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

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

Dear readers,

Niccolo Machiavelli believed that "there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things".

Niccolo Machiavelli is the proper person to introduce the legal issues and uncertainties related to retail Central Bank Digital Currencies (CBDC). According to the new paper with title *"Central bank digital currencies: ongoing policy perspectives"* from the Bank of Canada, the Swiss National Bank, the European Central Bank, the Bank of England, the Bank of Japan, the Board of Governors Federal Reserve System, the Sveriges Riskbank, and the Bank for International Settlements:

"The legal issues related to a retail CBDC span many different branches of a country's national law. Some of these issues also arise with traditional forms of money, although the solutions may differ. Legal issues include:

(i) the legal classification of a retail CBDC;

(ii) the authority of the central bank to issue one;

(iii) the concepts of settlement and payment finality in a retail CBDC system;

(iv) data governance, privacy and anonymity in a retail CBDC system;

(v) the potential imposition of restrictions on holdings;

(vi) non-resident access to a retail CBDC; and

(vii) the potential liabilities of participants in a retail CBDC system.

Regulatory issues such as competition and AML/CFT also need to be addressed."

Read more at number 10 below.

The European Union and the United States have held the fourth ministerial meeting of the EU-US Trade and Technology Council (TTC) in Sweden, and we have some major developments.

We read that the EU and US are deeply concerned about the *strategic use of disinformation narratives,* and *foreign information manipulation and interference (FIMI)* actions in third countries. They have issued a joint statement setting out actions to combat foreign information manipulation and interference in third countries, including a standard for structured threat intelligence and capacity building.

The EU and US have adopted a common standard for exchanging structured threat information on foreign information manipulation and interference (FIMI), through a more interoperable and machine-readable approach.

When fully operational, information will be shared more efficiently, effectively and with a greater level of detail when it comes to *understanding the manipulative tactics, techniques and procedures*.

The European Union and the United States *call upon online platforms* to ensure the integrity of their services and to effectively respond to disinformation and FIMI, building on the example of the EU's Code of Practice on Disinformation.

In particular, such responses should be targeted to the local or regional context, be grounded on research of local information environments and values, include adequate cultural and language capabilities, *ensure timely and effective responses* to requests from fact checkers, academic institutions, and media outlets, step-up efforts during critical periods, including elections and public emergencies, integrate the work of fact-checkers in their services, compensate factcheckers for their work, and provide increased transparency and accountability around their actions to counter disinformation and FIMI.

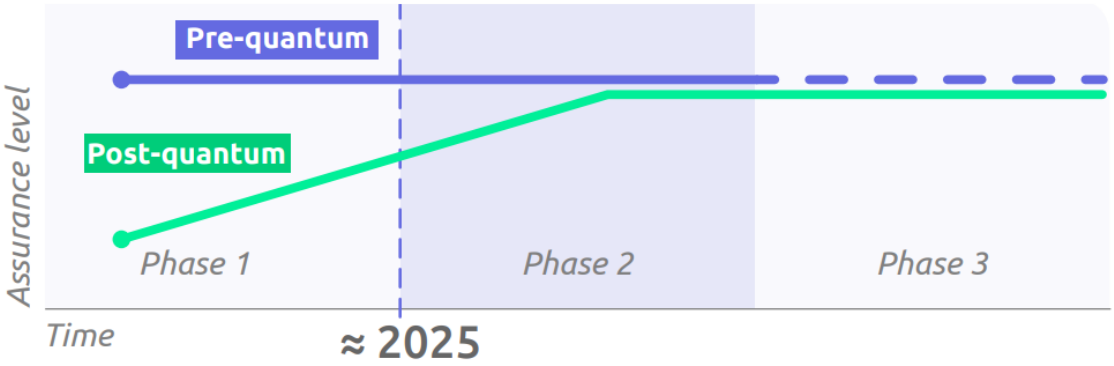
This is an interesting development. The word disinformation, believe it or not, is derived from the Russian word dezinformácija. The adjective dezinformaciónnyj can be found in Soviet military science journals published during the 1930's.

Read more at number 1 below.

"Project Leap", launched by the BIS Innovation Hub's Eurosystem Centre together with the Bank of France and Deutsche Bundesbank, prepares central banks and the global financial system for a *transition towards quantum-resistant encryption*.

We read: "Today, a significant number of information systems suffer from a lack of cryptographic agility because these systems are not designed with their easy replacement in mind. Shifting to new protocols would require in-depth infrastructure modifications.

Hence, post-quantum algorithms need to be tested in current hybrid systems that integrate adapted cryptographic solutions."



"In Project Leap, the open-source solution strongSwan was selected as it offers the required flexibility. Implementing post-quantum cryptography in a hybrid mode allows new algorithms to be implemented alongside traditional ones, with the flexibility required to drop any specific algorithm that is no longer recommended by national cyber security authorities."

I like the name of the project: Project Leap. I remember what Neil Armstrong had said: “That's one small step for a man, one giant leap for mankind”.

Read more at number 3 below.

The Digital Operational Resilience Act of the EU (DORA) solves an important problem in the EU financial regulation.

Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience.

After DORA, they must follow strict rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring. The Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, *even if there is "adequate" capital* for the traditional risk categories.

What is new? In light of the two delegated acts envisaged in DORA, the European Commission has requested technical advice to *further specify the criteria* for critical ICT third-party service providers (CTPPs) and determine the fees levied on such providers. The European Supervisory Authorities (ESAs) must deliver their technical advice by 30 September 2023.

The new “Joint European Supervisory Authority Discussion paper on DORA” asks market participants, in an open and transparent manner, on the ESAs’ proposals. We read:

“Relying on third-party services, including outsourcing, is not a new phenomenon in the financial sector. Financial entities have always cooperated with other financial and nonfinancial companies. This has been subject to EU regulatory requirements and supervision for a long time for most of the entities in scope of the DORA, including through effective governance and risk management requirements and outsourcing provisions.

However, technological developments and digitalisation are increasing the extent and ways by which financial entities rely on third parties within the value chain. Indeed, financial entities are increasingly relying on technology and data services provided by third parties for their digital

transformation—a trend that has accelerated in response to the COVID-19 pandemic.

The ESAs also observe growing interactions between incumbent financial entities and technology firms/ICT providers through a variety of co-operation models, e.g., partnerships, joint ventures, outsourcing and sub-outsourcing, or mergers and acquisitions.

These developments are creating new opportunities for consumers and businesses. Outsourcing to technology firms allows financial entities to focus on their core services, which brings flexibility and efficiency gains. Yet, these developments also bring new risks and regulatory / supervisory challenges.

The growing reliance of financial entities on tech companies may create risks to financial stability, e.g., if the same small number of companies are being used by many firms across the financial sector and in particular if ICT services provided by these companies support critical or important functions.

As already noted, amongst others, in the BCBS Principles of Operational Resilience, until recently, some of the most predominant operational risks resulted from vulnerabilities related to the rapid adoption of and increased dependency on technology infrastructure for the provision of financial services and intermediation, as well as the sector's growing reliance on technology-based services provided by third-parties."

Dear European Supervisory Authorities, good luck, we hope you will receive good advice. Be careful, Sophocles believed that "no enemy is worse than bad advice". You have the skills and the authority to make good decisions in this sensitive field, during a war in Europe.

We have some interesting developments in Switzerland. According to the Swiss National Cyber Security Centre (NCSC), an interesting combination of a phishing text message and subsequent voice phishing was reported to the NCSC.

After entering his credit card details on a website opened via a phishing text message, effective security measures enabled the victim to stop his payment to the phishers. When the phishers noticed this, they called the victim and offered telephone support.

The reported smishing attempt began in the typical manner with a text message supposedly from Netflix. It contained a link and stated that the last payment had been rejected and that the account needed to be

reactivated via a link.

The victim subsequently clicked on the link, which took him to a fake form page asking for various details. In addition to the email address, name, telephone number and Netflix password, the victim also provided his credit card number, expiry date and three-digit CVV code.

The fraudsters then initiated a payment using the data entered by the victim. Fortunately, in this case, 3D Secure was activated as an additional security layer for the credit card and the fraudulent payment needed to be confirmed by the victim. It was at this point that the fraud was detected and the payment was not authorised. Up to then, the approach was that of a typical phishing attempt and the security measures were effective.

The attackers persisted – smishing gave way to vishing

Naturally, the attackers discovered that the payment had been blocked. In order to get hold of the money after all, they called the victim shortly afterwards using a Swiss mobile phone number and posed as a Netflix employee.

During the conversation, the attacker promised to help unblock the supposedly blocked account and to make the credit card payment together with the victim. As the victim had noticed the attempted fraud, he turned down this help. The caller then insisted one last time that the victim should take some time to think about it. The victim then ended the phone call.

The NCSC Is currently receiving frequent reports of attempted voice phishing (vishing). The callers pose as employees of credit card institutions and banks. They claim that they want to clarify an incorrect booking or that e-banking is being updated. Internet telephony is usually used for such calls and the numbers are spoofed or concealed.

NCSC Recommendations:

- Be careful if you receive text messages or phone calls asking you to click on links or disclose information, even if the number displayed is apparently known.

- If you have any doubts, end the communication and contact the company using the usual channels.

- Never divulge personal data such as passwords or credit card details on a website that you accessed by clicking on a link in an email or text message.

- Install two-factor authentication whenever possible. This offers an additional layer of protection to prevent your account from being hacked.

- No bank or credit card company will ever ask you via email or on the phone to change your password or verify your credit card details.

- As soon as you realise that you have entered your password on a phishing site, change this password for all services where you use it.

- If you provided credit card details, contact your credit card company immediately to have the card blocked.

- In the case of an email password, you should also reset all passwords for web service providers that are linked to this account.

Welcome to our monthly newsletter.

Best regards,

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

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

Number 1 (Page 12)

EU-US Trade and Technology Council enhances cooperation in emerging technologies, sustainable trade and economic security

European Commission

Number 2 (Page 18)

DCSA Continuous Vetting Identifies Security Relevant Issues Early Enough to Mitigate Insider Threat Concerns

Beth Alber, Office of Communications and Congressional Affairs

Number 3 (Page 20)

Project Leap: Quantum-proofing the financial system

BIS Innovation Hub

BANQUE DE FRANCE EUROSYSTÈME

DEUTSCHE BUNDESBANK EUROSYSTEM

Number 4 (Page 23)

I-Familia: Identifying missing persons globally through family DNA matching

INTERPOL

Number 5 (Page 25)

2022 annual report on the implementation of the Federal Act on Private Security Services provided Abroad

(1 January – 31 December 2022)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

State Secretariat
International Security Division

Number 6 (Page 27)

Non-fungible tokens: what matters is the content

BaFin Federal Financial Supervisory Authority

Number 7 (Page 30)

Virtual Manipulation Brief 2023/1: Generative AI and its Implications for Social Media Analysis

By: Rolf Fredheim

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Number 8 (Page 32)

Intelligence Advanced Research Projects Activity (IARPA)

IARPA Kicks Off New Research Program to Detect Changes in Movement Patterns

Number 9 (Page 34)

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

Microsoft

Number 10 (Page 37)

Central bank digital currencies: ongoing policy perspectives

Bank of Canada	Swiss National Bank
European Central Bank	Bank of England
Bank of Japan	Board of Governors Federal Reserve System
Sveriges Riskbank	Bank for International Settlements

Number 11 (Page 39)

SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao

U.S. SECURITIES AND EXCHANGE COMMISSION

Number 12 (Page 42)

IOSCO Sets the Standard for Global Crypto Regulation

OICV-IOSCO
International Organization of Securities Commissions

Number 13 (Page 45)

Informing and Inspiring the Next Generation of Cyber Talent Through Competition

Antonio "T" Scurlock, Deputy Chief Learning Officer

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Number 14 (Page 47)

Understanding Strategic Communications

Number 15 (Page 49)

European Banking Authority (EBA), Consultation Paper on amendments to the Guidelines on money laundering and terrorist financing to include crypto-asset service providers

EBA EUROPEAN BANKING AUTHORITY

Number 16 (Page 51)

GIGABYTE Fortifies System Security with Latest BIOS Updates and Enhanced Verification

GIGABYTE™

Number 17 (Page 52)

Swiss–US dialogue continues on cybersecurity and digital technology

The Federal Council

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Number 18 (Page 54)

COSMICENERGY operational technology (OT) / industrial control system (ICS)-oriented malware, to Sabotage Power Grids

MANDIANT
NOW PART OF Google Cloud

Number 19 (Page 55)

NPSA Changes to Insider Risk Definitions

National Protective Security Authority

Number 20 (Page 58)

Blue Campaign Toolkits for the Hospitality Industry

Homeland Security

Number 21 (Page 61)

Financial Scams and How to Avoid Them

MFSA MALTA FINANCIAL SERVICES AUTHORITY

Number 1

EU-US Trade and Technology Council enhances cooperation in emerging technologies, sustainable trade and economic security

The European Union and the United States have held the fourth ministerial meeting of the EU-US Trade and Technology Council (TTC) in Luleå, Sweden.

It was co-chaired by European Commission Executive Vice-President Margrethe Vestager, European Commission Executive Vice-President Valdis Dombrovskis, United States Secretary of State Antony Blinken, United States Secretary of Commerce Gina Raimondo, and United States Trade Representative Katherine Tai, joined by European Commissioner Thierry Breton, and hosted by the Swedish Presidency of the Council of the European Union.

The EU and the US remain key geopolitical and trading partners. The EU-US bilateral trade is at historical highs, with over €1.55 trillion in 2022, including over €100 billion of digital trade.

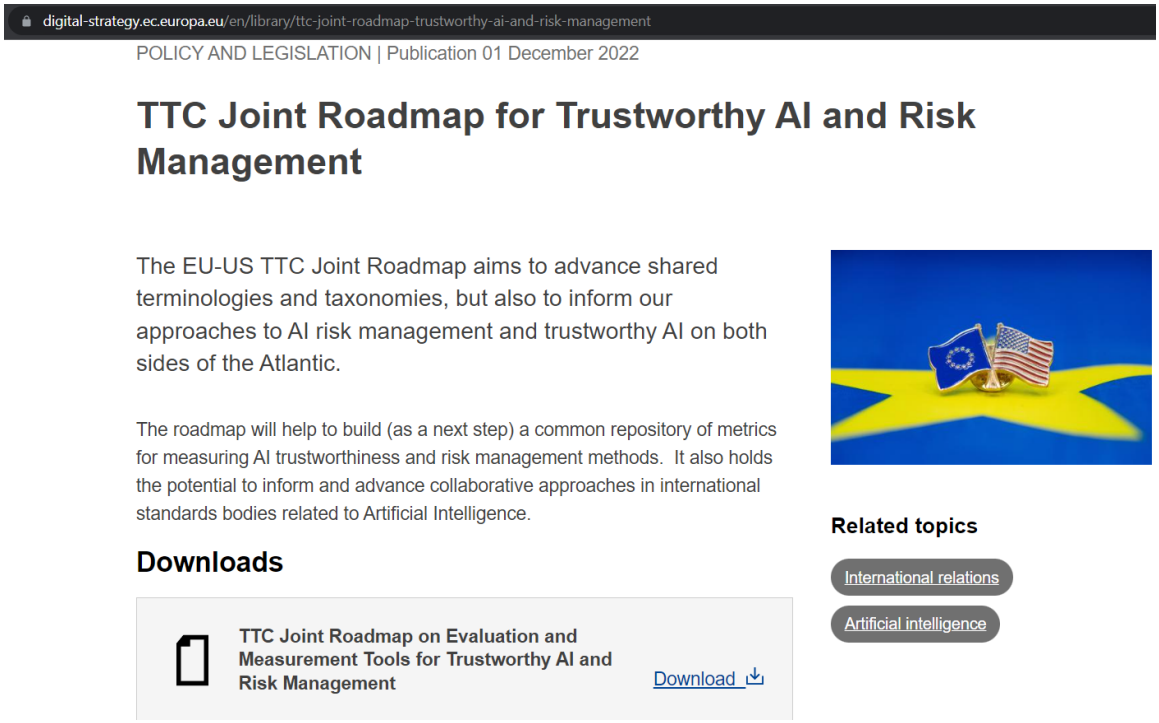
On the occasion of the ministerial meeting, the EU and the US agreed on a list of key outcomes to advance transatlantic cooperation on emerging technologies, sustainable trade, economic security and prosperity, secure connectivity and human rights in the digital environment. Both parties also reaffirmed their unwavering commitment to support Ukraine.

Key outcomes of the 4th TTC ministerial meeting

Transatlantic cooperation on emerging technologies, connectivity and digital infrastructure

The EU and the US share the common understanding that Artificial Intelligence (AI) technologies hold great opportunities but can also present risks for our societies.
They showcased the first results in the implementation of the TTC Joint Roadmap for Trustworthy AI and risk management through dedicated experts' groups, working notably on the identification of standards and tools for trustworthy AI. Going forward, this work will include a focus on generative AI systems.

You may visit: https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management



The EU and the US have advanced work on semiconductors, implementing agreements on supply chain early warning and subsidies transparency.

They have put in place a mechanism to prevent subsidy races, deepened cooperation on their respective Chips Acts and will join forces in research to replace PFAS in semiconductor supply chains.

The EU and the US are advancing their work in the area of e-mobility.

They agreed on a common international standard on megawatt charging systems for the recharging of electric heavy-duty vehicles.

This will facilitate transatlantic trade and investment by reducing the manufacturing and deployment costs.

They also developed recommendations for the government-funded implementation of e-vehicle charging infrastructure.

The recommendations: https://joint-research-centre.ec.europa.eu/system/files/2023-05/Transatlantic_Technical_Recommendations_for_Government_Funded_Implementation_of_Electric_Vehicle_Charging_Infrastructure_0.pdf

May 2023

Transatlantic Technical Recommendations for Government Funded Implementation of Electric Vehicle Charging Infrastructure

EU-U.S. Trade and Technology Council

Working Group 2 - Climate and Clean Tech

Workstream: **Electro-mobility and Interoperability with Smart Grids**
Co-Chairs: Maria Cristina Russo, European Commission, and Julie Cerqueira, U.S. Department of Energy

Authors: **Keith Hardy,** U.S. Department of Energy, Argonne National Laboratory
Harald Scholz, European Commission, Joint Research Centre

Both parties have accelerated their cooperation towards a common vision and industry roadmap on 6G wireless communication systems and issued a 6G outlook, which sets out guiding principles and next steps to develop this critical technology.

The EU and US are continuing their efforts to accelerate the roll-out of secure and resilient connectivity projects in third countries and announced today new initiatives in Costa Rica and the Philippines.

Human rights and values in a changing geopolitical digital environment

The EU and US consider that online platforms should exercise greater responsibility in protecting and empowering minors.

Data access for researchers is key to help understand risks on online platforms and to advance understanding of the online ecosystem.

The EU and the US developed a list of high-level principles on the protection and empowerment of minors and data access for researchers, which are in line with the EU's Digital Services Act.

Both parties are also deeply concerned about Russia's strategic use of disinformation narratives, and foreign information manipulation and interference (FIMI) actions in third countries.

The EU and the US have issued a joint statement setting out actions to combat foreign information manipulation and interference in third countries, including a standard for structured threat intelligence and capacity building, particularly in Africa and Latin-America.

You may visit: https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en

TTC Ministerial

Foreign information manipulation and interference in third countries

Foreign information manipulation and interference (FIMI) and disinformation is an ever-changing security and foreign policy issue, with a fast-evolving and complex threat situation. Russia's strategic and coordinated use of such activity in the preparation and execution of its war of aggression against Ukraine has increased global attention to the ways in which aggressors manipulate the information environment, amidst global conflict. Intentional manipulation by malign actors of the information environment and public debate threatens the functioning of democracies and the well-being of societies around the world. We are increasingly faced with hostile campaigns manipulating global, regional, and local audiences by spreading chaos and confusion, aiming to undercut trust in well-established/proven facts, global partnerships and alliances, universal values and international human rights, and democratic norms and processes. We also see attempts to corrode the international, rules-based order and fora such as the UN Security Council through manipulative behaviour that undermines democratic institutions and values.

The European Union and the United States are mutually concerned about foreign information manipulation and interference and disinformation; the long-standing cooperation on this issue between us has contributed to a mutual understanding of the threat and close exchanges on effective responses which respect human rights. The Trade and Technology Council proved to be a crucial forum to add another, even more strategic layer to existing and operational cooperation. Against this background, and next to other ongoing work in various different fora, the European Union and the United States have taken a number of actions to increase transatlantic cooperation to proactively address foreign information manipulation and interference and disinformation, while upholding human rights and fundamental freedoms.

Transatlantic cooperation for easier, greener and safer trade

The EU and US are working to grow their €1.5 trillion worth of bilateral trade further by making it easier to trade and they have today taken steps to facilitate trade in key sectors.

They have extended mutual recognition for pharmaceutical goods to include veterinary medicines and updated the existing EU-US marine equipment mutual recognition rules.

Work will continue to facilitate conformity assessment in certain key sectors, such as machinery.

As part of their commitment to greener and fairer trade, the EU and US have agreed on a work programme for the Transatlantic Initiative on Sustainable Trade.

This will lead to closer cooperation on jointly advancing the green transition.

The newly-launched Clean Energy Incentives Dialogue will help ensure that EU and US incentive programs for a clean economy are mutually reinforcing.

The second principal-level session of the Trade and Labour Dialogue deepened the discussion on the eradication of forced labour from global supply chains, based on joint recommendations from social partners.

The EU and US continue their work on challenges impacting their security.

This includes aligning their respective regulations related to export restrictions on sensitive items to Russia and Belarus.

They continue to coordinate adjustments to control lists, discuss emerging technologies, and cooperate to ensure the non-proliferation of weapons of mass destruction.

The TTC reiterated the importance of robust foreign investment screening to address specific national security risks, and of coordination to diversify our supply chains, to address non-market policies and practices as well as economic coercion.

The EU and US continue to advocate for digital solutions to make trade easier and to promote the digital trade principles agreed in G7.

Background

The European Union and the United States launched the EU-US Trade and Technology Council (TTC) at their ministerial in Brussels on 15 June 2021.

The TTC serves as a forum for the EU and the US to coordinate approaches to address key trade and technology issues, and to deepen transatlantic cooperation in this realm based on shared democratic values.

The inaugural meeting of the TTC took place in Pittsburgh on 29 September 2021.

Following this meeting, 10 working groups were set up covering issues such as technology standards, artificial intelligence, semiconductors, export controls and global trade challenges.

This was followed by a second ministerial in Paris on 16 May 2022 and a third ministerial in College Park, Maryland, in December 2022.

The next meeting of the TTC is planned towards the end of the year hosted by the US.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2922

Number 2

DCSA Continuous Vetting Identifies Security Relevant Issues Early Enough to Mitigate Insider Threat Concerns

Beth Alber, Office of Communications and Congressional Affairs

In conjunction with Trusted Workforce 2.0 (TW 2.0), the Defense Counterintelligence and Security Agency is implementing Continuous Vetting (CV) to mitigate vulnerabilities in real time.

Under the CV process, trusted individuals undergo continuous review to ensure the government and public's confidence that the individual will continue to protect people, property, information, and mission.

The program is supported by automated record checks that pull data from data categories such as financial activity, criminal behavior and terrorism databases.

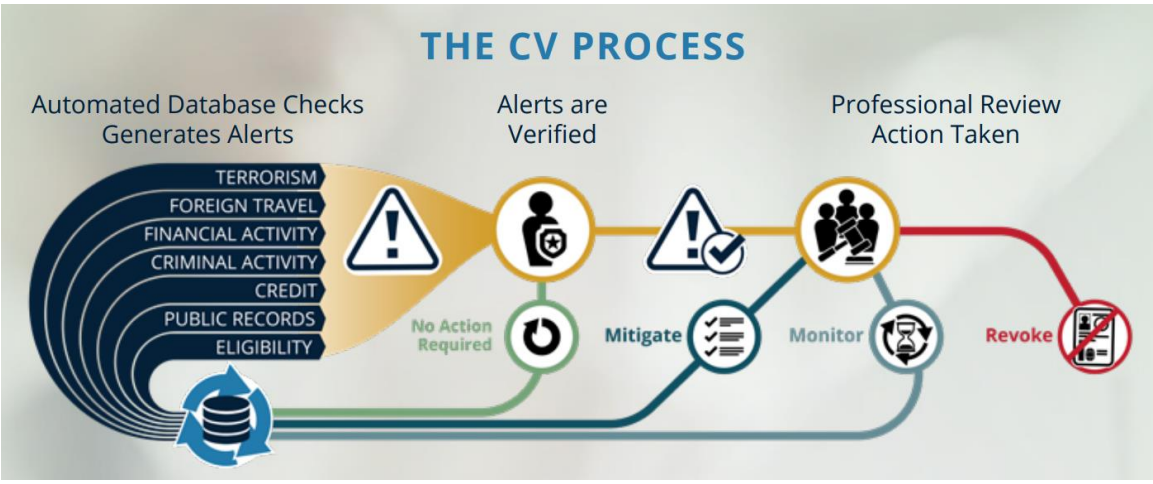
The goal of CV is to identify security relevant issues in near real-time to enable an individual the opportunity to mitigate the issue before it becomes an insider threat concern; or in situations where insider threat indicators are already present, to ensure classified information remains protected while conducting the appropriate investigation to collect the facts and make the appropriate adjudication of the issue.

When DCSA receives an alert through CV, it assesses whether the alert is valid and meets certain threshold criteria for further investigation.

DCSA investigators and adjudicators then gather facts and make clearance determinations.

CV helps DCSA mitigate personnel security situations before they become larger problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking clearances.

Under the periodic reinvestigation (PR) model, unreported issues would most likely be identified every five years in the case of Top Secret clearances and 10 years for Secret. For individuals enrolled in CV, the average to identify an issue for an individual with a Top Secret clearance is two years, seven months, and seven years, one month for a Secret clearance.



The majority of alerts received by DCSA are for financial considerations or personal conduct. For example, DCSA received an alert on an individual with a Secret clearance that was adjudicated in May 2019.

In December 2021, VRO sent a Request for Action with a Continuous Vetting Action Report to the subject's Security Management Office to notify them that the individual had accumulated more than $57,000 in delinquent debt and had recently filed a Chapter 13 bankruptcy.

The DCSA Consolidated Adjudication Services reviewed the material, determined the situation was isolated, the individual was taking positive action to address the debt, and followed up with a favorable eligibility determination.

CV led to early detection of delinquent financial information seven years, six months before the next PR under the legacy model.

To read more:
https://www.dcsa.mil/Portals/128/Documents/about/err/DCSA-Gatekeeper_v3i2_Web.pdf?ver=difbx-GJrOeege6i3Pi80Q%3d%3d

Number 3

Project Leap: Quantum-proofing the financial system

Project Leap was launched by the BIS Innovation Hub's Eurosystem Centre together with the Bank of France and Deutsche Bundesbank, the project partners within the Eurosystem, to prepare central banks and the global financial system for a transition towards quantum-resistant encryption.

Why quantum computers represent a cyber threat to financial data

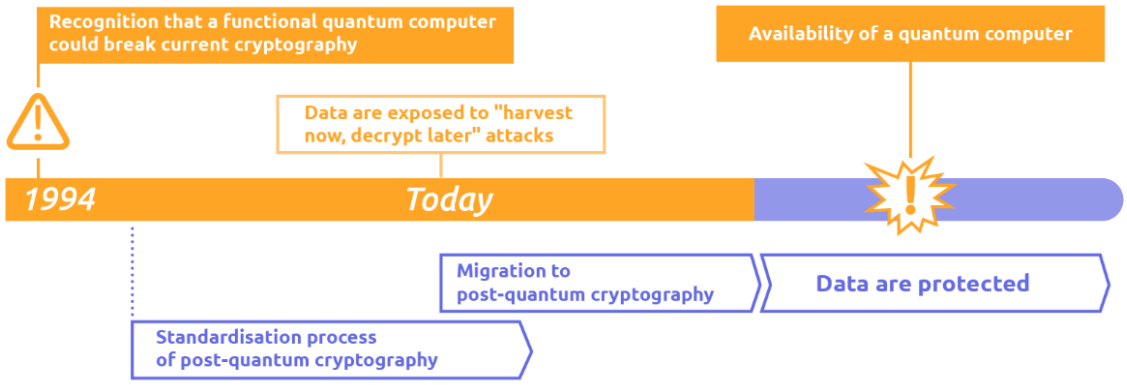
Quantum computers, should they reach sufficient size and power, may be able to break the encryption schemes widely used today to ensure secure financial transactions and data.

This makes quantum computing one of the most important cybersecurity threats facing the financial system, potentially exposing all financial transactions and much of our existing stored financial data to attack.

While it is still unclear when quantum computing technology might be adopted on a large scale, its potential as a cyber threat to the financial system is already a matter of concern.

Malicious actors can intercept and store confidential, classically encrypted data with the intention of decrypting it later when quantum computers become powerful enough to do so.

This means that data stored or transmitted today are, in fact, exposed to "harvest now, decrypt later" attacks by a future quantum computer.



Recognising these potential risks to its systems and data, the financial sector needs to pre-emptively implement robust quantum communication and data protection technologies. Given the long-term sensitivity of financial data and the complexity of central bank IT systems, a transition phase should be initiated well in advance so that quantum-resistant encryption schemes can be implemented.

Preparing for the cyber threat of quantum computers

The first phase of project Leap tested the implementation of post-quantum cryptographic protocols between two central banks with the aim of advancing the central banking community's knowledge of post-quantum cryptography.

To achieve this goal, one traditional public key algorithm was implemented alongside several quantum-resistant algorithms in a hybrid cyphering mode, with the aim of maintaining the confidentiality of messages sent across two distanced IT systems.

The quantum-resistant communication channel was first tested with payment messages transmitted between the Bank of France and the Deutsche Bundesbank. The objective was to test how existing products and processes perform using quantum-resistant technology.

To read more:
https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

https://www.bis.org/publ/othp67.pdf

Project Leap

Quantum-proofing the financial system

June 2023

Number 4

I-Familia: Identifying missing persons globally through family DNA matching

The first of its kind, I-Familia is a global database for identifying missing persons based on international DNA kinship matching.

The result of cutting-edge scientific research, the database seeks to identify missing persons or unidentified human remains when direct comparison is not possible, by using DNA samples from family members instead.

This is a complex process – even more so when carried out internationally – which is where INTERPOL can play a unique role through its global network.

I-Familia helps to reunite loved ones or to bring closure to cases and allow families to rebuild their lives.

There is growing international concern about the number of missing persons and unidentified victims around the world due to increased international travel, the prevalence of organized crime and human trafficking, the rise in global migration, conflicts and natural disasters.

Families of a missing person face continued distress from not knowing where their loved one is, often waiting years for news. Depending on the legislation in their countries, families might not be issued with a death certificate, which can have administrative and economic implications.

In cases where a missing person has died because of a criminal act, families are also denied an opportunity to seek justice.

DNA identification through direct matching

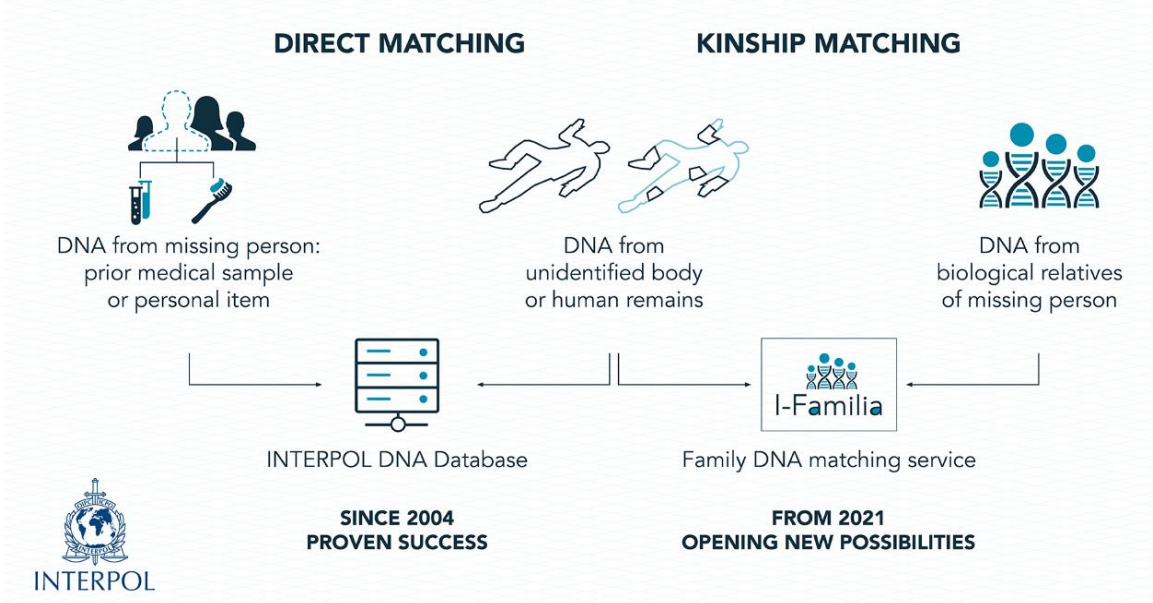
A direct DNA sample from the missing person, for example a prior medical sample or a personal item such as a toothbrush, can be compared to the DNA from an unidentified body or human remains to see if a match can be found.

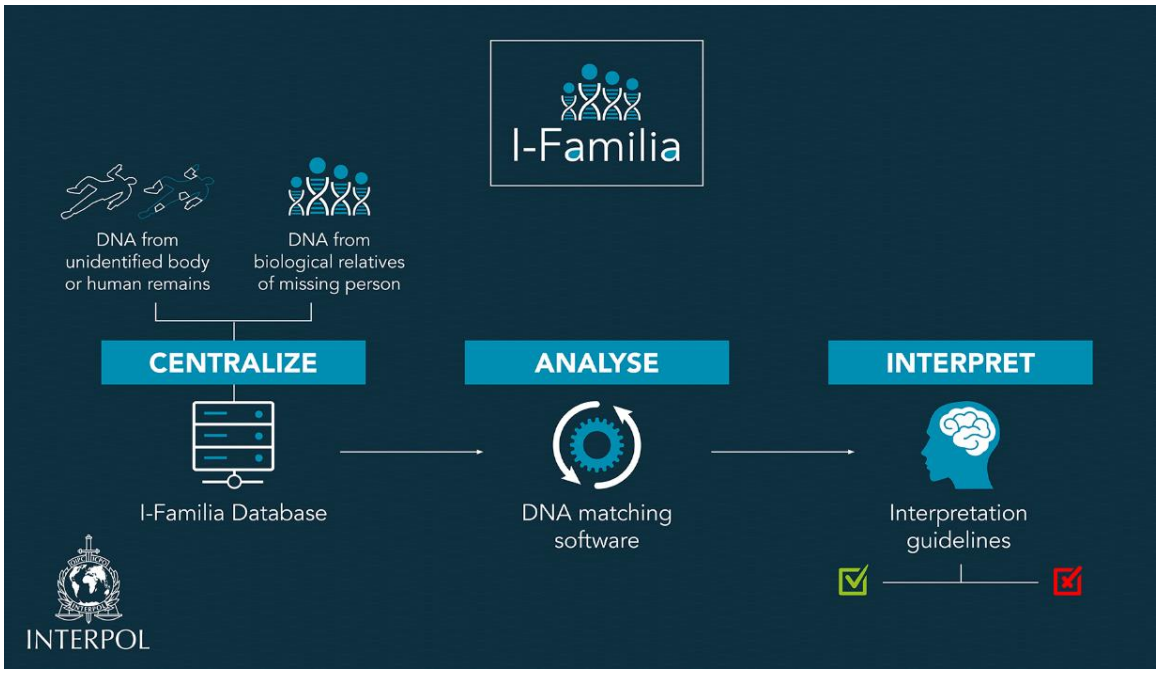
This type of identification has been carried out via the INTERPOL DNA Database since 2004.

DNA identification through kinship matching

Biological relatives share a percentage of their DNA, depending on their relationship. In the event that a DNA sample from the missing person cannot be obtained for direct matching, DNA from close family members (parents, children, siblings) can also be compared.

This is where I-Familia is set to make a difference.





To read more: https://www.interpol.int/How-we-work/Forensics/I-Familia

Number 5

2022 annual report on the implementation of the Federal Act on Private Security Services provided Abroad

(1 January – 31 December 2022)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
State Secretariat
International Security Division

Introduction

Russia's military aggression against Ukraine has brought war back to Europe. It strongly shaped Switzerland's foreign policy in 2022.

In this context, a multitude of peace and security policy issues have become more topical. The use of private military and security companies in conflicts also became a focus of public attention worldwide due to this war of aggression.

The extensive reporting on such use covered private actors' engagement in Ukraine in particular. The authority competent for implementation of the Federal Act on Private Security Services Provided Abroad (PSSA) has been monitoring these developments closely and the matter continues to be a source of concern.

Regarding the PSSA's implementation, the most important developments in 2022 were the audit conducted by the Swiss Federal Audit Office (SFAO) and, as in 2021, the effects of the revision of the Ordinance on Private Security Services provided Abroad (OPSA).

The PSSA's aim is to contribute to safeguarding the internal and external security of Switzerland, realising Switzerland’s foreign policy objectives, preserving Swiss neutrality, and guaranteeing compliance with international law (Art. 1).

To this end, it stipulates that private security services provided by Swiss companies abroad are to declare their activities and, if necessary, be subject to areview procedure.

According to Article 3 of the OPSA, the FDFA's State Secretariat is competent for implementing the PSSA. The Export Controls and Private Security Services Section (ECPS) of the International Security Division (ISD) is responsible for the operational implementation of the Act.

The ECPS' task is to conduct the administrative procedures provided for by the law, to help develop Swiss policy regarding private security services,

and to participate in the debate on rules and standards for private security service providers at national and international level.

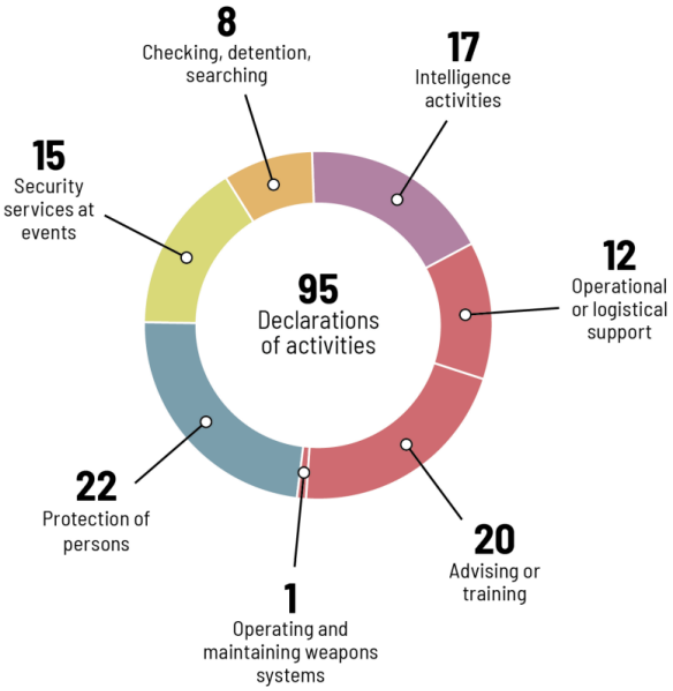
Article 37 of the PSSA stipulates that the 'competent authority', i.e. the ECPS, shall prepare a report on its activities, to be submitted to the Federal Council each year.

The report is published on the FDFA's website. Since it was reorganised in March 2020, the ECPS has also been responsible for the processing of the applications in the area of export controls that the State Secretariat for Economic Affairs (SECO) submits for consultation.

In close collaboration with the SECO, the ECPS also helps to prepare political briefs in the area of export controls and engages in national and multilateral dialogue in this regard.

Operationally, approximately 310 cases were submitted to the ECPS in 2022. These cases involved the export of goods under the War Material Act (WMA) and the Goods Control Act (GCA).

To read more:
https://www.newsd.admin.ch/newsd/message/attachments/79382.pdf



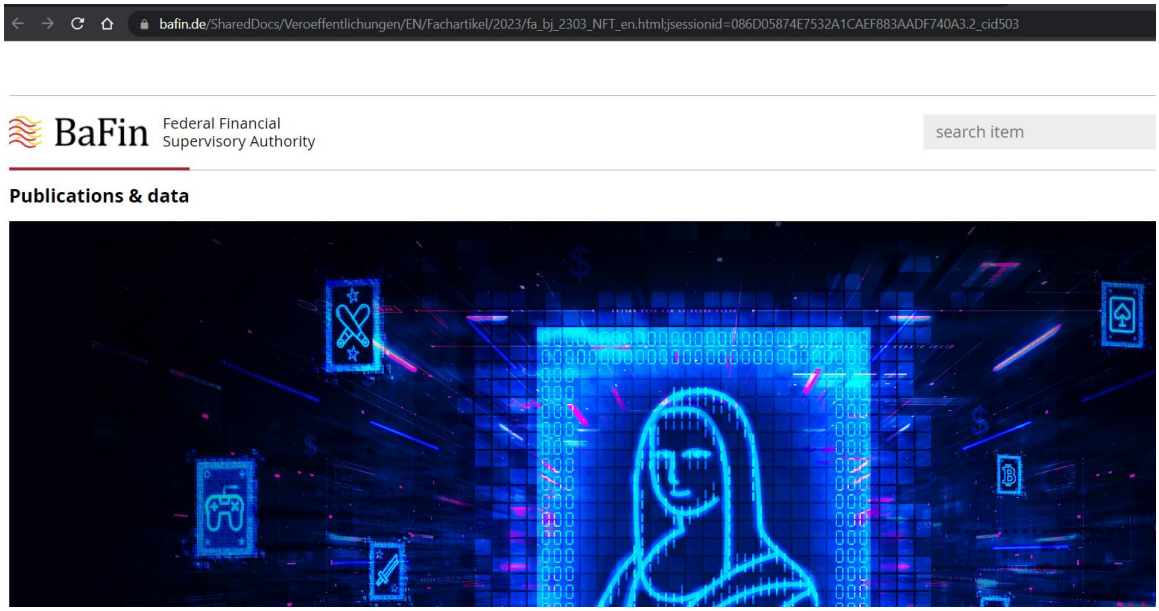
Number 6

Non-fungible tokens: what matters is the content

BaFin Federal Financial Supervisory Authority

Non-fungible tokens can be used in many different ways, also in the financial sector. This article explains how the Federal Financial Supervisory Authority (BaFin) currently categorises these tokens from a supervisory perspective.

Non-fungible tokens (NFTs) have been met with considerable interest in the last few years. After a period of tremendous growth, however, the NFT market experienced a sharp drop in demand and prices in mid-2022. Despite this downturn, there can be no doubt that NFTs continue to be highly relevant. Their technical characteristics make them eligible for many different forms of application.



NFTs are supposed to combine the special characteristics for which crypto tokens are known on the market, like good transferability and low risk of falsification, with the means of individually assigning the specific token to an address on the blockchain.

Since NFTs are also used in the financial sector, BaFin is examining the potential of this phenomenon and particularly also the risks associated with it. From the supervisors' perspective, it is important to find out what relevance NFTs have for the financial market and what the consequences will be for offerors, service providers and customers.

NFTs: unique cryptographic tokens?

NFTs are cryptographic tokens that are based on distributed ledger technology (DLT) – especially blockchains, which are a special form of DLTs. NFTs, as their name implies, are not fungible with each other due to their technical characteristics: they are non-interchangeable.

This design makes it possible to uniquely assign individually identifiable tokens to a particular address on the blockchain. With fungible tokens, on the other hand, it is not an individual token that is assigned to each address but only the respective share of all existing tokens of that kind. The best-known standard for fungible tokens is the ERC-20 standard on the Ethereum blockchain.

Both NFTs and fungible tokens can also be created on the basis of other blockchains – such as Solana, EOS or Tezos – as well as on the basis of other standards.

The criterion of uniqueness for NFTs merely conveys information about their technical characteristics – such as the individual identifier of a token (also called a token ID) – but not necessarily about the contents to which the token pertains or the rights associated with it.

For example, a smart contract can be used to create many NFTs, each of which has its own individual identifier but also all of which are assigned the same rights or contents.

Numerous fields of application

There are many different possible applications for NFTs. Probably the most prominent categories of NFTs are “collectibles” and digital art. Collectibles are collector’s items in digital form; some can also provide bonus functions enabling holders to interact with the tokens.

For artists, NFTs can make it possible, for example, to participate in any future proceeds generated when the collectibles are resold. NFTs are also put to use in the context of gaming and the metaverse, such as in the form of tokenised game objects or real estate in digital worlds.

Supervisory practice as in the case of fungible tokens

When conducting supervisory assessments of NFTs, BaFin takes the same approach that it takes for fungible tokens. Market participants can find more information in the interpretive letters BaFin has published on this subject.

Advisory letter (WA)

Ref. no.: WA 11-QB 4100-2017/0010

Supervisory classification of tokens or cryptocurrencies underlying "initial coin offerings" (ICOs) as financial instruments in the field of securities supervision

Given the rising number of queries to BaFin's Securities Supervision/Asset Management Directorate (WA) seeking to ascertain whether the tokens, coins or cryptocurrencies underlying "initial coin offerings" (ICOs)[1] (for the purposes of this advisory letter hereinafter referred to as "**tokens**") are deemed financial instruments in the field of securities supervision, BaFin states its position on the regulatory classification of tokens in the field of securities supervision as follows in this advisory letter:

BaFin (WA) determines on a case-by-case basis whether a token constitutes a financial instrument within the meaning of the German Securities Trading Act (*Wertpapierhandelsgesetz* – WpHG) or the Markets in Financial Instruments Directive (MiFID II), a security within the meaning of the German Securities Prospectus Act (*Wertpapierprospektgesetz* – WpPG), or a capital investment within the meaning of the German Capital Investment Act (*Vermögensanlagengesetz* – VermAnlG). BaFin bases its assessment on the criteria set out in the statutory provisions under securities supervision law, i.e. in particular the WpHG, WpPG, Market Abuse Regulation (MAR), VermAnlG as well as other relevant laws and applicable national and EU legal acts in the field of securities supervision.

Background information

NFT is the designation most often used on the market if, for the underlying smart contracts , an industry standard is used that assigns a unique identifier to each token. These standards serve as technical instructions for implementing and creating a token. They are designed to ensure that certain basic criteria are met, for example with regard to verification, traceability, tamper resistance and transferability.

The most prominent standards for the creation of NFTs are currently ERC-721 and ERC-1155, which – like all standards entitled "ERC" (Ethereum Request for Comments) – are based on the Ethereum blockchain.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2023/fa_bj_2303_NFT_en.html;jsessionid=086D05874E7532A1CAEF883AADF740A3.2_cid503

Number 7

Virtual Manipulation Brief 2023/1: Generative AI and its Implications for Social Media Analysis

By: Rolf Fredheim

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

This Virtual Manipulation report explores the impact of generative AI on social media analysis.

Large Language Models (LLMs), such as the powerful GPT-4, can create highly convincing content that appears legitimate and unique.

This makes it nearly impossible to distinguish between real and fake accounts. But, defenders can employ the same tools to more effectively monitor social media spaces.

Careless implementations by adversaries introduce weaknesses that can result in accounts inadvertently disclosing that they are bots.

As LLMs rely on prompts to shape their output, targeted psychological operations ('psyops') can provoke chatbots to reveal their true identities.

The fight against manipulation is entering a new phase, but it remains unclear whether, in the long run, defenders or attackers will derive greater benefit from AI systems.

At a cost of $130, we used GPT-4 to classify the content, relevance, and sentiment towards NATO for a total of 650 000 social media posts.

The single event that incited the highest level of hostile anti-NATO messaging was President Putin's speech declaring mobilisation in September 2022.

In contrast, Finland joining NATO in April 2023 passed with comparatively little online fuss.

In November 2022, and again in March- April 2023 the proportion of Tweets by hyperactive anonymous 'troll' accounts was ten times higher than in the first months of the war.

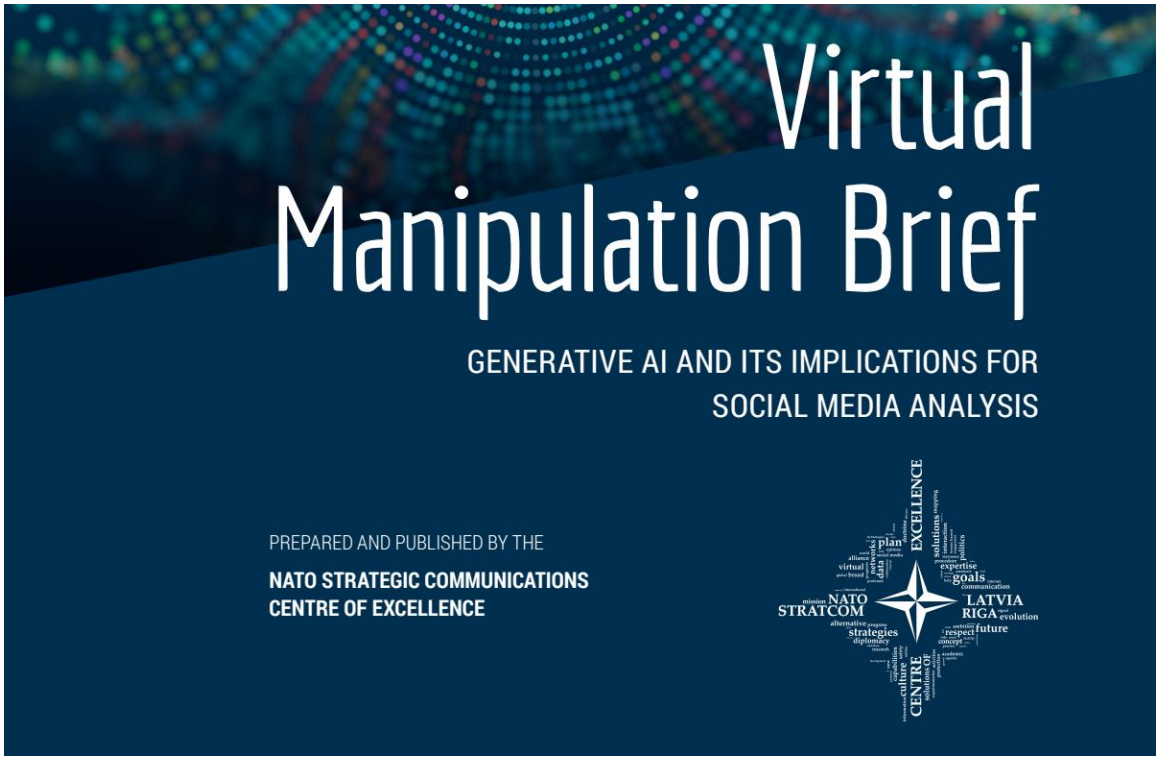
This increase may be associated with advances in generative AI, or lax content moderation under Twitter's owner, Elon Musk.

Twitter's decision to re-amplify Russian propaganda accounts at the end of March 2023 led to the Kremlin's messaging attracting 60 per cent more views.

The English language account of the Russian Ministry of Foreign Affairs saw its daily views rise from 0.44 million while de-amplified to 1.3 million per day when re-amplified.

Telegram and VKontakte have experienced consistent growth in user numbers. In March 2023, the proportion of Russians using Telegram daily exceeded that of YouTube for the first time.

More than 40 per cent of Russians use these platforms on a daily basis. Instagram and Facebook, on the other hand, are accessed by around 6 and 1.5 per cent respectively.



To read more: https://stratcomcoe.org/publications/virtual-manipulation-brief-20231-generative-ai-and-its-implications-for-social-media-analysis/287

Number 8

Intelligence Advanced Research Projects Activity (IARPA)

IARPA Kicks Off New Research Program to Detect Changes in Movement Patterns

The Intelligence Advanced Research Projects Activity (IARPA) — the advanced research and development arm of the Office of the Director of National Intelligence — recently announced the launch of a research program to develop systems capable of modeling population movement patterns around the globe and providing alerts when concerning anomalies emerge.

The Hidden Activity Signal and Trajectory Anomaly Characterization (HAYSTAC) program aims to establish "normal" movement models across times, locations, and populations and determine what makes an activity atypical.

Expansive data from the Internet of Things and Smart City infrastructures provides opportunities to build new models that understand human dynamics at unprecedented resolution and creates the responsibility to understand privacy expectations for those moving through this sensor-rich world.

"An ever-increasing amount of geospatial data is created every day," said HAYSTAC Program Manager Dr. Jack Cooper.

"With HAYSTAC, we have the opportunity to leverage machine learning and advances in artificial intelligence to understand mobility patterns with exceptional clarity. The more robustly we can model normal movements, the more sharply we can identify what is out of the ordinary and foresee a possible emergency."

Through a competitive Broad Agency Announcement, IARPA awarded HAYSTAC research contracts to the following lead organizations, which together bring 27 additional academic institutions, non-profits, and businesses into the program:

Raytheon Technologies Research Center
L3Harris Technologies, Inc.
STR

Kitware, Inc.
Leidos, Inc.
Novateur Research Solutions
Deloitte Consulting LLP
Raytheon BBN

The HAYSTAC test and evaluation team consists of Johns Hopkins Applied Physics Laboratory, MITRE, and Oak Ridge National Laboratory.

To read more: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2023/item/2381-iarpa-kicks-off-new-research-program-to-detect-changes-in-movement-patterns

Number 9

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

Microsoft has uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States.

The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering.

Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.

Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organizations in Guam and elsewhere in the United States. In this campaign, the affected organizations span the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors.

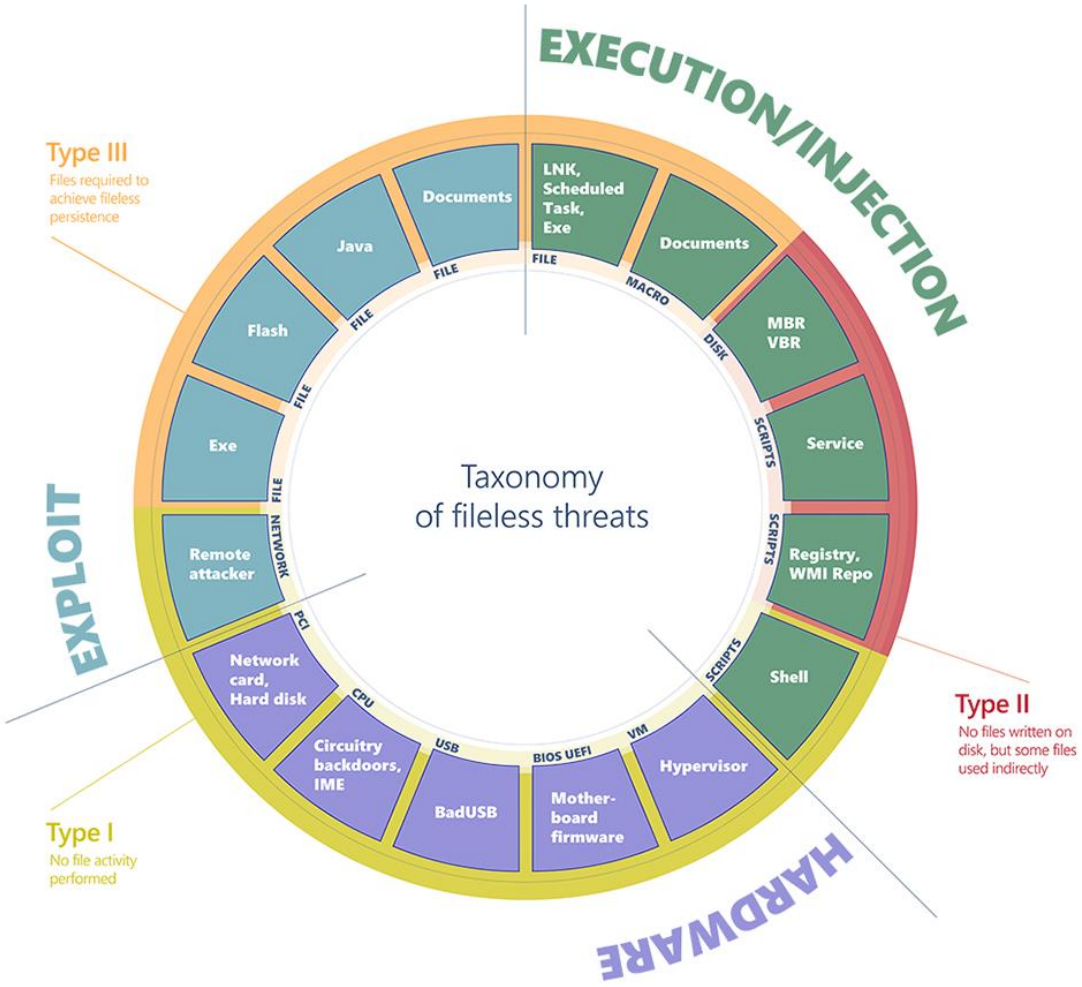
Observed behavior suggests that the threat actor intends to perform espionage and maintain access without being detected for as long as possible.

Microsoft is choosing to highlight this Volt Typhoon activity at this time because of our significant concern around the potential for further impact to our customers.

Although our visibility into these threats has given us the ability to deploy detections to our customers, the lack of visibility into other parts of the actor's activity compelled us to drive broader community awareness and further investigations and protections across the security ecosystem.

To achieve their objective, the threat actor puts strong emphasis on stealth in this campaign, relying almost exclusively on living-off-the-land techniques and hands-on-keyboard activity.

They issue commands via the command line to (1) collect data, including credentials from local and network systems, (2) put the data into an archive file to stage it for exfiltration, and then (3) use the stolen valid credentials to maintain persistence.



In addition, Volt Typhoon tries to blend into normal network activity by routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware.

They have also been observed using custom versions of open-source tools to establish a command and control (C2) channel over proxy to further stay under the radar.

In this blog post, we share information on Volt Typhoon, their campaign targeting critical infrastructure providers, and their tactics for achieving and maintaining unauthorized access to target networks. Because this activity relies on valid accounts and living-off-the-land binaries (LOLBins), detecting and mitigating this attack could be challenging.

Compromised accounts must be closed or changed. At the end of this blog post, we share more mitigation steps and best practices, as well as provide details on how Microsoft 365 Defender detects malicious and suspicious activity to protect organizations from such stealthy attacks.

The National Security Agency (NSA) has also published a Cybersecurity Advisory which contains a hunting guide for the tactics, techniques, and procedures (TTPs) discussed in this blog. You may visit: https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments. To learn about Microsoft's approach to threat actor tracking, read Microsoft shifts to a new threat actor naming taxonomy.

To read more: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Number 10

Central bank digital currencies: ongoing policy perspectives

Bank of Canada	Swiss National Bank
European Central Bank	Bank of England
Bank of Japan	Board of Governors Federal Reserve System
Sveriges Riskbank	Bank for International Settlements

A group of central banks, together with the Bank for International Settlements, are working together to explore central bank digital currencies (CBDCs) for the public ("general purpose" or "retail" CBDC).

Since publishing:

(i) a report in October 2020 setting out the common foundational principles and core features of a CBDC; and

(ii) an executive summary and three detailed reports on system design and interoperability, user needs and adoption and financial stability implications in September 2021, the group has continued to share ideas and perspectives on similar themes, which are summarised in this note.

Background/motivation

Most central banks are now exploring CBDCs, and more than a quarter of them are developing or running concrete pilots (Kosse and Mattei (2022)).

Many of our jurisdictions are examining whether there is a need to ensure ongoing retail access to central bank money at a time of profound, ongoing changes across finance, technology and society.

The motivation for introducing a retail CBDC may rest primarily on the role of central bank money as a public good.

At the same time, the introduction of a CBDC could be an innovative opportunity for the monetary system.

It is in this context that the central banks contributing to this group have continued their collaboration to deepen the practical policy and technical analysis of CBDC.

Annex 1 draws out some elements of the discussion in 2022. Some of the members of this group are approaching a point where they may decide on whether or not to move to the next stage of their CBDC work.

This may include deeper investment in design decisions relating to technology, end user preferences and business models, while leaving open the decision on whether to issue CBDC.

To date, none of our jurisdictions have yet decided to proceed with the issuance of a retail CBDC. CBDC issuance and design are sovereign decisions for relevant authorities based on their assessments and a jurisdiction's circumstances. However, there has been value in working collectively on common issues.

To read more: https://www.bis.org/publ/othp65.pdf

Number II

SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission charged Binance Holdings Ltd. ("Binance"), which operates the largest crypto asset trading platform in the world, Binance.com; U.S.-based affiliate, BAM Trading Services Inc. ("BAM Trading"), which, together with Binance, operates the crypto asset trading platform, Binance.US; and their founder, Changpeng Zhao, with a variety of securities law violations.

Case 1:23-cv-01599 Document 1 Filed 06/05/23 Page 1 of 136

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SECURITIES AND EXCHANGE COMMISSION, 100 F Street, N.E. Washington, DC 20549, **Plaintiff,** **v.** **BINANCE HOLDINGS LIMITED, BAM TRADING SERVICES INC., BAM MANAGEMENT US HOLDINGS INC., AND CHANGPENG ZHAO,** **Defendants.**	**Civil Action No. 1:23-cv-01599** **Jury Trial Demanded**

Among other things, the SEC alleges that, while Zhao and Binance publicly claimed that U.S. customers were restricted from transacting on Binance.com, Zhao and Binance in reality subverted their own controls to secretly allow high-value U.S. customers to continue trading on the Binance.com platform.

Further, the SEC alleges that, while Zhao and Binance publicly claimed that Binance.US was created as a separate, independent trading platform for U.S. investors, Zhao and Binance secretly controlled the Binance.US platform's operations behind the scenes.

The SEC also alleges that Zhao and Binance exercise control of the platforms' customers' assets, permitting them to commingle customer

assets or divert customer assets as they please, including to an entity Zhao owned and controlled called Sigma Chain.

The SEC's complaint further alleges that BAM Trading and BAM Management US Holdings, Inc. ("BAM Management") misled investors about non-existent trading controls over the Binance.US platform, while Sigma Chain engaged in manipulative trading that artificially inflated the platform's trading volume.

Further, the Complaint alleges that the defendants concealed the fact that it was commingling billions of dollars of investor assets and sending them to a third party, Merit Peak Limited, that is also owned by Zhao.

The Complaint also charges violations of critical registration-related provisions of the federal securities laws:

- Binance and BAM Trading with operating unregistered national securities exchanges, broker-dealers, and clearing agencies;

- Binance and BAM Trading with the unregistered offer and sale of Binance's own crypto assets, including a so-called exchange token, BNB, a so-called stablecoin, Binance USD (BUSD), certain crypto-lending products, and a staking-as-a-service program; and

- Zhao as a control person for Binance's and BAM Trading's operation of unregistered national securities exchanges, broker-dealers, and clearing agencies.

"Through thirteen charges, we allege that Zhao and Binance entities engaged in an extensive web of deception, conflicts of interest, lack of disclosure, and calculated evasion of the law," said SEC Chair Gary Gensler. "As alleged, Zhao and Binance misled investors about their risk controls and corrupted trading volumes while actively concealing who was operating the platform, the manipulative trading of its affiliated market maker, and even where and with whom investor funds and crypto assets were custodied. They attempted to evade U.S. securities laws by announcing sham controls that they disregarded behind the scenes so that they could keep high-value U.S. customers on their platforms. The public should beware of investing any of their hard-earned assets with or on these unlawful platforms."

"We allege that Zhao and the Binance entities not only knew the rules of the road, but they also consciously chose to evade them and put their customers and investors at risk – all in an effort to maximize their own profits," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement. "By engaging in multiple unregistered offerings and also

failing to register while at the same time combining the functions of exchanges, brokers, dealers, and clearing agencies, the Binance platforms under Zhao's control imposed outsized risks and conflicts of interest on investors. Those risks and conflicts are only heightened by the Binance platforms' lack of transparency, reliance on related-party transactions, and lies about controls to prevent manipulative trading. Despite their years-long efforts to not 'be held accountable,' today's complaint begins the process of doing so."

To read more: https://www.sec.gov/news/press-release/2023-101

https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf

Number 12

IOSCO Sets the Standard for Global Crypto Regulation

International Organization of Securities Commissions

The International Organization of Securities Commissions (IOSCO) has published this Consultation Report with the aim of finalizing IOSCO's policy recommendations to address market integrity and investor protection issues in crypto-asset markets in early-Q4 2023.

In line with IOSCO's established approach for securities regulation, the Crypto and Digital Asset Recommendations (CDA Recommendations) are addressed to relevant authorities and look to support jurisdictions seeking to establish compliant markets for the trading of crypto or 'digital' or 'virtual' assets (hereafter "crypto-assets" and read to include all relevant tokens) in the most effective way possible.

This consultation report proposes 18 policy recommendations that IOSCO plans to finalize in early Q4 this year to support greater consistency with respect to regulatory frameworks and oversight in its member jurisdictions, to address concerns related to market integrity and investor protection arising from crypto-asset activities.

The recommendations have been developed under the stewardship of the IOSCO Board's Fintech Task Force (FTF) in accordance with IOSCO's CryptoAsset Roadmap published in June 2022.

The proposed recommendations are principles-based and outcomes-focused and are aimed at the activities performed by crypto-asset service providers (CASPs).

They apply IOSCO's widely accepted global standards for securities markets regulation to address key issues and risks identified in cryptoasset markets.

The proposed recommendations are activities-based and follow a 'lifecycle' approach in addressing the key risks identified in this report.

They cover the range of activities in crypto-asset markets that involve CASPs from offering, admission to trading, ongoing trading, settlement, market surveillance and custody as well as marketing and distribution (covering advised and non-advised sales) to retail investors.

The proposed recommendations do not cover activities, products or services provided in the so-called "decentralized finance" or "DeFi" area.

Policy Recommendations for Crypto and Digital Asset Markets

Consultation Report

The FTF DeFi workstream is considering issues in relation to DeFi and will publish a consultation report with proposed recommendations later this summer.

One of IOSCO's goals is to promote greater consistency with respect to how IOSCO members approach the regulation and oversight of crypto-asset activities, given the cross-border nature of the markets, the risks of regulatory arbitrage and the significant risk of harm to which retail investors continue to be exposed.

IOSCO is also seeking to encourage optimal consistency in the way cryptoasset markets and securities markets are regulated within individual IOSCO jurisdictions, in accordance with the principle of 'same activities, same risks, same regulatory outcomes'.

The proposed recommendations also cover the need for enhanced cooperation among regulators.

They aim to provide a critical benchmark for IOSCO members to cooperate, coordinate and respond to cross-border challenges in enforcement and supervision, including regulatory arbitrage concerns, that arise from global crypto-asset activities conducted by CASPs that offer their services, often remotely, into multiple jurisdictions.

While the proposed recommendations are not directly addressed to markets participants, CASPs and all participants in crypto-asset markets are strongly encouraged to carefully consider the expectations and outcomes articulated through the proposed recommendations and the

respective supporting guidance in the conduct of registered/licensed, and cross-border activities.

Money Laundering / Fraud / Scams

As with other crypto-assets, stablecoins may appeal to money launderers and criminals who do not wish to subject the proceeds of crime to traditional financial system oversight. Stablecoins are also likely to be perceived as more stable than other crypto-assets, so are more attractive to money launderers and criminals who do not wish to be as exposed to crypto-asset market volatility.

In light of the price instability of crypto-assets, because of their relatively more stable nature scammers have turned to stablecoins, and are soliciting stablecoins from their victims.

To read more:
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf

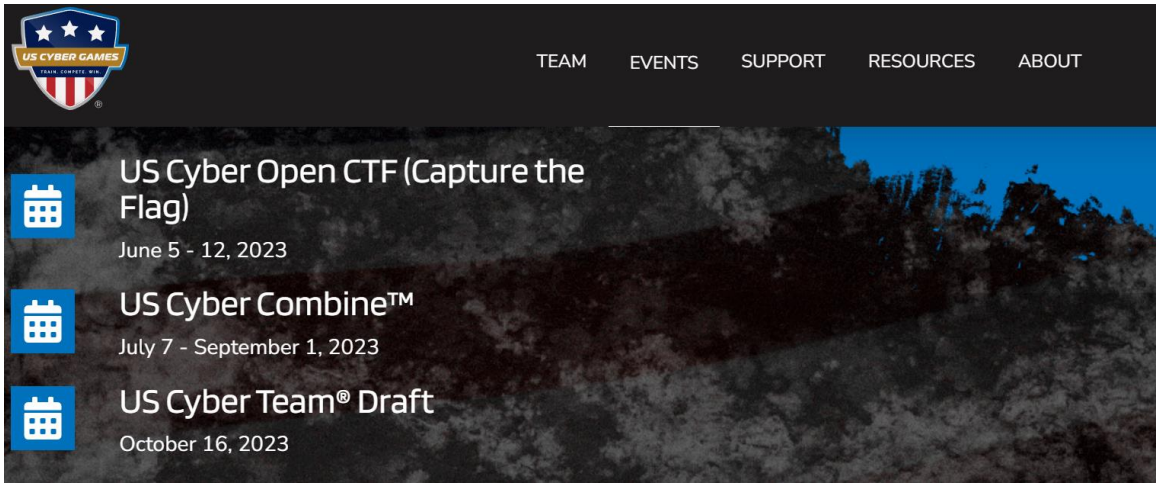
Number 13

Informing and Inspiring the Next Generation of Cyber Talent Through Competition

Antonio "T" Scurlock, Deputy Chief Learning Officer

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Last week, U.S. Cyber Games® began competition to identify and select the Season III, U.S. Cyber Team. Over the next few months, athletes aged 18-24 will compete in a series of events that will culminate with selecting the top cyber athletes in October for the Season III team to compete at the 2024 International Cybersecurity Challenge (ICC).I had the privilege of attending and speaking at the kickoff event for Season III, U.S. Cyber Open®.



You may visit: https://www.uscybergames.com/about

CISA's focus is on people, especially with helping to build a competent, resourceful and diverse cyber workforce.

To solve the most complicated, technical problems facing our nation, we need diversity of thought and skill that can enable better problem-solving.

This means partnering with organizations to create career pathways and provide resources and access to opportunities to pursue careers in cybersecurity.

Founded by Katzcy, in cooperation with the National Initiative for Cybersecurity Education (NICE) program at the National Institute of Standards and Technology (NIST), the U.S. Cyber Games® is one of our key partnerships to inspire and inform the next generation about pursing cybersecurity careers.

Together, we not only identify and nurture the nation's top cyber talent, but also reinforce the importance of cybersecurity in today's evolving digital landscape.

The next generation of cyber professionals play a critical role in helping to protect our nation and CISA is proud to be a founding sponsor of the U.S. Cyber Teams.

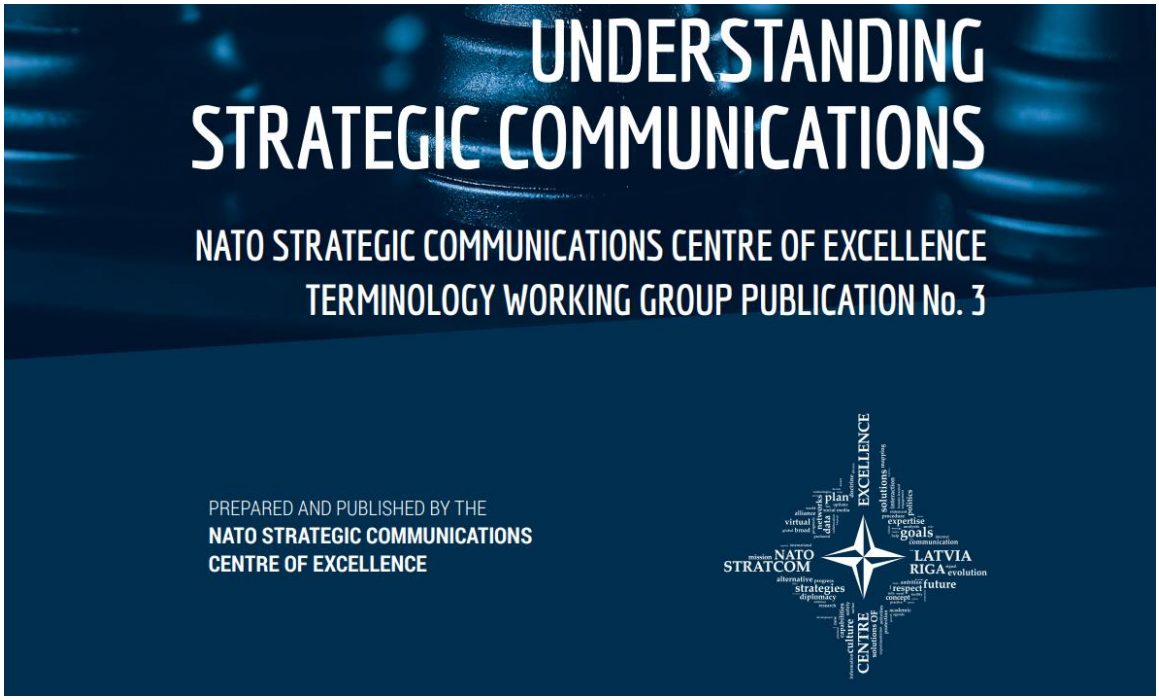
This year, the Season II team will participate in various global scrimmages and the ICC in San Diego, Calif., on August 1-3. In 2022, Season I team, the first-ever U.S. Cyber Team, competed at the ICC in Athens, Greece and earned Bronze in the competition.

I'm excited for the Season III games to commence and look forward to tracking the cyber athletes as they move through the competition for final team selection in October.

To read more: https://www.cisa.gov/news-events/news/informing-and-inspiring-next-generation-cyber-talent-through-competition

Number 14

Understanding Strategic Communications



You may visit: https://stratcomcoe.org/publications/understanding-strategic-communications-nato-strategic-communications-centre-of-excellence-terminology-working-group-publication-no-3/285

Number 15

European Banking Authority (EBA), Consultation Paper on amendments to the Guidelines on money laundering and terrorist financing to include crypto-asset service providers

In July 2021 the European Commission issued a legislative package with four proposals to reform the EU's legal and institutional anti-money laundering and countering the financing of terrorism (AML/CFT) framework.

The legislative package included a proposal for a recast of Regulation (EU) 2015/847.

This recast extends the scope of Regulation (EU) 2015/847 to transfers of crypto assets. It also extends the definition of 'financial institution' in Directive (EU) 2015/849 to CASPs that are regulated in accordance with the 'MiCA Regulation'.

CASPs as defined in the MiCA Regulation *will be subject to the same AML/CFT systems and controls requirements* as credit and financial institutions.

Article 38 of the recast Regulation (EU) 2015/847 amends Article 18 of the Directive (EU) 2015/849 and mandates the EBA to issue guidelines on the risk variables and risk factors CASPs should take into account when entering into a business relationship or carrying out transactions in crypto assets.

In particular, it requires the EBA to clarify the enhanced due diligence requirements CASPs should apply in high-risk situations, and the mitigating measures CASPs should apply when entering into similar correspondent relationships, particularly with entities that are not covered by Directive (EU) 2015/849.

To fulfill this mandate, the EBA is proposing to amend the EBA's Guidelines (EBA/2021/02) on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions under Articles 17 and 18(4) of Directive (EU) 2015/849 (the 'ML/TF Risk Factors Guidelines').

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2023/Consultation%20on%20revised%20Guidelines%20on%20money%20laundering%20and%20terrorist%20financing%20%28ML-TF%29%20risk%20factors/1055913/Consultation%20paper%20on%20amending%20Guidelines%20on%20ML%20FT%20risk%20factors.pdf

https://www.eba.europa.eu/eba-consults-amendments-guidelines-money-laundering-and-terrorist-financing-risk-factors-include

Number 16

GIGABYTE Fortifies System Security with Latest BIOS Updates and Enhanced Verification

GIGABYTE

GIGABYTE Technology, one of the leading global manufacturers of motherboards, graphics cards, and hardware solutions, has always prioritized cybersecurity and information security. GIGABYTE remains committed to fostering close collaboration with relevant units and implementing robust security measures to safeguard its users.

GIGABYTE engineers have already mitigated potential risks and uploaded the Intel 700/600 and AMD 500/400 series Beta BIOS to the official website after conducting thorough testing and validation of the new BIOS on GIGABYTE motherboards.

To fortify system security, GIGABYTE has implemented stricter security checks during the operating system boot process. These measures are designed to detect and prevent any possible malicious activities, providing users with enhanced protection:

1. Signature Verification: GIGABYTE has bolstered the validation process for files downloaded from remote servers. This enhanced verification ensures the integrity and legitimacy of the contents, thwarting any attempts by attackers to insert malicious code.

2. Privilege Access Limitations: GIGABYTE has enabled standard cryptographic verification of remote server certificates. This guarantees that files are exclusively downloaded from servers with valid and trusted certificates, ensuring an added layer of protection.

BIOS updates for the Intel 500/400 and AMD 600 series chipset motherboards will also be released on the GIGABYTE official website later today, along with updates for previously released motherboards. GIGABYTE recommends that users regularly visit the official GIGABYTE website for future BIOS updates.

For more information: www.gigabyte.com/Motherboard

Number 17

Swiss–US dialogue continues on cybersecurity and digital technology

The Federal Council

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Interdepartmental delegations from the Swiss and US governments met on 7 June 2023 in Washington, D.C., to report on mutual policy in the areas of cybersecurity and digitalisation, with a view to strengthening bilateral cooperation in these areas.

The Swiss delegation was led by Benedikt Wechsler, ambassador and head of the FDFA's Digitalisation Division.

This is the second bilateral dialogue on cybersecurity and digital matters to be organised between Switzerland and the United States. The first took place online at the beginning of July 2020.

The aim of the dialogue is to advance bilateral cooperation on a wide range of issues, compare priorities, exchange information and promote security and stability in the cyber and digital space.

This year's event provided an opportunity to strengthen cooperation on key issues, such as the application of international law in cyberspace and Switzerland's role as a host state in the digital domain.

In this context, the protection of the international organisations of International Geneva is of paramount importance.

A number of themes and initiatives have so far been identified where collaboration should be stepped up in the medium term, including combating ransomware and upholding internet freedom.

During the meeting, the two delegations discussed commitments and cooperation in multilateral bodies, as well as bilateral initiatives led by the US and Switzerland. Issues relating to digital commerce will continue to be handled by the Swiss–US joint economic commissions.

Interdepartmental cooperation essential for greater cybersecurity

The Swiss delegation was led by Benedikt Wechsler, ambassador and head of the FDFA's Digitalisation Division. In addition to representatives of the FDFA, the Swiss delegation included the Federal Office of

Communications, the National Cyber Security Centre, FEDPOL and the Federal Department of Defence, Civil Protection and Sport.

For its part, the US delegation comprised representatives of several agencies, led by the Department of State's Bureau of Cyberspace and Digital Policy, which was set up in 2022.

The wide range of participants reflects the multidimensional nature of the issue. Digitalisation is having an impact on every aspect of our daily lives and how we coexist. Switzerland gives priority to interdepartmental and international cooperation in implementing its digital foreign policy strategy.

It is committed to a free, open and secure digital space, both at the multilateral level and through bilateral dialogue. In addition, actors from the scientific and business communities have been involved, most recently in San Francisco as part of a 'tech retreat' organised by Denmark and Australia. In this area, the United States is a key partner for Switzerland.

To read more:
https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-95606.html

Number 18

COSMICENERGY operational technology (OT) / industrial control system (ICS)-oriented malware, to Sabotage Power Grids

MANDIANT
NOW PART OF Google Cloud

The discovery of COSMICENERGY illustrates that the barriers to entry for developing offensive OT capabilities are lowering as actors leverage knowledge from prior attacks to develop new malware.

Given that threat actors use red team tools and public exploitation frameworks for targeted threat activity in the wild, COSMICENERGY poses a plausible threat to affected electric grid assets.

To read more: https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

Number 19

NPSA Changes to Insider Risk Definitions

National Protective Security Authority

Background

Definitions enable us to have a common understanding of a word or subject; they allow us all to be on the same page and facilitate clear lines of communications. Having clear definitions of insider risk terminology is vital to support new and existing NPSA customers, who will have varying levels of knowledge in the subject area.

NPSA (formerly CPNI) has, until now, defined an insider as “a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes”.

This definition was utilised for the purposes of the research underpinning the 2009 and 2013 Insider Data Collection Study.

For the reasons outlined below, we felt it was the right time to refresh how we define our terms in relation to insider risk.

What is changing?

From May 2023 onwards NPSA will be utilising the following definitions through our various advice delivery and communications channels;

1. **Insider -** Any person who has, or previously had, authorised access to or knowledge of the organisation’s resources, including people, processes, information, technology, and facilities.

2. **Insider Risk -** The likelihood of harm or loss to an organisation, and its subsequent impact, because of the action or inaction of an insider.

3. **Insider Threat -** An insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organisation.

4. **Insider Event -** The activity, conducted by an insider (whether intentional or unintentional) that could result in, or has resulted in, harm or loss to the organisation.

Below summarises how the NPSA definition of insider will be communicated:

Rationale for changing
Insider risk comes from everyone 'inside' your organisation

NPSA's key message that we want to convey is that if you have people, you have risk. We therefore want all our customers to be insider risk ready.

Our extensive and ongoing research indicates that harm or loss to an organisation could be as a direct result of unintentional activity from those with legitimate access, as well as from personnel who intend to exploit their access.

Being research led

It's vital as an NTA we keep challenging our existing position. Following a rapid research review of literature, we found that most 'insider' definitions do not include exploitation or malice in the definition.

The definitions usually relate to access rather than exploitation. Close partners (e.g. CERT, US Government) similarly have also made recent changes to their definitions in a way aligns with NPSA's forthcoming changes.

Developing a consistent lexicon

To date, NPSA has only communicated one definition which related to an 'Insider'. This definition, however, failed to separate the community within which insider risk sits within and from those specific individuals that become an insider threat. This has resulted in language being utilised interchangeably and often in the wrong context. We want to change this, so we are all communicating in the same way.

Our next steps

Communications

NPSA Personnel & People Security Research & Development Team will be working alongside our communication colleagues to update existing guidance and products on our website to ensure it is consistent with this new terminology.

Please bear with us whilst these changes are made. This document will be made available on the NPSA Website under the Insider Risk Page. We ask that NPSA customers refer to the revised definitions contained within this update.

Evaluation

It's vital we evaluate whether changes to NPSA's Insider lexicon results in greater clarity for our customers and supports you in understanding and mitigating this risk in a coherent way. We would welcome your feedback either via utilising the contact us form or providing feedback here.

To read more: https://www.npsa.gov.uk/blog/personnel-security/npsa-changes-insider-risk-definitions

Number 20

Blue Campaign Toolkits for the Hospitality Industry

Homeland Security

The U.S. Department of Homeland Security's (DHS) Blue Campaign announced the release of a new human trafficking awareness toolkit tailored to tribal gaming and hospitality professionals.

Developed by DHS, the National Indian Gaming Commission (NIGC), the Bureau of Indian Affairs (BIA), and the U.S. Department of the Treasury, the "Human Trafficking Response Guide for the Tribal Gaming and Hospitality Industry" marks the first interagency partnership on a toolkit for the tribal gaming and hospitality community.

"Successfully combating human trafficking is a multi-disciplinary, 'whole-of-society' effort," said Secretary Alejandro N. Mayorkas. "The Human Trafficking Response Guide for the Tribal Gaming and Hospitality Industry, the first of its kind, will assist an industry that is vulnerable to traffickers and will help protect potential victims. The survivor-informed toolkit will aid in the detection and prevention of human trafficking crimes in tribal gaming and hospitality settings. I thank the NIGC, BIA, and U.S. Department of Treasury for their continued partnership to combat human trafficking within the Indian gaming and hospitality industry."

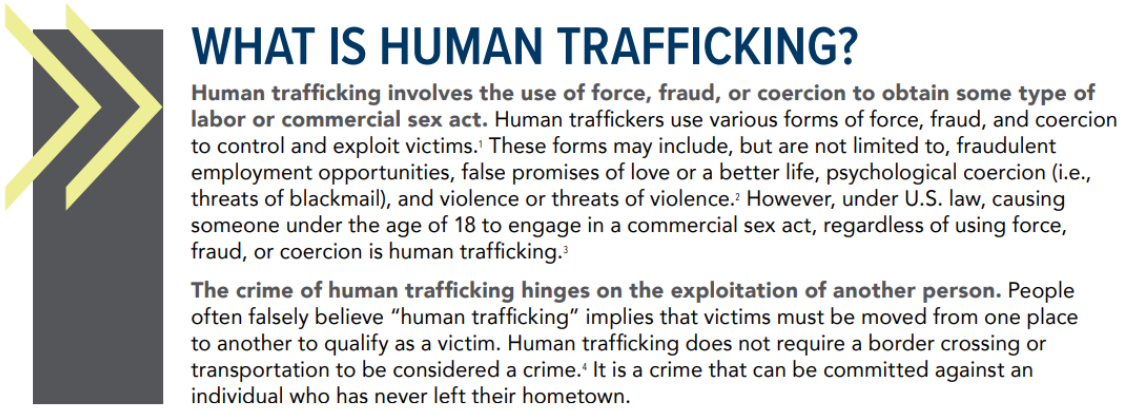
"This culturally tailored, survivor-informed toolkit combines the Department's human trafficking knowledge, tools, and resources with the invaluable expertise, perspective, and guidance of the tribal gaming and hospitality industry, and Indigenous communities," said DHS Center for Countering Human Trafficking Director Cardell T. Morant. "The toolkit empowers Indigenous communities to protect victims and provides them with the tools for identifying and reporting potential human trafficking situations to the proper authorities."

Created at the request of, and with input from, tribal leaders, tribal gaming employees, and indigenous communities, this toolkit provides culturally appropriate, survivor-informed tips and resources for front line tribal gaming and hospitality employees at all levels, including security, surveillance, and transportation staff; casino gaming attendants; food and beverage staff; housekeeping, maintenance, and room service; and front of house staff.

Along with specific definitions and examples of human trafficking, the guide contains printable posters with role-specific indicators of the crime and appropriate reporting information. The ultimate goal is prevention through detection and reporting.

“The fight against human trafficking includes highlighting industry best practices and maximizing coordination and resources across all of government,” said NIGC Chairman E. Sequoyah Simermeyer. “The Indian gaming regulatory community’s focus on preparedness can support both and includes efforts like the interagency toolkit.”

“Human trafficking is one of the worst forms of violence. As a partner in this process to develop training and outreach materials specific to human trafficking indicators in the tribal gaming industry, the Agency is grateful to share our expertise and the input we received from tribes and tribal gaming operations,” said Jeannie Hovland, NIGC Vice Chair and Office of Self-Regulation Director. “We’re hopeful this toolkit, infused with Indigenous culture and survivor informed content, helps those on the front lines identify potential victims and prevent abuse.”



WHAT IS HUMAN TRAFFICKING?

Human trafficking involves the use of force, fraud, or coercion to obtain some type of labor or commercial sex act. Human traffickers use various forms of force, fraud, and coercion to control and exploit victims.[1] These forms may include, but are not limited to, fraudulent employment opportunities, false promises of love or a better life, psychological coercion (i.e., threats of blackmail), and violence or threats of violence.[2] However, under U.S. law, causing someone under the age of 18 to engage in a commercial sex act, regardless of using force, fraud, or coercion is human trafficking.[3]

The crime of human trafficking hinges on the exploitation of another person. People often falsely believe “human trafficking” implies that victims must be moved from one place to another to qualify as a victim. Human trafficking does not require a border crossing or transportation to be considered a crime.[4] It is a crime that can be committed against an individual who has never left their hometown.

You may visit: https://www.dhs.gov/blue-campaign/materials/toolkits

INDICATORS OF HUMAN TRAFFICKING FOR HOUSEKEEPING, MAINTENANCE, AND ROOM SERVICE STAFF

Housekeeping, maintenance, and room service staff typically have the most access to guest rooms where signs of human trafficking may be apparent. By being conscious of human trafficking indicators, you can help identify possible trafficking activities and victims.

Does the guest…

- Use the "Do Not Disturb" sign constantly?
- Request additional towels, new linens, etc. multiple times a day but deny hotel/motel staff entry into the room?
- Refuse cleaning services for multiple days?
- Keep excessive amounts of cash in the room?
- Possess multiple computers, cell phones, credit card readers, or other technology?
- Reserve multiple rooms?
- Leave the room infrequently, not at all, or at odd hours?
- Possess children's items or clothing without having a child registered with the room?
- Loiter in the hallways and appear to monitor the area?
- Keep excessive amounts of alcohol or illegal drugs in their room?
- Possess evidence of pornography or sex paraphernalia (condoms, lubricant, lotion, etc.)?
- Leave minors alone in their room for long periods of time?
- Have an excessive number of people staying in their room?
- Stay for an extended period of time with few or no personal possessions?
- Allow a constant flow of people into a room at all hours?
- Keep their room stocked with merchandise, luggage, mail packages, and purses/wallets with different names?
- Loiter in the parking lot, lobby, or hallways and return to the room after a visitor leaves?

BLUE CAMPAIGN

One Voice. One Mission. End Human Trafficking.®

Number 21

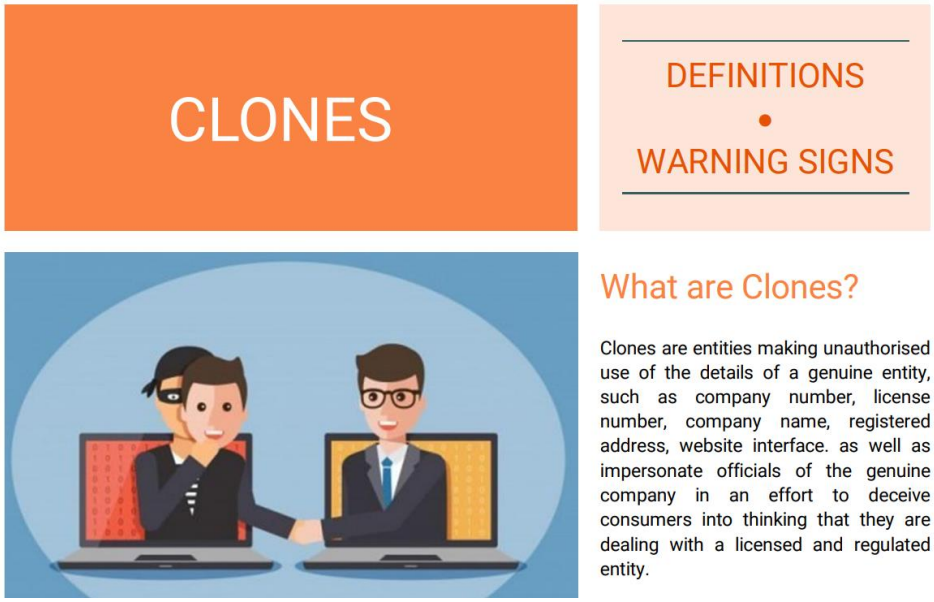
Financial Scams and How to Avoid Them

MFSA MALTA FINANCIAL SERVICES AUTHORITY

The Malta Financial Services Authority (MFSA) is the single regulator of financial services in Malta.

The MFSA regulates banking, financial institutions, insurance companies and insurance intermediaries, investment services companies and collective investment schemes, securities markets, recognized investment exchanges, trust management companies, company services providers and pension schemes.

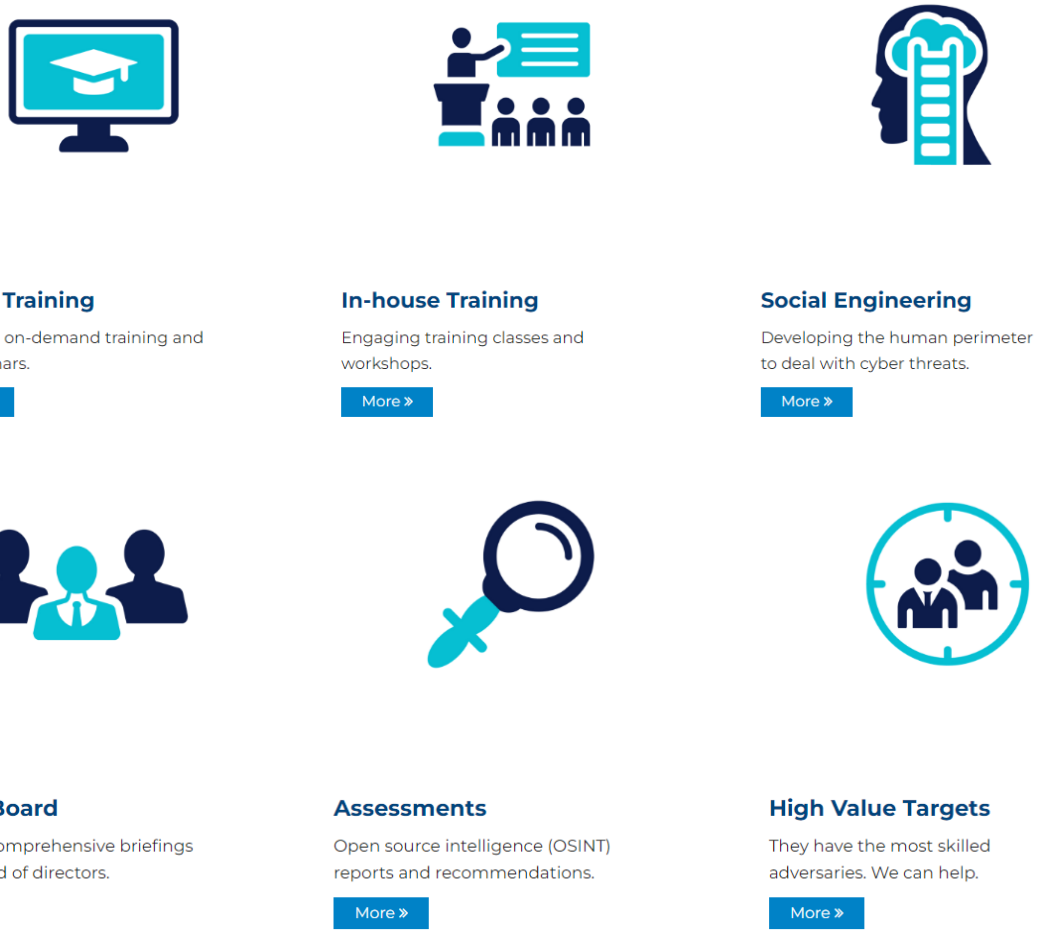
Since 2018, it is also responsible for regulating Virtual Financial Assets.



To read more: https://www.mfsa.mt/wp-content/uploads/2023/05/Financial-Scams-and-How-to-Avoid-Them-English-Version.pdf

Cyber Risk GmbH

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



Cyber security training

Overview

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

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

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

Duration

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

Our Education Method

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

Our Instructors

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

Our websites include:

a. Sectors and Industries.

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

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

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

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

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

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

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

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

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

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

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

b. Understanding Cybersecurity.

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

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

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

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

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

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

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

c. Understanding Cybersecurity in the European Union.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

You may contact:

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

Disclaimer

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

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

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

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

This information:

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

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

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

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

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

- is in no way constitutive of interpretative;

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

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

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

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

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