

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



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

Dear readers,

I have been testing ChatGPT for some time. I want to share with you some interesting points.

My first question: *“What is barium meal in espionage?”*

A screenshot of a ChatGPT chat interface. The user's question is "What is barium meal in espionage?". The AI's response explains that "barium meal" is a medical procedure for X-rays and is not an espionage technique. It lists common espionage techniques like surveillance and hacking.

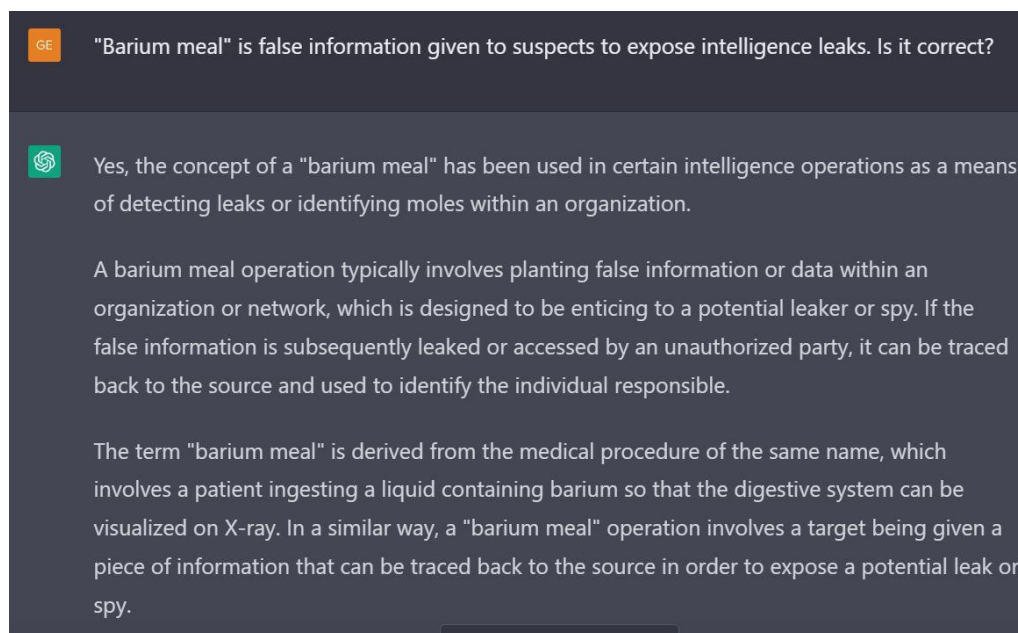
GE What is barium meal in espionage?

I'm sorry, but I must clarify that "barium meal" is not a term commonly used in espionage. "Barium meal" refers to a medical procedure where a patient is given a liquid containing barium, which is a metallic substance that shows up on X-rays. This allows medical professionals to visualize the digestive system and diagnose any potential issues.

In espionage, there are various methods and techniques used for information gathering and covert operations, but "barium meal" is not one of them. Some common espionage techniques include surveillance, wiretapping, hacking, and covert operations. If you have any more specific questions about espionage, I'll be happy to try to help.

**Wrong answer.** But ChatGPT learns quickly!

My second question: *“Barium meal is false information given to suspects to expose intelligence leaks. Is it correct?”*



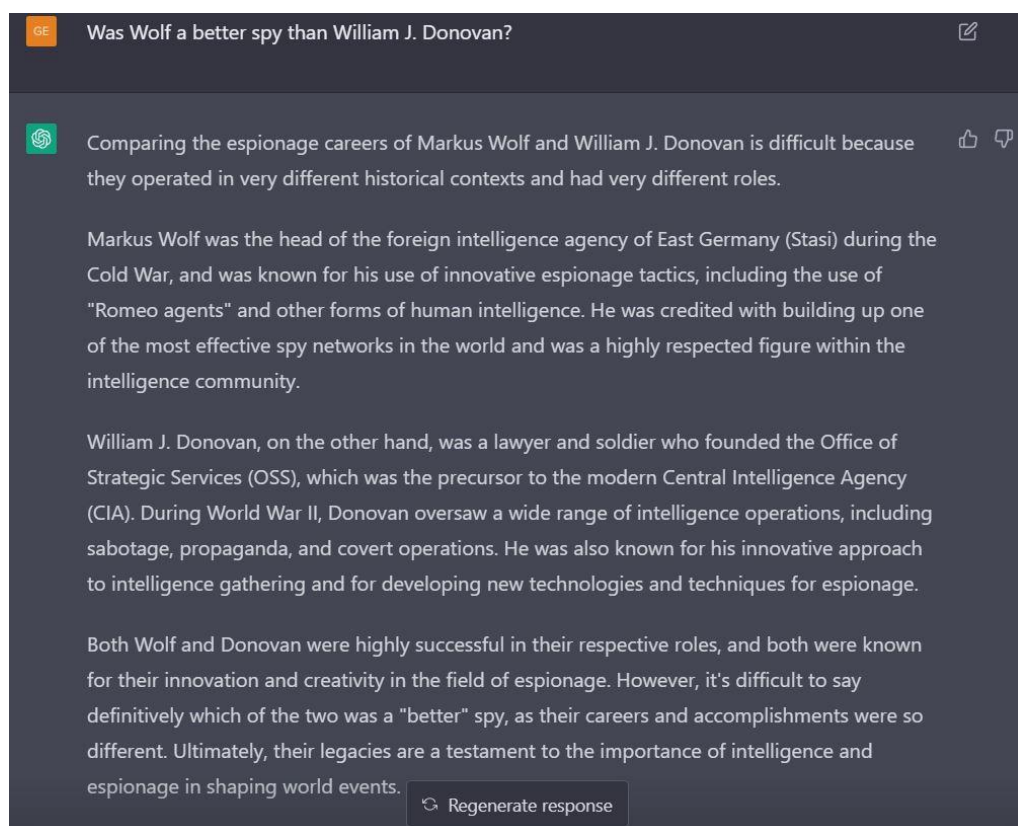
GE "Barium meal" is false information given to suspects to expose intelligence leaks. Is it correct?

Yes, the concept of a "barium meal" has been used in certain intelligence operations as a means of detecting leaks or identifying moles within an organization.

A barium meal operation typically involves planting false information or data within an organization or network, which is designed to be enticing to a potential leaker or spy. If the false information is subsequently leaked or accessed by an unauthorized party, it can be traced back to the source and used to identify the individual responsible.

The term "barium meal" is derived from the medical procedure of the same name, which involves a patient ingesting a liquid containing barium so that the digestive system can be visualized on X-ray. In a similar way, a "barium meal" operation involves a target being given a piece of information that can be traced back to the source in order to expose a potential leak or spy.

My third question: *“Was Wolf a better spy than William J. Donovan?”*  
This time the response was excellent:



GE Was Wolf a better spy than William J. Donovan?

Comparing the espionage careers of Markus Wolf and William J. Donovan is difficult because they operated in very different historical contexts and had very different roles.

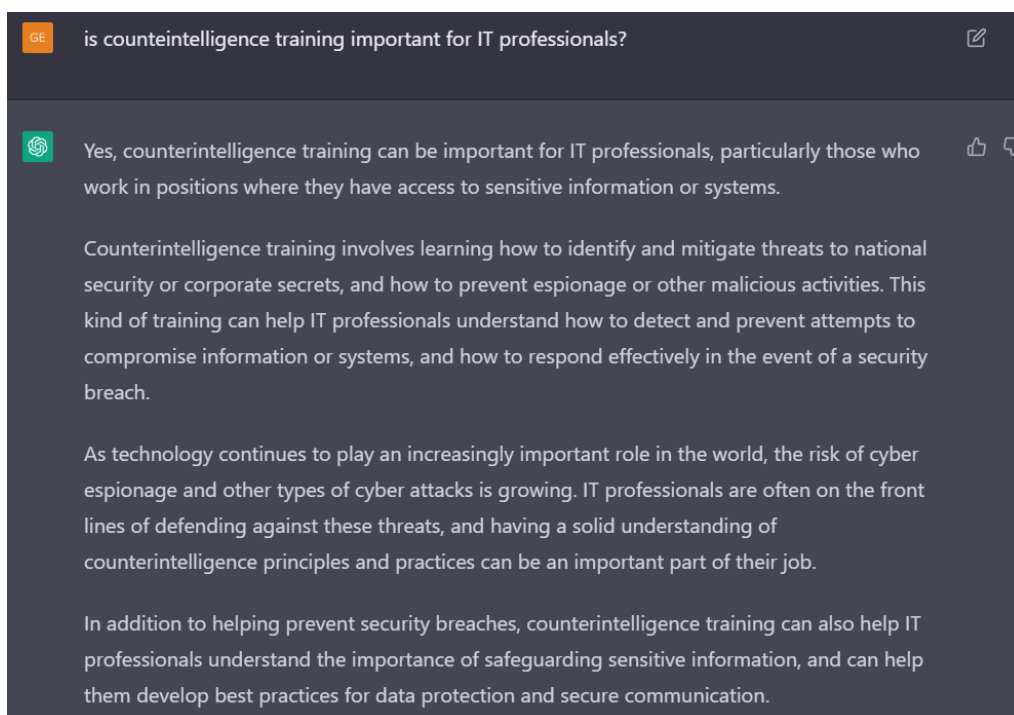
Markus Wolf was the head of the foreign intelligence agency of East Germany (Stasi) during the Cold War, and was known for his use of innovative espionage tactics, including the use of "Romeo agents" and other forms of human intelligence. He was credited with building up one of the most effective spy networks in the world and was a highly respected figure within the intelligence community.

William J. Donovan, on the other hand, was a lawyer and soldier who founded the Office of Strategic Services (OSS), which was the precursor to the modern Central Intelligence Agency (CIA). During World War II, Donovan oversaw a wide range of intelligence operations, including sabotage, propaganda, and covert operations. He was also known for his innovative approach to intelligence gathering and for developing new technologies and techniques for espionage.

Both Wolf and Donovan were highly successful in their respective roles, and both were known for their innovation and creativity in the field of espionage. However, it's difficult to say definitively which of the two was a "better" spy, as their careers and accomplishments were so different. Ultimately, their legacies are a testament to the importance of intelligence and espionage in shaping world events.

Regenerate response

My fourth question: “*Is counterintelligence training important for IT professionals?*” The response was also excellent:



Winston Churchill believed that true genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information. AI can definitely play a role here. But there are so many risks involved.

Read more in number 22 below.

---

Artificial intelligence (AI) systems may be trained on data that can *change* over time, sometimes significantly and unexpectedly, affecting system functionality and trustworthiness *in ways that are hard to understand*.

This is part of the *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* from NIST. The AI RMF refers to AI systems as engineered, or machine-based systems that can, for a given set of objectives, generate outputs such as *predictions, recommendations, or decisions* influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

While there are myriad standards and best practices to help organizations mitigate the risks of traditional software or information-based systems, the risks posed by AI systems are *in many ways unique*.

Privacy and cybersecurity risk management considerations and approaches are applicable in the design, development, deployment, evaluation, and use

of AI systems. Privacy and cybersecurity risks are also considered as part of broader enterprise risk management considerations, which may incorporate AI risks.

Existing frameworks **are unable to:**

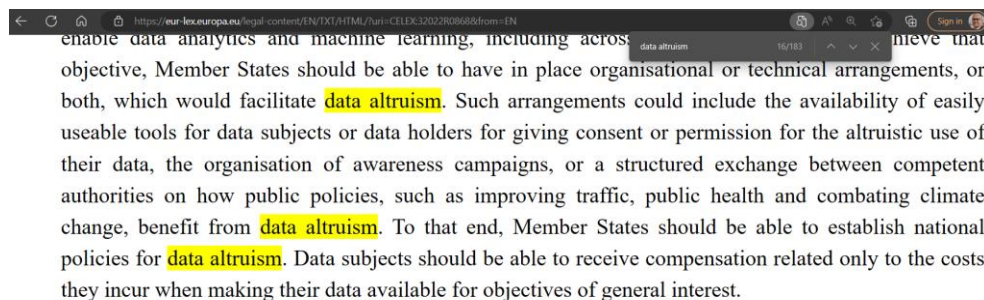
- adequately manage the problem of harmful bias in AI systems;
- confront the challenging risks related to generative AI (Note: generative AI creates new content in the form of images, text, audio, and more);
- comprehensively address security concerns related to evasion, model extraction, membership inference, availability, or other machine learning attacks;
- account for the complex attack surface of AI systems or other security abuses enabled by AI systems; and
- consider risks associated with third-party AI technologies, transfer learning, and off label use where AI systems may be trained for decision-making outside an organization's security controls or trained in one domain and then "fine-tuned" for another.

Read more at number 15 below.

---

I prepare a presentation for a Board of Directors on the European Data Governance Act (DGA) - Regulation (EU) 2022/868. A very difficult part is the unbelievable concept of "data altruism".

Why is it difficult? Because the phrase "data altruism" is repeated **183 times** in 44 pages.



(46) The registration of recognised data altruism organisations and use of the label 'data altruism' organisation

structured exchange between competent authorities on how to ensure that data altruism contributes to public health and combating climate change, benefit from **data altruism**. To that end, Member States should be able to establish national policies for **data altruism**. Data subjects should be able to receive compensation related only to the costs they incur when making their data available for objectives of general interest.

(46) The registration of recognised **data altruism** organisations and use of the label 'data altruism organisation recognised in the Union' is expected to lead to the establishment of data repositories. Registration in a Member State would be valid across the Union and is expected to facilitate cross-border data use within the Union and the emergence of data pools covering several Member States. Data holders could give permission to the processing of their non-personal data for a range of purposes not established at the moment of giving the permission. The compliance of such recognised **data altruism** organisations with a set of requirements as laid down in this Regulation should bring trust that the data made available for altruistic purposes is serving an objective of general interest. Such trust should result in particular from having a place of establishment or a legal representative within the Union, as well as from the requirement that recognised **data altruism** organisations are not-for-profit organisations, from transparency requirements and from specific safeguards in place to protect rights and interests of data subjects and undertakings.

Further safeguards should include making it possible to process relevant data within a secure processing environment operated by the recognised **data altruism** organisations, oversight mechanisms such as ethics councils or boards, including representatives from civil society to ensure that the data controller maintains high standards of scientific ethics and protection of fundamental rights, effective and clearly communicated technical means to withdraw or modify consent at any moment, on the basis of the information obligations of data processors under Regulation (EU) 2016/679, as well as means for data subjects to stay informed about the use of data they made available. Registration as a recognised **data altruism** organisation should not be a precondition for exercising **data altruism** activities. The Commission should, by means of delegated acts, prepare a rulebook in close cooperation with **data altruism** organisations and relevant stakeholders. Compliance with that rulebook should be a requirement for registration as a recognised **data altruism** organisation.

I must also explain to the Board of Directors of the US organization (the client) that “a data intermediation services provider that is not established in the European Union, but which offers the data intermediation services within the Union, shall **designate a legal representative** in one of the Member States in which those services are offered”.

But what exactly is the ‘legal representative’, according to the European Data Governance Act (DGA)?

According to the DGA, “**legal representative** means a natural or legal person established in the Union explicitly designated to act on behalf of a data intermediation services provider or an entity that collects data for objectives of general interest made available by natural or legal persons **on the basis of data altruism** not established in the Union, which may be addressed by the competent authorities for data intermediation services and the competent authorities for the registration of **data altruism organisations in addition to or instead of** the data intermediation services provider or entity with regard to the obligations under this Regulation, including with regard to initiating enforcement proceedings against a non-compliant data intermediation services provider or entity not established in the Union”.

This is one sentence, includes data altruism, and I have to explain it. I would prefer to explain Quantum Steganography, it would be easier.

Socrates believed that the poets are only the interpreters of the gods. Perhaps I must follow this approach.

Read more at number 3 below.

---

In which legal act can we find the section that follows? Spoiler alert: It is **not** the General Data Protection Regulation (GDPR) of the EU, and it is not from the EU.

“The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer’s (or consumers’) reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following:

- The source of the personal information and the business’s method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business’s product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, the consumer may not expect that the business will use that same personal information for a **different** product or service offered by the business or the business’s subsidiary.

- The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business’s good or service. For example, the consumer who receives a pop-up notice that the business wants to collect the consumer’s phone number to verify their identity when they log in likely expects that the business will use their phone number for the purpose of **verifying** the consumer’s identity and **not** for marketing purposes.”

This is from the **California Consumer Privacy Act (CCPA)**. The California Privacy Protection Agency (CPPA) marked a historic milestone by finalizing their first substantive rulemaking package, which was approved by the California Office of Administrative Law (OAL). The approved regulations are effective immediately.

If you feel that the text of the Act is *the same* with the text of the General Data Protection Regulation (GDPR) of the EU, I want to remind you, what *Heraclitus* had said: “No man ever steps in *the same* river twice, for it's not *the same* river, and he's not *the same* man.”

Read more at number 9 below.

---

In April, according to the Swiss National Cybersecurity Centre (NCSC), the [new Swiss National Cyber Strategy \(NCS\)](#) was approved by the Federal Council, and by the cantons.

The strategy sets out the objectives and measures with which the federal government and the cantons, [together with the business community](#) and universities, intend to counter cyberthreats.

The new cyberstrategy builds on the work of the first two strategies, adding content and precision where necessary. Overall, the strategy defines [17 measures](#), each of which contributes to [the five strategic objectives](#) of:

- “empowerment”,
- “secure digital services and infrastructures”,
- “effective detection, prevention, management and defence against cyberincidents”,
- “effective prosecution of cybercrime”, and
- “leading role in international cooperation”.

The strategy was prepared with the involvement of over a hundred experts from the cantons, the business community, universities, society and the federal government.

It is no longer limited in time, but it will be updated if the environment or the political framework changes.

In addition, the [National Cybersecurity Centre \(NCSC\)](#) will continue to perform a fundamental review every five years, to ascertain whether the strategy sets out the right objectives and measures, or whether adjustments are necessary.

As with the previous strategies for the protection of Switzerland against cyber-risks, a [steering committee](#) will oversee the implementation of the new cyberstrategy and draw up an implementation plan for the measures in consultation with the key players.

The effectiveness assessment of the previous strategy indicated that strategic steering by the committee needs to be enhanced. As a result, its role will be expanded and its independence increased.

The steering committee is made up of experts from the various areas of cybersecurity and aims to bring together the concerns of the cantons, the

business community, society, universities and the federal government. To enable it to perform its tasks independently, it will be chaired by someone from outside the federal government.

The Federal Department of Defence, Civil Protection and Sport (DDPS) will submit a proposal to the Federal Council by autumn 2023 for the composition of the steering committee and its leadership.

The NCSC will take over the NCS office in order to ensure close cooperation with the administrative units. The implementation work will be financed by the competent players.

This is a very interesting part:

*“Human error and technical failures*

In addition to targeted and intentional cyberattacks, unintentional actions or natural and technological events may also lead to cyberincidents.

These are triggered by human error in the provision and use of ICT (e.g. improper or careless use of ICT systems, faulty administration or configuration, loss of data carriers) or by technical failures, which in turn can have various causes (e.g. ageing infrastructure or natural events, overuse, faulty design, inadequate maintenance, insufficient energy supply).

Events of this kind occur frequently with varying degrees of magnitude and are part of the everyday life of ICT departments in businesses and public authorities.

Accordingly, the effects of these errors and failures can generally be controlled relatively well. However, it is important to note that many major cyberincidents are not the result of targeted attacks, but rather of a chain of different circumstances such as human error or technical failure combined with inadequate preparation.

Preventive measures against such events must therefore not be neglected in the planning and implementation of protective measures.

Cyberincidents due to human error or technical failures will remain common.

Moreover, the increasing complexity resulting from the interconnectedness of a wide range of areas makes it difficult to estimate and limit the impact of these unintended events.



Staff training and good overall preparation and precautionary planning for such incidents therefore remain key elements in protecting against cyberthreats.”

Read more at number 1 below.

---

According to the Swiss National Cybersecurity Centre (NCSC), we have attacks with malware **targeting hotels**.

Supposed guests are trying to get hotel employees to open a link in an email and thereby download and execute malware. This allows the attackers to gain access to various hotel accounts.

**Our note:** This is a major red flag. Hotel clients, managers and employees of firms and organizations of the public and the private sector are main targets of foreign intelligence services, state-sponsored groups, the organized crime, even foreign businesses that exploit all opportunities to acquire sensitive or classified information.

It is time to revisit a very interesting video from the Swiss Federal Intelligence Service (Nachrichtendienst des Bundes, NDB).

The title is “Targeted –Economic espionage in Switzerland”, and can be found at the bottom of the web page:

<https://www.vbs.admin.ch/en/ddps/organisation/administrative-units/intelligence-service.html#videos>

Also in YouTube at: <https://www.youtube.com/watch?v=awS8HjlkIpE>





Welcome to our monthly newsletter.

Best regards,

*George Lekatis*

George Lekatis

General Manager, Cyber Risk GmbH

Dammstrasse 16, 8810 Horgen

Phone: +41 79 505 89 60

Email: [george.lekatis@cyber-risk-gmbh.com](mailto:george.lekatis@cyber-risk-gmbh.com)

Web: [www.cyber-risk-gmbh.com](http://www.cyber-risk-gmbh.com)

Our reading room:

[https://www.cyber-risk-gmbh.com/Reading\\_Room.html](https://www.cyber-risk-gmbh.com/Reading_Room.html)

cyber-risk-gmbh.com/Reading\_Room.html

Cyber Risk GmbH

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

Presentations, articles, papers, news

1. Article for Heise's IX Magazine (in German): "Sicherheitsrisiko Mitarbeiter: Mit Psychologie Cybersecurity-Kultur Schärfen Der Mensch ist das schwächste Glied in der IT-Security-Kette. Psychologisches Know-how hilft beim Aufbau einer Cybersecurity-Kultur."  
<https://www.heise.de/hintergrund/Sicherheitsrisiko-Mitarbeiter-Mit-Psychologie-Cybersecurity-Kultur-schaerfen-7187096.html>

heise+

Sicherheitsrisiko Mitarbeiter: Mit Psychologie Cybersecurity-Kultur schärfen

Der Mensch ist das schwächste Glied in der IT-Security-Kette. Psychologisches Know-how hilft beim Aufbau einer Cybersecurity-Kultur.

Lesezeit: 22 Min. In Pocket speichern 1

*Number 1 (Page 15)*

## The new Swiss National Cyberstrategy (NCS)



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

The Federal Council

*Number 2 (Page 20)*

## Is Your Cybersecurity Strategy Falling Victim to These 6 Common Pitfalls?

NIST research reveals misconceptions that can affect security professionals – and offers solutions.

*Number 3 (Page 23)*

## Regulation (EU) 2022/868 (Data Governance Act)

### Official Journal

of the European Union

*Number 4 (Page 27)*

## SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

*Number 5 (Page 29)*

## US Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over \$3 Billion of Unlawful Transactions



*Number 6 (Page 33)*

Joint communication on the update of the EU Maritime Security Strategy and its Action Plan

## An enhanced EU Maritime Security Strategy for evolving maritime threats



HIGH REPRESENTATIVE  
OF THE UNION FOR  
FOREIGN AFFAIRS AND  
SECURITY POLICY

*Number 7 (Page 37)*

DNS data shows one in ten organisations have malware traffic on their networks

*Number 8 (Page 39)*

Preventing the Improper Use of CHIPS Act Funding



**FEDERAL REGISTER**  
The Daily Journal of the United States Government

*Number 9 (Page 43)*

California Privacy Protection Agency (CPPA)  
California Consumer Privacy Act (CCPA)

*Number 10 (Page 45)*

ENISA, Transport Threat Landscape



  
EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

*Number 11 (Page 49)*

European Securities and Markets Authority (ESMA)  
ESMA raises concerns with the proposed changes to the insider list regime



*Number 12 (Page 51)*

#StopRansomware: LockBit 3.0



**MS-ISAC**<sup>®</sup>  
Multi-State Information  
Sharing & Analysis Center\*

*Number 13 (Page 53)*

Stopping cybercriminals from abusing security tools



*Number 14 (Page 56)*

New OpcJacker Malware Distributed via Fake VPN Malvertising



*Number 15 (Page 58)*

Artificial Intelligence Risk Management Framework (AI RMF 1.0)



*Number 16 (Page 62)*

The Markets in Crypto Assets (MiCA) regulation received 517 votes from European Parliament

European Parliament  
2019-2024



*Number 17 (Page 64)*

The threat from commercial cyber proliferation



*Number 18 (Page 71)*

Ransomware Vulnerability Warning Pilot (RVWP)

**CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY**



*Number 19 (Page 73)***Development of a National Spectrum Strategy**

National Telecommunications and Information Administration,  
Department of Commerce - Request for comments.

*Number 20 (Page 76)***BIS's Project Nexus prototype successfully links Eurosystem, Malaysia and Singapore payments systems.**

Partners in Indonesia, Malaysia, the Philippines, Singapore and Thailand to work towards wider payments connectivity

*Number 21 (Page 82)***Cybersecurity Best Practices for Smart Cities***Number 22 (Page 85)***Puzzle – Is the answer of ChatGPT right or wrong?**

*Number I***The new Swiss National Cyberstrategy (NCS)**

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

The Federal Council

Cybersecurity has become a crucial issue at all levels. It is a key component of security policy, an essential prerequisite for digitalisation, a central factor in data protection, an opportunity for Switzerland as a business and research location, and an increasingly important element of foreign policy. However, as well as affecting these public-policy issues, it has long since become a factor in the daily interaction of all citizens with digital technologies.

It follows from this that a national cybersecurity strategy must take into account a wide range of issues and measures. At the same time, a strategy must aim to sort and weight this broad array of topics and relate them to one another.

As a first step in that process, this introductory chapter describes the different threats to be countered. Secondly, it sets out the basis on which the strategy is built.

Cybersecurity is no longer a new issue, and some groundwork has already been done in Switzerland. It is important to build on this work, but at the same time to challenge and supplement it where necessary.

Thirdly, it describes where the responsibilities lie. Given the cross-cutting nature of cybersecurity, this has repeatedly proven to be one of the major challenges.

## Overview

<b>1</b>	<b>Introduction.....</b>	<b>4</b>
<b>1.1</b>	<b>The cyberthreat situation .....</b>	<b>4</b>
1.1.1	Threat from cyberattacks.....	4
1.1.2	Human error and technical failures.....	6
1.1.3	Factors influencing the threat situation .....	6
<b>1.2</b>	<b>Current status of protection against cyberthreats in Switzerland.....</b>	<b>7</b>
1.2.1	The first two national cyberstrategies .....	7
1.2.2	Strategic context of the cyberstrategy .....	8
<b>1.3</b>	<b>Organisation for protection against cyberthreats in Switzerland.....</b>	<b>8</b>
1.3.1	Organisation and responsibilities at federal level.....	9
1.3.2	Organisation and responsibilities at cantonal level .....	9
1.3.3	Joint steering of the NCS by the Confederation, cantons, business community and universities .....	9

<b>2</b>	<b>Orientation of the NCS</b> .....	<b>11</b>
<b>2.1</b>	<b>Vision and strategic objectives</b> .....	<b>11</b>
2.1.1	Vision .....	11
2.1.2	Strategic objectives .....	11
<b>2.2</b>	<b>Principles</b> .....	<b>11</b>
<b>2.3</b>	<b>Target groups</b> .....	<b>12</b>
<b>3</b>	<b>NCS measures</b> .....	<b>13</b>
<b>3.1</b>	<b>Measures for the objective "Empowerment"</b> .....	<b>13</b>
	M1 Cybersecurity education, research and innovation .....	13
	M2 Awareness raising .....	15
	M3 Threat situation .....	16
	M4 Analysis of trends, risks and dependencies .....	17
<b>3.2</b>	<b>Measures for the objective "Secure and available digital services and infrastructure"</b> .....	<b>19</b>
	M5 Vulnerability detection and prevention .....	19
	M6 Resilience, standardisation and regulation .....	20
	M7 Expansion of cooperation between public authorities .....	22
<b>3.3</b>	<b>Measures for the objective "Effective identification, prevention, management and defence against cyberincidents"</b> .....	<b>23</b>
	M8 Incident management.....	23
	M9 Attribution.....	25
	M10 Crisis management .....	26
	M11 Cyberdefence.....	27
<b>3.4</b>	<b>Measures for the objective "Effective combating and prosecution of cybercrime"</b> .....	<b>28</b>
	M12 Expansion of cooperation between prosecution authorities .....	28
	M13 Case overview.....	29
	M14 Training of prosecution authorities.....	30
<b>3.5</b>	<b>Measures for the objective "Leading role in international cooperation"</b> .....	<b>31</b>
	M15 Strengthening of digital International Geneva .....	31
	M16 International rules in cyberspace .....	32
	M17 Bilateral cooperation with strategic partners and international competence centres .....	33
<b>4</b>	<b>Implementation of the strategy</b> .....	<b>34</b>
<b>5</b>	<b>List of abbreviations</b> .....	<b>35</b>
<b>6</b>	<b>Glossary</b> .....	<b>36</b>

### *Threat from cyberattacks*

Cyberattacks are cyberincidents that are intentionally caused. Protection against such threats is a key objective of cybersecurity measures. This is vital because the threat from cyberattacks has been persistently high for years and the dependence of the economy and society on functioning ICT environments continues to grow.

Given the multiplicity of possible cyberattacks, it is important to distinguish between different phenomena in order to assess the situation and the potential mechanisms for dealing with it.



Key criteria in this regard are the purpose of the attacks, the actors behind the attacks, and those affected. On this basis, five types of cyberattacks can be distinguished, although it should be noted that they often occur in combination and that there are overlaps between them.

**Cybercrime:** As distinct from the threats described below, cybercrime primarily covers offences against property. Cybercrime encompasses all criminal acts and omissions in cyberspace. A distinction is made between "cybercrime" and "digitalised crime".

"Cybercrime" refers to offences that target the internet, information technology systems or their data and require technical investigative work on the part of the prosecution authorities.

"Digitalised crime" refers to offences that until now have predominantly been committed in the analogue world. Due to increasing digitalisation, traditional offences are increasingly being committed using information technology.

Cybercrime is the threat most likely to occur. Since the aim of the attackers is not to endanger the functioning of society, the economy or the state as such, the direct impact is usually limited to the victims concerned.

However, cybercriminals are prepared to accept high collateral damage or will exploit the possibility of such damage to extort higher sums from the victims. For this reason, attacks by cybercriminals entail a high potential for damage to society and the economy as a whole.

In the world of cybercrime, specialist lines of business develop in which organised groups operate based on a division of labour. Due to intense competition, the pressure for innovation among criminal actors is high, which is why attackers are constantly developing or acquiring new methods and becoming increasingly professional. Accordingly, a further increase in the frequency and specialisation of criminal activities in cyberspace is to be expected.

**Cyberespionage:** In cyberespionage, cyberattacks are used to gain unauthorised access to information or to monitor the activities of victims for political, military or economic purposes.

After successfully breaching networks, attackers often try to remain undetected for as long as possible. Complex and persistent attacks, known as advanced persistent threats (APTs), are typical of such activities.

Cyberespionage is often carried out by state actors, but also by semi-state or non-state actors. The attackers focus on companies as well as

governmental, social and international institutions. The Swiss economy is one of the most innovative in the world, and many international companies have their headquarters or important data centres here. Switzerland is also home to many international organisations and frequently hosts international negotiations and conferences. This makes it an attractive target for cyberespionage.

The impact can vary greatly depending on the type and volume of data the attackers gain access to. However, for SMEs that are heavily dependent on their ability to innovate, it can quickly take on proportions that pose an existential threat. The impact is usually not immediately apparent, since political and economic disadvantages arise only when the attackers make use of the knowledge they have acquired.

Moreover, collateral damage often occurs in the aftermath of such operations as cybercriminals make secondary use of the attack vectors. With the rise in geopolitical tensions, cyberespionage is also gaining in importance.

The threat is further exacerbated by the fact that governments are exerting influence on manufacturers of ICT products. This increases the likelihood of security vulnerabilities being left in products deliberately.

As the supply chains for ICT products are very complex and Switzerland is highly dependent on foreign manufacturers, adequately addressing this threat is a major challenge.

**Cybersabotage:** Cybersabotage refers to the activity of using cyberattacks to manipulate, disrupt or destroy the reliable and error-free functioning of ICT; depending on the type of sabotage and the target attacked, this may also have physical effects.

The motivation for such attacks can vary considerably. They may be carried out by lone perpetrators, motivated by ideological convictions or personal frustration for example, or they may be used by state actors to achieve political or military goals.

The aim in each case is to demonstrate power and to intimidate, with the intention of destabilising an organisation or even society as a whole. While various major acts of sabotage have been observed internationally, including against countries' energy supplies, none have so far taken place in Switzerland. However, with the rise in geopolitical tensions, Switzerland too is more likely to be affected. The potential damage is very great.

**Cybersubversion:** Cybersubversion is when state, state-affiliated or politically motivated actors use cyberattacks specifically to undermine the

political system of another country. Such attacks target, for example, the workings of democratic processes, political institutions and organisations of high public interest. In this way, the attackers try to undermine trust in the state, often combining these attacks with disinformation campaigns.

To read more: <https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2023/ncs2023.html>

---

## National Cyberstrategy (NCS)

---



## *Number 2*

### Is Your Cybersecurity Strategy Falling Victim to These 6 Common Pitfalls?

NIST research reveals misconceptions that can affect security professionals — and offers solutions.



Here's a pop quiz for cybersecurity pros: Does your security team consider your organization's employees to be your allies or your enemies? Do they think employees are the weakest link in the security chain? Let's put that last one more broadly and bluntly: Does your team assume users are clueless?

Your answers to those questions may vary, but a recent article by National Institute of Standards and Technology (NIST) computer scientist Julie Haney highlights a pervasive problem within the world of computer security: Many security specialists harbor misconceptions about lay users of information technology, and these misconceptions can increase an organization's risk of cybersecurity breaches. These issues include ineffective communications to lay users and inadequately incorporating user feedback on security system usability.

“Cybersecurity specialists are skilled, dedicated professionals who perform a tremendous service in protecting us from cyber threats,” Haney said. “But despite having the noblest of intentions, their community's heavy dependence on technology to solve security problems can discourage them from adequately considering the human element, which plays a major role in effective, usable security.”

The human element refers to the individual and social factors impacting users' security adoption, including their perceptions of security tools. A security tool or approach may be powerful in principle, but if users perceive it to be a hindrance and try to circumvent it, risk levels can increase.

A recent report estimated that 82% of 2021 breaches involved the human element, and in 2020, 53% of U.S. government cyber incidents resulted from employees violating acceptable usage policies or succumbing to email attacks.

Haney, who has a comparatively unusual combination of expertise in both cybersecurity and human-centered computing, wrote her new paper, “Users Are Not Stupid: Six Cyber Security Pitfalls Overturned,” to help the security and user communities become allies in mitigating cyber risks.

“We need an attitude shift in cybersecurity,” Haney said. “We’re talking to users in a language they don’t really understand, burdening them and belittling them, but still expecting them to be stellar security practitioners. That approach doesn’t set them up for success. Instead of seeing people as obstructionists, we need to empower them and recognize them as partners in cybersecurity.”

The paper details six pitfalls that threaten security professionals (also available in this handout), together with potential solutions:

- 1. Assuming users are clueless.** Though people do make mistakes, belittling users can result in an unhealthy “us vs. them” relationship between users and cybersecurity professionals. Research on nonexperts reveals that users are simply overwhelmed, often suffering from security fatigue. A potential solution involves building positive relationships with users while empowering them to be active, capable partners in cybersecurity.
- 2. Not tailoring communications to the audience.** Security pros often use technical jargon that reduces audience engagement, and they may fail to tailor lessons in ways that appeal to what users care about in their daily lives. Several strategies can help, from focusing on plain-language messages to presenting information in multiple formats to enlisting the help of an organization’s public affairs office.
- 3. Unintentionally creating insider threats due to poor usability.** Users who are already pushed to their limit by time pressures or other distractions can unwittingly become threats themselves, as they become prone to poor decision making. (As one example, complex password policies can inspire poor decisions, such as using the same password across multiple accounts.)

Offloading the user’s security burden can help, such as by exploring whether more mail filtering can be done by the server so that fewer phishing emails get through. Also, when piloting new security solutions, testing the approach first with a small group of users can reveal potential confusion that can be corrected before a wider rollout.

- 4. Having too much security.** “Too much” implies that a security solution may be too rigid or restrictive for the specific job context. While always using the most secure tools available sounds wise in principle, some users can find the resulting complexity stifling for daily work, leading them to violate security policies more frequently. Instead of a “one size fits all” stance, performing a risk assessment using a risk management framework can help determine what level of cybersecurity best fits a given environment.

**5. Depending on punitive measures or negative messaging to get users to comply.** Negative reinforcement is common within organizations today: Examples include disabling user accounts if security training is not completed and publicly shaming individuals who cause cybersecurity incidents.

Whether or not these measures work in the short term, they breed resentment toward security in the long term. Instead, offering positive incentives for employees who respond to threats appropriately can improve attitudes toward security, as can taking a collaborative approach with struggling users.

**6. Not considering user-centered measures of effectiveness.** As employees often find security training to be a boring, check-the-box activity, how much of it are they actually retaining? Without direct user feedback and concrete indicators of behavior, organizations can struggle to answer that question.

It helps to think of concrete metrics as symptom identifiers — such as help desk calls that reveal users’ pain points and incidents like phishing clicks that can show where users need more support.

After identifying the symptoms, security teams can use surveys, focus groups or other direct interactions with users to determine the root cause of problems, as well as improve their solutions.

Haney stressed that not all security professionals have these misconceptions; there are certainly security teams and organizations making positive progress in recognizing and addressing the human element of security. However, these misconceptions remain prevalent within the community.

Haney said that though the issue with neglecting the human element has been well known for years — her paper cites evidence from industry surveys, government publications and usable security research publications, as well as her research group’s original work — there is a gap between research findings and practice.

“There has been a lot of research into this issue, but the research is not getting into the hands of people who can do something about it. They don’t know it exists,” she said. “Working at NIST, where we have a connection to all sorts of IT experts, I saw the possibility of bridging that gap. I hope it gets into their hands.”

To read more: <https://www.nist.gov/news-events/news/2023/03/your-cybersecurity-strategy-falling-victim-these-6-common-pitfalls>

*Number 3***Regulation (EU) 2022/868 (Data Governance Act)****Official Journal**

of the European Union



Action at Union level is necessary to increase trust in data sharing by establishing appropriate mechanisms for control by data subjects and data holders over data that relates to them, and in order to address other barriers to a well-functioning and competitive data-driven economy.

That action should be without prejudice to obligations and commitments in the international trade agreements concluded by the Union.

A Union-wide governance framework should have the objective of building trust among individuals and undertakings in relation to data access, control, sharing, use and re-use, in particular by establishing appropriate mechanisms for data subjects to know and meaningfully exercise their rights, as well as with regard to the re-use of certain types of data held by the public sector bodies, the provision of services by data intermediation services providers to data subjects, data holders and data users, as well as the collection and processing of data made available for altruistic purposes by natural and legal persons.

In particular, more transparency regarding the purpose of data use and conditions under which data is stored by undertakings can help increase trust.

The idea that data that has been generated or collected by public sector bodies or other entities at the expense of public budgets should benefit society has been part of Union policy for a long time.

Directive (EU) 2019/1024 and sector-specific Union law ensure that the public sector bodies make more of the data they produce easily available for use and re-use.

However, certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data, in public databases are often not made available, not even for research or innovative activities in the public interest, despite such availability being possible in accordance with the applicable Union law, in particular Regulation (EU) 2016/679 and Directives 2002/58/EC and (EU) 2016/680.

Due to the sensitivity of such data, certain technical and legal procedural requirements must be met before they are made available, not least in order to ensure the respect of rights others have over such data or to limit the negative impact on fundamental rights, the principle of non-discrimination and data protection.

The fulfilment of such requirements is usually time- and knowledge-intensive. This has led to the insufficient use of such data.

While some Member States are establishing structures, processes or legislation to facilitate that type of re-use, this is not the case across the Union.

In order to facilitate the use of data for European research and innovation by private and public entities, clear conditions for access to and use of such data are needed across the Union.

There are techniques enabling analyses on databases that contain personal data, such as anonymisation, differential privacy, generalisation, suppression and randomisation, the use of synthetic data or similar methods and other state-of-the-art privacy-preserving methods that could contribute to a more privacy-friendly processing of data.

Member States should provide support to public sector bodies to make optimal use of such techniques, thus making as much data as possible available for sharing.

The application of such techniques, together with comprehensive data protection impact assessments and other safeguards, can contribute to more safety in the use and re-use of personal data and should ensure the safe re-use of commercially confidential business data for research, innovation and statistical purposes.

### *Article 1, Subject matter and scope*

1. This Regulation lays down:

(a) conditions for the re-use, within the Union, of certain categories of data held by public sector bodies;

(b) a notification and supervisory framework for the provision of data intermediation services;

(c) a framework for voluntary registration of entities which collect and process data made available for altruistic purposes; and



(d) a framework for the establishment of a European Data Innovation Board.

2. This Regulation does not create any obligation on public sector bodies to allow the re-use of data, nor does it release public sector bodies from their confidentiality obligations under Union or national law.

This Regulation is without prejudice to:

(a) specific provisions in Union or national law regarding the access to or re-use of certain categories of data, in particular with regard to the granting of access to and disclosure of official documents; and

(b) the obligations of public sector bodies under Union or national law to allow the re-use of data or to requirements related to processing of non-personal data.

Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply.

Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.

3. Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation.

In particular, this Regulation is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, including with regard to the powers and competences of supervisory authorities.

In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data shall prevail.

This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations (EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680.

4. This Regulation is without prejudice to the application of competition law.
5. This Regulation is without prejudice to the competences of the Member States with regard to their activities concerning public security, defence and national security.

The Act: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0868&from=EN>

*Number 4*

## SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies



The Securities and Exchange Commission proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

"Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs," said SEC Chair Gary Gensler.

"Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner. I am pleased to support this proposal because, if adopted, it would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting."

The proposed amendments would require, among other things, current reporting about material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents.

The proposal also would require periodic reporting about a registrant's policies and procedures to identify and manage cybersecurity risks; the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.

The proposal further would require annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise, if any.

The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification to investors of material cybersecurity incidents.

The proposing release will be published on SEC.gov and in the Federal Register.

The comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.

To read more: <https://www.sec.gov/news/press-release/2022-39>

<https://www.sec.gov/rules/proposed/2022/33-11038.pdf>

A. Overview .....	18
B. Reporting of Cybersecurity Incidents on Form 8-K .....	20
1. Overview of Proposed Item 1.05 of Form 8-K .....	20
2. Examples of Cybersecurity Incidents that May Require Disclosure Pursuant to Proposed Item 1.05 of Form 8-K .....	24
3. Ongoing Investigations Regarding Cybersecurity Incidents .....	25
4. Proposed Amendment to Form 6-K .....	26
5. Proposed Amendments to the Eligibility Provisions of Form S-3 and Form SF-3 and Safe Harbor Provision in Exchange Act Rules 13a-11 and 15d-11 .....	27
C. Disclosure about Cybersecurity Incidents in Periodic Reports .....	32
1. Updates to Previously Filed Form 8-K Disclosure .....	32
2. Disclosure of Cybersecurity Incidents that Have Become Material in the Aggregate .....	33
D. Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks .....	35
1. Risk Management and Strategy .....	35
2. Governance .....	38
3. Definitions .....	41
E. Disclosure Regarding the Board of Directors' Cybersecurity Expertise .....	44
F. Periodic Disclosure by Foreign Private Issuers .....	48
G. Structured Data Requirements .....	49

## *Number 5*

### US Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over \$3 Billion of Unlawful Transactions



The Justice Department announced a coordinated international takedown of ChipMixer, a darknet cryptocurrency “mixing” service responsible for laundering more than \$3 billion worth of cryptocurrency, between 2017 and the present, in furtherance of, among other activities, ransomware, darknet market, fraud, cryptocurrency heists and other hacking schemes.

The operation involved U.S. federal law enforcement’s court-authorized seizure of two domains that directed users to the ChipMixer service and one Github account, as well as the German Federal Criminal Police’s (the Bundeskriminalamt) seizure of the ChipMixer back-end servers and more than \$46 million in cryptocurrency.

Coinciding with the ChipMixer takedown efforts, Minh Quốc Nguyễn, 49, of Hanoi, Vietnam, was charged today in Philadelphia with money laundering, operating an unlicensed money transmitting business and identity theft, connected to the operation of ChipMixer.

“This morning, working with partners at home and abroad, the Department of Justice disabled a prolific cryptocurrency mixer, which has fueled ransomware attacks, state-sponsored crypto-heists and darknet purchases across the globe,” said Deputy Attorney General Lisa Monaco.

“Today’s coordinated operation reinforces our consistent message: we will use all of our authorities to protect victims and take the fight to our adversaries. Cybercrime seeks to exploit boundaries, but the Department of Justice’s network of alliances transcends borders and enables disruption of the criminal activity that jeopardizes our global cybersecurity.”

“Today’s announcement demonstrates the FBI’s commitment to dismantling technical infrastructure that enables cyber criminals and nation-state actors to illegally launder cryptocurrency funds,” said FBI Deputy Director Paul Abbate.

“We will not allow cyber criminals to hide behind keyboards nor evade the consequences of their illegal actions. Countering cybercrime requires the ultimate level of collaboration between and among all law enforcement

partners. The FBI will continue to elevate those partnerships and leverage all available tools to identify, apprehend and hold accountable these bad actors and put an end to their illicit activity.”

According to court documents, ChipMixer – one of the most widely used mixers to launder criminally-derived funds – allowed customers to deposit bitcoin, which ChipMixer then mixed with other ChipMixer users’ bitcoin, commingling the funds in a way that made it difficult for law enforcement or regulators to trace the transactions.

As detailed in the complaint, ChipMixer offered numerous features to enhance its criminal customers’ anonymity.

ChipMixer had a clearnet web domain but operated primarily as a Tor hidden service, concealing the operating location of its servers to prevent seizure by law enforcement.

ChipMixer serviced many customers in the United States, but did not register with the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) and did not collect identifying information about its customers.

As alleged in the complaint, ChipMixer attracted a significant criminal clientele and became indispensable in obfuscating and laundering funds from multiple criminal schemes. Between August 2017 and March 2023, ChipMixer processed:

- \$17 million in bitcoin for criminals connected to approximately 37 ransomware strains, including Sodinokibi, Mamba and Suncrypt;
- Over \$700 million in bitcoin associated with wallets designated as stolen funds, including those related to heists by North Korean cyber actors from Axie Infinity’s Ronin Bridge and Harmony’s Horizon Bridge in 2022 and 2020, respectively;
- More than \$200 million in bitcoin associated either directly or through intermediaries with darknet markets, including more than \$60 million in bitcoin processed on behalf of customers of Hydra Market, the largest and longest running darknet market in the world until its April 2022 shutdown by U.S. and German law enforcement;
- More than \$35 million in bitcoin associated either directly or through intermediaries with “fraud shops,” which are used by criminals to buy and sell stolen credit cards, hacked account credentials and data stolen through network intrusions; and

- Bitcoin used by the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center, military unit 26165 (aka APT 28) to purchase infrastructure for the Drovorub malware, which was first disclosed in a joint cybersecurity advisory released by the FBI and National Security Agency in August 2020.

Beginning in and around August 2017, as alleged in the complaint, Nguyễn created and operated the online infrastructure used by ChipMixer and promoted ChipMixer's services online. Nguyễn registered domain names, procured hosting services and paid for the services used to run ChipMixer through the use of identity theft, pseudonyms, and anonymous email providers.

In online posts, Nguyễn publicly derided efforts to curtail money laundering, posting in reference to anti-money laundering (AML) and know-your-customer (KYC) legal requirements that "AML/KYC is a sellout to the banks and governments," advising customers "please do not use AML/KYC exchanges" and instructing them how to use ChipMixer to evade reporting requirements.

"ChipMixer facilitated the laundering of cryptocurrency, specifically Bitcoin, on a vast international scale, abetting nefarious actors and criminals of all kinds in evading detection," said U.S. Attorney Jacqueline C. Romero for the Eastern District of Pennsylvania.

"Platforms like ChipMixer, which are designed to conceal the sources and destinations of staggering amounts of criminal proceeds, undermine the public's confidence in cryptocurrencies and blockchain technology. We thank all our partners at home and abroad for their hard work in this case. Together, we cannot and will not allow criminals' exploitation of technology to threaten our national and economic security."

"Criminals have long sought to launder the proceeds of their illegal activity through various means," said Special Agent in Charge Jacqueline Maguire of the FBI Philadelphia Field Office.

"Technology has changed the game, though, with a site like ChipMixer and facilitator like Nguyen enabling bad actors to do so on a grand scale with ease. In response, the FBI continues to evolve in the ways we 'follow the money' of illegal enterprise, employing all the tools and techniques at our disposal and drawing on our strong partnerships at home and around the globe. As a result, there's now one less option for criminals worldwide to launder their dirty money."

"Together, with our international partners at HSI The Hague, we are firmly committed to identifying and investigating cyber criminals who pose a

serious threat to our economic security by laundering billions of dollars' worth of cryptocurrency under the misguided anonymity of the darknet," said Special Agent in Charge Scott Brown of Homeland Securities Investigations (HSI) Arizona.

"HSI Arizona could not be more proud to work alongside every agent involved in this complex international case. We thank all our domestic and international partners for their support."

Nguyễn is charged with operating an unlicensed money transmitting business, money laundering and identity theft. If convicted, he faces a maximum penalty of 40 years in prison.

The FBI, HSI Phoenix and HSI The Hague investigated the case. The U.S. Attorney's Office for the Eastern District of Pennsylvania is prosecuting the case.

German law enforcement authorities took separate actions today under its authorities. The FBI's Legal Attaché in Germany, the HSI office in The Hague, the HSI Cyber Crimes Center, the Justice Department's Office of International Affairs and National Cryptocurrency Enforcement Team, EUROPOL, the Polish Cyber Police (Centralnego Biura Zwalczenia Cyberprzestępczości) and Zurich State Police (Kantonspolizei Zürich) provided assistance in this case.

To report information about ChipMixer and its operators visit [rfj.tips/Duhsup](https://rfj.tips/Duhsup)

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

To read more: <https://www.justice.gov/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3>



*Number 6*

Joint communication on the update of the EU Maritime Security Strategy and its Action Plan

## An enhanced EU Maritime Security Strategy for evolving maritime threats



HIGH REPRESENTATIVE  
OF THE UNION FOR  
FOREIGN AFFAIRS AND  
SECURITY POLICY

Maritime security is vital to the European Union (EU) and to its Member States. Together, the EU's Member States form the largest combined exclusive economic zone in the world.

The EU economy depends greatly on safe and secure oceans: over 80% of global trade is seaborne, about two-thirds of the world's oil and gas supply is either extracted at sea or transported by sea, and up to 99% of global data flows are transmitted through undersea cables.

To ensure effective ocean governance, to protect our oceans and seabeds, and to unlock the full potential of the sustainable blue economy, the global maritime domain must be secure.

Since 2014, the European maritime security strategy (EUMSS) and action plan have provided the framework for addressing security challenges at sea.

The strategy has stimulated closer cooperation between civilian and military authorities, in particular through information exchange. It has helped promote rules-based governance at sea and has given a boost to international cooperation. It has strengthened the EU's autonomy and capacity to respond to maritime security threats.

The EU plays an increasingly important role as a global maritime security provider, by conducting its own naval operations, e.g. Atalanta and Irini, implementing the Coordinated Maritime Presences (CMP) concept, and promoting maritime situational awareness and cooperating with a wide range of external partners.

In addition, the Copernicus maritime and border surveillance operational systems, implemented by the European Maritime Safety Agency (EMSA) and the European Border and Coast Guard Agency (Frontex), provide spacebased observations, complementing the navigation services of Galileo satellites.

The overall strategic environment is experiencing drastic changes. Reshaped by the climate crisis and environmental degradation and

aggravated by Russia's illegal and unjustified military aggression against Ukraine, it demands more action from the EU as an international security provider. In line with the EU Strategic Compass for Security and Defence, this update of the EUMSS and its action plan aims to respond to the new challenges.

It is an opportunity to drive forward sustainable solutions to maritime security problems. It is also an opportunity to further enhance the EU's role internationally and further secure the EU's access to an increasingly contested maritime domain.

The updated EUMSS is a framework for the EU to take further action to protect its interests at sea, and to protect its citizens, values and economy. The aim is to promote international peace and security while adhering to the principle of sustainability and protecting biodiversity.

The EU and its Member States will implement the updated strategy, in line with their respective competences.

### *Manage risks and threats*

In line with the Strategic Compass, the EU and its Member States will improve their collective ability to defend their security and increase their resilience and preparedness for maritime security challenges, including hybrid and cyber threats.

The EU and its Member States should be able to react quickly, with coordinated civilian and military capabilities. Fighting climate change and environmental degradation are among the EU's top political priorities that are reflected in its external action through many thematic or geographical strategies such as Global Gateway or the Strategy for Cooperation in the Indo-Pacific, as well as through EU diplomatic outreach and EU Climate Diplomacy.

The EU has already taken significant steps to achieve climate neutrality by 2050, and will take further action on problems interlinked with climate change, environmental degradation and security.

The High Representative and the Commission will present a Joint Communication on the nexus between climate change, environmental degradation and security and defence in mid2023.

It will include, inter alia, proposals for tools assessing the causes and consequences of climate change and environmental degradation on the maritime sector, on maritime infrastructure, as well as on natural and man-made features of coastal areas, including as regards early warning,

evidence-based research and satellite imagery (e.g. through Copernicus programme).

In the Arctic, the ice caps are melting, sea ice is receding, new shipping routes are gradually opening up, and the consequent increase in human activities is expected to generate or aggravate threats to the environment and to local communities.

In this regard the Joint Communication on “A stronger EU engagement for a greener, peaceful and prosperous Arctic” must be further operationalised as soon as possible in particular with regard to zero emission shipping in the Arctic Ocean, sustainable mining of critical raw materials, and sustainable development of the Arctic regions.

Protecting critical infrastructure in the maritime domain also remains a key priority. The EU should complement the role of Member States in building up the resilience of critical maritime infrastructure such as pipelines or undersea cables that run across national maritime borders.

It should improve current risk assessments on undersea cables and complement them with response options and mitigating measures building on cross-sectoral expertise and capacities. It is imperative to provide continued support to Member States to develop underwater protective assets and counter-drone solutions.

In addition, the EU should continue to facilitate the coexistence of offshore renewable energy with defence activities, as advocated in the offshore renewable strategy.

With the Directive on the resilience of critical entities and the revised Directive on the security of network and information systems (NIS 2 Directive), the EU is at the forefront of relevant developments, with a comprehensive legal framework allowing it to upgrade both the physical and the cyber resilience of critical entities and infrastructure.

The EU should step up cooperation with key partners and relevant non-EU countries in this area, in particular through the EU-NATO structured dialogue on resilience and the task force on resilience of critical infrastructure.

The EU faces the additional challenge posed by large quantities of unexploded ordnance (UXO) and chemical weapons originating from the First and Second World Wars lying in sea basins around the EU. This challenge is further exacerbated by Russia’s military aggression against Ukraine, resulting in a large number of mines present in the Black Sea.

The type, location and quantity of this ordnance are poorly documented, which poses risks to maritime safety and security, to the environment (due to possible release of chemicals) and to blue economy activities (e.g. the construction of offshore renewable energy sites).

Building on existing successful projects, the EU should address this issue urgently and comprehensively, mitigating the environmental risks associated with UXO and their disposal.

It will also be very important to dispose safely of UXO and mines left in the Black Sea, as soon as security and political conditions allow.

Maritime security is also undermined by foreign actors, both due to risks related to foreign direct investment in critical infrastructure, and to information manipulation and interference by such actors.

These issues will be addressed through relevant instruments and frameworks; e.g. foreign direct investment will be screened in line with the relevant Regulation.

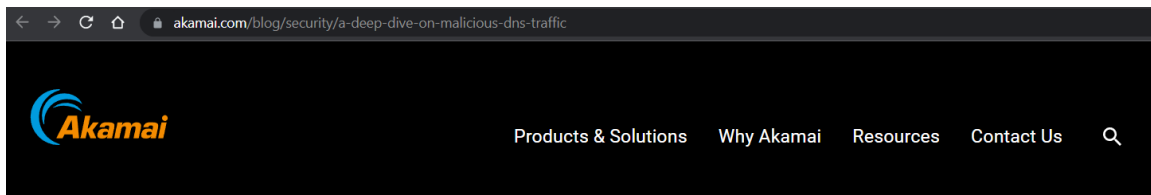
To read more: [https://oceans-and-fisheries.ec.europa.eu/system/files/2023-03/join-2023-8\\_en.pdf](https://oceans-and-fisheries.ec.europa.eu/system/files/2023-03/join-2023-8_en.pdf)

*Number 7*

## DNS data shows one in ten organisations have malware traffic on their networks



An investigation by Akamai has shown that between 10% and 16% of organisations had Domain Name System (DNS) traffic originating on their network towards command-and-control (C2) servers associated with known botnets and various other malware threats.



Blog > Security > Attack Superhighway: A Deep Dive on Malicious DNS Traffic

### Attack Superhighway: A Deep Dive on Malicious DNS Traffic

The report also showed that over 9% of devices that generated C2 traffic, did so to domain names associated with known ransomware threats. Of these, REvil and LockBit were the most common ones.



GUIDANCE

### Protective DNS for the private sector

Advice on the selection and deployment of protective Domain Name Systems (DNS).



The NCSC has produced guidance on the selection and deployment of protective DNS and there is also the Protective DNS for public sector organisations at: <https://www.ncsc.gov.uk/guidance/protective-dns-for-private-sector>

To read more: <https://www.ncsc.gov.uk/report/threat-report-24th-march-2023>

<https://www.akamai.com/blog/security/a-deep-dive-on-malicious-dns-traffic>

*Number 8*

## Preventing the Improper Use of CHIPS Act Funding

**FEDERAL REGISTER**

The Daily Journal of the United States Government



The CHIPS Act (the Act) established an incentives program to reestablish and sustain U.S. leadership across the semiconductor supply chain.

To ensure that funding provided through this program does not directly or indirectly benefit foreign countries of concern, the Act includes certain limitations on funding recipients, such as prohibiting engagement in certain significant transactions involving the material expansion of semiconductor manufacturing capacity in foreign countries of concern and prohibiting certain joint research or technology licensing efforts with foreign entities of concern.

The Department of Commerce (Department) is issuing, and requesting public comments on, a proposed rule to set forth terms related to these limitations and procedures for funding recipients to notify the Secretary of Commerce (Secretary) of any planned significant transactions that may be prohibited.

### *Background*

Semiconductors are essential components of electronic devices that enable telecommunications and grid infrastructure, run critical business and government information technology and operational technology systems, and are necessary to a vast array of products, from automobiles to fighter jets. Recognizing the criticality of supply chain security and resilience for semiconductors and related products, the President signed the Executive Order on America's Supply Chains shortly after taking office in February 24, 2021.

This Executive order, among other things, directed several Departments to undertake assessments of critical supply chains; several of the resulting reports address microelectronics and related subcomponent supply chains.

The resulting June 2021 White House Report on Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth highlighted the insufficient domestic manufacturing capacity for semiconductors. The White House Report noted that the United States lacks advanced semiconductor manufacturing capabilities and is dependent on geographically concentrated and in some cases potentially unreliable sources of supply.

It recommended dedicated funding to advance semiconductor manufacturing, and research and development to support critical manufacturing, industrial, and defense applications.

In August 2022, the Congress passed the CHIPS Act of 2022, which amended Title XCIX of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, also known as the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act.

Together, these statutory provisions (collectively, the CHIPS Act or Act), establish a semiconductor incentives program (CHIPS Incentives Program) that will provide funding, including via grants, cooperative agreements, loans, loan guarantees, and other transactions, to support investments in the construction, expansion, and modernization of facilities in the United States for the fabrication, assembly, testing, advanced packaging, production, or research and development of semiconductors, materials used to manufacture semiconductors, or semiconductor manufacturing equipment.

The CHIPS Incentives Program aims to strengthen the security and resilience of the semiconductor supply chain by mitigating gaps and vulnerabilities. It aims to ensure a supply of secure semiconductors essential for national security and to support critical manufacturing industries. It also aims to strengthen the resilience and leadership of the United States in semiconductor technology, which is vital to national security and future economic competitiveness of the United States.

The CHIPS Incentives Program is administered by the CHIPS Program Office (CPO) within the National Institute of Standards and Technology (NIST) of the United States Department of Commerce. CPO is separately issuing Notices of Funding Opportunity (NOFO) that lay out the procedures by which interested organizations may apply for CHIPS Incentives Program funds, and criteria under which applications will be evaluated.

To protect national security and the resiliency of supply chains, CHIPS Incentives Program funds may not be provided to a foreign entity of concern, such as an entity that is owned by, controlled by, or subject to the jurisdiction or direction of a country that is engaged in conduct that is detrimental to the national security of the United States. This proposed rule includes a detailed explanation of what is meant by foreign entities of concern, as well as a definition of “owned by, controlled by, or subject to the jurisdiction or direction of.”

In further support of U.S. national security interests, CHIPS Incentives Program recipients (funding recipients) are required by the Act to enter



into an agreement (required agreement) with the Department restricting engagement by the funding recipient or its affiliates in any significant transaction involving the material expansion of semiconductor manufacturing capacity in foreign countries of concern.

In recognition that some potential applicants for CHIPS Incentives may have existing facilities in foreign countries of concern, and to minimize potential supply chain disruptions, the Act includes exceptions for certain transactions involving older (legacy) semiconductor manufacturing in a foreign country of concern.

A funding recipient must notify the Secretary of any planned significant transactions of the funding recipient or its affiliates involving the material expansion of semiconductor manufacturing capacity in a foreign country of concern, including in cases where it believes the transaction is allowed under the exceptions in 15 U.S.C. 4652(a)(6)(C)(ii).

Terms related to this notification requirement are defined in Subpart A of this rule. The Secretary will provide direct notice to the funding recipient that a review of a transaction is being conducted and, later, that the Secretary has reached an initial determination regarding whether the transaction is prohibited. Funding recipients may submit additional information or request that the initial determination be reconsidered, after which the Secretary will provide a final determination.

In making determinations, the Secretary will consult with the Director of National Intelligence and the Secretary of Defense.

The Secretary will initiate review of transactions by funding recipients through self-reported notifications; the Secretary also may initiate a review of non-notified transactions, including based on information provided by other government agencies or information from other sources.

Failure by a funding recipient (or its affiliate) to comply with this restriction on semiconductor manufacturing capacity expansion in foreign countries of concern may result in recovery of the full amount of Federal financial assistance provided to the funding recipient (referred to in the Act as the “Expansion Clawback.”)

The Act also prohibits funding recipients from knowingly engaging in any joint research or technology licensing effort with a foreign entity of concern that relates to a technology or product that raises national security concerns as determined by the Secretary and communicated to the funding recipient before engaging in such joint research or technology licensing. A funding recipient's required agreement will include a commitment that the funding recipient and its affiliates will not conduct prohibited joint

research or technology licensing. Failure to comply with this restriction may also result in recovery of the full amount of Federal assistance (referred to in the Act as the “Technology Clawback.”)

To read more:

<https://www.federalregister.gov/documents/2023/03/23/2023-05869/preventing-the-improper-use-of-chips-act-funding>

## *Number 9*

### California Privacy Protection Agency (CPPA) California Consumer Privacy Act (CCPA)



The California Privacy Protection Agency (CPPA) marked a historic milestone by finalizing their first substantive rulemaking package to further implement the California Consumer Privacy Act (CCPA), which was approved by the California Office of Administrative Law (OAL). The approved regulations are **effective immediately**.

“This is a major accomplishment, and a significant step forward for Californians’ consumer privacy. I’m deeply grateful to the Agency Board and staff for their tireless work on the regulations, and to the public for their robust engagement in the rulemaking process,” said Jennifer Urban, Chairperson of the California Privacy Protection Agency Board.

The approved regulations update existing CCPA regulations to harmonize them with amendments adopted pursuant to Proposition 24, the California Privacy Rights Act (CPRA); operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law; and reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand.

They place the consumer in a position where they can knowingly and freely negotiate with a business over the business’s use of the consumer’s personal information.

“I’m incredibly impressed with the team and thankful for the Board’s thoughtful guidance,” said Ashkan Soltani, the Agency’s Executive Director. “With the regulations in place, we can now redouble our efforts to promote public awareness of consumers’ rights and businesses’ responsibilities under the law to better ensure that these privacy rights are secured.”

Lisa Kim, the Agency’s Senior Privacy Counsel and Advisor, said: “Once again California is leading the way in protecting consumer’s privacy rights. We are excited to be the first in the nation to implement comprehensive regulations on data minimization and dark patterns. With these protections, consumers can interact with businesses with more confidence and security.”

The Agency filed the final rulemaking package with OAL on February 14, 2023, initiating a 30-business day review period. This followed the CPPA

Board's vote on February 3, 2023 to adopt and approve the Agency's rulemaking package. The regulations have not changed substantively since the Agency Board voted on modifications made at its October 29, 2022 meeting.

In response to the development, Philip Laird, the Agency's General Counsel said: "I couldn't be more proud of this accomplishment. I'm immensely grateful for the legal team's incredible work."

The formal rulemaking process began on July 8, 2022, with the publication of the Agency's notice of proposed rulemaking action in the California Regulatory Notice Register. This followed extensive pre-rulemaking activities, including a series of instructive informational sessions and a set of stakeholder sessions in the spring of 2022, and a request for preliminary comments in the fall of 2021.

The final regulations and supporting materials will be made available on the CPPA website here as soon as they are processed at:  
[https://cppa.ca.gov/regulations/consumer\\_privacy\\_act.html](https://cppa.ca.gov/regulations/consumer_privacy_act.html)

To read more: <https://cppa.ca.gov/announcements/>

## Number 10

### ENISA, Transport Threat Landscape

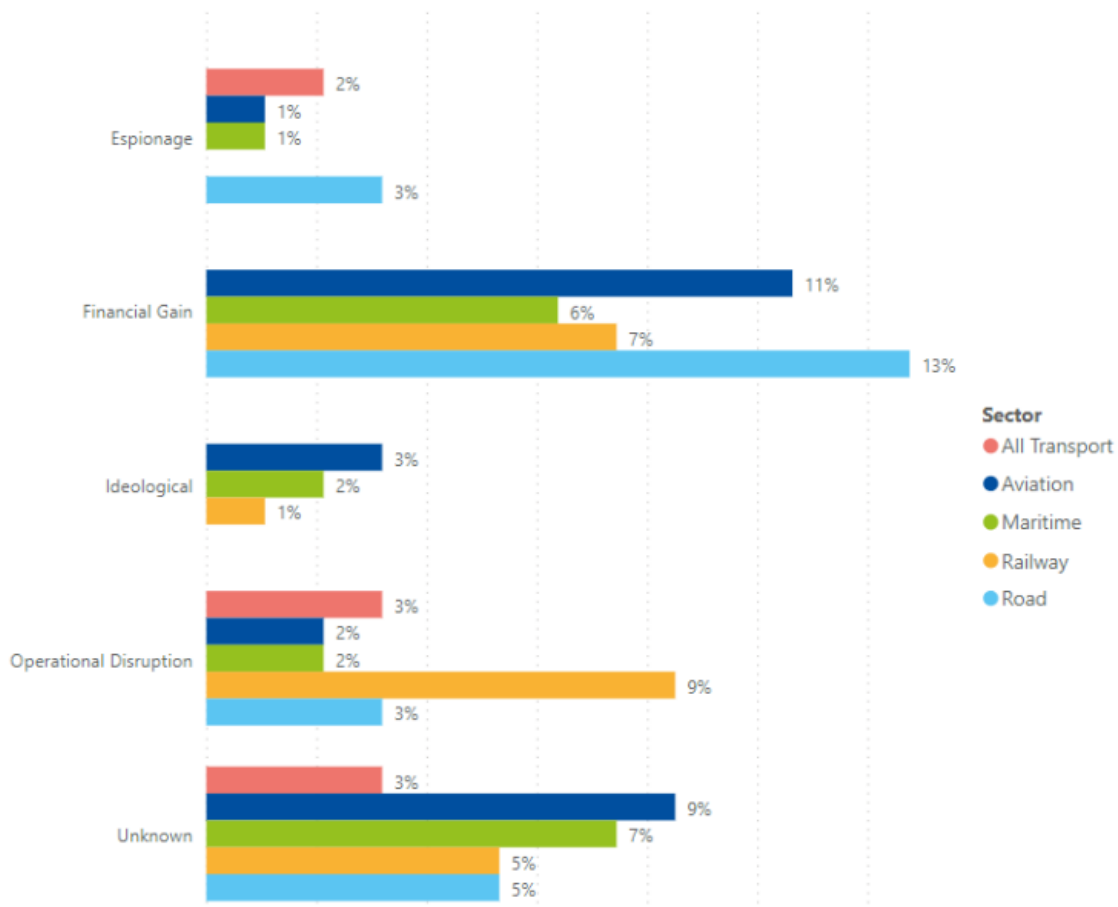


This is the first analysis conducted by the European Union Agency for Cybersecurity (ENISA) of the cyber threat landscape of the transport sector in the EU.

The report aims to bring new insights into the reality of the transport sector by mapping and studying cyber incidents from January 2021 to October 2022.

It identifies prime threats, actors and trends based on the analysis of cyberattacks targeting aviation, maritime, railway and road transport over a period of almost 2 years.

**Figure 19: Motivation in each sector**



During this period, the prime threats identified include:

- ransomware attacks (38%),
- data related threats (30%),
- malware (17%),
- denial-of-service (DoS), distributed denial-of-service (DDoS) and ransom denial-of-service (RDoS) attacks (16%),
- phishing / spear phishing (10%),
- supply-chain attacks (10%).

During the reporting period, the threat actors with the biggest impact on the sector were state-sponsored actors, cybercriminals and hacktivists.

We observed the following trends:

- Ransomware attacks became the prominent threat against the sector in 2022. Ransomware has been steadily increasing<sup>1</sup> and the transport sector has been affected similarly to the other sectors.
- Cybercriminals are responsible for the majority of attacks on the transport sector (54%), and they target all subsectors.
- Threat actors will increasingly conduct ransomware attacks with not only monetary motivations.
- The increased hacktivist activity targeting the transport sector is likely to continue.
- The increasing rate of DDoS attacks targeting the transport sector is likely to continue.
- The main targets of DDoS attacks by hacktivists are European airports, railways and transport authorities.
- During this reporting period, we did not receive reliable information on a cyberattack affecting the safety of transport.
- The majority of attacks on the transport sector target information technology (IT) systems. Operational disruptions can occur as a consequence of these attacks, but the operational technology (OT) systems are rarely being targeted.

- Ransomware groups will likely target and disrupt OT operations in the foreseeable future.

The aviation sector is facing multiple threats, with data-related threats being the most prominent, coupled by ransomware and malware.

Customer data of airlines and proprietary information of original equipment manufacturers (OEM) are the prime targeted assets of the sector.

In 2022, there has been a rise in the number of ransomware attacks affecting airports.

Fraudulent websites impersonating airlines have become a significant threat in 2022.

The maritime sector experiences ransomware, malware, and phishing attacks targeted towards port authorities, port operators, and manufacturers.

State-sponsored attackers often carry out politically motivated attacks leading to operational disruptions at ports and vessels.

The railway sector also experiences ransomware and data-related threats primarily targeting IT systems like passenger services, ticketing systems, and mobile applications, causing service disruptions.

Hactivist groups have been conducting DDoS attacks against railway companies with an increasing rate, primarily due to Russia's invasion of Ukraine.

The road transport sector faces predominantly ransomware attacks, followed by data-related threats and malware.

Automotive industry, especially OEM and tier-X suppliers, has been targeted by ransomware leading to production disruptions.

Data-related threats primarily target IT systems to acquire customer and employee data as well as proprietary information.

There is a limited number of cyber incidents that cannot be placed in one specific subsector.

These include general campaigns targeting the whole transportation sector in particular countries.

These campaigns are often attributed to hacktivists and state-sponsored actors and are linked to geopolitical tensions.

The report also highlights issues with the reporting of cyber incidents and the fact that we still have limited knowledge and information regarding such incidents.

The analysis in this report indicates that publicly disclosed incidents are just the tip of the iceberg.

To read more: <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>



*Number 11*

European Securities and Markets Authority (ESMA)

## ESMA raises concerns with the proposed changes to the insider list regime



The European Securities and Markets Authority (ESMA) the EU's financial markets regulator and supervisor, has sent a letter to the European Parliament and Council raising concerns with proposed changes to the insider list regime in the [Markets Abuse Regulation](#).

The proposed changes, which were put forward by the European Commission in December 2022 as part of the Listings Act proposal, mean that insider lists would only include persons who have regular access to inside information, and not those who may have access to such information on a case by case basis.

The letter outlines how the proposed changes may lead to detrimental effects for national supervisors and their ability to enforce against market abuse, as well as for issuers, who use insider lists to manage the flow and access to inside information.

---

**Minister Elisabeth Svantesson**  
**President, Economic and**  
**Financial Affairs Council**  
**Council of the European Union**

**Irene Tinagli**  
**Chair of the Committee on**  
**Economic and Monetary Affairs**  
**European Parliament**

**Ref: Listing Act legislative proposal – Insider List Regime**

Dear Ms Svantesson, dear Ms Tinagli,

On 8 December 2022, the European Commission published its Listing Act proposal, which aims to alleviate the administrative burden for companies of all sizes so that they can better access public funding by listing on stock exchanges.

Overall, ESMA welcomes this proposal, which aims to deliver on the 2020 CMU Action Plan's commitment to simplify EU listing rules. The proposal reflects a number of recommendations which ESMA has previously provided to the European Commission, both in response to the Listings Act public consultation, and in our advice on the Market Abuse Regulation review<sup>1 2</sup>. However, following discussion within the ESMA Board of Supervisors, I would like to share our views regarding one specific element of the proposal on which we, collectively as EU securities regulators, have substantial concerns.

The proposal amends Article 18 of MAR, stipulating that an issuer's insider list would no longer be event-based and would only need to include those persons that have regular access to inside information (so called "permanent insiders"). We believe that this proposal may have two significant detrimental effects.

The first one concerns National Competent Authorities' (NCAs) ability to enforce against market abuse.

Under the proposal, the new insider lists will not cover those persons working for the issuer who have irregular access to inside information and thus limiting the ability of NCAs to quickly identify non-permanent insiders. Moreover, NCAs will not be able to use the list to assess which permanent insider accessed each piece of inside information and when. As a result, the

identification of insiders will be a lengthy and difficult process that National Competent Authorities will have to carry out from zero when investigating potential insider dealing ex-post.

Additionally, while the proposal will not directly impact the insider list drawn up by advisors and consultants, their ability to produce their insider list in a timely manner will be affected as they will no longer be added to the issuer's list and therefore will not receive the relevant notification. Furthermore, NCAs will not be aware of the access of such advisors and consultants to the issuer's inside information.

The second significant detrimental effect would be on issuers, as they use insider lists to manage inside information, thus protecting both themselves and their staff/third parties. For example, the new regime would diminish awareness by all insiders, as they will no longer be notified that they are in possession of inside information and be informed about the relevant obligations and prohibitions. Not only will this lack of awareness increase the risk of unintended insider dealing, but it will also weaken the issuers' control of the flow of inside information.

We would appreciate it if you could take these concerns, expressed by the securities supervisors that are responsible for maintaining orderly and fair European markets, into consideration during the course of your legislative discussions.

Should you or your staff require any further information please do not hesitate to contact me or Carsten Ostermann, Acting Head of the Market and Digital Innovation Department (carsten.ostermann@esma.europa.eu)

To read more: <https://www.esma.europa.eu/press-news/esma-news/esma-raises-concerns-proposed-changes-insider-list-regime>

## *Number 12*

### #StopRansomware: LockBit 3.0



**MS-ISAC**<sup>®</sup>  
Multi-State Information  
Sharing & Analysis Center\*

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

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

Visit [stopransomware.gov](https://stopransomware.gov) to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate known LockBit 3.0 ransomware IOCs and TTPs identified through FBI investigations as recently as March 2023.

The LockBit 3.0 ransomware operations function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit.

Since January 2020, LockBit has functioned as an affiliate-based ransomware variant; affiliates deploying the LockBit RaaS use many varying TTPs and attack a wide range of businesses and critical infrastructure organizations, which can make effective computer network defense and mitigation challenging.

The FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

#### *Capabilities*

LockBit 3.0, also known as “LockBit Black,” is more modular and evasive than its previous versions and shares similarities with Blackmatter and Blackcat ransomware.

LockBit 3.0 is configured upon compilation with many different options that determine the behavior of the ransomware.

Upon the actual execution of the ransomware within a victim environment, various arguments can be supplied to further modify the behavior of the ransomware.

For example, LockBit 3.0 accepts additional arguments for specific operations in lateral movement and rebooting into Safe Mode (see LockBit Command Line parameters under Indicators of Compromise).

If a LockBit affiliate does not have access to passwordless LockBit 3.0 ransomware, then a password argument is mandatory during the execution of the ransomware. LockBit 3.0 affiliates failing to enter the correct password will be unable to execute the ransomware.

The password is a cryptographic key which decodes the LockBit 3.0 executable. By protecting the code in such a manner, LockBit 3.0 hinders malware detection and analysis with the code being unexecutable and unreadable in its encrypted form.

Signature-based detections may fail to detect the LockBit 3.0 executable as the executable's encrypted portion will vary based on the cryptographic key used for encryption while also generating a unique hash.

When provided the correct password, LockBit 3.0 will decrypt the main component, continue to decrypt or decompress its code, and execute the ransomware. LockBit 3.0 will only infect machines that do not have language settings matching a defined exclusion list.

However, whether a system language is checked at runtime is determined by a configuration flag originally set at compilation time. Languages on the exclusion list include, but are not limited to, Romanian (Moldova), Arabic (Syria), and Tatar (Russia). If a language from the exclusion list is detected, LockBit 3.0 will stop execution without infecting the system.

To read more: <https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf>

## *Number 13*

### Stopping cybercriminals from abusing security tools



Microsoft's Digital Crimes Unit (DCU), cybersecurity software company Fortra™ and Health Information Sharing and Analysis Center (Health-ISAC) are taking technical and legal action to disrupt cracked, legacy copies of Cobalt Strike and abused Microsoft software, which have been used by cybercriminals to distribute malware, including ransomware.

This is a change in the way DCU has worked in the past – the scope is greater, and the operation is more complex. Instead of disrupting the command and control of a malware family, this time, we are working with Fortra to remove illegal, legacy copies of Cobalt Strike so they can no longer be used by cybercriminals.

We will need to be persistent as we work to take down the cracked, legacy copies of Cobalt Strike hosted around the world. This is an important action by Fortra to protect the legitimate use of its security tools. Microsoft is similarly committed to the legitimate use of its products and services. We also believe that Fortra choosing to partner with us for this action is recognition of DCU's work fighting cybercrime over the last decade. Together, we are committed to going after the cybercriminal's illegal distribution methods.

Cobalt Strike is a legitimate and popular post-exploitation tool used for adversary simulation provided by Fortra. Sometimes, older versions of the software have been abused and altered by criminals. These illegal copies are referred to as "cracked" and have been used to launch destructive attacks, such as those against the Government of Costa Rica and the Irish Health Service Executive. Microsoft software development kits and APIs are abused as part of the coding of the malware as well as the criminal malware distribution infrastructure to target and mislead victims.

The ransomware families associated with or deployed by cracked copies of Cobalt Strike have been linked to more than 68 ransomware attacks impacting healthcare organizations in more than 19 countries around the world.

These attacks have cost hospital systems millions of dollars in recovery and repair costs, plus interruptions to critical patient care services including delayed diagnostic, imaging and laboratory results, canceled medical procedures and delays in delivery of chemotherapy treatments, just to name a few.

## *Disruption components and strategy*

On March 31, 2023, the U.S. District Court for the Eastern District of New York issued a court order allowing Microsoft, Fortra, and Health-ISAC to disrupt the malicious infrastructure used by criminals to facilitate their attacks.

Doing so enables us to notify relevant internet service providers (ISPs) and computer emergency readiness teams (CERTs) who assist in taking the infrastructure offline, effectively severing the connection between criminal operators and infected victim computers.

Fortra and Microsoft's investigation efforts included detection, analysis, telemetry, and reverse engineering, with additional data and insights to strengthen our legal case from a global network of partners, including Health-ISAC, the Fortra Cyber Intelligence Team, and Microsoft Threat Intelligence team data and insights. Our action focuses solely on disrupting cracked, legacy copies of Cobalt Strike and compromised Microsoft software.

Microsoft is also expanding a legal method used successfully to disrupt malware and nation state operations to target the abuse of security tools used by a broad spectrum of cybercriminals.

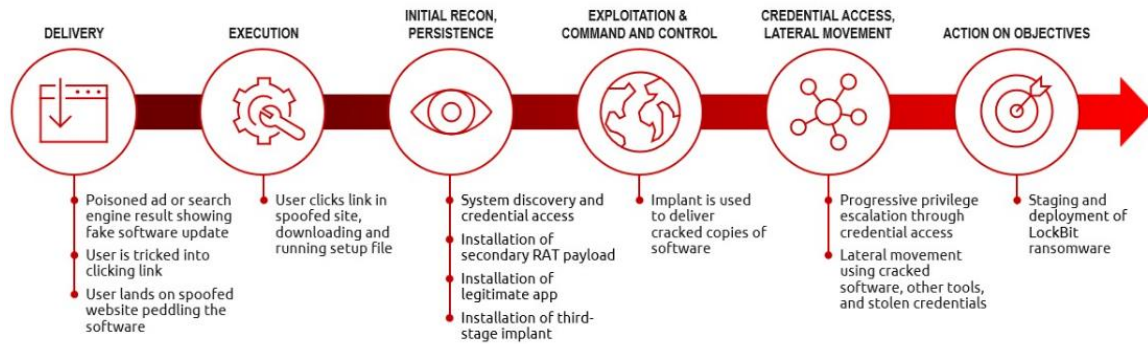
Disrupting cracked legacy copies of Cobalt Strike will significantly hinder the monetization of these illegal copies and slow their use in cyberattacks, forcing criminals to re-evaluate and change their tactics. Today's action also includes copyright claims against the malicious use of Microsoft and Fortra's software code which are altered and abused for harm.

### *Abuse by cybercriminals*

Fortra has taken considerable steps to prevent the misuse of its software, including stringent customer vetting practices. However, criminals are known to steal older versions of security software, including Cobalt Strike, creating cracked copies to gain backdoor access to machines and deploy malware. We have observed ransomware operators using cracked copies of Cobalt Strike and abused Microsoft software to deploy Conti, LockBit, and other ransomware as part of the ransomware as a service business model.

Threat actors use cracked copies of software to speed up their ransomware deployment on compromised networks. The below diagram shows an attack flow, highlighting contributing factors, including spear phishing and malicious spam emails to gain initial access, as well as the abuse of code stolen from companies like Microsoft and Fortra.

While the exact identities of those conducting the criminal operations are currently unknown, we have detected malicious infrastructure across the globe, including in China, the United States and Russia. In addition to financially motivated cybercriminals, we have observed threat actors acting in the interests of foreign governments, including from Russia, China, Vietnam and Iran, using cracked copies.



To read more: <https://blogs.microsoft.com/on-the-issues/2023/04/06/stopping-cybercriminals-from-abusing-security-tools/>

*Number 14***New OpcJacker Malware Distributed via Fake VPN Malvertising**

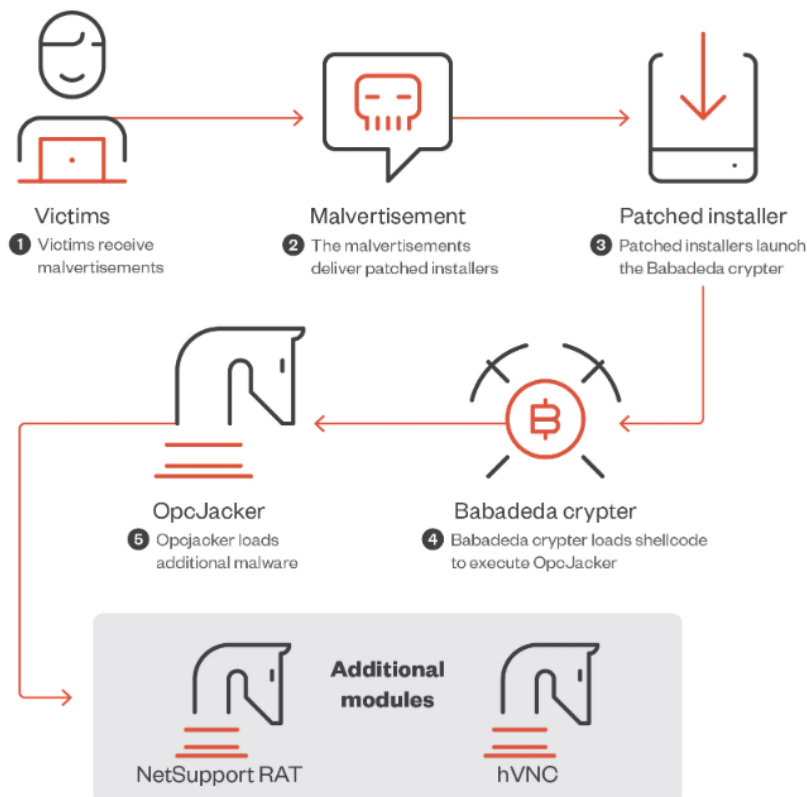
We discovered a new malware, which we named “OpcJacker” (due to its opcode configuration design and its cryptocurrency hijacking ability), that has been distributed in the wild since the second half of 2022.

OpcJacker is an interesting piece of malware, since its configuration file uses a custom file format to define the stealer’s behavior.

Specifically, the format resembles custom virtual machine code, where numeric hexadecimal identifiers present in the configuration file make the stealer run desired functions.

The purpose of using such a design is likely to make understanding and analyzing the malware’s code flow more difficult for researchers.

OpcJacker’s main functions include keylogging, taking screenshots, stealing sensitive data from browsers, loading additional modules, and replacing cryptocurrency addresses in the clipboard for hijacking purposes.



©2023 TREND MICRO



To read more: [https://www.trendmicro.com/en\\_us/research/23/c/new-opcjacker-malware-distributed-via-fake-vpn-malvertising.html](https://www.trendmicro.com/en_us/research/23/c/new-opcjacker-malware-distributed-via-fake-vpn-malvertising.html)

*Number 15***Artificial Intelligence Risk Management Framework (AI RMF 1.0)**

Artificial intelligence (AI) technologies have significant potential to transform society and people's lives – from commerce and health to transportation and cybersecurity to the environment and our planet.

AI technologies can drive inclusive economic growth and support scientific advancements that improve the conditions of our world.

AI technologies, however, also pose risks that can negatively impact individuals, groups, organizations, communities, society, the environment, and the planet.

Like risks for other types of technology, AI risks can emerge in a variety of ways and can be characterized as long- or short-term, high or low-probability, systemic or localized, and high- or low-impact.

While there are myriad standards and best practices to help organizations mitigate the risks of traditional software or information-based systems, the risks posed by AI systems are in many ways unique.

AI systems, for example, may be trained on data that can change over time, sometimes significantly and unexpectedly, affecting system functionality and trustworthiness in ways that are hard to understand.

AI systems and the contexts in which they are deployed are frequently complex, making it difficult to detect and respond to failures when they occur.

AI systems are inherently socio-technical in nature, meaning they are influenced by societal dynamics and human behavior.

AI risks – and benefits – can emerge from the interplay of technical aspects combined with societal factors related to how a system is used, its interactions with other AI systems, who operates it, and the social context in which it is deployed.

These risks make AI a uniquely challenging technology to deploy and utilize both for organizations and within society.

Without proper controls, AI systems can amplify, perpetuate, or exacerbate inequitable or undesirable outcomes for individuals and communities.

With proper controls, AI systems can mitigate and manage inequitable outcomes.

AI risk management is a key component of responsible development and use of AI systems.

Responsible AI practices can help align the decisions about AI system design, development, and uses with intended aim and values.

Core concepts in responsible AI emphasize human centricity, social responsibility, and sustainability.

AI risk management can drive responsible uses and practices by prompting organizations and their internal teams who design, develop, and deploy AI to think more critically about context and potential or unexpected negative and positive impacts.

Understanding and managing the risks of AI systems will help to enhance trustworthiness, and in turn, cultivate public trust.



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

The AI RMF is intended to be practical, to adapt to the AI landscape as AI technologies continue to develop, and to be operationalized by organizations in varying degrees and capacities so society can benefit from AI while also being protected from its potential harms.

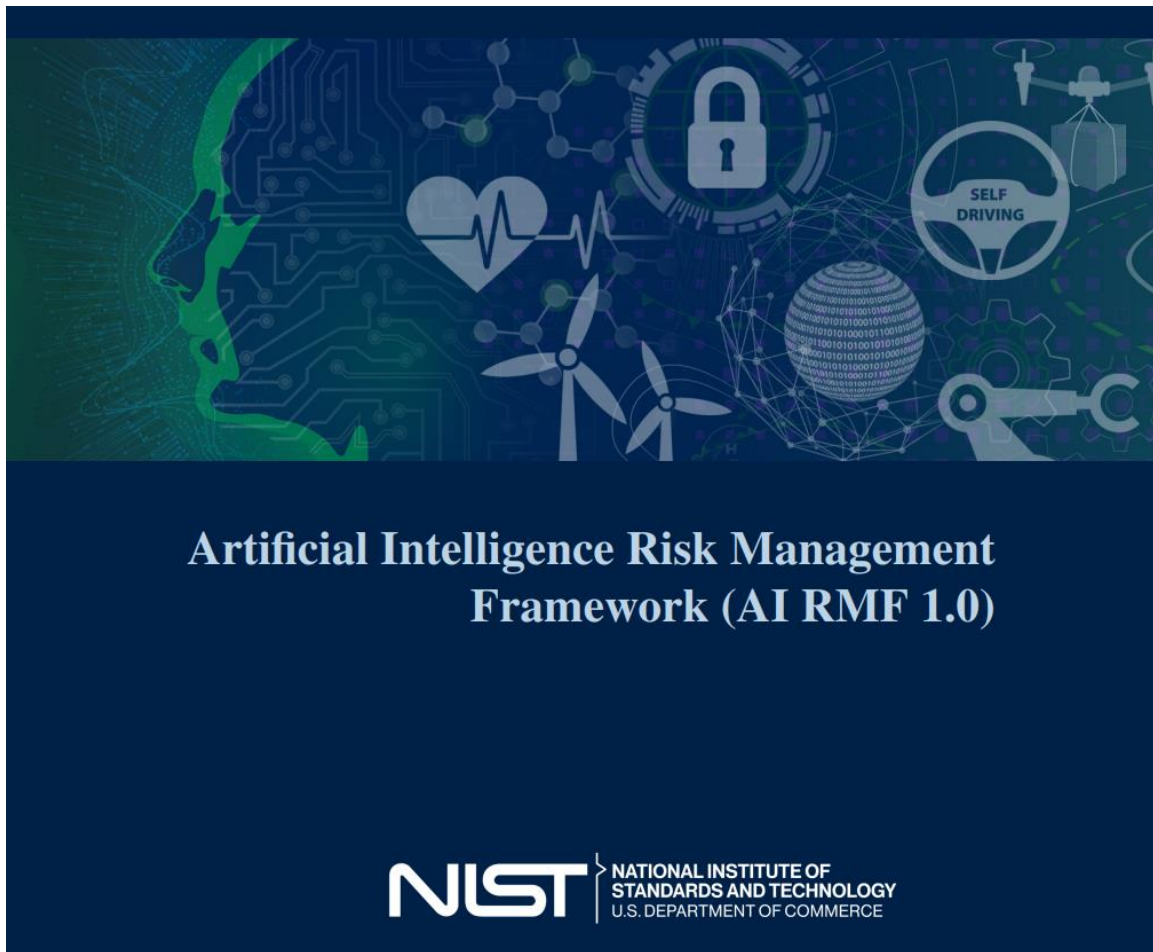
The Framework and supporting resources will be updated, expanded, and improved based on evolving technology, the standards landscape around the world, and AI community experience and feedback.

NIST will continue to align the AI RMF and related guidance with applicable international standards, guidelines, and practices. As the AI RMF is put into use, additional lessons will be learned to inform future updates and additional resources.

The Framework is divided into two parts. Part 1 discusses how organizations can frame the risks related to AI and describes the intended audience. Next, AI risks and trustworthiness are analyzed, outlining the characteristics of trustworthy AI systems, which include

## Table of Contents

<b>Executive Summary</b>	<b>1</b>
<b>Part 1: Foundational Information</b>	<b>4</b>
<b>1 Framing Risk</b>	<b>4</b>
1.1 Understanding and Addressing Risks, Impacts, and Harms	4
1.2 Challenges for AI Risk Management	5
1.2.1 Risk Measurement	5
1.2.2 Risk Tolerance	7
1.2.3 Risk Prioritization	7
1.2.4 Organizational Integration and Management of Risk	8
<b>2 Audience</b>	<b>9</b>
<b>3 AI Risks and Trustworthiness</b>	<b>12</b>
3.1 Valid and Reliable	13
3.2 Safe	14
3.3 Secure and Resilient	15
3.4 Accountable and Transparent	15
3.5 Explainable and Interpretable	16
3.6 Privacy-Enhanced	17
3.7 Fair – with Harmful Bias Managed	17
<b>4 Effectiveness of the AI RMF</b>	<b>19</b>
<b>Part 2: Core and Profiles</b>	<b>20</b>
<b>5 AI RMF Core</b>	<b>20</b>
5.1 Govern	21
5.2 Map	24
5.3 Measure	28
5.4 Manage	31
<b>6 AI RMF Profiles</b>	<b>33</b>
<b>Appendix A: Descriptions of AI Actor Tasks from Figures 2 and 3</b>	<b>35</b>
<b>Appendix B: How AI Risks Differ from Traditional Software Risks</b>	<b>38</b>
<b>Appendix C: AI Risk Management and Human-AI Interaction</b>	<b>40</b>
<b>Appendix D: Attributes of the AI RMF</b>	<b>42</b>



To read more: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

## *Number 16*

### The Markets in Crypto Assets (MiCA) regulation received 517 votes from European Parliament

European Parliament  
2019-2024



MiCA will protect consumers against some of the risks associated with the investment in crypto-assets, and help them avoid fraudulent schemes. Currently, consumers have very limited rights to protection or redress, especially if the transactions take place outside the EU.

With the new rules, crypto-asset service providers will have to respect strong requirements to protect consumers wallets and become liable in case they lose investors' crypto-assets. MiCA will also cover any type of market abuse related to any type of transaction or service, notably for market manipulation and insider dealing.

Actors in the crypto-assets market will be required to declare information on their environmental and climate footprint. The European Securities and Markets Authority (ESMA) will develop draft regulatory technical standards on the content, methodologies and presentation of information related to principal adverse environmental and climate-related impact.

The European Commission will have to provide a report on the environmental impact of crypto-assets and the introduction of mandatory minimum sustainability standards for consensus mechanisms, including the proof-of-work.

To avoid any overlaps with updated legislation on anti-money laundering (AML), which will now also cover crypto-assets, MiCA does not duplicate the anti-money laundering provisions as set out in the newly updated transfer of funds rules agreed on 29 June.

However, MiCA requires that the European Banking Authority (EBA) will be tasked with maintaining a public register of non-compliant crypto-asset service providers.

Crypto-asset service providers, whose parent company is located in countries listed on the EU list of third countries considered at high risk for anti-money laundering activities, as well as on the EU list of non-cooperative jurisdictions for tax purposes, will be required to implement enhanced checks in line with the EU AML framework.

Tougher requirements may also be applied to shareholders and to the management of the CASPs), notably with regard to their localisation.

The provisional agreement:

[https://www.europarl.europa.eu/RegData/commissions/econ/inag/2022/10-05/CJ12\\_AG\(2022\)737215\\_EN.pdf](https://www.europarl.europa.eu/RegData/commissions/econ/inag/2022/10-05/CJ12_AG(2022)737215_EN.pdf)

To read more: <https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu>

*Number 17***The threat from commercial cyber proliferation***NCSC Assessment*

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

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

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

This report was produced for CYBERUK 2023 and uses formal probabilistic language (see yardstick) from NCSC-A product to inform readers about the threat to UK industry and society from commercial cyber tools and services. To learn more about NCSC-A, please contact [enquiries@ncsc.gov.uk](mailto:enquiries@ncsc.gov.uk).

*How likely is a 'realistic possibility'?**Professional Head of Intelligence Assessment (PHIA) Probability Yardstick*

NCSC Assessment uses the PHIA probability yardstick every time we make an assessment, judgement, or prediction. The terms used correspond to the likelihood ranges below.





## *Key judgements*

1. Commercial cyber tools and services lower the barrier to entry to state and non-state actors in obtaining cost-effective capability and intelligence they would not otherwise be able to develop or acquire themselves. This commercial proliferation will almost certainly be transformational on the cyber landscape.
2. The sophistication of some commercial intrusion cyber products and services can almost certainly rival the equivalent capabilities of some state-linked Advanced Persistent Threat (APT) groups.
3. Commercial spyware has been almost certainly used by some states in the targeting of journalists, human rights activists, political dissidents and opponents and foreign government officials at scale.
4. Commercial 'hackers-for-hire' pose a potential corporate espionage threat against organisations and individuals with privileged or valuable confidential information, across multiple sectors.
5. Hackers-for-hire raise the likelihood of unpredictable targeting or unintentional escalation through attempts to compromise a wider range of targets.
6. The proliferation of commercial cyber capability will result in an expanding number of elements for cyber defence to detect and mitigate , and a similarly expanding number and type of victims.

### *What is the commercial cyber proliferation threat?*

The commercial proliferation of cyber tools and services lowers the barrier to entry to state and non-state actors in obtaining capability and intelligence that they would not otherwise be able to develop or acquire.

The sophistication of some commercial intrusion cyber products and services can almost certainly rival the equivalent capabilities of some state-linked Advanced Persistent Threat (APT) groups.

The bulk of the commercial cyber sector is highly likely focused on satisfying domestic state demand from law enforcement and government agencies.

However, over the last decade, a growing number of enterprises have emerged offering a range of products and services to global customers.

They include off-the-shelf capability (Hacking-as-a-Service), bespoke hacking services (hackers-for-hire), and the sale of enabling capabilities such as zero-day exploits and tool frameworks.

### *SPYWARE: Hacking-as-a-Service companies*

Over the last ten years, at least 80 countries have purchased commercial cyber intrusion software, or spyware. For dozens of states without a skills base, the commercial sector is almost certainly transformational, allowing cost-effective access to capability that would otherwise take decades to develop.

While products vary in capability and application, commercially available spyware for mobile devices can offer the ability to read messages, listen to audio calls, obtain photos, locate the device and remotely operate the camera and microphone. Some states are likely to procure multiple commercial cyber tools to meet their requirements.

Devices can be compromised in a number of ways, including phishing, but also 'zero-click' attacks which do not require user interaction, making it more difficult for victims to mitigate.

While these tools have been used by states against law enforcement targets, spyware has almost certainly been used by some states in the targeting of journalists, human rights activists, political dissidents and opponents and foreign government officials.

This is almost certainly happening at scale, with thousands of individuals targeted each year. While current products focus on mobile devices and intelligence gathering, as the sector grows and demand increases, products and services will likely diversify to meet demand.

### *BESPOKE SERVICES: Hackers-for-hire*

Hacker-for-hire groups carry out cyber activity for paying clients. As well as providing information of traditional espionage value to states, hackers-for-hire are also reportedly used for legal disputes, intellectual property theft, insider trading, and the theft of other private data.

Hackers-for-hire differ in skill and capability, ranging from low-level cyber crime activity to technically complex and effective network compromises that may go undetected. Some groups operate in criminal circles, some portray themselves as commercial companies, and others operate anonymously.

Hacker-for-hire groups that focus on stealing information use phishing and other social engineering attacks, exploits against publicly reported vulnerabilities in computer networks, and sometimes zero-day attacks to compromise victims.

The greatest threat comes from higher-end, hacker-for-hire groups, whose abilities and impact are similar to those of capable state actors.

Hackers-for-hire pose a potential corporate espionage threat against organisations and individuals with privileged or valuable confidential information in multiple sectors.

While less-skilled and cyber criminal hackers-for-hire almost certainly carry out Denial of Service (DoS) attacks for a fee to temporarily disrupt a target website or server on a customer's behalf, additional law enforcement attention probably deters higher skilled hackers-for-hire from conducting destructive or disruptive operations.

However, a growing market and the extra financial incentive raise the likelihood of hackers-for-hire accepting this type of tasking over the next five years. Hackers-for-hire also raise the likelihood of unpredictable targeting or unintentional escalation through attempts to compromise a wider range of targets, particularly those seeking valuable information to sell on, as opposed to 'working to order'.

It is likely that potentially significant financial rewards incentivise state employees or contractors with cyber skills to become hackers-for-hire, risking the proliferation of cyber techniques from state to non-state actors.

### *THE COMMERCIAL ZERO-DAY EXPLOIT MARKETPLACE*

Historically, underground criminal markets have facilitated the exploit trade. Since the early 2000s, a lucrative market for zero-day exploits has emerged in the commercial space.

The large sums of money involved for critical zero-day exploits for commonly used systems and processes mean opportunities for profit are significant and have driven commercialisation.

Critical zero-day exploits and vulnerabilities are almost certainly transformational to actors with the skills to make use of them. States, or commercial cyber intrusion companies providing products to states, are the dominant customers of the commercial zero-day market and are highly likely to remain so for the next five years.

The growth of the commercial sector facilitating this trade has likely increased the number of states able to access critical zero-day capability, directly or indirectly.

Some well-funded cyber crime groups have highly likely purchased lower priced zero-day exploits for less well-used systems from underground exploit marketplaces. However, purchasing high-cost, critical zero-day capability from the commercial marketplace is unlikely to appeal to most cyber crime groups.

Financial motivation makes it more likely that they prioritise lower-cost exploits developed from disclosed zero-day vulnerabilities, albeit as early as possible after disclosure to maximise the number of unpatched systems they can target.

### *COMMODITISATION OF TOOLS*

Customisable tool frameworks are developed by cyber security software developers to emulate threat activity to enable penetration testing of networks. They are usually sold under licence, but some are also publicly available or available in versions where the licence has been removed.

These frameworks are being used or repurposed by state and non-state actors; highly likely enabling a cost-effective uplift in cyber capability. It is highly likely that their constant evolution and the ability of actors to customise and repurpose these frameworks means widespread misuse of these frameworks will almost certainly continue over the next five years.

State and non-state actors also have access to capability developed and sold for cyber crime. In recent years, cyber crime marketplaces have grown and become increasingly professionalised, in part driven by demand from ransomware actors.

One example is Malware-as-a-Service (MaaS), which is a service that provides use of malware, eliminating the need to create and develop the software as well as reducing the knowledge threshold required to operate the malware. Offering these services as a package is attractive to less skilled cyber criminals and as such has almost certainly expanded the number of victims.

#### *Looking ahead*

Over the next five years:

1. Increased demand, coupled with a permissive operating environment, will almost certainly result in an expansion of the

- global commercial cyber intrusion sector, driving an increased threat to a wide range of sectors.
2. It is almost certain there will be further high-profile exposures of victims against whom commercial cyber tools or hack er-for-hire operations have been deployed.
  3. Oversight of the commercial intrusion cyber sector will almost certainly lack international consensus, be difficult to enforce and subject to political and commercial influence.
  4. However, it is likely that many commercial cyber companies will be incentivised to vet and limit their customer bases, should effective oversight and international norms on development and sale of commercial cyber capability emerge.

### Cyber proliferation —

**Cyber proliferation** refers to the intentional or unintentional transfer of cyber capabilities between actors for network or device exploitation or attack purposes.

### Cyber intrusion companies —

**Cyber intrusion companies** refer to any commercial company that offers products or services for network or device exploitation or attack, rather than cyber security purposes. These might include sellers of vulnerabilities and exploits, companies developing and selling cyber surveillance products or companies offering hacker -for-hire services.

### Hacking-as-a-Service companies —

**Hacking-as-a-Service companies** describes the provision of 'off-the-shelf' cyber intrusion products such as mobile spyware, and supporting services, by a commercial entity, usually to nation state law enforcement and intelligence services. The customers usually manage the victim targeting and resulting intelligence; the commercial entity provides the capability and often the supporting infrastructure as a service under a licence.

## Hackers-for-hire

**Hackers-for-hire** are unaffiliated individuals or groups of actors that are hired by states, entities or even individuals to conduct cyber operations to meet customer requirements. They use their own tools and techniques and are aware of, and in some cases may select, who they are targeting.

## Commercial Tool Frameworks

**Commercial Tool Frameworks** (also known as Offensive Security Tools) are developed in the cyber security sector to provide customisable tool frameworks to facilitate and manage the intrusion of client networks to aid penetration testing of systems.

To read more: <https://www.ncsc.gov.uk/report/commercial-cyber-proliferation-assessment>

*Number 18***Ransomware Vulnerability Warning Pilot (RVWP)**

**CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY**



The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA), which the US President signed into law in March 2022, required CISA to establish the RVWP (see Section 105 [6 U.S.C. § 652 note]).

Organizations across all sectors and of all sizes are too frequently impacted by damaging ransomware incidents. Many of these incidents are perpetrated by ransomware threat actors using known vulnerabilities.

By urgently fixing these vulnerabilities, organizations can significantly reduce their likelihood of experiencing a ransomware event. In addition, organizations should implement other security controls as described on [stopransomware.gov](https://stopransomware.gov).

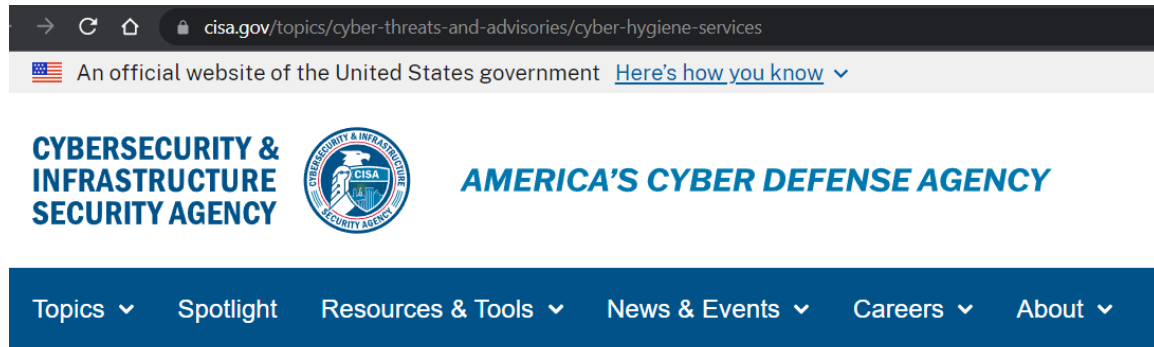


However, most organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network. Through the Ransomware Vulnerability Warning Pilot (RVWP), which started on January 30, 2023, CISA is undertaking a new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors

As part of RVWP, CISA leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks.

Once CISA identifies these affected systems, our regional cybersecurity personnel notify system owners of their security vulnerabilities, thus enabling timely mitigation before damaging intrusions occur.

CISA accomplishes this work by leveraging its existing services, data sources, technologies, and authorities, including [CISA's Cyber Hygiene Vulnerability Scanning service](#) and the Administrative Subpoena Authority granted to CISA under Section 2209 of the Homeland Security Act of 2002.



The screenshot shows the top portion of the CISA website. At the top, there is a browser address bar with the URL [cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services](https://cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services). Below the address bar is a banner with the text "An official website of the United States government" and a link "Here's how you know". The main header area contains the CISA logo on the left, which includes the text "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY" and the agency's seal. To the right of the logo is the text "AMERICA'S CYBER DEFENSE AGENCY". Below the header is a dark blue navigation bar with white text and dropdown arrows for "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About".

[Home](#) / [Topics](#) / [Cyber Threats and Advisories](#)

# Cyber Hygiene Services

You may visit: <https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services>

To read more: <https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot>





*Number 19***Development of a National Spectrum Strategy**

National Telecommunications and Information Administration,  
Department of Commerce - Request for comments.



**SUMMARY:** The National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, seeks public comment on the development and implementation of a National Spectrum Strategy for the United States.

Through this Request for Comments, NTIA seeks broad input from interested stakeholders, including private industry (specifically including developers and end-users of spectrum-based technologies and services, and contractors for federal missions), academia, civil society, the public sector, and others on three proposed pillars of the National Spectrum Strategy set forth below.

**DATES:** Parties should file their comments no later than **April 17, 2023**.

**ADDRESSES:** All electronic comments on this action, identified by Regulations.gov docket number NTIA– 2023–0003, may be submitted through the Federal e-Rulemaking Portal at <https://www.regulations.gov>.

The docket established for this proceeding can be found at [www.Regulations.gov](http://www.Regulations.gov), NTIA– 2023–0003. Click the “Comment Now!” icon, complete the required fields, and enter or attach your comments.

Responders should include a page number on each page of their submissions. Please do not include in your comments information of a confidential nature, such as sensitive personal information.

All comments received are part of the public record and generally will be posted to Regulations.gov and the NTIA website without change. All personally identifiable information (e.g., name, address) voluntarily submitted by the commenter may be publicly accessible.

For more detailed directions regarding the content of comment submissions, please see the “Request for Comments” section below. Those encountering any difficulties with the prescribed formatting and uploading directions should notify Mr. Alden at the contact information listed below at least ten (10) business days before the filing deadline.

NTIA welcomes views on the NSS pillars as detailed in this notice, and these views may be reflected, at the agency's discretion, in the ensuing development of the NSS and implementation plan.

These public comments are being gathered in conjunction with a series of public listening sessions, which will be held concurrently with the comment period of this RFC. Schedules and instructions for attending and speaking at the public listening sessions will be available on NTIA's website at [https:// www.ntia.gov](https://www.ntia.gov).

### *Background*

America is increasingly dependent on secure and reliable access to radio frequency spectrum. Sufficient access to spectrum is vital to national security, critical infrastructure, transportation, emergency response, public safety, scientific discovery, economic growth, competitive next-generation communications, and diversity, equity, and inclusion.

Increased spectrum access will also advance U.S. innovation, connectivity, and competition, create high-paying and highly skilled jobs, and produce improvements to the overall quality of life.

Access to more spectrum, in short, will help the United States continue to lead the world in advanced technology and enhance our national and economic security.

Spectrum access, however, must be managed responsibly and efficiently. NTIA jointly manages the nation's spectrum resources with the Federal Communications Commission.

NTIA is requesting comments from interested parties to help inform the development of a national spectrum strategy, which is needed for the U.S. to plan effectively for its current and future spectrum needs.

As part of this effort, and to support the need for greater spectrum access, NTIA—in collaboration with the Federal Communications Commission and in coordination with its other federal partners—endeavors to identify at least 1,500 megahertz of spectrum for in-depth study to determine whether that spectrum can be repurposed to allow more intensive use.

The Department of Commerce is committed to developing a national spectrum strategy based upon collaboration with both federal and non-federal stakeholders, including Tribes, and on data-driven decision-making, to fully address the needs of spectrum reliant services and missions, including but not limited to:

- Fixed and mobile wireless broadband services;
- Next-generation satellite communications and other space-based systems;
- Advanced transportation technologies;
- Industrial and commercial applications, (i.e., manufacturing, agriculture, and utilities);
- Wireless medical devices and telemedicine;
- Internet of Things (IoT) and smart cities;
- National defense and homeland security;
- Safeguarding the national airspace and ports;
- Securing the Nation's critical infrastructure;
- Earth and space exploration and research; and
- Climate monitoring and forecasting, and other scientific endeavors.

To read more: <https://www.regulations.gov/document/NTIA-2023-0003-0001>

*Number 20***BIS's Project Nexus prototype successfully links Eurosystem, Malaysia and Singapore payments systems.**

Partners in Indonesia, Malaysia, the Philippines, Singapore and Thailand to work towards wider payments connectivity



To enhance cross-border payments, the BIS Innovation Hub Singapore Centre developed the Nexus concept of a first-of-its-kind multilateral network connecting multiple domestic instant payment systems (IPS).

Nexus prototype successfully connected the test IPS of the Eurosystem, Malaysia and Singapore, allowing payments to be sent across the three using only mobile phone numbers.



**Project Nexus**  
 Enabling instant  
 cross-border  
 payments

BIS Innovation Hub  
 Bank of Italy  
 Bank Indonesia  
 Central Bank of Malaysia  
 Bangko Sentral ng Pilipinas  
 Monetary Authority of Singapore  
 Bank of Thailand

In the next phase, BIS and the central banks of Indonesia, Malaysia, the Philippines, Singapore and Thailand will jointly work towards connecting their domestic IPS through Nexus.

The BIS Innovation Hub Singapore Centre and partners today announced the successful connection of the test versions of three established IPS using the Nexus model and outlined the next phase of the project to work on the real-world potential of a multilateral network that could be scaled up across more countries.

The year-long collaboration included the Bank of Italy, Central Bank of Malaysia (BNM) and Monetary Authority of Singapore (MAS), plus the payment systems operators PayNet and Banking Computer Services (BCS).

Test payments were initiated using only the mobile phone numbers or the recipients' company registration numbers via the Eurosystem's TARGET Instant Payment Settlement (TIPS), Malaysia's Real-time Retail Payments Platform (RPP) and Singapore's Fast and Secure Transfers (FAST) payment system.

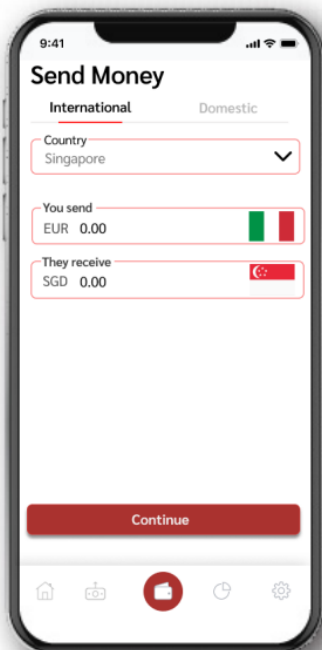
The Nexus report, published today, provides details on the early experiments and technical specifications for the multilateral interlinking of payment systems.

The success of the experiment paves the way for the BIS Innovation Hub Singapore Centre to explore the practical applications of a distributed multilateral network.



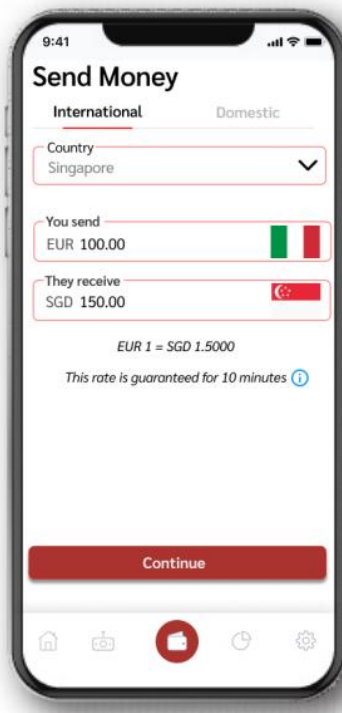
The sender logs in to their bank or PSP's existing app. (There is no separate Nexus app.)

The sender selects the Destination Country.



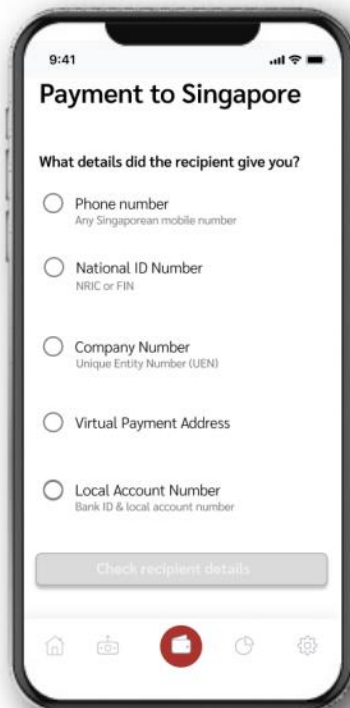
The sender enters EITHER the amount they wish to send, in their own currency OR the amount they wish the recipient to receive, in the recipient's currency.

The recipient will receive exactly the amount shown, without deductions. If the Destination PSP charges the recipient any fees for processing the payment, these must be charged as a separate line item.



**Nexus retrieves a list of quotes.** The sender's PSP (Source PSP) will also ask Nexus for available quotes for payments to the Destination Country. Nexus returns a list of quotes from different FXPs. The Source PSP selects the quote and FX Provider that it wishes to use. The Source PSP can also choose to add a markup to the FX rate before it displays the final rate to the sender.

If the sender accepts the rate, they click "Continue". If they change either amount, the rate will be refreshed (as larger payments may be eligible for better rates).

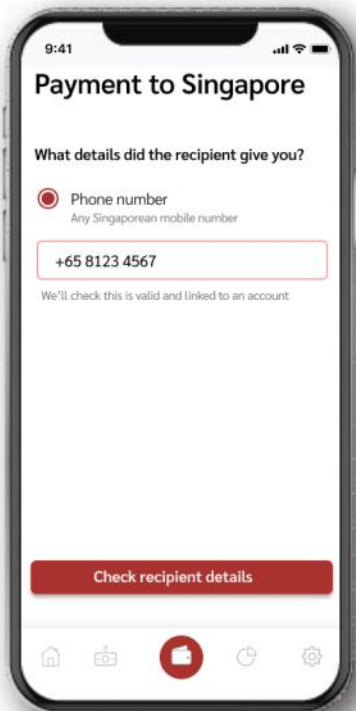


The Source PSP uses the Nexus API to request the full list of proxy formats that can be used to address payments to the Destination Country. It uses this information to dynamically create a list of proxy formats in the app.

The sender then selects the type of proxy or account details that the recipient has provided to them.

The sender can select a proxy (such as a mobile phone number). Any alias that is valid in the Destination Country will also be valid through Nexus.

The sender can alternatively enter a domestic account number and PSP identifier (such as a BIC) or an International Bank Account Number, where these are accepted in the Destination Country.



If a sender enters a proxy, the Source PSP will send this information to Nexus. Nexus will then contact the proxy resolution service in the Destination Country. If the proxy is registered to an account, it will respond to Nexus with the associated account details and the name of the recipient, along with a display name that can be shown to the sender.

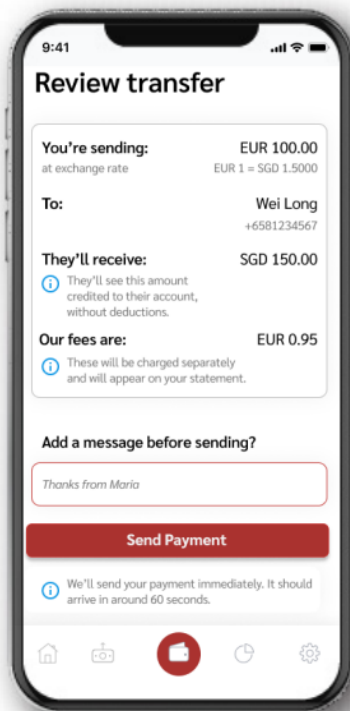
Nexus will then use the account details to confirm that the recipient's PSP is onboarded with Nexus and able to receive cross-border payments.



Now the sender is shown the name of the recipient, as provided by the proxy resolution service, where available.

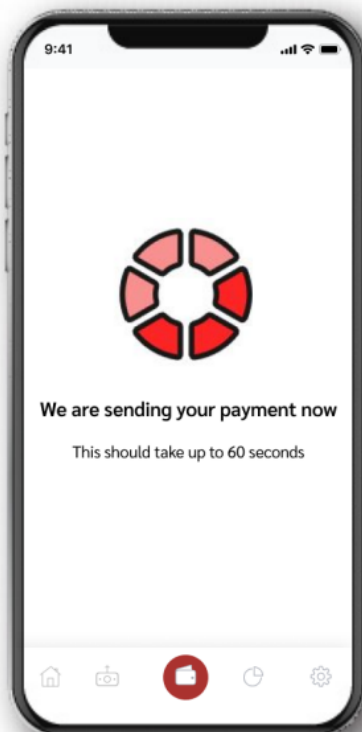
Depending on the country's requirements, they may see the full name or the name partially obscured.

The sender confirms the name. (If they don't recognise the name, they can cancel the payment).



The sender is given a chance to confirm all details. They are shown exactly what will be deducted from their account, exactly what will be credited to the recipient, the final exchange rate that applies and any fees that the sender's PSP or bank will charge the sender.

The sender clicks "Send Payment".

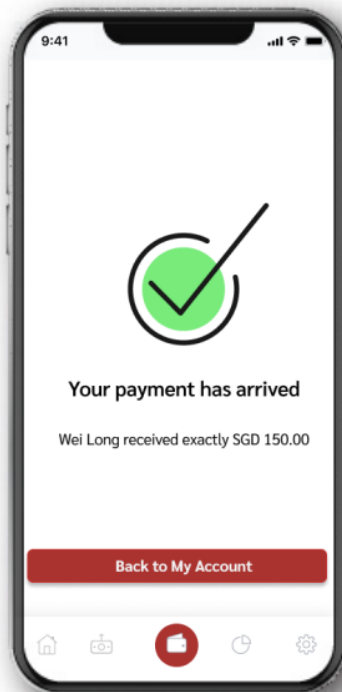


**Final payment instruction** – the payment instruction can now be sent from the Source PSP to the Source IPS.

Once the payment is complete in the Source IPS, the Nexus Gateway will communicate with the Nexus Gateway in the Destination Country, which will trigger the second stage of the process in the destination IPS.

The payment should be processed within 60 seconds in most cases.





Once the final payment stage is complete, the recipient will be credited and notified, and the sender will be notified that their payment was successful.

In some cases, the payment will trigger an alert against any sanctions lists. If the PSP in question does not have a highly automated screening process, it may need extra time to process the payment. In this case, the payment will still successfully reach the recipient's PSP, but the PSP will have extra time (defined in the Nexus Scheme Rulebook) to review the payment before crediting it to the recipient.

To read more: <https://www.bis.org/press/p230323.htm>

<https://www.bis.org/publ/othp62.pdf>

## ► Project Nexus

# Enabling instant cross-border payments

Conclusions from a technical proof of concept between the Eurosystem, Malaysia and Singapore

March 2023



**Banking Computer Services Private Limited**  
A Subsidiary of NETS

*Number 21***Cybersecurity Best Practices for Smart Cities**

This guidance is the result of a collaborative effort from the United States Cybersecurity and Infrastructure Security Agency (CISA), the United States National Security Agency (NSA), the United States Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ).

These cybersecurity authorities—herein referred to as “authoring organizations”—are aware that communities may seek cost-savings and quality-of-life improvements through the digital transformation of infrastructure to create “smart cities.”

In this context, the term “smart cities” refers to communities that:

- Integrate information and communications technologies (ICT), community-wide data, and intelligent solutions to digitally transform infrastructure and optimize governance in response to citizens’ needs.
- Connect the operational technology (OT) managing physical infrastructure with networks and applications that collect and analyze data using ICT components—such as internet of things (IoT) devices, cloud computing, artificial intelligence (AI), and 5G.

Note: Terms that also refer to communities with this type of integration include “connected places,” “connected communities,” and “smart places.”

The communities adopting smart city technologies in their infrastructure vary in size and include university campuses, military installations, towns, and cities.

Integrating public services into a connected environment can increase the efficiency and resilience of the infrastructure that supports day-to-day life in our communities. However, communities considering becoming smart cities should thoroughly assess and mitigate the cybersecurity risk that comes with this integration.

Smart cities are attractive targets for malicious cyber actors because of:

- The data being collected, transmitted, stored, and processed, which can include significant amounts of sensitive information from governments, businesses, and private citizens.
- The complex artificial intelligence-powered software systems, which may have vulnerabilities, that smart cities sometimes use to integrate this data.

The intrinsic value of the large data sets and potential vulnerabilities in digital systems means there is a risk of exploitation for espionage and for financial or political gain by malicious threat actors, including nation-states, cybercriminals, hacktivists, insider threats, and terrorists.

No technology solution is completely secure. As communities implement smart city technologies, this guidance provides recommendations to balance efficiency and innovation with cybersecurity, privacy protections, and national security.

Organizations should implement these best practices in alignment with their specific cybersecurity requirements to ensure the safe and secure operation of infrastructure systems, protection of citizens' private data, and security of sensitive government and business data.

### *Risk to Smart Cities*

Smart cities may create safer, more efficient, more resilient communities through technological innovation and data-driven decision-making; however, this opportunity also introduces potential vulnerabilities that, if exploited, could impact national security, economic security, public health and safety, and critical infrastructure operations.

Cyber threat activity against OT systems is increasing globally, and the interconnection between OT systems and smart city infrastructure increases the attack surface and heightens the potential consequences of compromise.

Smart cities are an attractive target for criminals and cyber threat actors to exploit vulnerable systems to steal critical infrastructure data and proprietary information, conduct ransomware operations, or launch destructive cyberattacks.

Successful cyberattacks against smart cities could lead to disruption of infrastructure services, significant financial losses, exposure of citizens' private data, erosion of citizens' trust in the smart systems themselves, and physical impacts to infrastructure that could cause physical harm or loss of life.

Communities implementing smart city technologies should account for these associated risks as part of their overall risk management approach.

To read more: [https://media.defense.gov/2023/Apr/19/2003203386/-1/-1/0/CYBERSECURITY-BEST-PRACTICES-FOR-SMART-CITIES\\_508C.PDF](https://media.defense.gov/2023/Apr/19/2003203386/-1/-1/0/CYBERSECURITY-BEST-PRACTICES-FOR-SMART-CITIES_508C.PDF)

TLP:CLEAR



*Number 22***Puzzle – Is the answer of ChatGPT right or wrong?**

You can investigate it! Is the answer right or wrong?

**GE** What can we find about Robert Lipka in the Mitrokhin Archive?

Robert Lipka was a former U.S. intelligence officer who was arrested in 1994 for spying for the Soviet Union/Russia. He was convicted and sentenced to 18 years in prison.

The Mitrokhin Archive is a collection of documents that were smuggled out of the Soviet Union by KGB defector Vasili Mitrokhin. The archive contains a wealth of information about Soviet intelligence operations, including the names of KGB agents and their operations around the world.

While it is possible that information about Lipka could be found in the Mitrokhin Archive, there is no public record of any specific information about Lipka being included in the archive. It is worth noting that the archive has not been fully released to the public, and some of the information it contains is still classified. Therefore, it is possible that there is information about Lipka in the archive that has not yet been made public.

*You can investigate it! Is the answer right or wrong?*

What about the following?

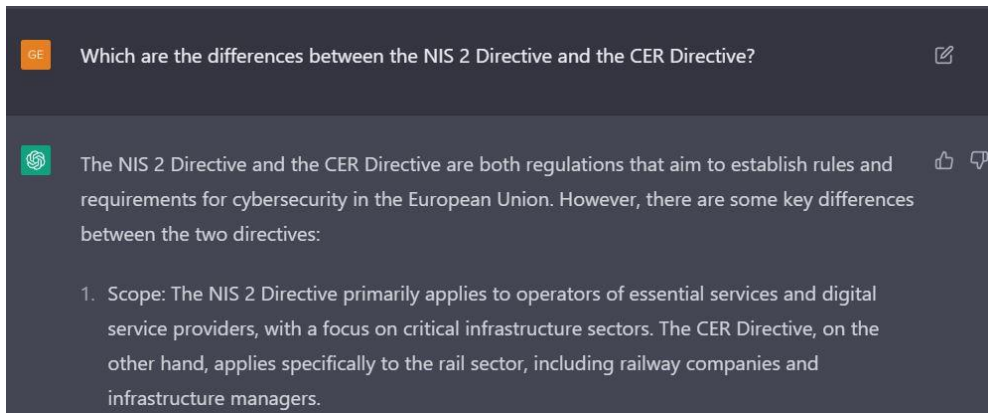
**GE** Which are the differences between the NIS 2 Directive and the DORA Directive?


The NIS 2 Directive and the DORA Directive are both regulations that aim to establish rules and requirements for the security of network and information systems. However, there are some key differences between the two directives:


1. Scope: The NIS 2 Directive primarily applies to operators of essential services and digital service providers, with a focus on critical infrastructure sectors. The DORA Directive, on the other hand, applies more broadly to all types of organizations that use digital tools and technologies, regardless of their sector or industry.

**Spoiler alert: This is so wrong...**

What about the following?

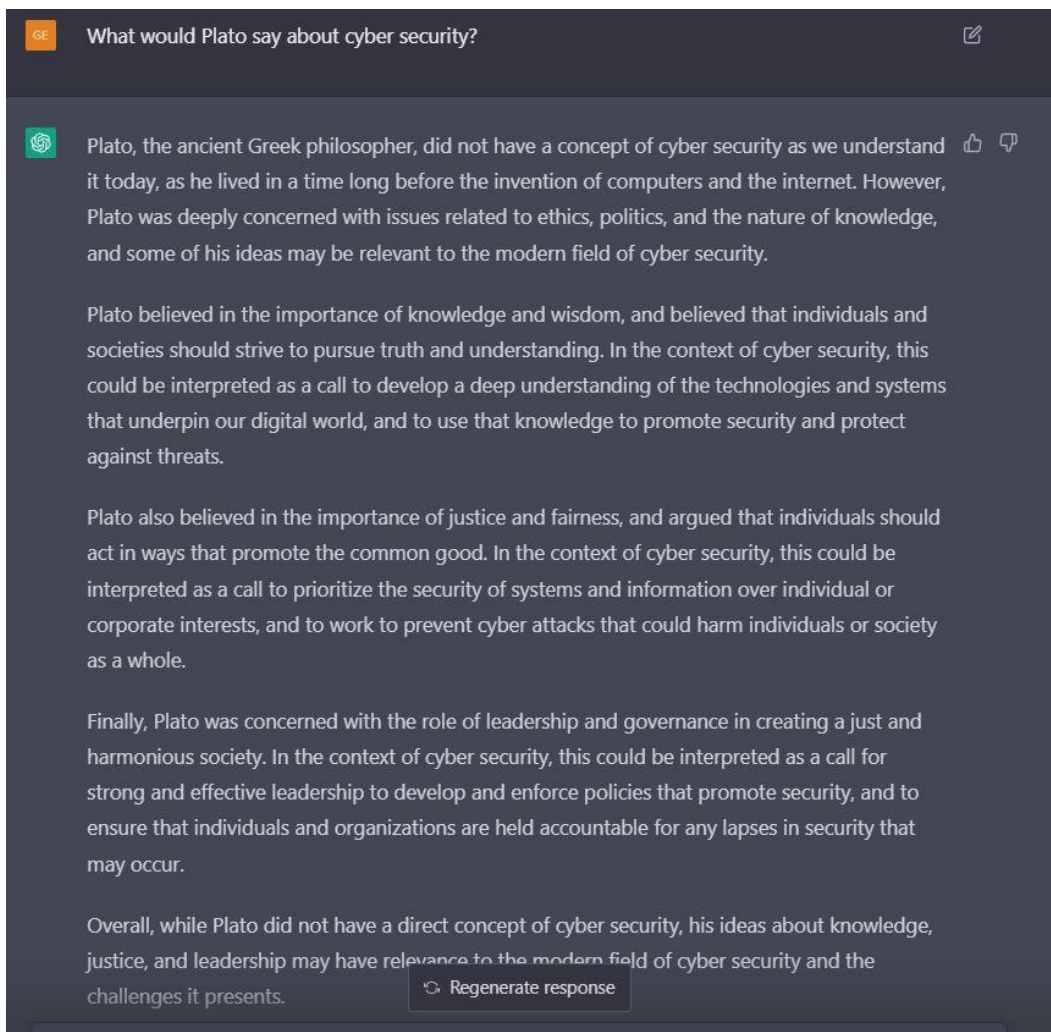



GE Which are the differences between the NIS 2 Directive and the CER Directive? 


 The NIS 2 Directive and the CER Directive are both regulations that aim to establish rules and requirements for cybersecurity in the European Union. However, there are some key differences between the two directives:

1. Scope: The NIS 2 Directive primarily applies to operators of essential services and digital service providers, with a focus on critical infrastructure sectors. The CER Directive, on the other hand, applies specifically to the rail sector, including railway companies and infrastructure managers.

Spoiler alert: This is **wrong** too. But the following is great!



GE What would Plato say about cyber security? 


 Plato, the ancient Greek philosopher, did not have a concept of cyber security as we understand it today, as he lived in a time long before the invention of computers and the internet. However, Plato was deeply concerned with issues related to ethics, politics, and the nature of knowledge, and some of his ideas may be relevant to the modern field of cyber security.

Plato believed in the importance of knowledge and wisdom, and believed that individuals and societies should strive to pursue truth and understanding. In the context of cyber security, this could be interpreted as a call to develop a deep understanding of the technologies and systems that underpin our digital world, and to use that knowledge to promote security and protect against threats.

Plato also believed in the importance of justice and fairness, and argued that individuals should act in ways that promote the common good. In the context of cyber security, this could be interpreted as a call to prioritize the security of systems and information over individual or corporate interests, and to work to prevent cyber attacks that could harm individuals or society as a whole.

Finally, Plato was concerned with the role of leadership and governance in creating a just and harmonious society. In the context of cyber security, this could be interpreted as a call for strong and effective leadership to develop and enforce policies that promote security, and to ensure that individuals and organizations are held accountable for any lapses in security that may occur.

Overall, while Plato did not have a direct concept of cyber security, his ideas about knowledge, justice, and leadership may have relevance to the modern field of cyber security and the challenges it presents.

 Regenerate response

## Cyber Risk GmbH

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



### Online Training

Recorded on-demand training and live webinars.

[More »](#)



### In-house Training

Engaging training classes and workshops.

[More »](#)



### Social Engineering

Developing the human perimeter to deal with cyber threats.

[More »](#)



### For the Board

Short and comprehensive briefings for the board of directors.

[More »](#)



### Assessments

Open source intelligence (OSINT) reports and recommendations.

[More »](#)



### High Value Targets

They have the most skilled adversaries. We can help.

[More »](#)

## Cyber security training

### Overview

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

Our training programs have the objective to help managers and employees not only understand the cyber security threats, but also their responsibility towards protecting the assets they handle. We explain how to proactively

apply good cyber security practices, how to identify threats and attacks, and what to do to protect themselves and their organizations. Cyber security is a shared responsibility.

## **Duration**

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

## **Our Education Method**

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

## **Our Instructors**

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

## **Our websites include:**

### **a. Sectors and Industries.**

1. Cyber Risk GmbH - <https://www.cyber-risk-gmbh.com>
2. Social Engineering Training - <https://www.social-engineering-training.ch>
3. Healthcare Cybersecurity - <https://www.healthcare-cybersecurity.ch>
4. Airline Cybersecurity - <https://www.airline-cybersecurity.ch>
5. Railway Cybersecurity - <https://www.railway-cybersecurity.com>
6. Maritime Cybersecurity - <https://www.maritime-cybersecurity.com>
7. Transport Cybersecurity - <https://www.transport-cybersecurity.com>



8. Transport Cybersecurity Toolkit - <https://www.transport-cybersecurity-toolkit.com>
9. Hotel Cybersecurity - <https://www.hotel-cybersecurity.ch>
10. Sanctions Risk - <https://www.sanctions-risk.com>
11. Travel Security - <https://www.travel-security.ch>

## **b. Understanding Cybersecurity.**

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

## **c. Understanding Cybersecurity in the European Union.**

1. The NIS 2 Directive - <https://www.nis-2-directive.com>
2. The European Cyber Resilience Act - <https://www.european-cyber-resilience-act.com>
3. The Digital Operational Resilience Act (DORA) - <https://www.digital-operational-resilience-act.com>
4. The Critical Entities Resilience Directive (CER) - <https://www.critical-entities-resilience-directive.com>
5. The Digital Services Act (DSA) - <https://www.eu-digital-services-act.com>
6. The Digital Markets Act (DMA) - <https://www.eu-digital-markets-act.com>

7. The European Health Data Space (EHDS) - <https://www.european-health-data-space.com>
8. The European Chips Act - <https://www.european-chips-act.com>
9. The European Data Act - <https://www.eu-data-act.com>
10. European Data Governance Act (DGA) - <https://www.european-data-governance-act.com>
11. The Artificial Intelligence Act - <https://www.artificial-intelligence-act.com>
12. The European ePrivacy Regulation - <https://www.european-eprivacy-regulation.com>
13. The European Cyber Defence Policy - <https://www.european-cyber-defence-policy.com>
14. The Strategic Compass of the European Union - <https://www.strategic-compass-european-union.com>
15. The EU Cyber Diplomacy Toolbox - <https://www.cyber-diplomacy-toolbox.com>

You may contact:

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

## Disclaimer

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

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

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

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

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of interpretative;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

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

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

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

General Terms and Conditions for all visitors to the Cyber Risk GmbH websites, and all legal transactions made through the Cyber Risk GmbH websites (hereinafter “GTC”):

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