial Intelligence, Quantum Technologies and Biotechnologies.

These technology areas should, as a matter of highest priority, be subject to a collective risk assessment with Member States by the end of the year. Subject to scoping work with Member States, this collective assessment may focus on subsets of technologies within these four technology areas.

(13) The structuring of the list reflects the Commission's assessment of which technology areas, among these, are more likely to present the most sensitive and immediate risks related to technology security and technology leakage. This can serve as an aid to decision-making on further steps.

The Commission will engage in an open dialogue with Member States on the appropriate calendar and scope of further risk assessments, having regard inter alia to the contribution of the time factor to the evolution of risks.

The Commission would welcome a timely exchange on this aspect of the Economic Security Strategy in Council, in the context of its overall political deliberations and orientations in response to the Joint Communication.

The Commission may present further initiatives in this respect by Spring 2024, in light of such dialogue and of the first experience with the initial collective assessments, as well as of further inputs that may be received on the listed technology areas.

In deciding on proposals for further collective risk assessments with Member States on one or more of the listed additional technology areas, or subsets thereof, the Commission will take into account ongoing or planned actions to promote or partner in the technology area under consideration.

More generally, the Commission will bear in mind that measures taken to enhance the competitiveness of the EU in the relevant areas can contribute to reducing certain technology risks.

(14) The objective of the risk assessment should be to identify and analyse vulnerabilities of a systemic nature according to their potential impact on the EU's economic security and the degree of likelihood that the negative impact materialises.

To structure the upcoming risk assessment exercise with Member States, the Commission has identified some guiding principles.

(15) This Recommendation does not prejudge the outcome of the risk assessment. Only the outcome of the detailed collective assessment of the level and nature of the risks presented can serve as the basis for a further discussion on the need for any precise and proportionate measures to promote, partner or protect on any of these technology areas, or any subset thereof.

Member States and the Commission may use this information in designing future policy actions, including promotion, partnership or protection measures at national, EU or international level, which should be proportional to the level of risk addressed and precise in terms of scope.

No conclusion can therefore be drawn at this pre-assessment stage on recourse to any particular instrument in the EU's or the Member States' toolboxes of measures to promote, partner or protect with others in view of enhanced economic security.

(16) Any measures that may be taken will be proportionate and precisely targeted to the assessed risks of each critical technology area, or of a relevant technology. Any implemented measures will aim at reinforcing the Union's strength in these areas and be designed to minimise any negative spill-over effects on the market and the economy.

In particular, these assessments will contribute to the development of Union policies in support of innovation and industrial development for the identified technologies, including through international initiatives.

To read more: https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

Note: https://defence-industry-space.ec.europa.eu (the website where we can found the Recommendation) belongs to the Directorate-General for Defence Industry and Space (DEFIS), that leads the European Commission's activities in the Defence Industry and Space sector.

In the area of Defence, DEFIS is in charge of upholding the competitiveness and innovation of the European Defence industry by ensuring the evolution of an able European defence technological and industrial base.

In the area of Space, DEFIS is in charge of implementing the EU Space programme consisting of the European Earth Observation Programme

(Copernicus), the European Global Navigation Satellite System (Galileo) and the European Geostationary Navigation Overlay Service (EGNOS).

Some key actions and priorities for the year ahead:

- implementation and oversight of the European Defence Fund
- building an open and competitive European defence equipment market and enforcing EU procurement rules on defence;
- leading on the implementation of the Action Plan on Military Mobility
- fostering a strong and innovative space industry, maintaining the EU's autonomous, reliable and cost-effective access to space;
- implementing the future Space Programme, covering Galileo, EGNOS and Copernicus;
- exploring ways in which we can make the most of our assets to deliver on climate objective, improving the crucial link between space and defence and security.

Number 2

The U.S. Federal Bureau of Investigation (FBI) about dual ransomware attacks targeting the same victims.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

Ransomware attacks against the same victim occurring within 10 days, or less, of each other were considered dual ransomware attacks. The majority of dual ransomware attacks occurred within 48 hours of each other.

Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification to highlight emerging ransomware trends and encourage organizations to implement the recommendations in the "Mitigations" section to reduce the likelihood and impact of ransomware incidents.

Threat

As of July 2023, the FBI noted two trends emerging across the ransomware environment and is releasing this notification for industry awareness. These new trends included multiple ransomware attacks on the same victim in close date proximity and new data destruction tactics in ransomware attacks.

The FBI noted a trend of dual ransomware attacks conducted in close proximity to one another.

During these attacks, cyber threat actors deployed two different ransomware variants against victim companies from the following variants: AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal. Variants were deployed in various combinations.

This use of dual ransomware variants resulted in a combination of data encryption, exfiltration, and financial losses from ransom payments.

Second ransomware attacks against an already compromised system could significantly harm victim entities.

In early 2022, multiple ransomware groups increased use of custom data theft, wiper tools, and malware to pressure victims to negotiate.
In some cases, new code was added to known data theft tools to prevent detection.
In other cases in 2022, malware containing data wipers remained dormant until a set time, then executed to corrupt data in alternating intervals.

Preparing for Cyber Incidents

1. Maintain offline backups of data, and regularly maintain backup and restoration. By instituting this practice, the organization ensures they will not be severely interrupted, and that backup data will be accessible when it is needed.

2. Ensure all backup data is encrypted, immutable (that is, cannot be altered or deleted), and covers the entire organization's data infrastructure. Ensure your backup data is not already infected.

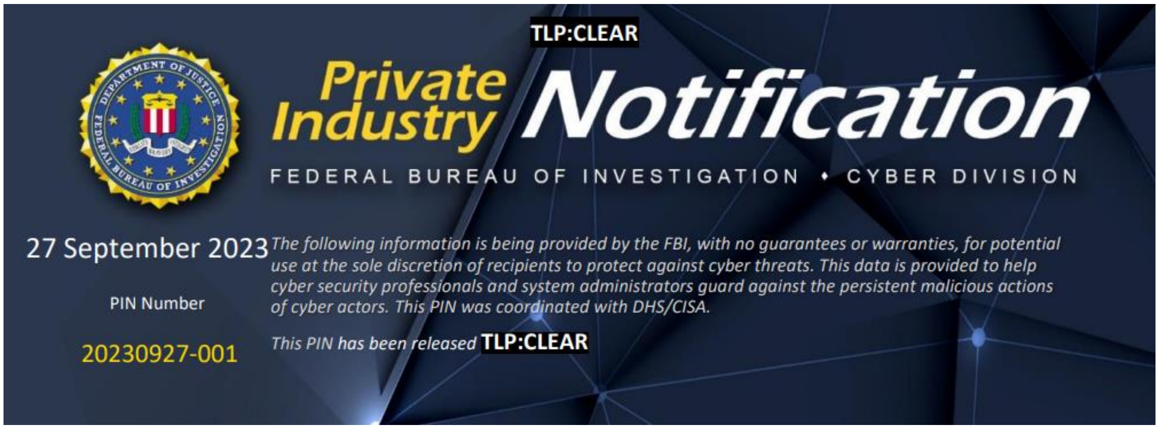
3. Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.

4. Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.

5. Document and monitor external remote connections. Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.

6. Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (that is, a hard drive, other storage device, or the cloud).

To read more: https://www.ic3.gov/Media/News/2023/230928.pdf



TLP:CLEAR

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

27 September 2023

PIN Number

20230927-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released TLP:CLEAR

Number 3

BLUE OLEX 2023: Getting Ready for the Next Cybersecurity Crisis in the EU

enisa
European Network and Information Security Agency

Together with the European Commission under the Spanish Presidency of the EU Council, the European Union Agency for Cybersecurity (ENISA) co-organised and co-hosted the Blue Olex table-top cyber exercise in the Hague, Netherlands.

With the upcoming EU elections and cyber threats spreading widely, the EU needs to strengthen its capacities. This was precisely the objective of the Blue Olex exercise to test the preparedness of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), the cooperation network for Member States national authorities in charge of cyber crisis management.

Launched in 2020, the EU CyCLONe network was formally established by the NIS 2 directive on 16 January 2023.

Roberto Viola, Director General for Communications Networks, Content and Technology (CNECT): ”Cyber crises have no borders and the EU must continue strengthening its capacities especially when it comes to cyber crisis management. I am pleased that the EU-CyCLONe, combining EU and Member States capabilities is testing its resilience and how to act in the case of cyberattacks and large-scale cyber incidents. A stronger cyber response makes the EU a safer continent.”

Juhan Lepassaar, Executive Director of the European Union Agency for Cybersecurity (ENISA) said: “The EU CyCLONe is an invaluable asset. Only a stronger cyber crisis coordination will allow us to best mitigate future large-scale incidents and cross-border crises in the EU.”

The Chair of the EU-CyCLONe Network (Spain) said: "Crisis management has been a priority for Spain for years. I would like to remember that the origin of CyCLONe was set up in our country, with the celebration of a Seminar in 2019 in Madrid on Large scale cyber incidents and crisis. The first conclusion was the need to set up an Exercise (BlueOlex) to develop the operational layer.

These exercise series allow to test EU preparedness in the event of a cyber-related crisis affecting the EU Member States for strengthening the cooperation between all relevant actors. Since then, CyCLONe has been maturing in its procedures, tools, mechanisms and capabilities, managing to lay its legal foundations in the NIS 2 Directive. The 2023 BlueOlex edition, has again showed us the strong commitment that all Member States, European Commission and ENISA have against threats and challenges that, for sure, we will face in a near future to guarantee a more cyber secure and resilient Europe."

What is the objective of the EU CyCLONe?

The network collaborates and develops information sharing and situational awareness based on the support and tools provided by ENISA, also acting as the CyCLONe Secretariat. The network is chaired in turns by a representative from the Presidency of the Council of the EU.

Formed by the representatives of Member States' cyber crisis management authorities, the EU CyCLONe intervenes together with the European Commission in case of large-scale cybersecurity incidents likely to have a significant impact on services and activities falling into the scope of the NIS2 Directive.

About Blue Olex '23

BlueOlex '23 tested the EU preparedness in the event of a cyber-related crisis affecting the EU Member States and to strengthen the cooperation between the national cybersecurity authorities, the European Commission and ENISA.

The aim of the exercise is to build a stronger relationship among the cybersecurity community participating in the exercise, increase the situational awareness and share best practices.

Finally, it sets the scene for a high-level political discussion, on strategic cyber policy issues, in particular, shaping a coherent framework for crisis management at EU level.

This edition of the exercise gathered high level executives of the 27 Members States' competent authorities in charge of cyber crisis management and/or cyber policy, the European Commission and the EU Agency for Cybersecurity.

It was the opportunity for them to exercise the interaction between the new network and the EU political level and to strengthen trust and collaboration that is key for joint response.

Cyber Exercises

ENISA also supports the organisation of exercises for EU CyCLONe members, such as CySOPex (played by officers) and as in this case BlueOLEx (played by executives).

These exercises aim to identify improvements and potential gaps in the standardised way of responding to incidents and crises (i.e. Standard Operating Procedures), train on situational awareness and information sharing processes. EU CyCLONe Members also participated in Cyber Europe 2022 and are gearing up for CySOPex 2023 and Cyber Europe 2024.

To read more: https://www.enisa.europa.eu/news/blue-olex-2023-getting-ready-for-the-next-cybersecurity-crisis-in-the-eu

Number 4

Crypto-assets regulation: from patchwork to framework

Hello everyone – offline, and also, hello everyone online.

It is a pleasure to be back in London. Back at the Bank of England. Back at the 'Old Lady of Threadneedle Street'. The Old Lady that battles inflation, safeguards financial stability and firmly protects… the gold in her vaults. Gold that lies right here, under our feet. 400 000 bars of gold, to be precise.

Now, I am not here to take a peek at that small fraction of gold that is ours. No, today, I was invited to talk about a new type of gold – or, at least, to some it is. I am referring to crypto-assets. Something the Financial Stability Board has consistently been monitoring since 2018.

For a long time, crypto-assets were an experiment on the fringes of the financial system. No shop owner would accept bits and bytes instead of cash or card.

But soon, certain illicit online marketplaces got wind of this new digital asset: selling illegal services or products online had never been this easy. So, regulators and law enforcement agencies sprang into action and took coordinated action to combat money laundering.

Nonetheless, in those early days, chances were very slim that someone had heard of bitcoin or ether, let alone owned them.

And then suddenly – seemingly overnight – crypto-assets became the talk of the town, and everybody seemed to wonder: is this the new gold?

As a result, the total market capitalization of crypto-assets exploded. At the same time, ties with traditional financial parties grew. As did the interest in the underlying technologies.

When the 'crypto winter' hit us last year, it became crystal clear however, that not all that glitters is gold. A sudden change in investor sentiment caused a sharp decrease in crypto-asset prices. That, in turn, led to the spectacular failure of several crypto-intermediaries. Total crypto-asset market capitalization was never really able to recover after that.

But even as crypto-asset prices are in a rut presently, crypto-asset market structures continue to develop at a rapid pace. And at the same time, we see a growing involvement of traditional finance with the crypto-ecosystem – which means that the financial interlinkages between these two worlds are growing as well.

So we cannot exclude that, sooner rather than later, vulnerabilities in crypto-asset markets become big enough to form an actual, transmissible risk to global financial stability. And this risk looms larger if we don't implement comprehensive regulation.

All over the world, national regulators have not been waiting on me to say this. A lot of decisive action has been taken already.

The FSB welcomes these initiatives because they show much-needed willingness to act.

But at the same time, we see a challenge due to crypto's inherent global reach. And that is: how do we ensure consistency between all these regulations?

And how do we deal with crypto parties that choose to operate exactly from those jurisdictions that don't really prioritise the effective regulation and supervision of crypto-asset activities?

To overcome these challenges, the FSB developed a Global Regulatory Framework. This framework, published last July, aims to promote the consistency of regulatory and supervisory practices to address the financial stability risks of crypto-asset activities.

Developing this framework on the basis of consensus among the FSB member authorities has required a careful threading of the needle. And so, I think it is fitting that we find ourselves on Threadneedle Street, today. The perfect place to discuss the FSB's finalized policy work on broader crypto-asset markets and global stablecoin arrangements.

The latter is a specific type of crypto-asset – one that aims to maintain a stable value relative to a pool of assets, usually fiat money. One that carries heightened risks to global financial stability because of its potential systemic relevance in multiple jurisdictions. And so, one that requires special attention.

Because the FSB recommendations are high-level, national authorities can apply these recommendations flexibly, whilst also ensuring a baseline – a baseline that provides for a consistent application of comprehensive regulation across the globe. A baseline that embraces both already existing rules in some countries, and to be drafted regulations in others. A baseline with a clear thread of gold – and that is the principle of "same activity, same risk, same regulation".

Many crypto-asset activities perform functions and, hence, carry risks, that strongly resemble those of traditional financial activities. Think, for example, of the similarities between staking and deposit-taking, or between crypto-lending and securities financing transactions. And so, we believe they should be regulated as such.

A number of our recommendations have to do with the vulnerabilities of centralized crypto-asset intermediaries. And I stress 'centralized' because, however 'de-centralized' the crypto-asset ecosystem claims to be, economic reality tells a different story. In fact, some of these intermediaries already seem to play a systemic role within the crypto-ecosystem.

That is why we recommend that authorities require a number of things from these entities. For instance to have in place robust governance frameworks and to set up risk management practices.

Of course, I know that implementation takes time. But I also know it's high time – as I have often heard my British colleagues say – to 'crack on'. So, let's prioritise the full and consistent implementation of our high-level recommendations.

Because in the meantime, people investing in crypto-assets continue to run serious risks. In the meantime, linkages between the crypto-ecosystem and traditional finance may very well continue to grow. So, in the meantime, risks to financial stability can still escalate.

There are several ways through which we can prevent crypto-asset volatility from spilling over to the traditional financial system. One important way to do this, is with the full and consistent implementation of the BCBS prudential framework for the treatment of banks' crypto-asset exposures.

Putting this global framework into practice limits the chance that crypto-volatility reaches banks and hence becomes a threat to financial stability.

To keep a close eye on the progress made, the FSB will start monitoring implementation. Our first review should be finalized by the end of 2025.

And the FSB will not only monitor progress. If we are serious about regulating what is essentially a cross-border phenomenon, we also need to be serious about cross-border cooperation. About information sharing. About working together.

This also means that we need to venture outside of the FSB jurisdictions. Because several jurisdictions with material crypto-asset activities are not members of the FSB.

Nevertheless, global financial stability ties all of us together. And to safeguard that stability, the FSB members need to engage with these jurisdictions. We need to ensure the needle of their regulatory compass points in the same direction as ours.

To do so, we want to start with positive incentives like outreach, technical workshops, and capacity building to get them prepared. We'll work closely with the IMF, the World Bank and other international organizations on this.

However, chances are we may still see regulatory competition. And so, we cannot exclude that a toughening of regulation in one part of the world pushes crypto-asset parties to relocate to other parts of the world. Parts of the world with weaker regulatory standards.

What we can do, though, is require that traditional financial institutions take additional measures to manage the risks of interacting with crypto intermediaries operating in such jurisdictions. Measures necessary to protect global financial stability. We are not there yet, but if you ask me, we should be heading in that direction.

Just like crypto-asset threats don't stop at national borders, the thread of crypto-asset risks doesn't only weave through financial stability. There are also macroeconomic risks. Specifically for emerging markets and developing countries.

In EMDEs, crypto-assets are relatively popular. The more popular they are, the more they could erode the effectiveness of domestic monetary policy. Because people may start preferring crypto-assets or stablecoins over domestic currencies.

This risk of currency substitution, or so-called 'crypto-ization', means EMDE's might face even greater risks from crypto-assets than advanced economies. A potentially dangerous cocktail of financial stability and macroeconomic risks.

For this reason, the Indian G20 Presidency asked the FSB and the IMF to combine their work on this subject in a synthesis paper. This was published in September. A key conclusion is that crypto-assets do indeed have implications for macroeconomic and financial stability, but even more, that these implications are mutually interactive and reinforcing.

In our view, this underlines, once more, the need for a global regulatory and supervisory baseline to oversee crypto-asset activities.

A baseline that addresses both financial stability and macroeconomic risks. A baseline that all national regulators can adhere to, but at the same time allows them to take targeted and time-bound measures to address jurisdiction-specific circumstances.

To help EMDEs address these serious risks to financial stability, the FSB will investigate how cross-border cooperation between advanced and developing economies can practically be enhanced.

Dear colleagues, today, I've talked about crypto-assets – a concept that is not even 20 years old. The Bank of England's nickname, the 'Old Lady of Threadneedle Street', dates back more than two hundred years. To 1797.

When crypto-assets were still the distant future. Banknotes could still be converted to gold. And France declared war on Britain, and landed on its shores.

Within hours, people rushed to the Bank of England. Asking for gold. The very gold that lies under our feet. And the famous vaults were rapidly emptying out.

Then-prime minister, William Pitt the Younger, tried to put a halt to that. Not because he wanted to preserve gold for financial stability reasons, but to use it to defend Britain.

In a famous cartoon, probably familiar to many of you, you can see William Pitt the Younger trying to 'woo' an old lady (more information(Refers to an external site)).

But in fact, all he wants, is the gold in her pockets and in the chest she sits on. Of course, she is not inclined to give in. Ever since, the Bank of England has been known as the 'Old Lady of Threadneedle Street'.

Today, the 'Old Ladies' many of us work for, will no longer exchange banknotes for gold. But still people look for stable assets – assets that maintain their value over time and allow them to transact with people from around the globe.

Today, these 'Old Ladies', can still not easily be 'woo-ed'. And remain firmly seated on their chests of gold – or, rather, vaults. And today, once more, these 'Old Ladies' are willing to defend what knits us all together and helps to bring global prosperity – and that's financial stability.

Thank you.

To read more: https://www.dnb.nl/en/general-news/speech-2023/crypto-assets-regulation-from-patchwork-to-framework/

Number 5

Dive into the Deep Sea: A View of the Subsea Cable Ecosystem

More than 97% of the world's internet traffic passes through subsea cables at some point. Subsea cables are a vital component of the global internet infrastructure, and it is critical to protect them from cyberattacks, physical attacks and other threats.

What are the challenges?

With the growing reliance on the internet, and the growing amounts of data being transmitted, subsea cable incidents could cause outages and disruptions. The cable landing stations as well as subsea areas, where many cables are close to each other are considered weak points.

The International Cable Protection Committee in its 2022 report concludes that most subsea cable incidents are accidental, due to anchoring and fishing. Some cable incidents are caused by natural phenomena like underwater earthquakes. In rare cases, system failures are responsible for incidents.

Malicious actions such as sabotage attacks and espionage have to be considered also. Particularly, a coordinated sabotage attack on multiple cables at once could cause significant disruptions of internet connectivity. Repairing subsea cables is complex, takes a long time, and requires highly specialised cable repair ships, only few in the world. While eavesdropping on cables on the seabed is considered unlikely, accessing communications data at the cable landing stations or at cable landing points is feasible, and should be considered as a threat.

Global subsea cable ecosystem in a nutshell

- Subsea cables can fall under a wide range of regulatory regimes, laws and authorities. At national level, there may be several authorities involved in their protection, including national telecom authorities, authorities under the NIS Directive, cybersecurity agencies, national coastguard, military, etc.
- There are also international treaties in place to be considered, establishing universal norms and the legal boundaries of the sea,
- On the private sector side, the subsea cable ecosystem consists of undersea cable owners and operators, integrated suppliers, suppliers

without a fleet, owners of installation and repair vessels, and undersea cable maintenance companies.

Key takeaways

- Accidental, unintentional damage through fishing or anchoring has so far been the cause of most subsea cable incidents.
- Natural phenomena such as undersea earthquakes or landslides can have a significant impact, especially in places where there is a high concentration of cables.
- Chokepoints, where many cables are installed close to each other, are single points of failure, where one physical attack could strain the cable repair capacity.
- Physical attacks and cyberattacks should be considered as threats for the subsea cables, the landing points, and the ICT at the landing points.
- There is a lack of information about the resilience, redundancy and capacity of subsea cables and further analysis is needed. The European Commission recently launched a dedicated study for this.
- At a national level, the mandate and supervision over the subsea cables should be clarified, to ensure that the cables and landing points are protected, and that chokepoints are avoided.
- National authorities should exchange good practices about subsea cable protection, involving also authorities for the energy sector, who have experience with protection of subsea power cables, as well as authorities under the Critical Entities Resilience Directive, whose experience with physical protection of critical infrastructure could be insightful.

What are subsea cables?

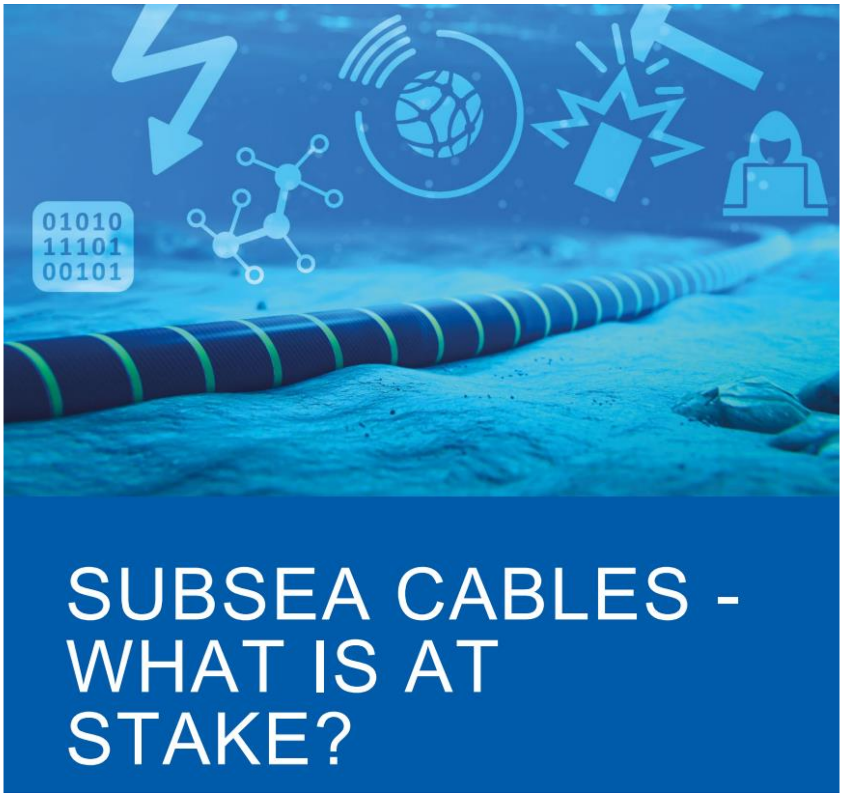
There are about 400 subsea cables across the world, connecting islands, countries, regions, and continents. Subsea cables use optical fibre technology, transmitting electronic communications data at the speed of light. Subsea cables are about as thick as a garden hose. Subsea cables come on land at landing stations, where they connect to the land-based internet backbone, the underground cables. Landing stations can be at beaches or in ports.

Target audience

ENISA publishes this report to support national authorities in the EU Member States supervising telecom networks and core internet infrastructure, under the European Electronic Communications Code (EECC) and the Directive on measures for a high common level of cybersecurity across the Union (the NIS1 and the NIS2). Undersea cables are specifically mentioned in the NIS2 directive, and have to be addressed in national cybersecurity strategies.

To read more: https://www.enisa.europa.eu/news/dive-into-the-deep-sea-a-view-of-the-subsea-cable-ecosystem

SUBSEA CABLES - WHAT IS AT STAKE?



Subsea cables, are some of the most critical components of the global internet infrastructure. Estimates say that more than 97% of the world's internet traffic is transmitted via subsea cables.

Subsea cables are therefore critical for the EU and protecting them from physical and cyber-attacks is strategically important. Modern subsea cables use optical fibre technology to transmit communications data literally at the speed of light.

Close to shore subsea cables are thicker and strengthened with armour, but for most of their length subsea cables have a diameter that is not much greater than that of a garden hose.

Figure 1: Legal boundaries of the ocean *(source: UNCLOS)*

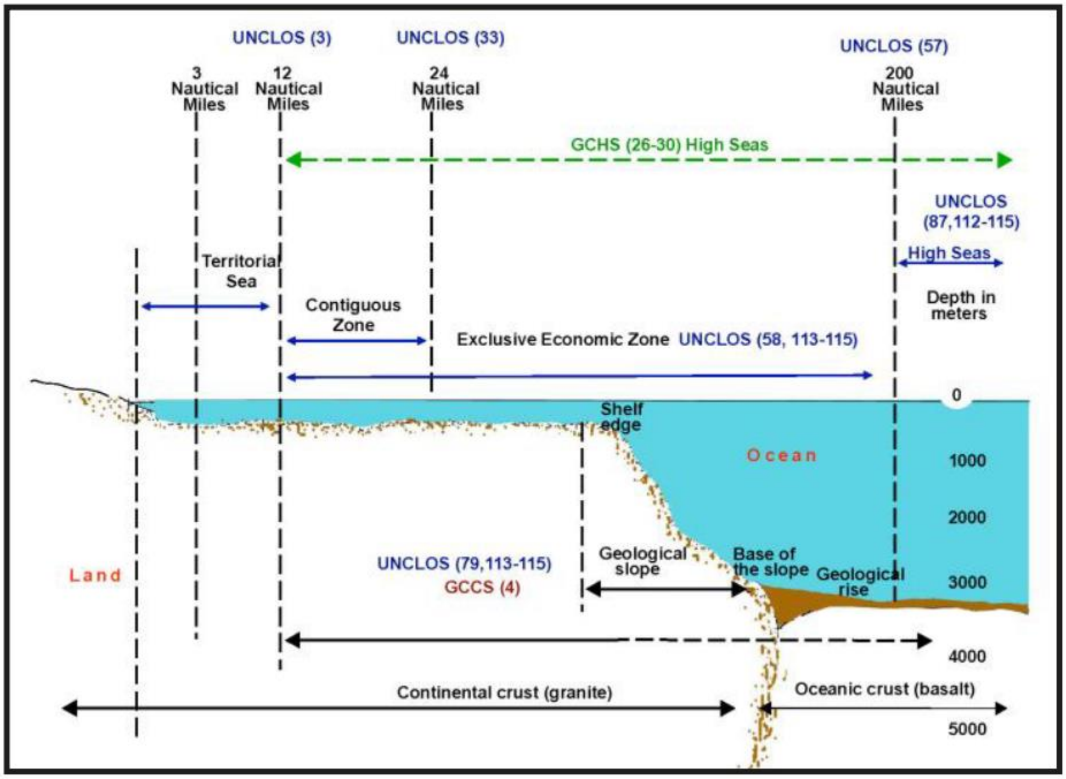
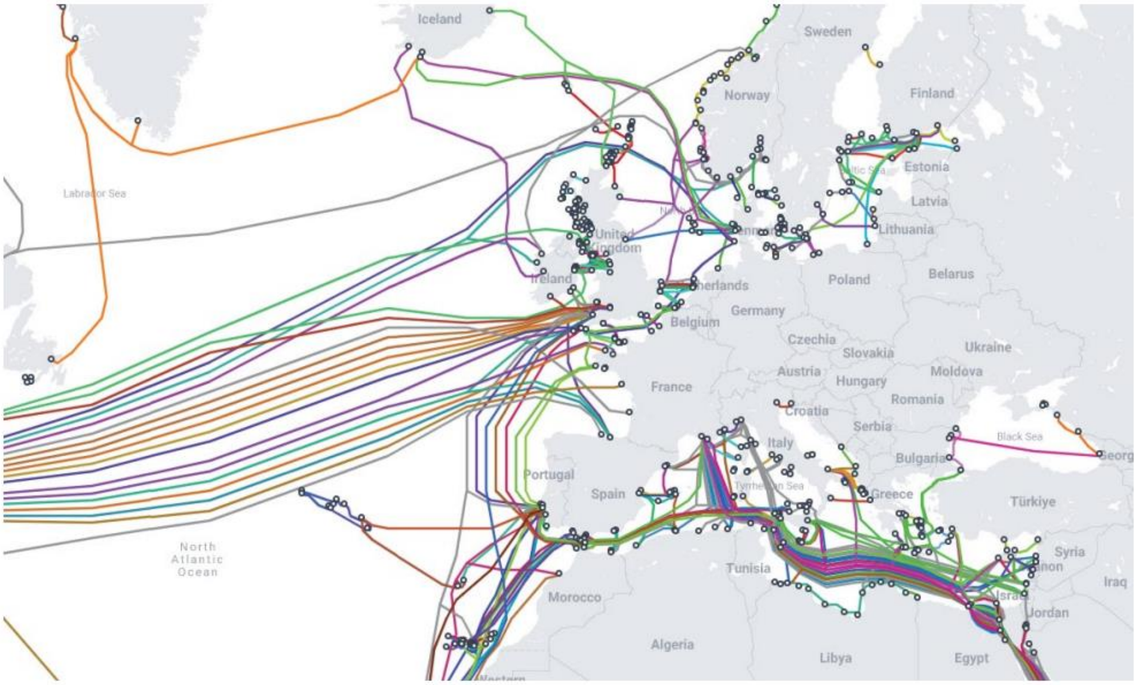


Figure 2: Subsea cable map *(source: SubseaCableMap.org)*



While the number of subsea cables is growing constantly, in 2019 there were more than 378 subsea cables worldwide, spanning more than 1.2 million kilometres.

Subsea cables are covered by national telecom laws, but also by international treaties. In practice, a wide range of different authorities may be involved in the protection of subsea cables, including currently national competent authorities for telecom security, cybersecurity agencies, civil protection, defence, and coast guard.

Although subsea cables can be targets of malicious actions, for instance sabotage attacks, currently, the most common incidents affecting subsea cables have been accidental, unintentional incidents.

Most often the unintentional cable damage is caused by commercial fishing and shipping activities. Sometimes, also natural phenomena can cause cable breaks, for instance underwater earthquakes.

There are about 150-200 accidental, unintentional subsea cable faults every year. The subsea cable landing stations, where the cable surfaces and connects to land-based infrastructure, are located on beaches or in cities, and they can be a weak point.

Cable landing stations can be targeted by attackers, for example, with espionage attacks, deliberate power cuts, sabotage attacks with explosives, or even missile attacks in the case of a military conflict.

Repairing the damage to a subsea cable or to a subsea cable landing station is a complex and difficult, lengthy operation.

Repair is also highly dependent on the availability of specialized and dedicated repair ships, of which there is only a limited number worldwide. In some areas repair may require powerful icebreakers, for instance.

Given the complexity of repair operations and the scarcity of repair capacity, a coordinated attack against multiple subsea cables could have a major impact on global internet connectivity.

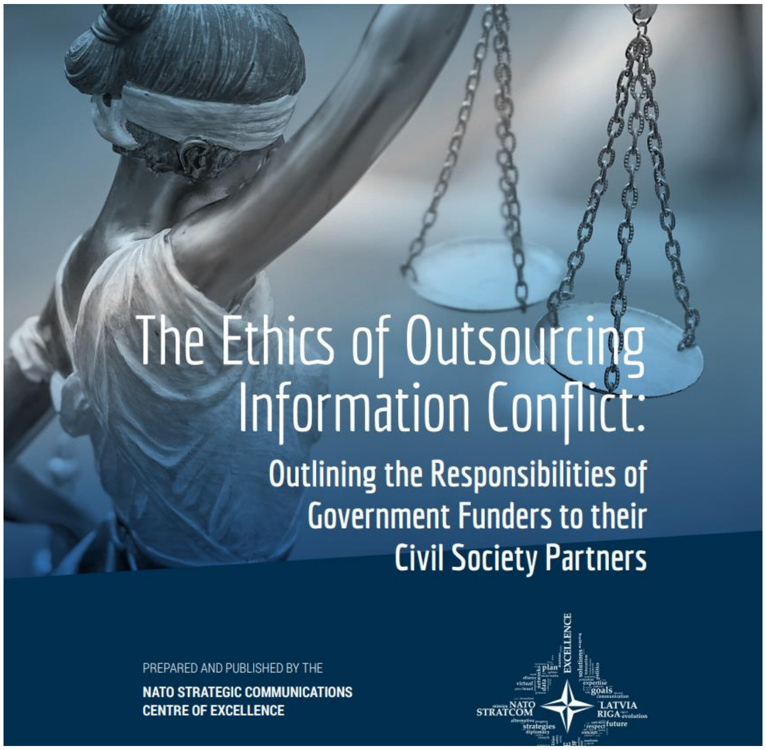
https://www.enisa.europa.eu/publications/undersea-cables

Number 6

The Ethics of Outsourcing Information Conflict

Outlining the Responsibilities of Government Funders to their Civil Society Partners

Non-governmental organisations (NGOs), researchers, journalists, and the private sector are often the main actors actively countering disinformation and influence operations.



The Ethics of Outsourcing Information Conflict:

Outlining the Responsibilities of Government Funders to their Civil Society Partners

PREPARED AND PUBLISHED BY THE

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

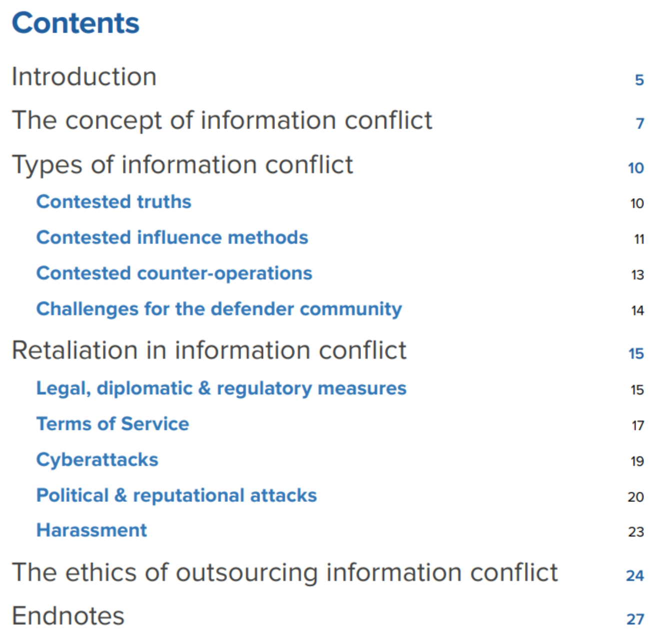
While governments maintain some counter-disinformation capabilities, they tend to outsource much of the day-to-day work through, for example, programmatic funding.

It is more cost effective and credible to fund independent, nonpartisan NGOs to debunk disinformation than for a government to get caught up in trying to correct the sensitive issues that disinformation often entails. Indeed, in a recent Washington Post op-ed, former Radio Free Europe / Radio Liberty President Thomas Kent lauds the role of NGOs in countering disinformation and urges governments to keep finding funding for them:

"Volunteer activists fight it out with trolls online, penetrate and disrupt conspiracy chat rooms, campaign for companies to stop advertising on disinformation sites, and post memes ridiculing Russian propaganda."

They do all the things, in other words, that governments can't or won't do at scale. Similarly, journalists play a central role in exposing and countering disinformation, though they are often not directly backed by governments.

Nor are private sector actors such as intelligence firms and social media companies, although the relationship can be close.



Contents

For the purposes of this report, outsourced (operators/agencies) is then best defined as NGOs, researchers, and other actors who receive direct tasking from a government, as opposed to those who participate in countering disinformation for other (personal, commercial, or ideological) motivations.

This report investigates the roles and responsibilities governments assume when they collaborate in areas of information conflict.

In particular, it assesses the risks to civil society and the private sector when they engage in countering hostile foreign influence operations with funding from governments.

What are governments' options and limitations when supporting civilian populations to counter information attacks? To what extent can and should governments outsource these activities? And what are governments' responsibilities to civil society and the private sector if and when they come under attack by hostile actors?

Conceptually, this report contributes to the field by developing the term information conflict. While disinformation and influence operations are typically the preferred vocabulary for this policy area, both lack a sense of adversarial interaction that characterises the operational realities of countering influence operations.

Information conflict is used to reposition actors engaged in countering disinformation and influence operations as participants in adversarial contestation over questions such as asserting matters of fact and truth, determining the legitimacy of public influence methods, and in the ability to take effective countermeasures.

In practical terms, this report contributes to the field by mapping out a range of adversarial measures that can be taken against non-governmental actors who directly or indirectly support the objectives of governments in information conflict.

This is not a question of connecting influence operations to methods of countering them. It is about the attacks organisations face for participating in information conflict, often designed to remove them from the disinformation-countermeasure dynamic.

It reflects the practical realities of adversarial contestation as it is faced by civil society and the private sector when they take responsibility for engaging adversaries head on.

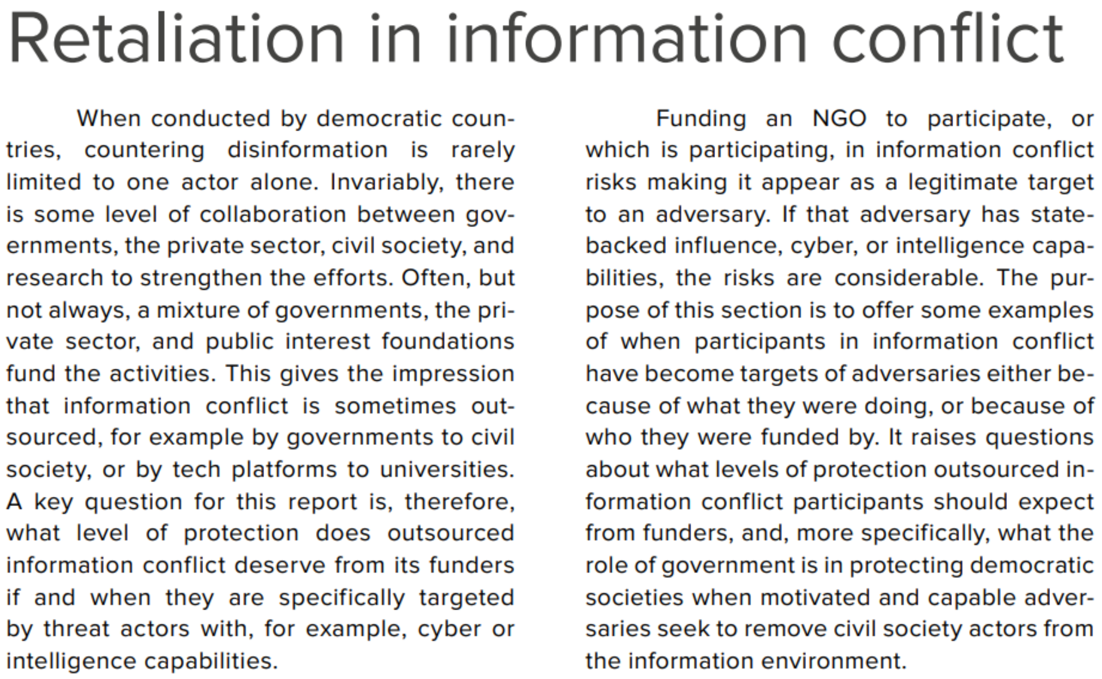
In addressing several areas of information conflict targeting civilian activities, this report maps out some of the most serious risks and makes recommendations for improving the ways in which civil society is protected.

This includes better understanding of vulnerabilities such as legal and regulatory measures, application of terms of service on tech platforms, hack and leak attacks, political and reputational attacks, and harassment of individuals.

There are at present no international norms or standards governing the responsibilities of governments over the organisations they fund or support in information conflict; this report may be seen as the start of a conversation about what best practice could and should look like.

To read more:

https://stratcomcoe.org/publications/the-ethics-of-outsourcing-information-conflict-outlining-the-responsibilities-of-government-funders-to-their-civil-society-partners/292



Retaliation in information conflict

When conducted by democratic countries, countering disinformation is rarely limited to one actor alone. Invariably, there is some level of collaboration between governments, the private sector, civil society, and research to strengthen the efforts. Often, but not always, a mixture of governments, the private sector, and public interest foundations fund the activities. This gives the impression that information conflict is sometimes outsourced, for example by governments to civil society, or by tech platforms to universities. A key question for this report is, therefore, what level of protection does outsourced information conflict deserve from its funders if and when they are specifically targeted by threat actors with, for example, cyber or intelligence capabilities.

Funding an NGO to participate, or which is participating, in information conflict risks making it appear as a legitimate target to an adversary. If that adversary has state-backed influence, cyber, or intelligence capabilities, the risks are considerable. The purpose of this section is to offer some examples of when participants in information conflict have become targets of adversaries either because of what they were doing, or because of who they were funded by. It raises questions about what levels of protection outsourced information conflict participants should expect from funders, and, more specifically, what the role of government is in protecting democratic societies when motivated and capable adversaries seek to remove civil society actors from the information environment.

Number 7

The Commission sends request for information to X under the Digital Services Act

The European Commission services has formally sent X a request for information under the Digital Services Act (DSA).

This request follows indications received by the Commission services of the alleged spreading of illegal content and disinformation, in particular the spreading of terrorist and violent content and hate speech.

The request addresses compliance with other provisions of the DSA as well.

Following its designation as Very Large Online Platform, X is required to comply with the full set of provisions introduced by the DSA since late August 2023, including the assessment and mitigation of risks related to the dissemination of illegal content, disinformation, gender-based violence, and any negative effects on the exercise of fundamental rights, rights of the child, public security and mental well-being.

In this particular case, the Commission services are investigating X's compliance with the DSA, including with regard to its policies and actions regarding notices on illegal content, complaint handling, risk assessment and measures to mitigate the risks identified.

The Commission services are empowered to request further information to X in order to verify the correct implementation of the law.

Next Steps

X needs to provide the requested information to the Commission services. Based on the assessment of X replies, the Commission will assess next steps. This could entail the formal opening of proceedings pursuant to Article 66 of the DSA.

Pursuant to Article 74 (2) of the DSA, the Commission can impose fines for incorrect, incomplete or misleading information in response to a request for information. In case of failure to reply by X, the Commission may decide to request the information by decision. In this case, failure to reply by the deadline could lead to the imposition of periodic penalty payments.

Background

The DSA is a cornerstone of the EU's digital strategy and sets out an unprecedented new standard for the accountability of online platforms regarding disinformation, illegal content, such as illegal hate speech, and other societal risks. It includes overarching principles and robust guarantees for freedom of expression and other users' rights.

On 25 April 2023, the Commission had designated 19 Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) on the ground of their number of users being above 45 million, or 10% of EU population. These services need to comply with the full set of provisions introduced by the DSA since the end of August 2023.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953

Number 8

NIST Interagency Report - NIST IR 8473

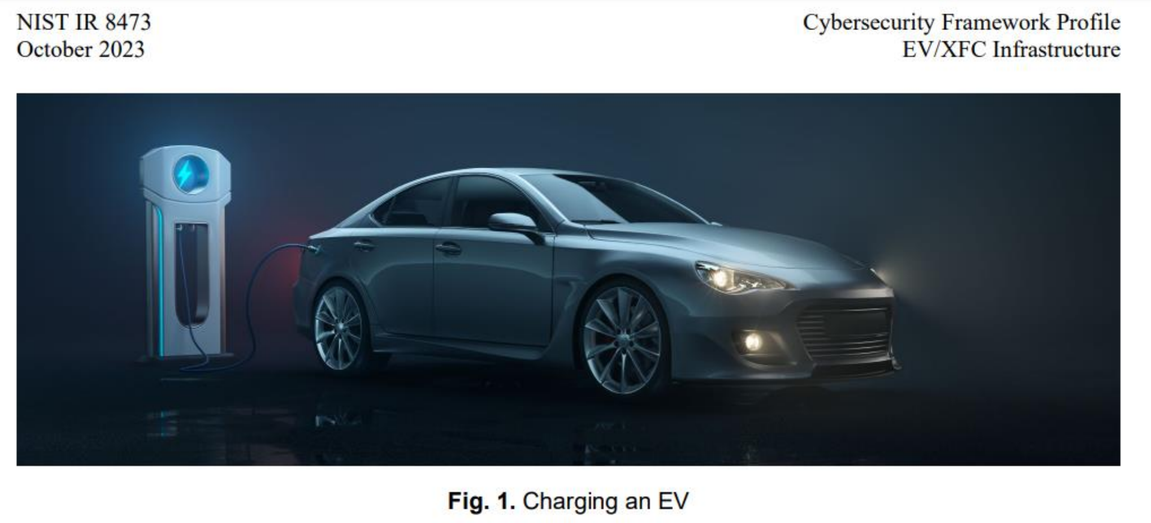
Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure

This document is the Cybersecurity Framework Profile (Profile) developed for the Electric Vehicle Extreme Fast Charging (EV/XFC) ecosystem, including the four domains that relies on the ecosystem:

- (i) Electric Vehicles (EV);
- (ii) Extreme Fast Charging (XFC);
- (iii) XFC Cloud or Third-Party Operations; and
- (iv) Utility and Building Networks.

This Profile utilizes the NIST Cybersecurity Framework Version 1.1 and provides voluntary guidance to help relevant parties develop Profiles specific to their organization to understand, assess, and communicate their cybersecurity posture as a part of their risk management process.

The Profile is intended to supplement, not replace, an existing risk management program or cybersecurity standards, regulations, and industry guidelines that are in current use by the EV/XFC industry.



NIST IR 8473
October 2023

Cybersecurity Framework Profile
EV/XFC Infrastructure

Fig. 1. Charging an EV

The EV/XFC Cybersecurity Framework Profile is designed to be part of an enterprise risk management program to aid organizations in managing threats to systems, networks, and assets within the EV/XFC ecosystem.

The EV/XFC Cybersecurity Framework Profile is not intended to serve as the only solution or as a compliance checklist.

Users of this profile will understand that its application cannot eliminate the likelihood of disruption or guarantee some level of assurance.

NIST IR 8473
October 2023

Cybersecurity Framework Profile
EV/XFC Infrastructure

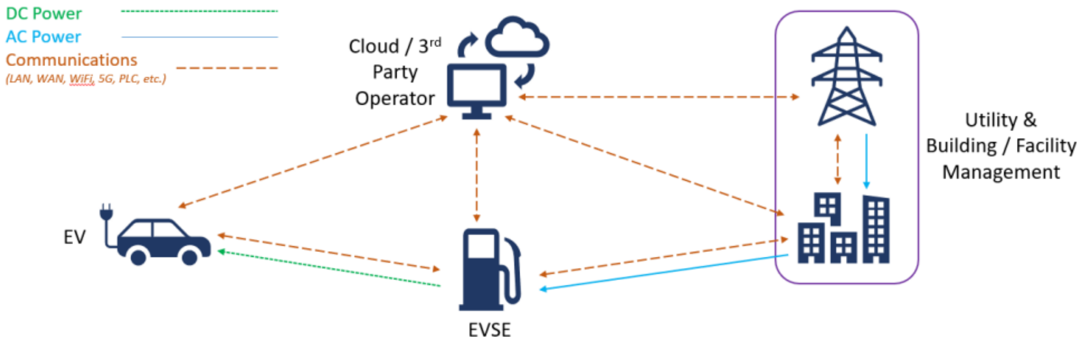

DC Power
AC Power
Communications
(LAN, WAN, WiFi, 5G, PLC, etc.)
Cloud / 3rd Party Operator
Utility & Building / Facility Management
EV
EVSE

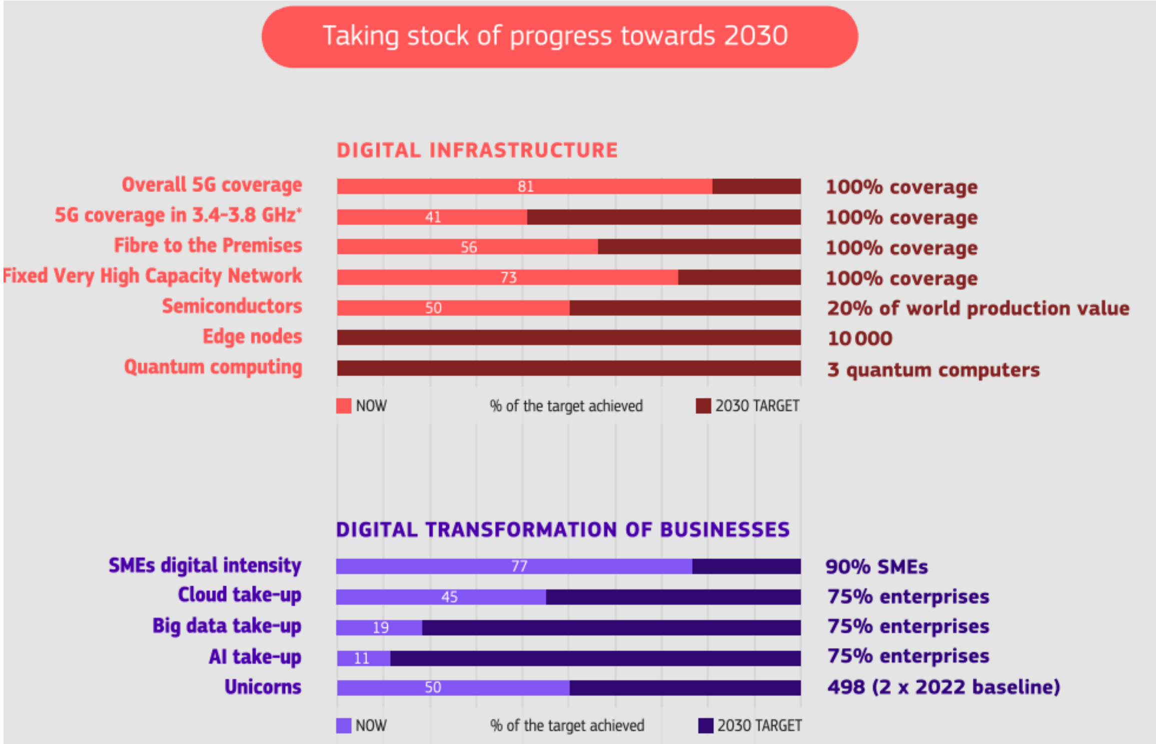
Fig. 2. EV/XFC Ecosystem Domains and Profile Scope

To read more:
https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.pdf

Number 9

27 September 2023 - The first State of the Digital Decade report

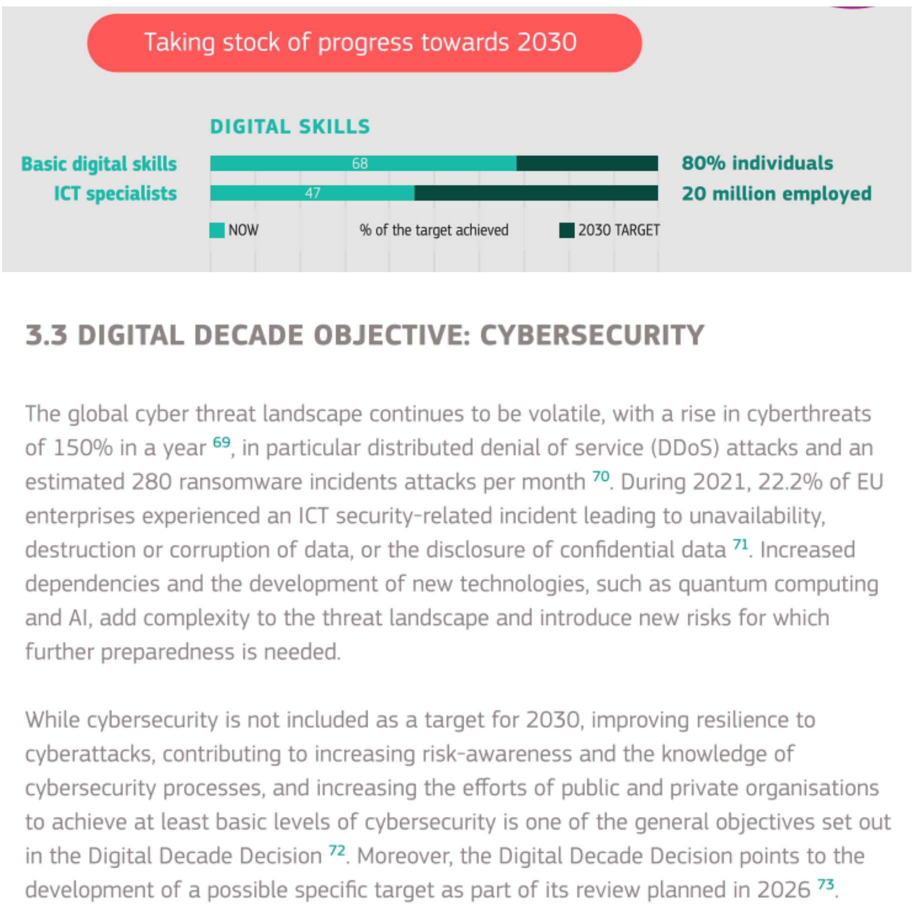
1. Introduction: Delivering the Digital Decade



The first State of the Digital Decade report takes stock of the EU's progress towards a successful digital transformation for people, businesses, and the environment as set out in the Decision establishing the Digital Decade Policy Programme 2030 ("the Digital Decade Decision").

It reviews digital policy developments and describes how the EU is advancing towards the agreed targets and objectives, thus outlining where the EU stands at the outset of the implementation of the Digital Decade Policy Programme.

The overall analysis of the EU's progress against the Digital Decade objectives and targets is shown in Figure 1 and the country reports presented in an annex to this report provide a more detailed picture.


Taking stock of progress towards 2030
DIGITAL SKILLS
Basic digital skills
ICT specialists
68
47
80% individuals
20 million employed
NOW
% of the target achieved
2030 TARGET

3.3 DIGITAL DECADE OBJECTIVE: CYBERSECURITY

The global cyber threat landscape continues to be volatile, with a rise in cyberthreats of 150% in a year [69], in particular distributed denial of service (DDoS) attacks and an estimated 280 ransomware incidents attacks per month [70]. During 2021, 22.2% of EU enterprises experienced an ICT security-related incident leading to unavailability, destruction or corruption of data, or the disclosure of confidential data [71]. Increased dependencies and the development of new technologies, such as quantum computing and AI, add complexity to the threat landscape and introduce new risks for which further preparedness is needed.

While cybersecurity is not included as a target for 2030, improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity is one of the general objectives set out in the Digital Decade Decision [72]. Moreover, the Digital Decade Decision points to the development of a possible specific target as part of its review planned in 2026 [73].

To read more: https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

Number 10

Project Mariana: BIS and central banks of France, Singapore and Switzerland successfully test cross-border wholesale CBDCs

BIS Innovation Hub

Foreign exchange (FX) is the largest financial market in the world, trading about $7.5 trillion a day (BIS (2022b)).

It operates 24 hours a day, five and a half days a week.

Project Mariana looks to the future and envisions a world in which central banks have issued central bank digital currencies (CBDCs) and explores how foreign exchange (FX) trading and settlement might look.

Mariana borrows ideas and concepts from decentralised finance (DeFi) and studies whether so-called automated market-makers (AMMs) can simplify FX trading and settlement with a view to enhancing market efficiency and reducing settlement risk.

Project Mariana is a proof of concept (PoC) for a global interbank market for spot FX featuring both an AMM and wholesale CBDCs (wCBDCs).

In the PoC, wCBDCs circulate on domestic platforms and so-called bridges allow them to be moved on to a transnational network that hosts the AMM.

Project Mariana extends previous experimentation on cross-border settlement using wCBDC arrangements and distributed ledger technology.

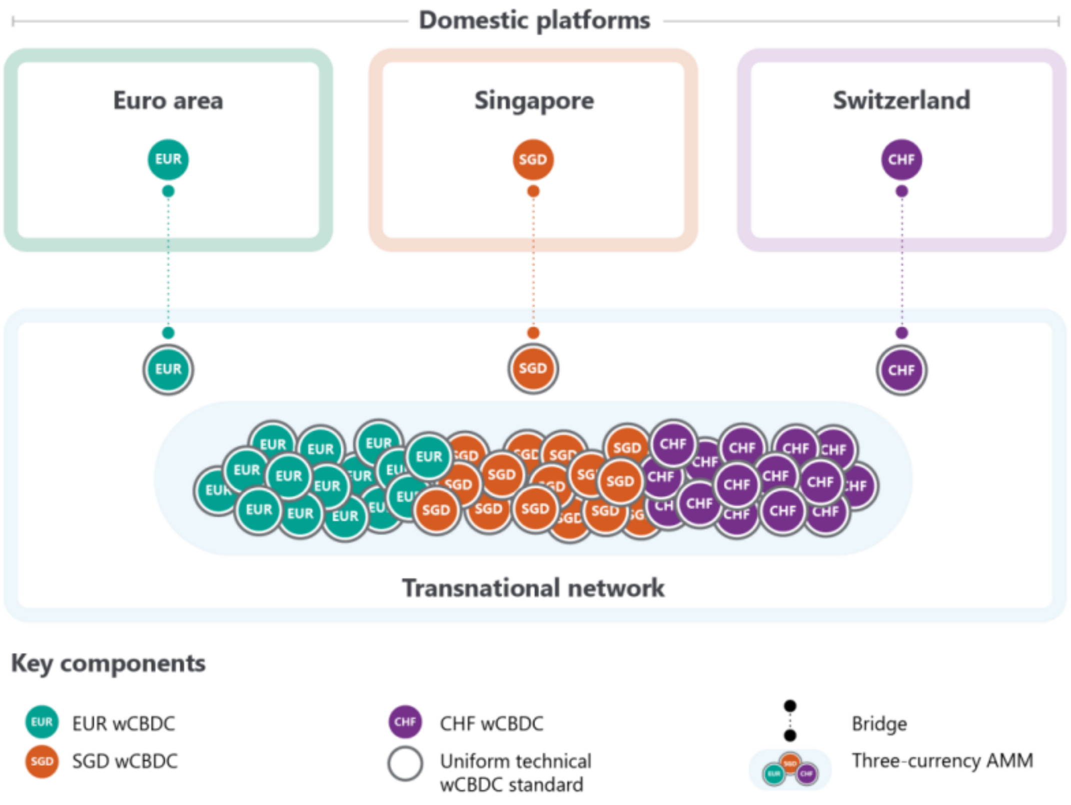
It successfully demonstrates the technical feasibility of the proposed architecture and adds novel insights on the potential of tokenisation in three dimensions.

First, wCBDCs are implemented as smart contracts, enabling central banks to manage their wCBDC without the need to directly operate or control the underlying platform.

Their design followed best practices from the public blockchain space, building on a widely used standard (ie ERC-20), as well as enabling upgradeability.

Second, bridges may serve as a mechanism to enable broader interoperability in an emerging tokenised ecosystem.

Mariana high-level architecture Graph 1



As implemented in the PoC, they may enable the seamless and safe transfer of wCBDC between domestic platforms and the transnational network without manual intervention.

The bridge design features controls and safeguards and ensures resilience through on-chain (ie bridge smart contracts) and off-chain (ie communication between bridge smart contracts) infrastructure managed by central banks.

Third, the AMM, as tested and calibrated in Mariana, fulfilled requirements based on selected FX Global Code (FXGC) principles. It delivers the contours of a possible future tokenised FX market that has a number of potential benefits.

These include supporting simple and automated execution of FX transactions, providing options to broaden the range of currencies, eliminating settlement risk and enabling transparency.

However, the use of AMMs requires the pre-funding of liquidity and their adoption would therefore entail a significant departure from the ex post funding (deferred net settlement) in use in today's FX markets.

To learn more: https://www.bis.org/publ/othp75.pdf

Project Mariana

Cross-border exchange of wholesale CBDCs using automated market-makers

Final report

September 2023

BANQUE DE FRANCE
EUROSYSTÈME

MAS
Monetary Authority of Singapore

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

Number 11

ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA in response to the European Commission's call for advice

The European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published their joint response to the European Commission's Call for Advice on two EC delegated acts under the Digital Operational Resilience Act (DORA) specifying further criteria for critical ICT third-party service providers (CTPPs) and determining oversight fees levied on such providers.

In relation to the criticality criteria, the ESAs propose 11 quantitative and qualitative indicators along with the necessary information to build up and interpret such indicators following a two-step approach.

The ESAs also put forward minimum relevance thresholds for quantitative indicators, where possible and applicable, to be used as starting points in the assessment process to designate critical third-party providers.

This joint response does not include any details of the designation procedure nor of the related methodology as these are out of the scope of this Call for Advice.

However, the ESAs plan to define these details no later than six months after the adoption of the delegated act by the Commission.

Regarding the oversight fees, the ESAs make proposals for determining the amount of the fees to be levied on CTPPs and the way in which they are to be paid.

The ESAs' proposals cover the types of estimated expenditures (for both the ESAs and the competent authorities) that shall be covered by oversight fees as well as the basis for the expenditures' calculation and the available information for determining the applicable turnover of the CTPPs (the basis of fee calculation) and the method of fee calculation together with other practical issues regarding the collection of fees.

In addition, the advice proposes a financial contribution for voluntary opt-in requests. The ESAs will specify other practical aspects on the estimation of oversight expenditures and operational aspects in the context of the implementation of the oversight framework.

Background

In December 2022, the Commission issued to the ESAs a Call for Advice (CfA) in relation to two delegated acts under DORA to:

1) specify further criteria for critical ICT third-party service providers, and

2) determine the fees levied on such providers.

To inform the responses, the ESAs held a public consultation (May-June 2023). In light of the 41 responses received from various stakeholders, the ESAs have amended the draft advice on the criticality criteria to increase the role of critical or important functions in the assessment and further streamlined the proposed set of indicators.

Regarding the oversight fees, the ESAs have, among others, adapted their advice by proposing to define the scope of the applicable turnover on a narrower basis.

Overall, market participants expressed support to the proposals related to the other aspects of the advice, while requesting clarifications on some other points.

To read more: https://www.eiopa.europa.eu/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party-providers-under-dora-2023-09-29_en

Number 12

CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence

Consumers must receive accurate and specific reasons for credit denials

cfpb Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau (CFPB) issued guidance about certain legal requirements that lenders must adhere to when using artificial intelligence and other complex models.

The guidance describes how lenders must use specific and accurate reasons when taking adverse actions against consumers.

This means that creditors cannot simply use CFPB sample adverse action forms and checklists if they do not reflect the actual reason for the denial of credit or a change of credit conditions.

This requirement is especially important with the growth of advanced algorithms and personal consumer data in credit underwriting.

Explaining the reasons for adverse actions help improve consumers' chances for future credit, and protect consumers from illegal discrimination.

"Technology marketed as artificial intelligence is expanding the data used for lending decisions, and also growing the list of potential reasons for why credit is denied," said CFPB Director Rohit Chopra. "Creditors must be able to specifically explain their reasons for denial. There is no special exemption for artificial intelligence."

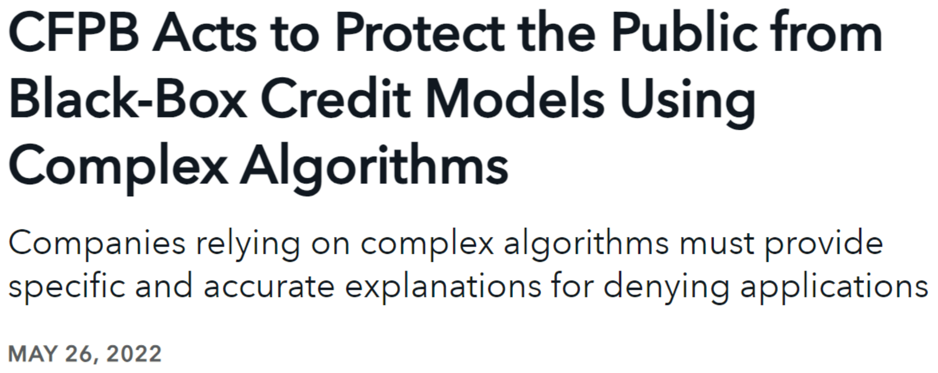
In today's marketplace, creditors are increasingly using complex algorithms, marketed as artificial intelligence, and other predictive decision-making technologies in their underwriting models.

Creditors often feed these complex algorithms with large datasets, sometimes including data that may be harvested from consumer surveillance.

As a result, a consumer may be denied credit for reasons they may not consider particularly relevant to their finances.

Despite the potentially expansive list of reasons for adverse credit actions, some creditors may inappropriately rely on a checklist of reasons provided in CFPB sample forms. However, the Equal Credit Opportunity Act does not allow creditors to simply conduct check-the-box exercises when delivering notices of adverse action if doing so fails to accurately inform consumers why adverse actions were taken.

In fact, the CFPB has confirmed in a circular from last year, that the Equal Credit Opportunity Act requires creditors to explain the specific reasons for taking adverse actions.



CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms

Companies relying on complex algorithms must provide specific and accurate explanations for denying applications

MAY 26, 2022

You may visit: https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/

This requirement remains even if those companies use complex algorithms and black-box credit models that make it difficult to identify those reasons. Today's guidance expands on last year's circular by explaining that sample adverse action checklists should not be considered exhaustive, nor do they automatically cover a creditor's legal requirements.

Specifically, today's guidance explains that even for adverse decisions made by complex algorithms, creditors must provide accurate and specific reasons. Generally, creditors cannot state the reasons for adverse actions by pointing to a broad bucket.

For instance, if a creditor decides to lower the limit on a consumer's credit line based on behavioral spending data, the explanation would likely need to provide more details about the specific negative behaviors that led to the reduction beyond a general reason like "purchasing history."

Creditors that simply select the closest factors from the checklist of sample reasons are not in compliance with the law if those reasons do not sufficiently reflect the actual reason for the action taken.
Creditors must disclose the specific reasons, even if consumers may be surprised, upset, or angered to learn their credit applications were being graded on data that may not intuitively relate to their finances.

In addition to today's and last year's circulars, the CFPB has issued an advisory opinion that consumer financial protection law requires lenders to provide adverse action notices to borrowers when changes are made to their existing credit.

CFPB Issues Advisory Opinion on Coverage of Fair Lending Laws

Equal Credit Opportunity Act continues to protect borrowers after they have applied for and received credit

MAY 09, 2022

You may visit: https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-advisory-opinion-on-coverage-of-fair-lending-laws/

The CFPB has made the intersection of fair lending and technology a priority.

For instance, as the demand for digital, algorithmic scoring of prospective tenants has increased among corporate landlords, the CFPB reminded landlords that prospective tenants must receive adverse action notices when denied housing.

The CFPB also has joined with other federal agencies to issue a proposed rule on automated valuation models, and is actively working to ensure that black-box models do not lead to acts of digital redlining in the mortgage market.

To read more: https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/

Number 13

Extreme Weather and Climate Change

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

CISA protects the critical infrastructure from damage caused by extreme weather and promotes resiliency planning and recovery through collaboration and engagement with stakeholders across the country.

Overview

Over the last 50 years, much of the U.S. has seen increases in prolonged periods of excessively high temperatures and an associated expansion of drought. This contributes to larger wildfires burning more acreage per incident, heavier downpours leading to torrential flooding, more intense winter weather events, stronger tropical storms, and a persistent increase in sea level rise across all coasts as baseline temperatures continue to rise.

These shifts from severe weather to more damaging events nation-wide has led to impacts across all 16 critical infrastructure sectors and a growing need to improve resiliency. Extreme weather events have become far more disruptive and destructive than ever recorded and are projected to steadily worsen as global warming progresses.

CISA's Role

It is CISA's mission to ensure critical infrastructure is protected against extreme weather threats and events. Infrastructure built in the 1900s to early 2000s using climate data from the mid-1900s lacks the ability to withstand the changes occurring in both intensity and frequency of extreme weather events and could experience excessive damage or destruction.

CISA analyzes extreme weather and its impacts to critical infrastructure. We discuss potential increases in weather damages with infrastructure owners and operators, conduct exercises centered around damages from major weather events with stakeholders, and develop resiliency focus documents to outline practical guidelines and strategies for implementation.

CISA analyzes and shares current data trends and findings through:

- Weekly summaries on the national-international climate

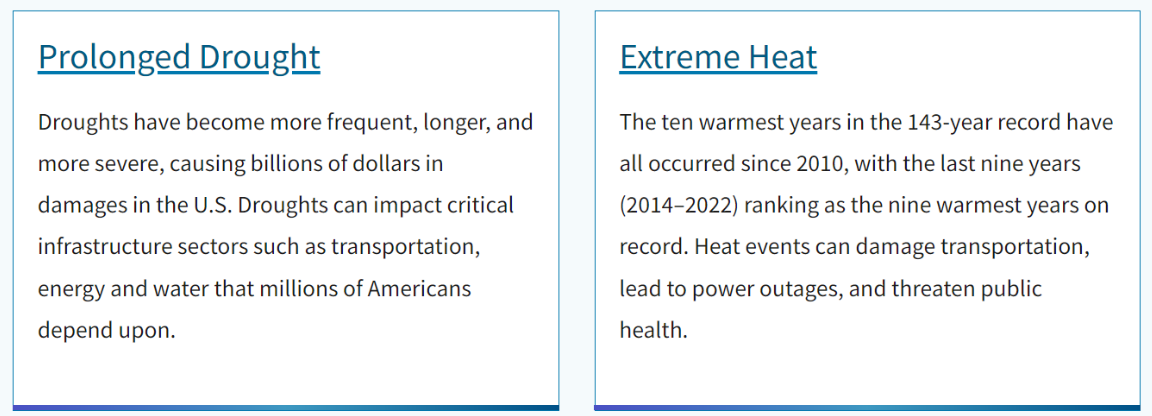
- Presentations about national, regional, state, or infrastructure-related climate shift and the cascading impacts to physical infrastructure, site operations, and community resilience
- Impact analyses of National Critical Functions
- Factsheets to address mitigation options for consideration against climate extremes

Severe Weather vs. Extreme Weather

Severe weather is considered to be an intense variation of a regionally common weather event, such as a heavy rainfall event or damaging winds. Extreme weather identifies the trend of more severe weather events both in frequency and intensity, such as torrential rain (excessive rain periods where over one month of rain can fall during a single storm) or record breaking peak gusts with widespread wind damage.

Extreme weather is the most intense climate element observed during a given period, typically longer lasting or more damaging than the historical 'worst case' events. Infrastructure is built to climatological norms for the 20-40 years prior to development, accounting for typical severe weather events experienced regionally but not planning for withstanding extreme weather events. As climate change continues to amplify extreme weather events, critical infrastructure sites will need to revisit building codes, material limitations, and regional damages during past severe events to address areas at greatest immediate risk.

Extreme Weather Threats



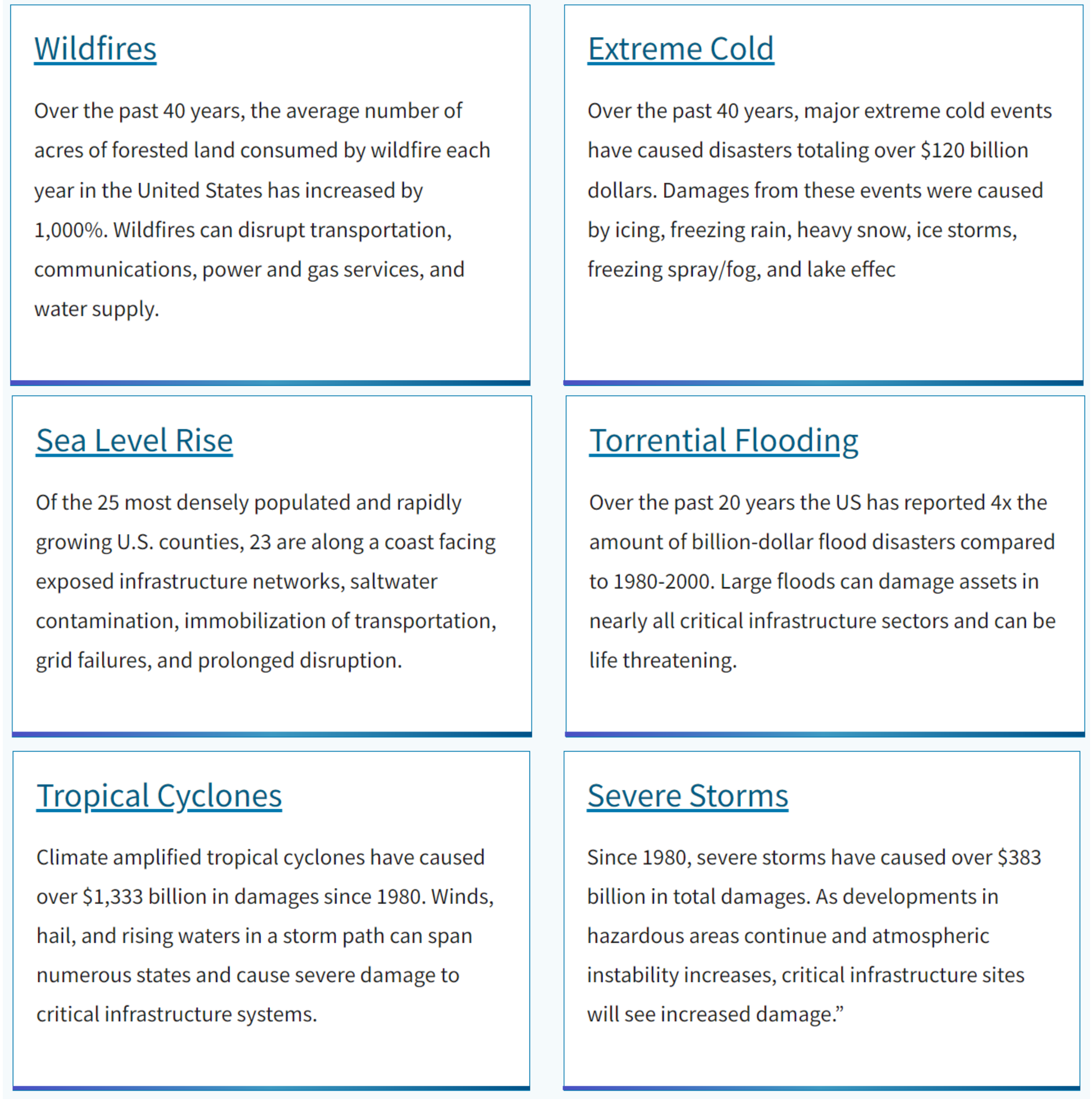
Prolonged Drought

Droughts have become more frequent, longer, and more severe, causing billions of dollars in damages in the U.S. Droughts can impact critical infrastructure sectors such as transportation, energy and water that millions of Americans depend upon.

Extreme Heat

The ten warmest years in the 143-year record have all occurred since 2010, with the last nine years (2014–2022) ranking as the nine warmest years on record. Heat events can damage transportation, lead to power outages, and threaten public health.

Extreme weather threats are occurrences of unusually severe weather of climate conditions that can cause devastating impacts on communities and agricultural and natural ecosystems. Climate change fuels extreme weather threats.



Wildfires

Over the past 40 years, the average number of acres of forested land consumed by wildfire each year in the United States has increased by 1,000%. Wildfires can disrupt transportation, communications, power and gas services, and water supply.

Extreme Cold

Over the past 40 years, major extreme cold events have caused disasters totaling over $120 billion dollars. Damages from these events were caused by icing, freezing rain, heavy snow, ice storms, freezing spray/fog, and lake effec

Sea Level Rise

Of the 25 most densely populated and rapidly growing U.S. counties, 23 are along a coast facing exposed infrastructure networks, saltwater contamination, immobilization of transportation, grid failures, and prolonged disruption.

Torrential Flooding

Over the past 20 years the US has reported 4x the amount of billion-dollar flood disasters compared to 1980-2000. Large floods can damage assets in nearly all critical infrastructure sectors and can be life threatening.

Tropical Cyclones

Climate amplified tropical cyclones have caused over $1,333 billion in damages since 1980. Winds, hail, and rising waters in a storm path can span numerous states and cause severe damage to critical infrastructure systems.

Severe Storms

Since 1980, severe storms have caused over $383 billion in total damages. As developments in hazardous areas continue and atmospheric instability increases, critical infrastructure sites will see increased damage.”

To read more: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/extreme-weather-and-climate-change

Number 14

Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation

RICHARD
BLUMENTHAL
U.S. SENATOR FOR CONNECTICUT

U.S. Senators Richard Blumenthal (D-CT) and Josh Hawley (R-MO), Chair and Ranking Member of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, announced a bipartisan legislative framework to establish guardrails for artificial intelligence.

The framework lays out specific principles for upcoming legislative efforts, including the establishment of an independent oversight body, ensuring legal accountability for harms, defending national security, promoting transparency, and protecting consumers and kids.

The announcement follows multiple hearings in the Subcommittee featuring witness testimony from industry and academic leaders, including OpenAI CEO Sam Altman, Anthropic CEO Dario Amodei, and Microsoft President and Vice Chair Brad Smith who will testify before the Subcommittee on Tuesday.

“This bipartisan framework is a milestone—the first tough, comprehensive legislative blueprint for real, enforceable AI protections. It should put us on a path to addressing the promise and peril AI portends,” said Blumenthal.

“We’ll continue hearings with industry leaders and experts, as well as other conversations and fact finding to build a coalition of support for legislation. License requirements, clear AI identification, accountability, transparency, and strong protections for consumers and kids—such common sense principles are a solid starting point.”

“Congress must act on AI regulation, and these principles should form the backbone,” said Hawley. “Our American families, workers, and national security are on the line. We know what needs to be done—the only question is whether Congress has the willingness to see it through.”

Specifically, the framework would:

Establish a Licensing Regime Administered by an Independent Oversight Body. Companies developing sophisticated general purpose AI models (e.g.,GPT-4) or models used in high risk situations (e.g., facial recognition) should be required to register with an independent oversight body, which would have the authority to audit companies seeking licenses and cooperating with other enforcers such as state Attorneys General. The entity should also monitor and report on technological developments and economic impacts of AI.

Ensure Legal Accountability for Harms. Congress should require AI companies to be held liable through entity enforcement and private rights of action when their models and systems breach privacy, violate civil rights, or cause other harms such as non-consensual explicit deepfake imagery of real people, production of child sexual abuse material from generative AI, and election interference. Congress should clarify that Section 230 does not apply to AI and ensure enforcers and victims can take companies and perpetrators to court.

Defend National Security and International Competition. Congress should utilize export controls, sanctions, and other legal restrictions to limit the transfer of advanced AI models, hardware, and other equipment to China Russia, other adversary nations, and countries engaged in gross human rights violations.

Promote Transparency. Congress should promote responsibility, due diligence, and consumer redress by requiring transparency from companies. Developers should be required to disclose essential information about training data, limitations, accuracy, and safety of AI models to users and other companies. Users should also have a right to an affirmative notice when they are interacting with an AI model or system, and the new agency should establish a public database to report when significant adverse incidents occur or failures cause harms.

Protect Consumers and Kids. Consumers should have control over how their personal data is used in AI systems and strict limits should be imposed on generating AI involving kids. Companies deploying AI in high-risk or consequential situations should be required to implement safety brakes and give notice when AI is being used to make adverse decisions.

A copy of the bipartisan framework can be found at:
https://www.blumenthal.senate.gov/imo/media/doc/09072023bipartisanaiframework.pdf

To read more:
https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-hawley-announce-bipartisan-framework-on-artificial-intelligence-legislation

Number 15

New Spin-Squeezing Techniques Let Atoms Work Together for Better Quantum Measurements

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Opening new possibilities for quantum sensors, atomic clocks and tests of fundamental physics, JILA researchers have developed new ways of “entangling” or interlinking the properties of large numbers of particles.

In the process they have devised ways to measure large groups of atoms more accurately even in disruptive, noisy environments.

The new techniques are described in a pair of papers published in Nature. JILA is a joint institute of the National Institute of Standards and Technology (NIST) and the University of Colorado Boulder.

“Entanglement is the holy grail of measurement science,” said Ana Maria Rey, a theoretical physicist and a JILA and NIST Fellow. “Atoms are the best sensors ever. They’re universal. The problem is that they’re quantum objects, so they’re intrinsically noisy. When you measure them, sometimes they’re in one energy state, sometimes they’re in another state. When you entangle them, you can manage to cancel the noise.”

When atoms are entangled, what happens to one atom affects all the atoms entangled to it. Having dozens — better yet, hundreds — of entangled atoms working together reduces the noise, and the signal from the measurement becomes clearer, more certain.

Entangled atoms also reduce the number of times scientists need to run their measurements, getting results in less time.

One means of entanglement is with a process called spin squeezing. Like all objects that obey the rules of quantum physics, atoms can exist in multiple energy states at once, an ability known as superposition.

Spin squeezing reduces all those possible superposition states in an atom to just a few possibilities. It’s like squeezing a balloon.

When you squeeze the balloon, the middle shrinks and the opposite ends become bigger.

When atoms are spin squeezed, the range of possible states they can be in narrows in some directions and expands in others.

But it's harder to entangle atoms that are farther away from each other. Atoms have stronger interactions with atoms that are closest to them; the farther away the atoms, the weaker their interactions.

Think of it like people talking at a crowded party. People closest to each other can have a conversation, but those across the room can barely hear them, and the information gets lost down the line.

Scientists want the whole party of atoms to talk to each other at the same time. Physicists around the world are all looking at different ways to achieve that entanglement.

"A major goal in the community is to produce entangled states to get higher-precision measurements in a shorter amount of time," said Adam Kaufman, a physicist and JILA Fellow.

Kaufman and Rey worked together on proposals to achieve that entanglement, one of which Rey and her collaborators at the University of Innsbruck in Austria demonstrated.

In this experiment, the team lined up 51 calcium ions in a trap and used lasers to induce interactions between them. This is because the laser excites phonons, vibrations sort of like sound waves between the atoms.

Those phonons spread down the line of atoms, linking them together. In prior experiments, these links were engineered to be static, so an ion could only talk to a specific set of ions when illuminated by the lasers.

By adding external magnetic fields, it was possible to make the links dynamic, growing and changing over time. That meant an ion that could talk to only one group of ions at first could talk to a different group, and eventually, it was able to talk to all other ions in the array.

This overcomes that distance problem, Rey says, and the interactions were strong all the way down the line of atoms. Now all the atoms were working together, and they could all talk to each other without losing the message along the way.

Within a short amount of time, the ions became entangled, forming a spin-squeezed state, but with a little more time, they transformed into what's called a cat state.

This state is named for Erwin Schrodinger's famous thought experiment about superposition, in which he proposed that a cat trapped in a box is both alive and dead until the box is opened and its state can be observed. For atoms, a cat state is a special kind of superposition in which the atoms are in two diametrically opposed states, like up and down, at the same time. Cat states are highly entangled, Rey points out, making them especially great for measurement science.

The next step will be to try this technique with a two-dimensional array of atoms, upping the number of atoms to improve how long they can stay in these entangled states. Additionally, it could potentially let scientists make measurements more precisely and much quicker.

Spin-squeezing entanglement could also benefit optical atomic clocks, which are an important measurement science tool. Kaufman and his group at JILA, along with collaborators in NIST/JILA colleague Jun Ye's group, tested a different method in another study of Nature.

The researchers loaded 140 strontium atoms into an optical lattice, a single plane of light to hold the atoms. They used finely controlled beams of light, called optical tweezers, to place the atoms into little subgroups of 16 to 70 atoms each.

With a high-power ultraviolet laser, they excited the atoms into a superposition of their usual "clock" state and a higher-energy Rydberg state. This technique is called Rydberg dressing.

The clock state atoms are like the quiet people at the crowded party; they don't strongly interact with others. But for atoms in the Rydberg state, the outermost electron is so far from the center of the atom that the atom is effectively very large in size, enabling it to interact more strongly with the other atoms.

Now the whole party is talking. With this spin-squeezing technique, they can create entanglement across the entire array of 70 atoms.

The researchers compared frequency measurements between 70-atom groups and found that this entanglement improved precision below the limit for unentangled particles, known as the standard quantum limit.

Quicker, more precise measurements will allow these clocks to be better sensors to search for dark matter and produce better time and frequency measurements.

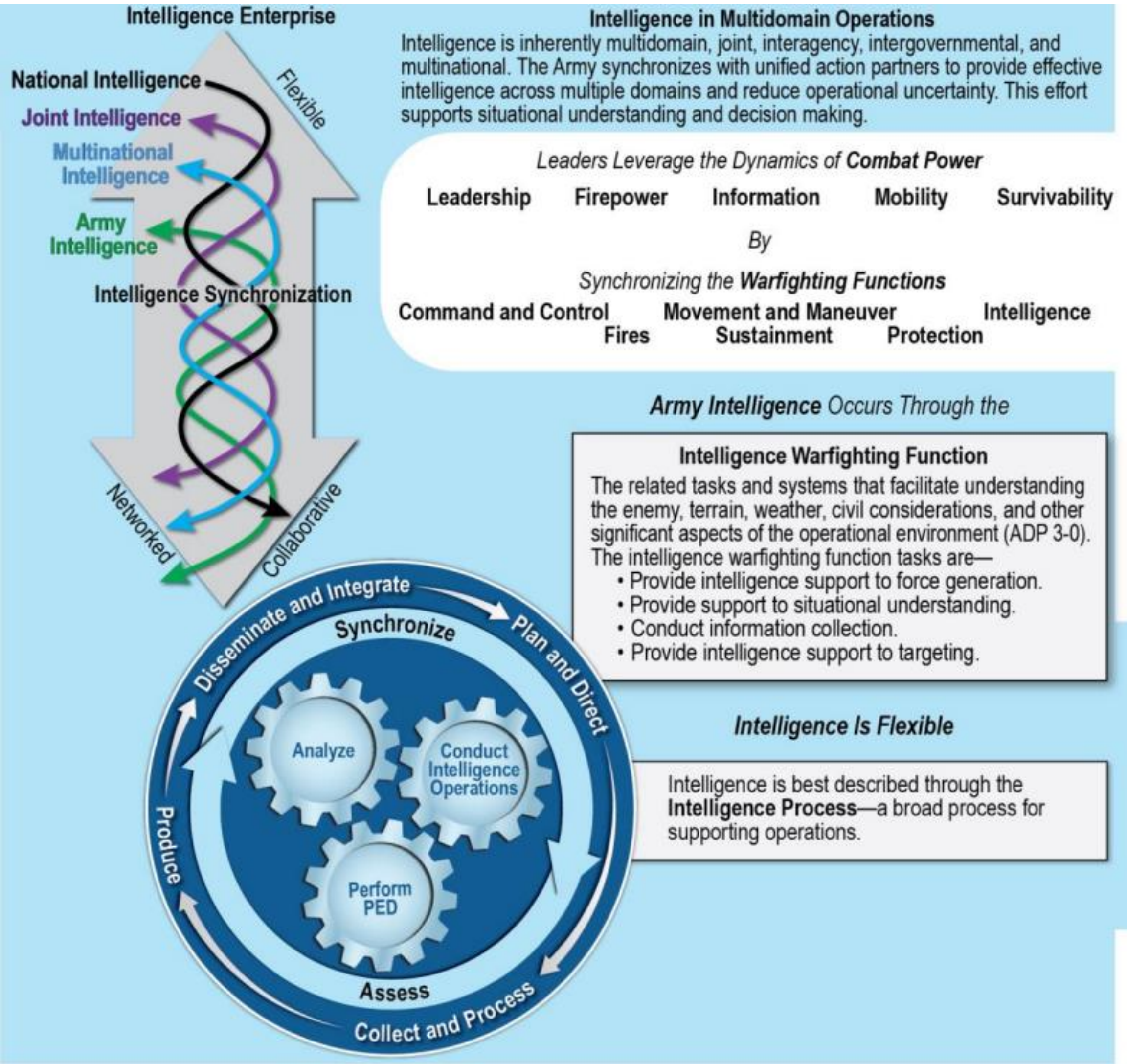
To read more: https://www.nist.gov/news-events/news/2023/09/new-spin-squeezing-techniques-let-atoms-work-together-better-quantum

Number 16

Field Manual (FM) 2-0 - INTELLIGENCE

October 2023, Headquarters, Department of the Army

FM 2-0 represents an important step toward changing the Army culture and improving Army readiness by addressing the fundamentals and tactics associated with intelligence across the Army strategic contexts, within multidomain operations—the Army's operational concept.



Intelligence in Multidomain Operations

Intelligence is inherently multidomain, joint, interagency, intergovernmental, and multinational. The Army synchronizes with unified action partners to provide effective intelligence across multiple domains and reduce operational uncertainty. This effort supports situational understanding and decision making.

Leaders Leverage the Dynamics of ***Combat Power***

Leadership Firepower Information Mobility Survivability

By

Synchronizing the ***Warfighting Functions***

Command and Control Movement and Maneuver Intelligence Fires Sustainment Protection

Army Intelligence *Occurs Through the*

Intelligence Warfighting Function

The related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment (ADP 3-0). The intelligence warfighting function tasks are—

- Provide intelligence support to force generation.
- Provide support to situational understanding.
- Conduct information collection.
- Provide intelligence support to targeting.

Intelligence Is Flexible

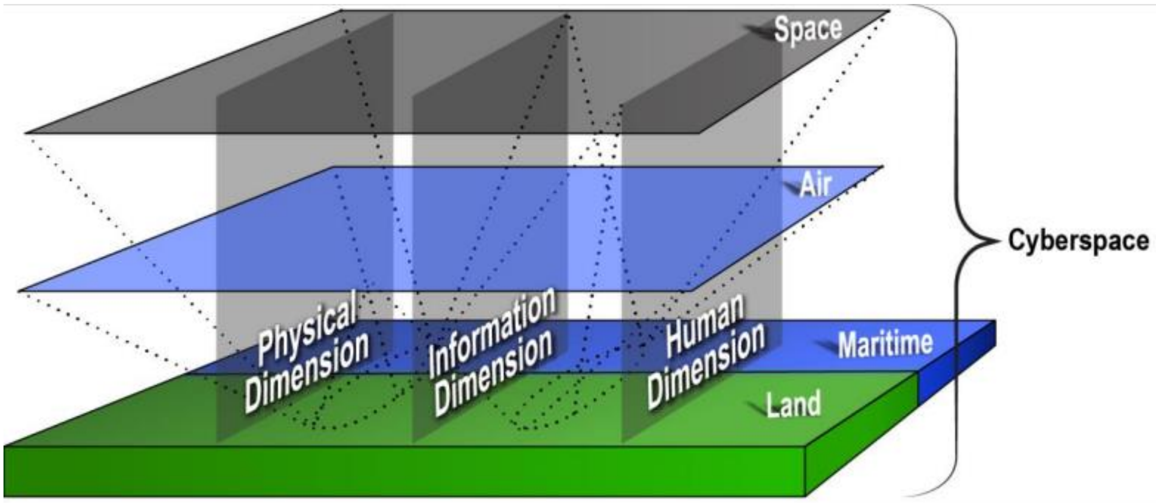
Intelligence is best described through the **Intelligence Process**—a broad process for supporting operations.

This publication describes the role of the commander and staff in intelligence, intelligence staff activities, and how military intelligence (MI) units conduct intelligence operations as part of information collection.

FM 2-0 also contains descriptions of the intelligence warfighting function tasks as well as doctrine on force projection and language support.

The principal audience for FM 2-0 is every Soldier, Army Civilian, and Army contractor participating in or with the intelligence warfighting function. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning joint intelligence.

FM 2-0 also serves as a reference for personnel who are developing doctrine, leader development, material and force structure, and institutional and unit training for intelligence operations.



INTELLIGENCE AS A PRODUCT

Through the effective integration of intelligence into operations, intelligence and operational products are mutually supportive and enhance the commander and staff's situational understanding—the product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables (ADP 6-0).

Intelligence professionals ultimately disseminate intelligence products, either analog (face-to-face, radio, hardcopy) or digital, in many ways. These intelligence products are tailored to the commander and staff's needs and preferences, and they are dictated by the OE, current situation, standard operating procedures (SOPs), and battle rhythm.

It is an art to describe intelligence production and dissemination and to ensure it is effectively integrated into unit planning, execution, and targeting, but it is not an exact science to execute intelligence as a function and create it as a product.

There is always a degree of uncertainty when producing intelligence. Understanding intelligence as a product, with its strengths and limitations, includes understanding the categories of intelligence products, characteristics of effective intelligence, and the goal to adhere to the highest analytic standards.

CATEGORIES OF INTELLIGENCE PRODUCTS

Intelligence products are generally placed in one of eight production categories, based primarily on the purpose of the produced intelligence.

The categories of intelligence products can and do overlap; analysts can find and use some of the same intelligence and information in each of the categories (see JP 2-0):

1. Warning intelligence are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests (JP 2-0). For Army purposes, warning intelligence includes the threat's use of new or first-use of significant existing capabilities, tactics, or courses of action (COAs).

2. Current intelligence provides updated support for ongoing operations. It involves the integration of time-sensitive, all-source intelligence analysis and information reporting on the area of operations (AO). The term current is relative to the commander or decision maker's time sensitivity and the context of the type of operation that is supported.

3. General military intelligence is intelligence concerning the military capabilities of foreign countries or organizations, or topics affecting potential United States or multinational military operations (JP 2-0).

4. Target intelligence is intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance (JP 3-60).

5. Scientific and technical intelligence is foundational all-source intelligence that covers:

   a. foreign developments in basic and applied research and applied engineering techniques and

b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture (JP 2-0).

6. Counterintelligence is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities (JP 2-0).

7. Estimative intelligence is intelligence that identifies and describes adversary capabilities and intentions, and forecasts the full range of alternative future situations in relative order of probability that may have implications for the development of national and military strategy, and planning and executing military operations (JP 2-0).

8. Identity intelligence is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest (JP 2-0).

To read more (328 pages, 28.4 MB) you may visit:
https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39259-FM_2-0-000-WEB-2.pdf

Number 17

The Next Wave - recent advances in NSA's hardware-oriented research.

THE Next Wave Vol. 24 | No. 1 | 2023
The National Security Agency's review of emerging technologies

Note:The Next Wave (TNW) is a journal discussing the research and technological innovation taking place at the NSA. TNW began in 1992 as an internal employee newsletter known as Tech Trend Notes, but as a result of an increase in readership and external requests for the publication, it was released to the public in 2004 with a new name: The Next Wave.

In this issue of The Next Wave (TNW), we conclude our series reviewing recent advances in NSA's hardware-oriented research.

In the last issue, we focused almost exclusively on hardware that will enable the future of high-performance computers, as technologies driven by Moore's Law are sunsetting.

In this issue, we review a broad range of novel architecture, hardware, and sensor research that will enable multiple applications including high - performance and secure computing, radio-frequency (RF) monitoring for secure facilities, localizing electric fields for device fault detection, and flexible antenna arrays for detecting multidirectional signals.

We also include an article that reviews recent results using additive manufacturing techniques to enable electronics and sensors that adapt and conform to the application geometry and environmental constraints of the system.

This issue features authors from multiple research organizations including NSA's research laboratories, the Pacific Northwest National Laboratory, the University of Cambridge, and the University of Maryland. We are extremely grateful for their contributions to this issue.

In the first article, "The road less traveled: Eliminating bottlenecks in high-performance computing networking," the authors provide a historical perspective on the development of different multi-node supercomputing topologies and compare three of the most promising architectures.
In their analysis, the authors argue that nontraditional workloads, such as data analytics and artificial intelligence, will require topologies that dynamically remove bottlenecks and adapt to unpredictable workloads driven by new high-performance computing applications.

The next article introduces new extensions to instruction set architectures developed under the CHERI project to address one of the most difficult and long-standing challenges in cybersecurity: memory security.

Developed over 10 years, CHERI provides new mechanisms for software developers and hardware designers to enforce finegrained memory protection to prevent common bugs that have plagued computing systems for decades.

The authors discuss a CHERI prototype for the Arm processor called Morello that will allow evaluation of the new security enhancements and encourage future adoption.

With the end of Moore's Law, new materials and devices will be required to achieve future computing performance gains.

Some of these devices will operate at cryogenic temperatures, creating a challenging environment for high-bandwidth interconnects which can dissipate significant heat.

The authors of "Evaluating novel interconnects for future cryogenic computers," present their work to establish a test bed for evaluating cryogenic electrical-to-optical devices that provide high-bandwidth data egress from novel devices operating at 4 Kelvin.

Ubiquitous wireless communications protocols and systems have transformed how we communicate.

In the article, "Next-generation radio-frequency monitoring in security environments," the authors consider the security risks posed by the wide proliferation of these signals and discuss the RF monitoring requirements to detect and prevent malicious and unintentional emissions that could transmit sensitive data beyond secure facility boundaries.

Localizing faults in today's integrated circuits is essential to improve the manufacturing process but has become extremely challenging due to shrinking feature size and complex fabrication techniques.

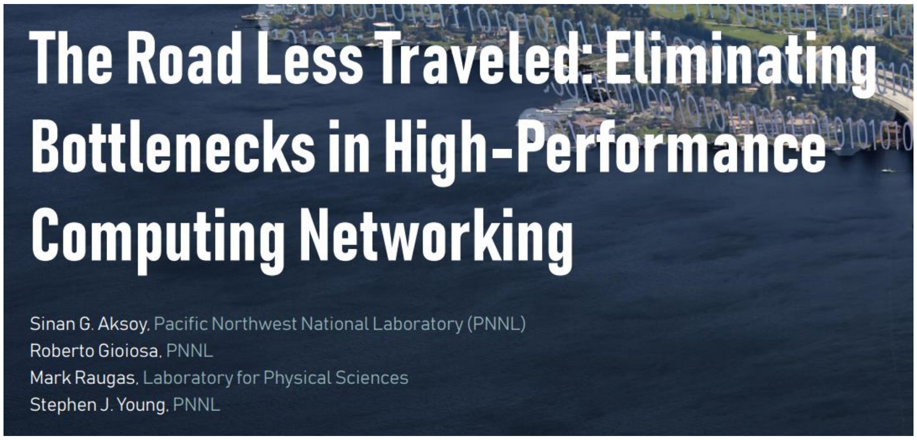
In "Detecting radio-frequency electric fields with optics," the authors present a novel electro-optic sensor that can detect and localize electric fields with high sensitivity to within less than one millimeter of spatial resolution.

These new sensors have potential for a wide range of applications including integrated circuit fault localization and electrical-to-optical conversion of signals.

NATIONAL SECURITY AGENCY

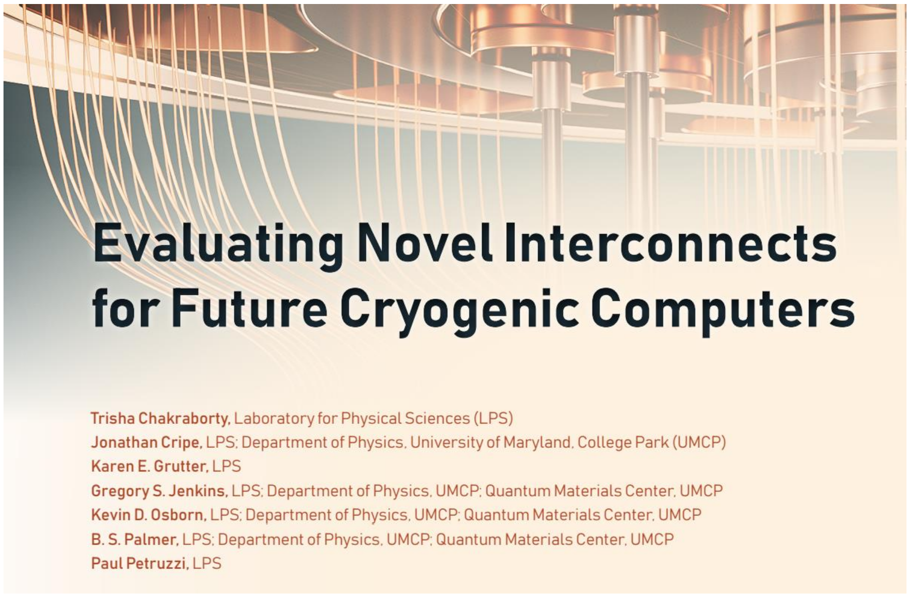
CENTRAL SECURITY SERVICE

To read more: https://media.defense.gov/2023/Jan/23/2003148354/-1/-1/0/TNW_24-1_2023_20230112.PDF



The Road Less Traveled: Eliminating Bottlenecks in High-Performance Computing Networking

Sinan G. Aksoy, Pacific Northwest National Laboratory (PNNL)
Roberto Gioiosa, PNNL
Mark Raugas, Laboratory for Physical Sciences
Stephen J. Young, PNNL



Evaluating Novel Interconnects for Future Cryogenic Computers

Trisha Chakraborty, Laboratory for Physical Sciences (LPS)
Jonathan Cripe, LPS; Department of Physics, University of Maryland, College Park (UMCP)
Karen E. Grutter, LPS
Gregory S. Jenkins, LPS; Department of Physics, UMCP; Quantum Materials Center, UMCP
Kevin D. Osborn, LPS; Department of Physics, UMCP; Quantum Materials Center, UMCP
B. S. Palmer, LPS; Department of Physics, UMCP; Quantum Materials Center, UMCP
Paul Petruzzi, LPS

Number 18

GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT

GEN Paul M. Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), Director of NSA, and Chief of the Central Security Service (CSS), offered insight into what the future of cybersecurity and signals intelligence may look like during a conference in Washington earlier this month.

Looking to the future, GEN Nakasone focused on what he called "the three P's": the imminent period of intense competition with the People's Republic of China (PRC); the need for persistent engagement with public-private partners; and the critical role that the next generation of people will have in providing the United States with a competitive advantage against its adversaries.

"As we think about the future five years hence, I'm very encouraged. I am very, very optimistic," he said during a fireside chat at the annual Billington Cybersecurity Summit. "I look to the future, and I think that our Nation, obviously the folks that work here in the public and the private sector, will all be the beneficiaries."

When GEN Nakasone took the reins in 2018, he said the leading priority for the Command and Agency was securing the 2018 midterm elections. Since then, the continued rise of the PRC and Russia as global threats and the protection of critical systems and infrastructure from cyber threats have grown to become leading priorities.

"Everything that we've done since, we weren't talking about in 2018," said GEN Nakasone, who explained how cybersecurity has become synonymous with national security during his time atop USCYBERCOM and NSA/CSS.

"Now, if I would have said that in 2018, that probably would have raised a lot of eyebrows. But what have we seen since 2018? We've seen supply chain, we've seen zero days, we've seen ransomware, we've seen a number of different actors that have changed and really provided an inflection point for all of us to say, 'Hey, this is a national security issue, and we've got to treat it differently.'"

The Challenge of Artificial Intelligence

At the Billington Cybersecurity Summit, GEN Nakasone revealed the blueprint for AI and machine learning that the Command and Agency will lean on moving forward.

"Much in the sense that the private sector has been doing artificial intelligence for quite a while, we've been doing it for a long time, as well. It's something that we're familiar with," GEN Nakasone said. "We use artificial intelligence primarily with our signals intelligence mission. Now, how do we look at it for our cybersecurity mission? How do we look at it differently for our cybersecurity mission?"

"As we look at the future, we do see tremendous changes. We see the speed, coupled with the security, and coupled with the safeguards that we will ensure are put in place," he added, pointing to how Congress has also tasked USCYBERCOM with developing a five-year plan for AI. ". This is something that we will continue to work at very, very hard going into the future."

The Importance of FISA Section 702 Reauthorization

Leaning on quantitative and qualitative metrics and bolstered by declassified examples, GEN Nakasone took advantage of his participation in the fireside chat to highlight one of the Intelligence Community's most critical foreign intelligence authorities: Section 702 of the Foreign Intelligence Surveillance Act (FISA).

According to GEN Nakasone, FISA Section 702 is an authority that ensures national security and the protection of civil liberties and privacy.

"Of the things that we look at today, 702 reauthorization is among the most important national security issues I think our Nation faces," GEN Nakasone said at the conference.

Among the metrics the Director shared was that FISA Section 702 contributes to 100% of NSA's reporting on the President's intelligence requirements. He noted that in 2022, 59% of the President's Daily Brief articles contained 702 information reported by NSA, and 20% of all NSA's reporting includes 702 acquired information.

GEN Nakasone also highlighted how FISA Section 702 provided insights into the Chinese origins of precursor chemicals key to the production of fentanyl — a drug responsible for more than 100,000 deaths in the U.S. last year. The authority also enabled the U.S. to recover the majority of the ransom from the Colonial Pipeline attack in 2021, and played a key role in the 2022 takedown of al-Qa'ida leader Ayman al-Zawahiri, according to GEN Nakasone.

"It's an authority that has saved lives and assured the protection of our homeland," he said.

To read more: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3533425/gen-nakasone-offers-insight-into-future-of-cybersecurity-and-sigint/

Number 19

Opinion 02/2023

concerning the proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents of 18 April 2023

CURIA RATIONUM
EUROPEAN COURT OF AUDITORS

On 18 April 2023, the Commission published a proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (the "EU Cyber Solidarity Act").

The proposed EU Cyber Solidarity Act lays down measures to detect, prepare for and respond to cybersecurity threats and incidents, in particular through:

- the European Cyber Shield to build and enhance coordinated detection and situational awareness capabilities;

- the Cyber Emergency Mechanism to support member states in preparing for, responding to, and recovering from significant and large-scale cybersecurity incidents;

- the Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.

The legal basis of the Commission's proposal means that consultation with the European Court of Auditors is mandatory.

The European Parliament and the Council of the European Union wrote to us on 2 and 7 June 2023 respectively, asking for our views. This opinion fulfils the consultation requirement.

General observations

Member states bear primary responsibility for preventing, preparing for, and responding to cybersecurity incidents and crises affecting them.

In accordance with Article 4(2) of the Treaty on European Union, national security remains the sole responsibility of each member state.

However, the potential impact of significant or large-scale cybersecurity incidents means that common action at EU level may be necessary.

The ECA welcomes the proposal's objectives to strengthen the EU's collective cyber resilience.

In this opinion, we provide specific comments on the three components of the proposed EU Cyber Solidarity Act and highlight some risks that we have identified in relation to the lack of impact assessment, the financial aspects, and how the measures laid down in the proposal might be implemented.

In particular, we highlight that the proposed Regulation risks making the whole EU cybersecurity galaxy more complex and suggest ways to mitigate this risk (see paragraphs 13-20).

Lack of an impact assessment

The Commission’s better regulation guidelines suggest using impact assessments and stakeholder consultations as part of a comprehensive analysis of policy design and implementation options.

We consider comprehensive impact assessments as an essential tool to consider whether EU action is needed and analyse the potential impacts of available solutions before any proposal is adopted.

This proposed Regulation was not subject to an impact assessment.

In section 3 of the accompanying explanatory memorandum, the Commission explained that it had opted not to carry out such an assessment due to the “urgent nature of the proposal”.

It also said that the measures introduced by the proposed Regulation would be supported by the Digital Europe Programme (DEP), and were in line with the DEP Regulation, which had undergone a specific impact assessment in 2018.

Additionally, the Commission explained that the proposed measures were built upon previous actions prepared in close coordination with the main stakeholders and member states, integrating lessons learned.

However, we note that the DEP impact assessment does not cover the new measures introduced by the proposed Regulation.

There is thus limited information on available policy options and the costs related to the proposal.

Partial information on funding and human resource needs 09 Funding for the measures laid down in the EU Cyber Solidarity Act will come from the DEP.

The Commission stated in section 4 of its explanatory memorandum that €115 million had already been allocated to the European Cyber Shield in the form of pilots during 2021-2022.

It also stated that the proposal would increase the budget of €743 million allocated in 2023-2027 to the DEP's specific objective of cybersecurity and trust by €100 million, through an internal reallocation of funding.

After this reallocation, the EU funding available for cybersecurity will be €843 million for 2023-2027.

We note that this amount covers not only actions laid down in the proposed Regulation, but also other cybersecurity actions in the DEP (such as support for industry or for standardisation).

The proposal does not provide an estimate of the total expected costs related to establishing and implementing the proposed measures (the European Cyber Shield, the Cyber Emergency Mechanism (including the EU Cybersecurity Reserve), and the Cybersecurity Incident Review Mechanism).

As the proposal is not accompanied by an impact assessment, we suggest that the Commission makes these cost estimates available to enhance transparency.

Partial information on the financial set-up of the European Cyber Shield

Chapter II of the proposed Regulation establishes the "European Cyber Shield" composed of national security operations centres (SOCs) and cross-border security operations centres (cross-border SOCs).

The proposed Regulation provides that eligible national SOCs may receive an EU financial contribution covering up to 50 % of the acquisition costs of their tools and infrastructures, and up to 50 % of their operating costs.

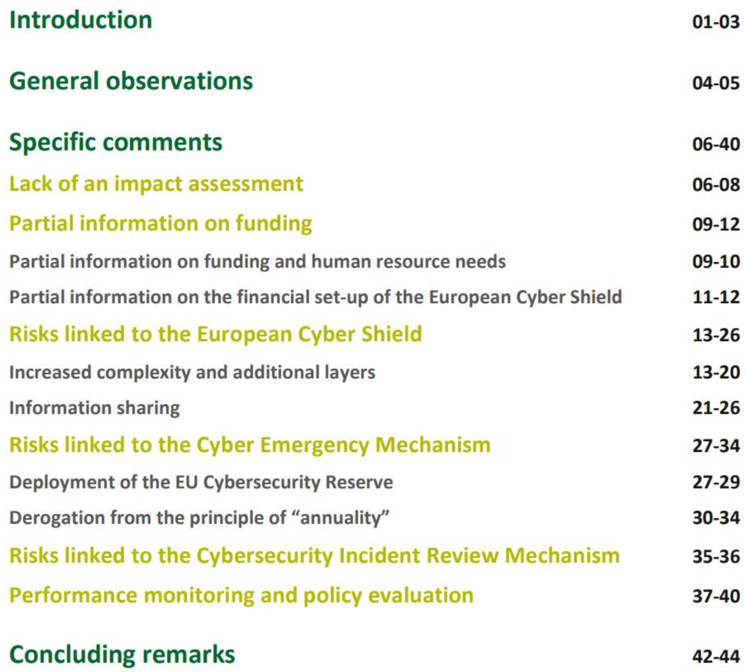
For cross-border SOCs, the EU co-financing is to cover up to 75 % of the acquisition costs of tools and infrastructures, and up to 50 % of the operating costs.

The proposed Regulation does not specify why additional tools and infrastructures, supported at a higher co-financing rate, are needed in cross-border SOCs compared to the tools available to national SOCs in a consortium.

The proposed Regulation also does not specify how long national and cross-border SOCs' operating costs will be co-financed by the EU.

This creates a risk that the operation of the European Cyber Shield and its sustainability become dependent on EU financing

To read more: https://www.eca.europa.eu/ECAPublications/OP-2023-02/OP-2023-02_EN.pdf



Number 20

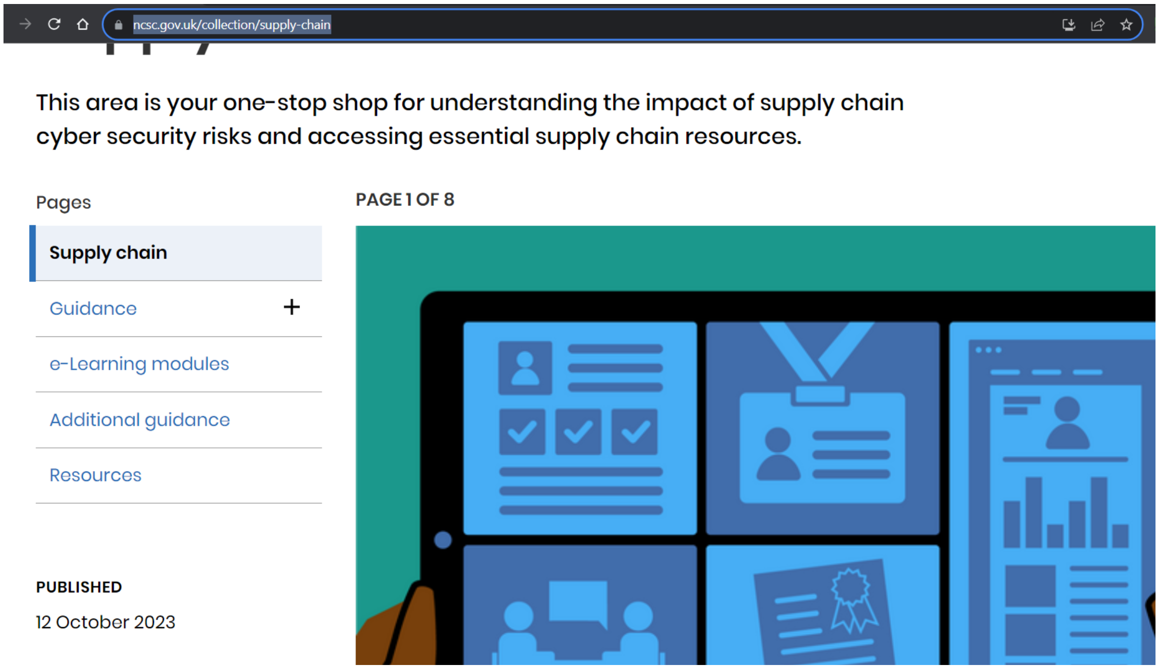
Mastering your supply chain

A new collection of resources from the NCSC can help take your supply chain knowledge to the next level

National Cyber
Security Centre

Whether you're a seasoned professional or just starting your journey in the world of supply chain security, we've got something special for you.

We're delighted to introduce a new collection of content that's dedicated to supply chain cyber security. You can think of it as your one-stop shop for understanding the impact of supply chain cyber security risks. You may visit: https://www.ncsc.gov.uk/collection/supply-chain



ncsc.gov.uk/collection/supply-chain

This area is your one-stop shop for understanding the impact of supply chain cyber security risks and accessing essential supply chain resources.

PUBLISHED

12 October 2023

We've created this collection so no matter what your level of expertise, everyone will be able to quickly access valuable resources, guidance, and knowledge. This includes:

1. **An introduction to supply chain risk.** If you're new to the domain, this section can help you understand the complexities and nuances of supply chain risk. It includes insightful information and guides to help you navigate supply chain challenges effectively.

2. **Supply chain guidance.** This section is for those looking for expert, detailed advice that covers best practices in supply chain management. This guidance is the fundamental framework for enhancing your supply chain cyber security assurance.

3. **Supply chain learning modules.** This section features two e-learning modules, designed to accompany the supply chain guidance. No login is required, just click on the link and start learning. Alternatively, you can integrate these training packages into your own training platform by downloading the SCORM-compliant files that are included.

There's also a wide range of downloadable resources, infographics, and additional guidance that we'd encourage you to share within your organisation (and amongst your suppliers).

This includes guidance from our colleagues at the US government's CISA (Cybersecurity and Infrastructure Security Agency) and the UK's NPSA (National Protective Security Authority).

To learn more: https://www.ncsc.gov.uk/blog-post/mastering-your-supply-chain

Number 21

Wearable sensor to monitor 'last line of defense' antibiotic

Sandia sensor system can track antibiotic levels in real time

Since the discovery of penicillin in 1928, bacteria have evolved numerous ways to evade or outright ignore the effects of antibiotics. Thankfully, healthcare providers have an arsenal of infrequently used antibiotics that are still effective against otherwise resistant strains of bacteria.

Researchers at Sandia National Laboratories have combined earlier work on painless microneedles with nanoscale sensors to create a wearable sensor patch capable of continuously monitoring the levels of one of these antibiotics.

The specific antibiotic they're tracking is vancomycin, which is used as a last line of defense to treat severe bacterial infections, said Alex Downs, a Jill Hruby Fellow and project lead. Continuous monitoring is crucial for vancomycin because there is a narrow range within which it effectively kills bacteria without harming the patient, she added.

"This is a great application because it requires tight control," said Philip Miller, a Sandia biomedical engineer who advised on the project. "In a clinical setting, how that would happen is a doctor would check on the patient on an hourly basis and request a single time-point blood measurement of vancomycin. Someone would come to draw blood, send it to the clinic and get an answer back at some later time. Our system is one way to address that delay."

The researchers shared how to make these sensors and the results of their tests in a paper recently published in the scientific journal Biosensors and Bioelectronics.

Making electrochemical microneedle sensors

The sensor system starts with a commercially available microneedle, commonly used in insulin pens. Adam Bolotsky, a Sandia materials scientist, takes a polymer-coated gold wire about ¼ the thickness of a human hair and trims one end at an angle. He then carefully inserts the gold wire into the needle, solders it to a connector and ensures it is electrically insulated.

The researchers also construct reference and counter electrodes in a similar manner, using coated silver and platinum wires inside commercial microneedles, respectively.

These needles are then inserted into a plastic patch, the size of a silver dollar, designed by Sandia technologists Bryan Weaver and Haley Bennett. This patch includes room for nine microneedles but can be adjusted for any number desired, Downs said. On the exposed, diagonal surface of each gold wire, the researchers chemically attach the nanoscale sensors.

The sensors, called aptamers, are strands of DNA with a surface linker on one end and an electrically sensitive chemical on the other. Downs explained that when the DNA binds to the antibiotic vancomycin, it changes its shape, bringing the electrically sensitive chemical closer to the gold surface. This movement increases the current detected by the sensor system. When the concentration of vancomycin decreases, some of the DNA returns to its original shape, which is also detected electrically.

“This reversibility is useful for things like real-time measurements,” Downs said. “If you want to see the concentration of a certain chemical present in the skin or in the blood at any given time, then being able to measure increases and decreases is really important.”

Downs worked with the aptamer sensor during her doctoral research and brought the knowledge with her to Sandia, where she worked to combine it with Sandia’s expertise with microneedles that can provide doctors with similar information of a blood draw with less pain.

“I merged my knowledge of aptamer-based sensing and real-time monitoring with the technology that Ronen Polsky and Phil Miller had developed at Sandia,” Downs said. “By integrating these two tools, we substantially miniaturized the sensing system and verified that it worked in a microneedle.”

To read more: https://newsreleases.sandia.gov/antibiotic_sensor/

Number 22

A New Take on Modeling & Simulation for Improved Autonomy

DARPA seeks proposals to rapidly repurpose or transfer autonomy to new and different missions

Multiple factors limit the potential of modern autonomous systems (e.g., self-driving vehicles and uncrewed aircraft and watercraft).

Autonomy is learned through modeling and simulation, given the expense of training in the real world. Generally, it goes like this:

1. A model of the intended platform requiring autonomy is created.

2. The model goes through various simulations in an environment as realistic as possible to generate the data that trains the autonomous system to make the right decisions.

3. After sufficiently training the model, those learnings are transferred to a physical system and tested to ensure the training works.

Training models in high-fidelity environments for Defense Department platforms can sometimes take months to even years. Furthermore, autonomy becomes vulnerable when faced with unknown situations/observations in the real world.

This brittleness is known as the simulation-to-real (sim-to-real) gap. For example, a drone moving from a dense city to a coastal environment would encounter a dramatically different observation space.

Unlike commercial autonomous systems, such as warehouse robotics or autonomous vehicles operating in a controlled environment using geofencing, military systems have far more unknown variables.

For instance, flight dynamics could be off, the lighting conditions are likely to vary, and it's often impossible to model an adversary precisely as they act in the real world.

Contrary to the conventional wisdom of high-fidelity simulation, DARPA experts theorize that learning and transferring autonomy across diverse, low-fidelity simulations leveraging their shared semantics (e.g., rules of engagement) instead can lead to a more rapid transfer of autonomy from simulation to reality – perhaps even as early as the same-day versus weeks/months with traditional approaches.

Moreover, moving from complex/realistic simulations to abstract and imprecise ones could allow systems to better adapt to the quick and inevitable changes in dynamic environments.

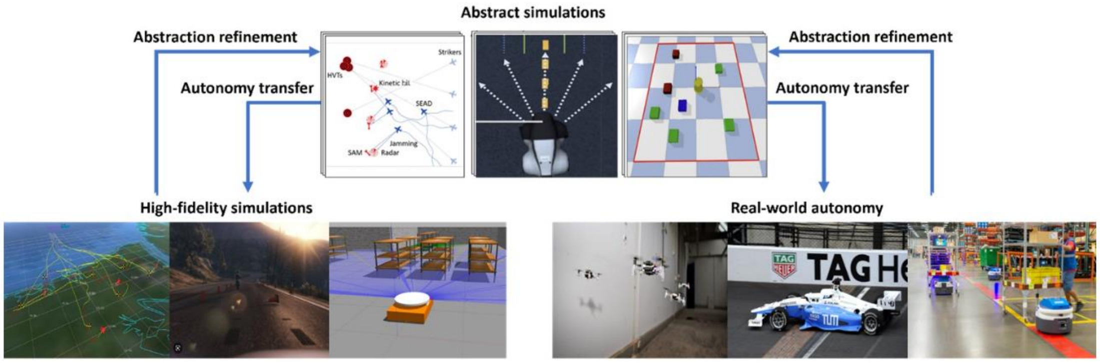
The Transfer from Imprecise and Abstract Models to Autonomous Technologies program seeks proposals that put this theory to the test.

Modeling everything in high fidelity makes it so the AI agent overfits to the dynamics of the simulation," said Dr. Alvaro Velasquez, DARPA's program manager for the effort.

"When you go to the real world, nothing looks exactly like what you modeled/simulated. We want generalizable autonomy across a variety of platforms and domains."

Velasquez hypothesized that low-fidelity simulations would generate data at a much greater speed and scale, introducing the possibility of generalization rather than memorization.

Our vision is to learn autonomy over very diverse and abstract simulations," said Velasquez. "We're going to transfer that autonomy to our diversity of platforms and environments, and we're going to explore the reverse direction. Once we collect this real-world experience, we'll explore how to refine our abstractions, models, simulations, and semantic representation to establish a feedback loop for more robust transfer learning.



The program will feature sim-to-sim and sim-to-real competitions at the end of Phases 1 and 2, respectively, with the results of the first competition being used to down-select from six performers to three.

The program is organized into two phases.
Phase 1 is 18 months and will develop sim-to-sim autonomy transfer techniques and novel methods for automatically developing or refining low-fidelity models and simulations to be used for transfer.

Phase 2 is 18 months and will develop sim-to-real autonomy transfer techniques and novel methods for automatically developing or refining low-fidelity models and simulations to be used for transfer.

There will be two in-program competitions corresponding to the two phases of the program.

For technical details and abstract and proposal instructions, visit the program solicitation at SAM.gov:
https://sam.gov/opp/0399474725314fd58f34bc29849ce305/view

The replay video of the program's Proposers Day is available here:
https://www.youtube.com/watch?v=KK2ubcDONRg

To read more: https://www.darpa.mil/news-events/2023-10-16

Disclaimer

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

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

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

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

This information:

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

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

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

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

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

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

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

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

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

General Terms and Conditions for all visitors to the Cyber Risk GmbH websites, and all legal transactions made through the Cyber Risk GmbH websites:
https://www.cyber-risk-gmbh.com/Impressum.html

Cyber Risk GmbH

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

Cyber Risk GmbH offers:

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

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

Instructor-led training in Baur au Lac, Zurich

BAUR AU LAC

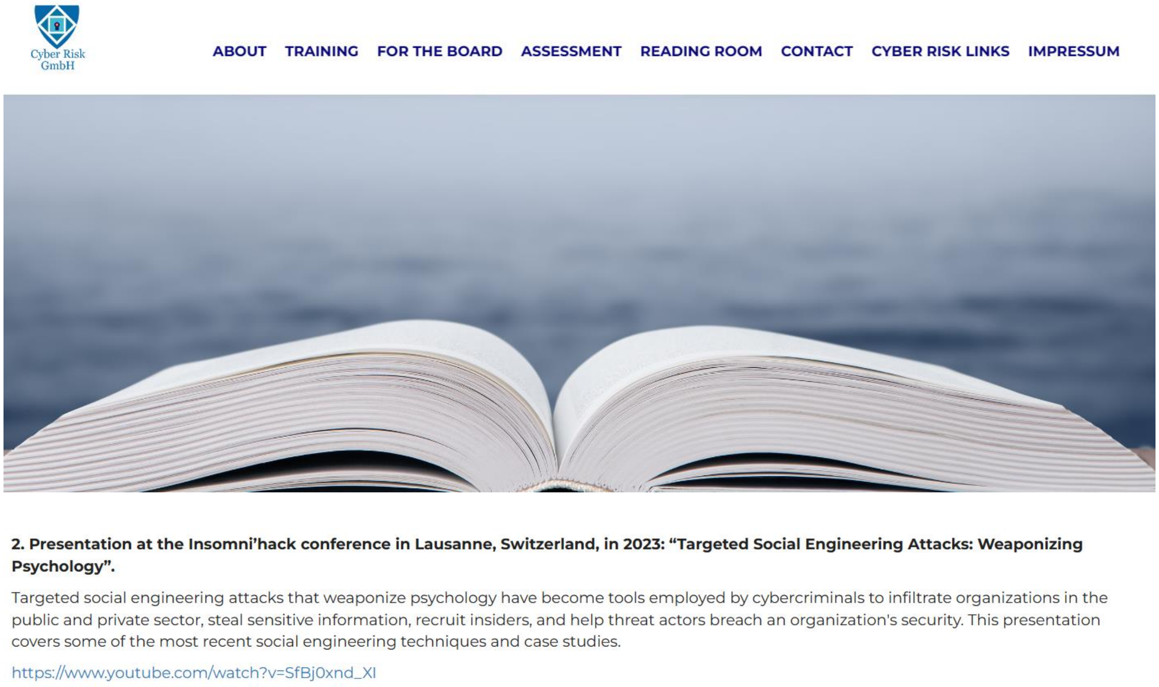
- Great training, exceptional venues.
- Presentations for the Board and the C-Suite.

CEO Briefings in Baur au Lac, Zurich

BAUR AU LAC

- CEO Briefings, answering the questions of the CEO.

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



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

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

https://www.youtube.com/watch?v=SfBj0xnd_XI

Our websites include:

a. Sectors and Industries.

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

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

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

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

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

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

7. Oil Cybersecurity - https://www.oil-cybersecurity.com

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

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

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

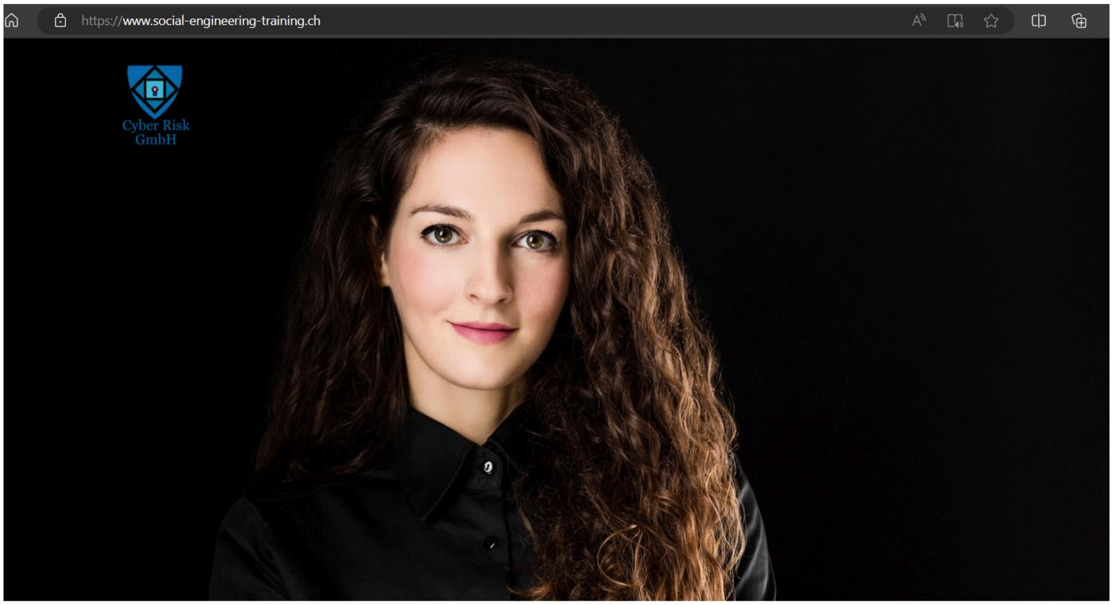
11. Transport Cybersecurity - https://www.transport-cybersecurity.com

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

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

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

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



b. Understanding Cybersecurity.

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

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

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

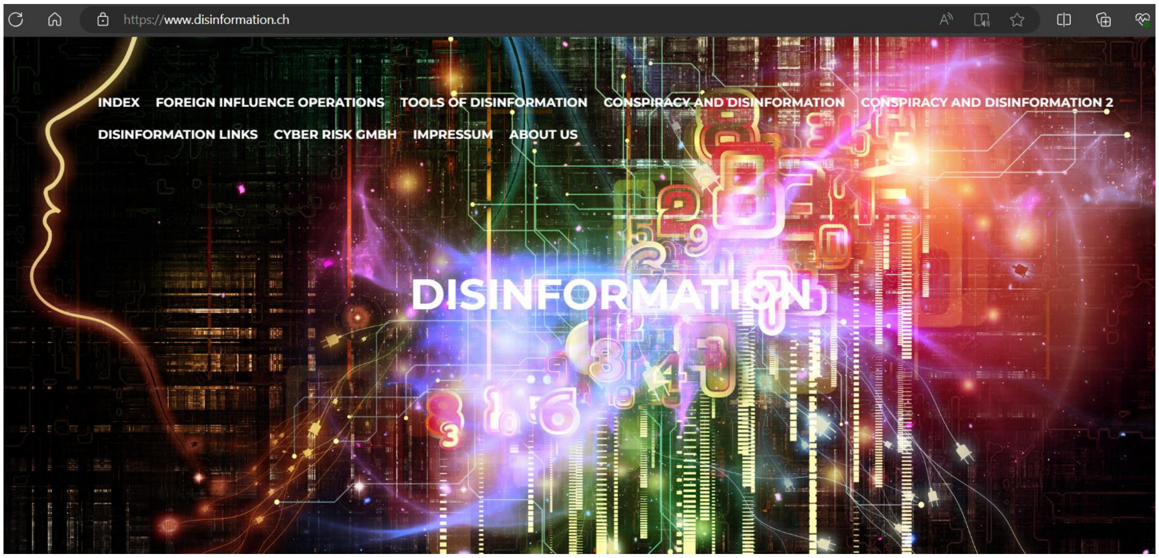
4. What is Synthetic Identity Fraud? - https://www.synthetic-identity-fraud.com

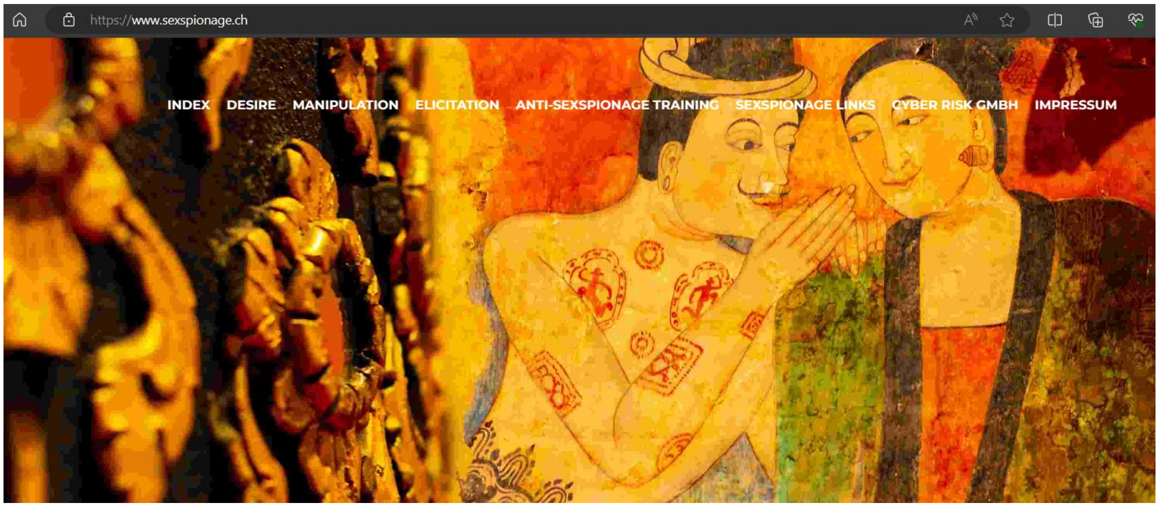
5. What is a Romance Scam? - https://www.romance-scams.ch

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

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

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


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



c. Understanding Cybersecurity in the European Union.

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

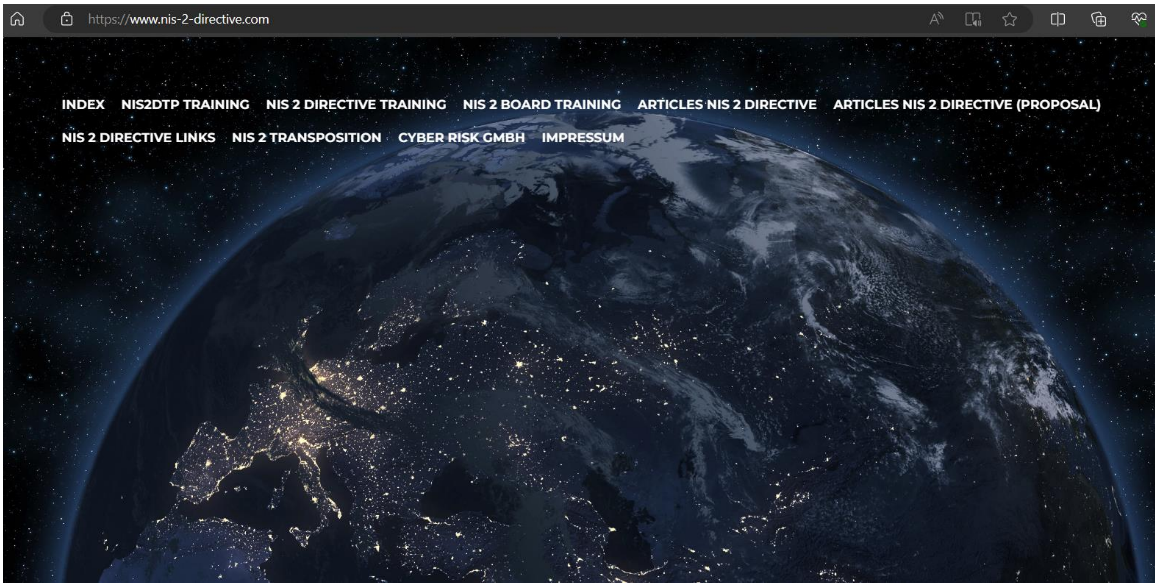
2. The European Cyber Resilience Act - https://www.european-cyber-resilience-act.com

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

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

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

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



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

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

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

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

11. The EU Cyber Solidarity Act - https://www.eu-cyber-solidarity-act.com

12. The Digital Networks Act (DNA) - https://www.digital-networks-act.com

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

14. The Artificial Intelligence Liability Directive - https://www.ai-liability-directive.com

15. The Framework for Artificial Intelligence Cybersecurity Practices (FAICP) - https://www.faicp-framework.com

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

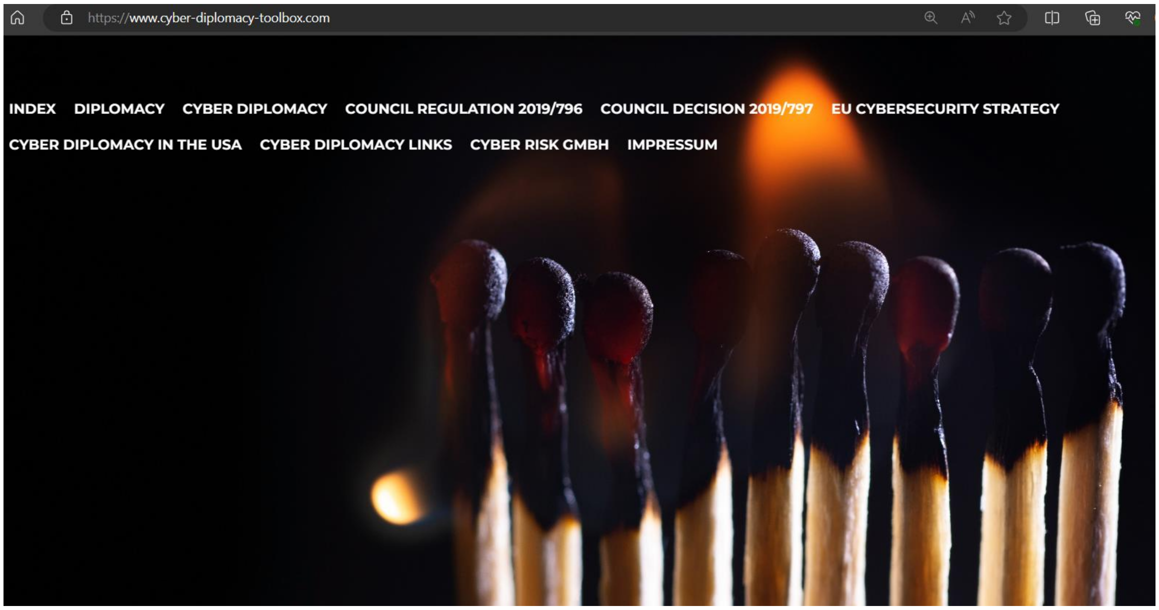
17. The European Digital Identity Regulation - https://www.european-digital-identity-regulation.com

18. The European Media Freedom Act (EMFA) - https://www.media-freedom-act.com

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

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

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


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

You may contact:

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