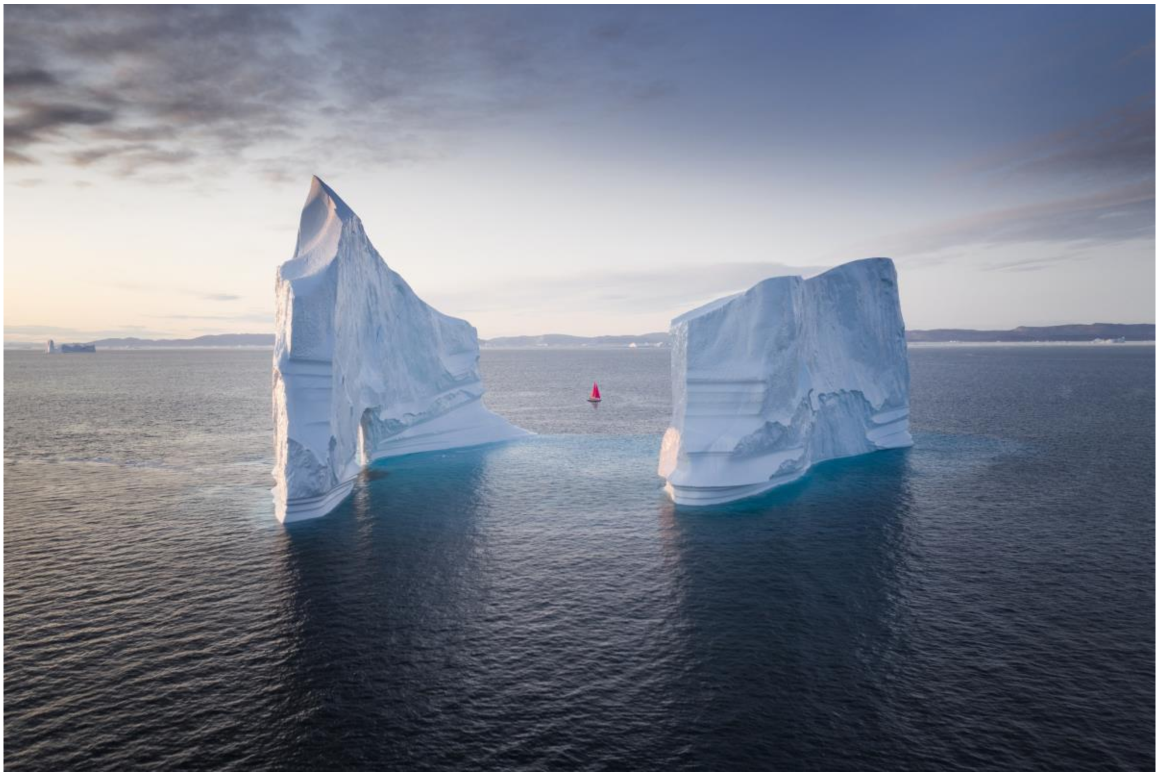


Cyber Risk and Compliance News and Alerts, January 2024

Paracelsus believed that poison is in everything, and no thing is without poison. The dosage makes it either a poison or a remedy.

Well, poison *is* in everything, even in Artificial Intelligence (AI) systems. According to the US National Institute of Standards and Technology, adversaries can deliberately confuse or even poison AI systems to make them malfunction — and there's no foolproof defense that their developers can employ.

Poisoning attacks occur in the training phase by introducing corrupted data. An example would be slipping numerous instances of inappropriate language into conversation records, so that a chatbot interprets these instances as common enough parlance to use in its own customer interactions.

Evasion attacks, which occur after an AI system is deployed, attempt to alter an input to change how the system responds to it. Examples would include adding markings to stop signs to make an autonomous vehicle misinterpret them as speed limit signs or creating confusing lane markings to make the vehicle veer off the road.

Privacy attacks, which occur during deployment, are attempts to learn sensitive information about the AI or the data it was trained on in order to misuse it. An adversary can ask a chatbot numerous legitimate questions, and then use the answers to reverse engineer the model so as to find its weak spots — or guess at its sources. Adding undesired examples to those online sources could make the

AI behave inappropriately, and making the AI unlearn those specific undesired examples after the fact can be difficult.

Abuse attacks involve the insertion of incorrect information into a source, such as a webpage or online document, that an AI then absorbs. Unlike the aforementioned poisoning attacks, abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source to repurpose the AI system's intended use.

Marcus Tullius Cicero has said: "When you have no basis for an argument, abuse the plaintiff."

Read more at number 7 below.

Enrico Fermi (the physicist renowned for being the creator of the world's first nuclear reactor, the Chicago Pile-1), had said: "There are two possible outcomes: if the result confirms the hypothesis, then you've made a measurement. If the result is contrary to the hypothesis, then you've made a discovery."

I have just read carefully the Initial Public Draft, NIST SP 800-55v1 ipd, "Measurement Guide for Information Security, Volume 1 — Identifying and Selecting Measures".

We read: "The terms measurement and assessment are often used interchangeably in the information security field. This document provides a lexicon for key terminology and an overview of foundational concepts to those looking to measure and assess information security risk and clarifies the distinction between measurement and assessment.

As described in Sec. 1.4, assessment refers to the process of evaluating, estimating, or judging against defined criteria, and measurement is the process of obtaining quantitative values. Hence, assessment is a broader concept that also includes measurement.

Organizations perform multiple kinds of assessment when evaluating information security risk, such as risk assessments, program assessments, and control assessments. Risk assessments are used to identify the risks that an organization faces and can support decision-making.

Program-level assessments are used for decision-making about the strategies, policies, procedures, and operations that determine the security posture of an information security program.

In control assessments, organizations evaluate whether specific controls are performing the way they were intended and achieving the desired results. Both program assessments and control assessments are in and of themselves a form of risk assessment and provide a different lens for viewing information security risk.

SP 800-55 is intentionally agnostic on specific risk assessment models. However, many identify threat, likelihood, vulnerability, and impact as areas to assess."

Later in the paper, we read: "Measures are numerically expressed data that are gathered through the process of measurement. Measures can be derived from any operations or systems that can be measured with numbers. Quantitative assessments judge measures data against a set criteria or target and can be used to analyze information security risks using frequency, rates, financial impacts, and other numeric indicators."

Ben Bernanke, the economist who served as the 14th chairman of the Federal Reserve, has said: "In many spheres of human endeavor, from science to business to education to economic policy, good decisions depend on good measurement." Well, I do understand that, but I always have doubts about our ability for "good measurement" in areas like economic policy and risk management. Sometimes we follow Galileo Galilei's advice: "Measure what is measurable and make measurable what is not so."

Read more at number 1 below.

I have just read the inspection priorities for 2024 of the Division of Registration and Inspections of the Public Company Accounting Oversight Board (PCAOB). We read:

"Our 2024 inspection program will consider overall business risks present in the audits inspected. A few of these business risks include:

1. Persistent high interest rates, tightening of credit availability, and/or inflationary challenges.
2. Disruptions in the supply chain and rising costs.
3. Business models that are significantly impacted by rapidly changing technology.
4. Geopolitical conflicts.
5. Financial statements that include areas with a higher inherent risk of fraud, estimates involving complex models or processes, and/or presentation and disclosures that may be impacted by complexities in the public company's activities."

This is not going to be easy. Rapidly changing technologies and geopolitical conflicts (numbers 3 and 4 above) can be approached using models, but estimates involving complex models or processes (number 5 above) are also an area of concern.

Dear auditors, are you ready for some training? We read in the inspection priorities paper:

"New technologies often require new skills and considerations. One of the potential challenges for new technologies is ensuring that auditors have the appropriate knowledge and skills to efficiently and, perhaps more importantly, effectively incorporate or address these new technologies in their audit.

Given the rapid pace of technological evolution in financial reporting and auditing, our inspectors will also focus on the following technology-related areas:

Digital Assets

Activities associated with digital assets may involve heightened risks to investors, public companies, and broker-dealers. These risks include volatility of digital assets values, lack of transparency related to ownership and purpose, and fraud. Digital assets require:

(1) an appropriate risk assessment,

(2) understanding of the control environment, including information technology controls,

(3) an understanding of the controls over the existence and ownership of the digital assets, including ongoing safeguarding of private keys, and

(4) an appropriately planned audit response."

I was thinking about the "understanding of the control environment" part, in activities associated with digital assets. Steve Jobs has said: "Some people aren't used to an environment where excellence is expected".

Well, the environment where "digital assets may involve heightened risks to investors, public companies, and broker-dealers" is often not an environment where excellence is expected, especially in terms of risk management and compliance.

Read more at number 2 below.

___

In Switzerland we have major developments.

According to the General Secretariat GS-DDPS (Department of Defence, Civil Protection and Sport), from 1 January 2024, the Staatssekretariat für Sicherheitspolitik (SEPOS) - State Secretariat for Security - and the Bundesamt für Cybersicherheit (BACS) - Federal Office for Cyber Security - will commence operations as administrative units in the DDPS.

The Federal Council has created the two administrative units in order to make Switzerland's security policy more effective in dealing with increasing threats and dangers. At its meeting on November 22, 2023, the Federal Council adjusted the legal basis for these new entities.

The former National Cybersecurity Centre (NCSC), which was previously part of the Federal Department of Finance (FDF), will be transformed into the Federal

Office for Cybersecurity (BACS).

It coordinates the implementation of the National Cyber Strategy (NCS), is the point of contact for authorities, business and the general public on cyber issues and, as a centre of excellence for cyber threats, coordinates the work of the federal government.

The State Secretariat for Security Policy (SEPOS) develops the conceptual basis and guidelines for shaping Swiss security policy. In cooperation with the other departments and in compliance with their responsibilities, it coordinates security policy and cooperation, and prepares strategic guidelines for international security policy cooperation for the Federal Council.

SEPOS's area of responsibility also includes the three specialized departments for information security, personal security checks and operational security. In this way, the State Secretariat contributes to the implementation of the Information Security Act and thus the secure processing of information for which the federal government is responsible.

According to the Swiss Federal Department of Defence, Civil Protection and Sports (DDPS), the 17th of January 2024 several websites run by the Swiss Federal Administration were temporarily unavailable, as a result of a DDoS attack.

The websites affected included those of the federal departments and a number of federal offices. A DDoS attack occurs when a high volume of requests are sent in order to overload online services.

Responsibility for the attack has once again been claimed by the hacker group 'NoName', which previously targeted the Swiss Federal Administration in June 2023. The presumed pro-Russian group cited Ukrainian President Zelenskyy's attendance at the WEF Annual Meeting in Davos as the reason for the DDoS attack.

The NCSC collaborates with the administrative units concerned to analyse the risk of such attacks and provides support in implementing the appropriate measures.

As an attack had been expected in the run-up to the visit, the NCSC warned the operators of critical infrastructures of this kind of attack on 10 January and called on them to take the necessary precautions.

The Federal Administration had therefore adopted the appropriate security arrangements. The NCSC also liaises closely with national and international partners and with the operators of critical infrastructures.

Hackers generally use such attacks on website availability as a means of gaining media attention for their cause. They do this by flooding a website with a massive volume of requests so as to overload it and make it unavailable for a period of time. No data is lost or compromised in a DDoS attack.

Dear Herr Doktor Markus Mäder, dear Frau Pälvi Pulli, congratulations on your outstanding new roles!

At its meeting on 22 December 2023, the Federal Council appointed Dr Markus Mäder as State Secretary for Security Policy. The current head of International Relations Defence will become head of the new State Secretariat for Security Policy (SEPOS) on 1 January 2024.

Mr Mäder, 52, studied History, Geography and Swiss History and Constitutional Studies at the University of Zurich, graduating in 1999 with a lic. phil. degree. From 1997-2001, he worked as a research assistant at the Centre for Security Studies at ETH Zurich. During this time, he also worked as a research assistant in the General Staff of the Armed Forces, and as a staff and liaison officer in a KFOR peace support operation in Kosovo.

From 2001-2003, Mr Mäder was a visiting fellow at the Centre for Defence Studies at King's College London. He received his doctorate (DPhil) from the University of Zurich in 2003. He then worked as a security policy advisor and was the Deputy Head of Forces and Armament Planning in the Directorate for Security Policy of the DDPS. He went on to serve as Deputy Military Representative for the Swiss mission to NATO in Brussels. During his career as a conscript officer in the Swiss Armed Forces, he held various command and staff positions, and commanded Armoured Battalion 14 from 2008-2010.

In 2010 and 2011, Mr Mäder underwent training to become a defence attaché. He then served for four years in Islamabad as defence attaché to Pakistan, Afghanistan and Iran. From 2015-2016, he studied at the National War College of the National Defense University in Washington DC, graduating with a Master of Science in National Security Strategy. After serving as personal assistant to the Chief of Defence International Relations, he was appointed Director of International Relations Defence by the Federal Council on 1 December 2016, and at the same time was promoted to the rank of brigadier general. He was employed by the Defence Group as a civilian employee in this capacity.

As State Secretary, Mr Mäder will have overall responsibility for SEPOS, the State Secretariat for Security Policy. He and his staff of around 100 will help strengthen Switzerland's security by ensuring a coherent federal security policy.

The head of the DDPS, Federal Councillor Viola Amherd, also informed the Federal Council that she has appointed Pälvi Pulli as Deputy State Secretary. For this role, the Federal Council has conferred the title of ambassador on Ms Pulli.

Ms Pulli, 53, in addition to deputising for the State Secretary, will head SEPOS's Strategy and Cooperation unit. Ms Pulli majored in Swiss History and English and minored in Political Science at the University of Neuchâtel, graduating in 1998 with a licence ès lettres. In addition to her native Finnish, she is fluent in German, French, Italian, English, Swedish and Russian.

From 1999-2008, Ms Pulli held various security policy positions in the General Secretariat of the DDPS and in the Staff of the Federal Council Security Committee. She then worked as an advisor on foreign relations, security policy and federal police matters for the Federal Department of Justice and Police. In July 2017, she was appointed head of Security Policy in the General Secretariat of the DDPS.

The Swiss National Cybersecurity Centre (NCSC) received several messages in January concerning the e-commerce platform Etsy. Immediately after creating an account, new sellers received a message, purportedly from Etsy, stating that the seller must verify payment before the shop can be activated.

Think about that. Even persons that understand social engineering could fall victims. If you create an account and you are contacted from the "platform" immediately after that, you can believe this is an official communication, not a scam.

The attack is aimed at new sellers who start a shop on Etsy. The attackers have found a way to quickly locate these new customers. In a test conducted by the NCSC, it was found that it took the fraudsters just 30 minutes to contact the new seller after they had started the shop.

The perfidious thing is that, in order to gain the new seller's trust, the fraudsters contact them not by email but via Etsy's internal notification system, the chat. They select a name to make it appear as if the message comes from an internal support or verification centre.

For example, in one case the surname 'Verificativ' was used, and the surname 'Support' has also been observed. This name is then displayed in the notification system, making it appear like an official request from the support team or an official verification procedure of the payment process.

In a further communication, the fraudsters claim that verification of the future payment method is necessary before the shop is fully set up. The new seller is redirected to a page where they are asked to enter their credit card details.

This triggers a payment – e.g. of USD 1,000. At the same time, the alleged support person assures the seller via Etsy's internal notification system that the credit card payment has not been directly booked, but the amount is merely a deposit, as is the case when you hire a car. They claim that the payment is being held provisionally and will not yet be booked.

The new seller is then immediately sent a second message, this time asking them to reverse the payment of USD 1,000. However, no payments are actually reserved or cancelled, but rather, payments totalling USD 2,000 are booked. When the victim asks for a telephone contact to discuss the matter, they are told that this can only be given on completion of the verification process.

In this type of fraud, the good faith of new platform users is shamelessly exploited through social engineering. New users usually have no knowledge of any of the service provider's processes. Furthermore, the fraudsters win their trust by contacting them via the internal chat.

Welcome to our monthly newsletter.

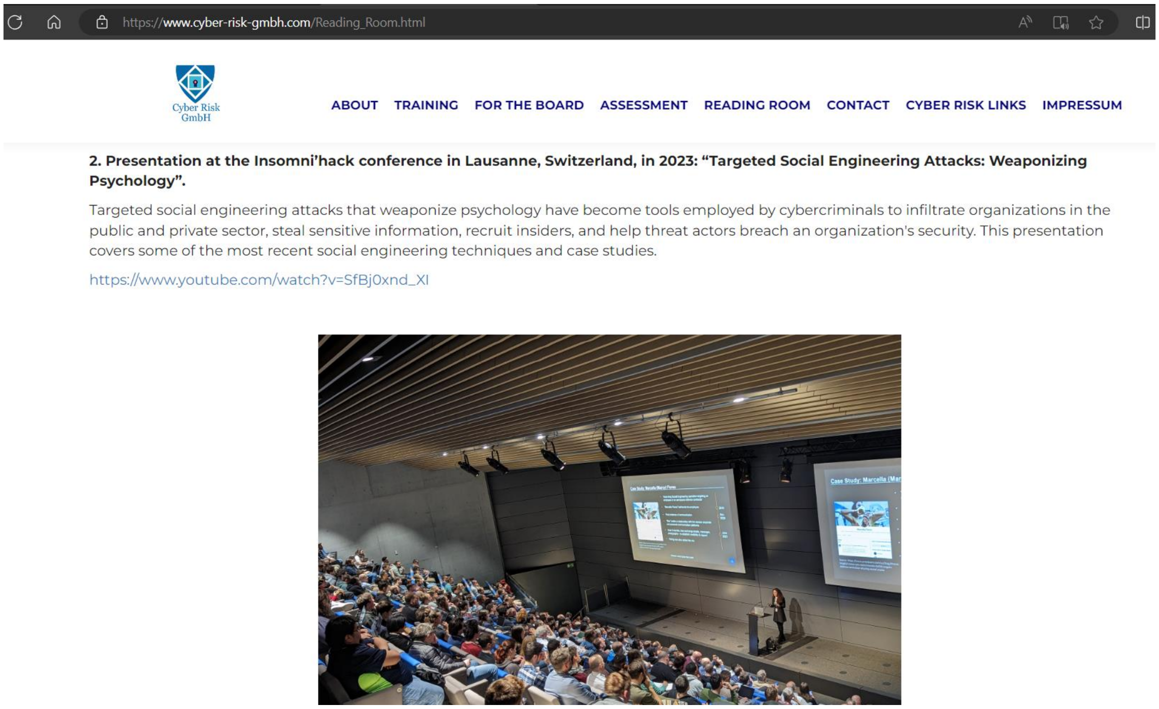
Best regards,

George Lekatis

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

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

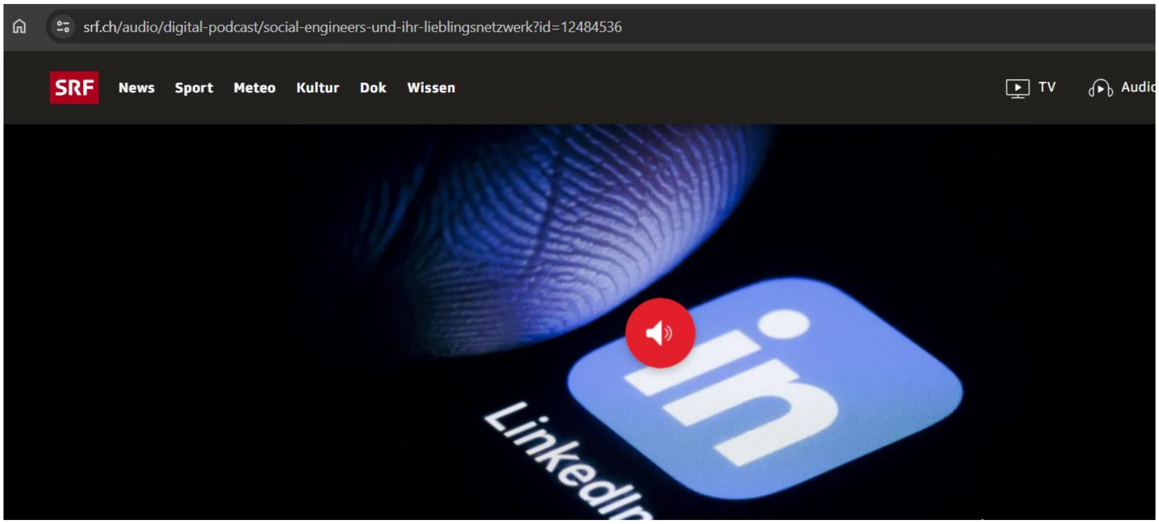
Our reading room: https://www.cyber-risk-gmbh.com/Reading_Room.html

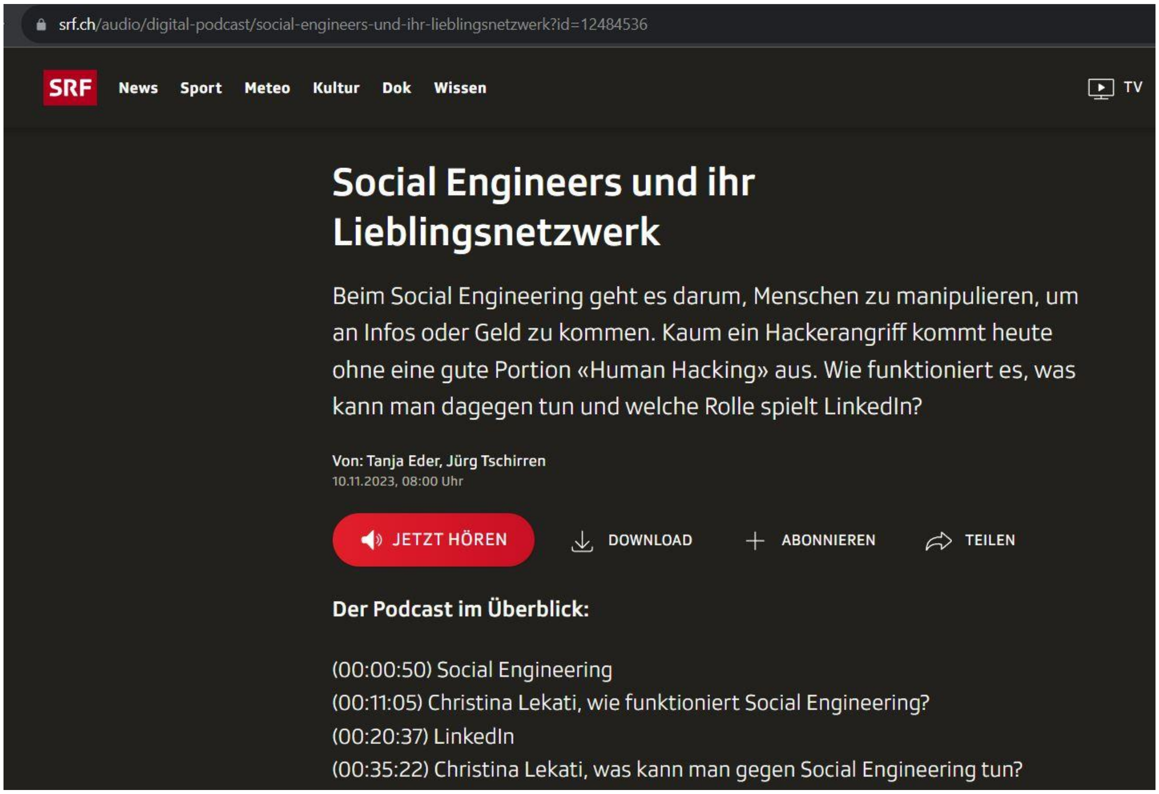


2. Presentation at the Insomni'hack conference in Lausanne, Switzerland, in 2023: "Targeted Social Engineering Attacks: Weaponizing Psychology".

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

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


srf.ch/audio/digital-podcast/social-engineers-und-ihr-lieblingsnetzwerk?id=12484536
SRF
News
Sport
Meteo
Kultur
Dok
Wissen
TV
Audio
LinkedIn


srf.ch/audio/digital-podcast/social-engineers-und-ihr-lieblingsnetzwerk?id=12484536
SRF
News
Sport
Meteo
Kultur
Dok
Wissen
TV

Social Engineers und ihr Lieblingsnetzwerk

Beim Social Engineering geht es darum, Menschen zu manipulieren, um an Infos oder Geld zu kommen. Kaum ein Hackerangriff kommt heute ohne eine gute Portion «Human Hacking» aus. Wie funktioniert es, was kann man dagegen tun und welche Rolle spielt LinkedIn?

Von: Tanja Eder, Jürg Tschirren
10.11.2023, 08:00 Uhr

JETZT HÖREN
DOWNLOAD
ABONNIEREN
TEILEN

Der Podcast im Überblick:

(00:00:50) Social Engineering
(00:11:05) Christina Lekati, wie funktioniert Social Engineering?
(00:20:37) LinkedIn
(00:35:22) Christina Lekati, was kann man gegen Social Engineering tun?

You may visit:
https://www.srf.ch/audio/digital-podcast/social-engineers-und-ihr-lieblingsnetzwerk?id=12484536

Number 1 (Page 13)

NIST SP 800-55 Vol. 1 (Initial Public Draft)
Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures

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

Number 2 (Page 15)

PCAOB Staff Outline 2024 Inspection Priorities with Focus on Driving Improvements in Audit Quality

PCAOB PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Number 3 (Page 19)

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

Microsoft

Number 4 (Page 21)

Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021

MANDIANT NOW PART OF Google Cloud

Number 5 (Page 22)

Operationalising the Framework for Evaluating Capability against Information Influence Operations
A Case Study of the Psychological Defence Agency's Courses

Number 6 (Page 25)

Pioneering a New National Security

GCHQ

Number 7 (Page 27)

NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

Number 8 (Page 30)

Testing the cognitive limits of large language models
Fernando Perez-Cruz and Hyun Song Shin

Number 9 (Page 32)

GCHQ software and apps
GCHQ is a world-leading intelligence, cyber and security agency with a mission to keep the UK safe

Number 10 (Page 34)

2023 National Security Agency (NSA) Cybersecurity

Number 11 (Page 37)

US Allies Offensive Cyber: Entrapment Risk or Entanglement Nuisance
Major Mikkel Storm Jensen, Ph.D.

Number 12 (Page 39)

ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

Number 13 (Page 40)

FBI, Human Trafficking Prevention Month

Number 14 (Page 42)

CISA and ENISA enhance their Cooperation

Number 15 (Page 44)

Voices from DARPA

Podcast Episode 75: The Metamaterial Visionary

Program manager in DARPA's Defense Sciences Office highlights fascinating optics programs made possible by novel engineered materials

Number 16 (Page 45)

Ghidra

Number 1

NIST SP 800-55 Vol. 1 (Initial Public Draft) Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures

The initial public drafts of NIST Special Publication (SP) 800-55, Measurement Guide for Information Security, Volume 1 – Identifying and Selecting Measures and Volume 2 – Developing an Information Security Measurement Program are available for comment after extensive research, development, and customer engagement.

In response to the feedback from the pre-draft call for comment and initial working draft (annotated outline), NIST continued to refine the publications by organizing the guidance into two volumes and developing more actionable and focused guidance in each.

Volume 1 – Identifying and Selecting Measures is a flexible approach to the development, selection, and prioritization of information security measures. This volume explores both quantitative and qualitative assessment and provides basic guidance on data analysis techniques as well as impact and likelihood modeling.

Volume 2 — Developing an Information Security Measurement Program is a methodology for developing and implementing a structure for an information security measurement program.

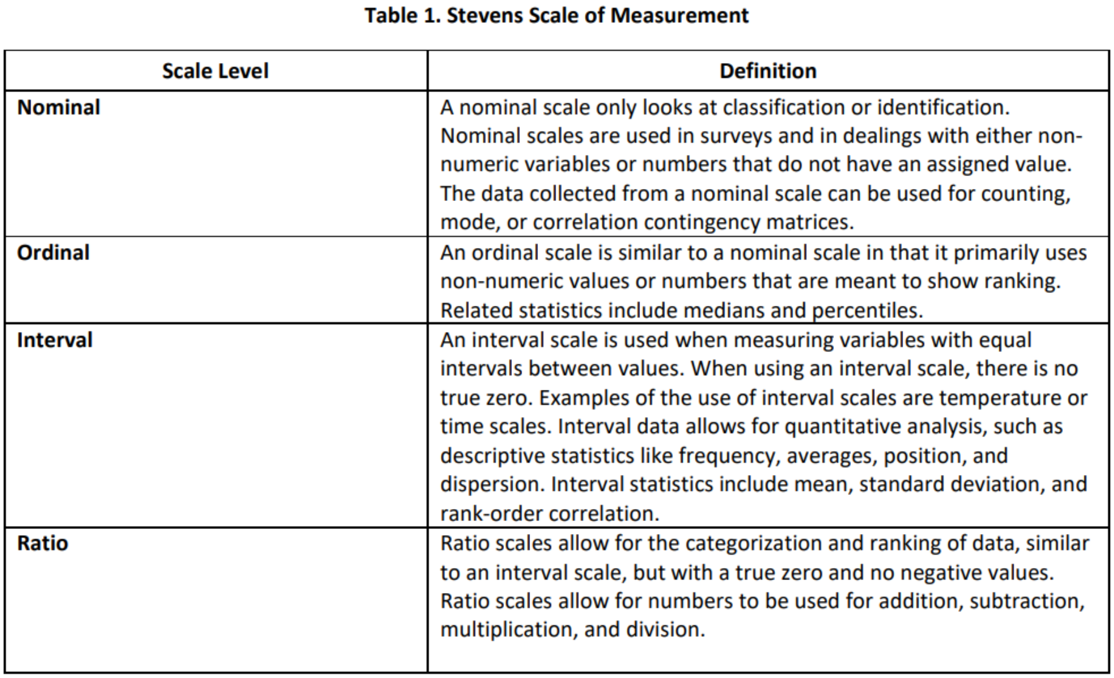
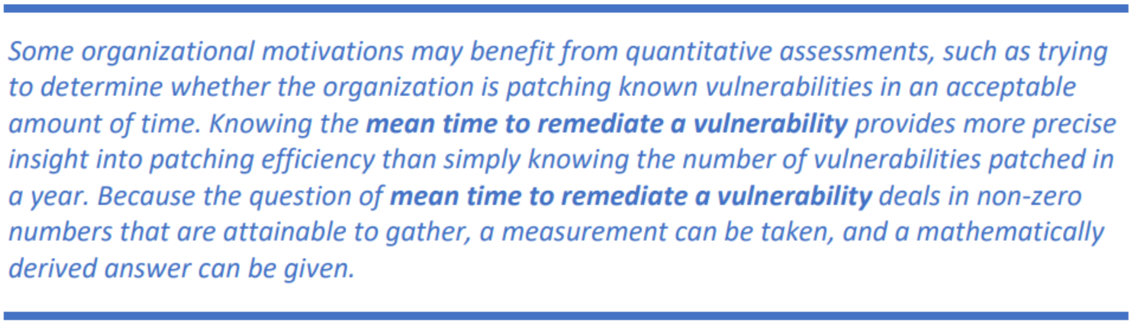
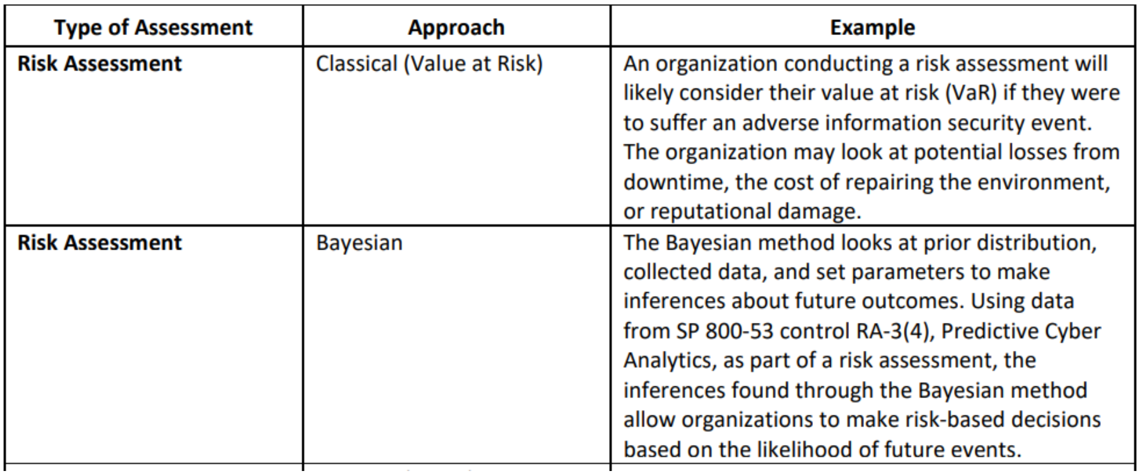


Table 1. Stevens Scale of Measurement

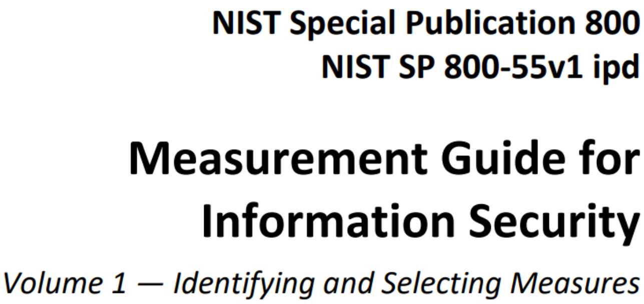
Scale Level	Definition
Nominal	A nominal scale only looks at classification or identification. Nominal scales are used in surveys and in dealings with either non-numeric variables or numbers that do not have an assigned value. The data collected from a nominal scale can be used for counting, mode, or correlation contingency matrices.
Ordinal	An ordinal scale is similar to a nominal scale in that it primarily uses non-numeric values or numbers that are meant to show ranking. Related statistics include medians and percentiles.
Interval	An interval scale is used when measuring variables with equal intervals between values. When using an interval scale, there is no true zero. Examples of the use of interval scales are temperature or time scales. Interval data allows for quantitative analysis, such as descriptive statistics like frequency, averages, position, and dispersion. Interval statistics include mean, standard deviation, and rank-order correlation.
Ratio	Ratio scales allow for the categorization and ranking of data, similar to an interval scale, but with a true zero and no negative values. Ratio scales allow for numbers to be used for addition, subtraction, multiplication, and division.



*Some organizational motivations may benefit from quantitative assessments, such as trying to determine whether the organization is patching known vulnerabilities in an acceptable amount of time. Knowing the **mean time to remediate a vulnerability** provides more precise insight into patching efficiency than simply knowing the number of vulnerabilities patched in a year. Because the question of **mean time to remediate a vulnerability** deals in non-zero numbers that are attainable to gather, a measurement can be taken, and a mathematically derived answer can be given.*



Type of Assessment	Approach	Example
Risk Assessment	Classical (Value at Risk)	An organization conducting a risk assessment will likely consider their value at risk (VaR) if they were to suffer an adverse information security event. The organization may look at potential losses from downtime, the cost of repairing the environment, or reputational damage.
Risk Assessment	Bayesian	The Bayesian method looks at prior distribution, collected data, and set parameters to make inferences about future outcomes. Using data from SP 800-53 control RA-3(4), Predictive Cyber Analytics, as part of a risk assessment, the inferences found through the Bayesian method allow organizations to make risk-based decisions based on the likelihood of future events.



NIST Special Publication 800
NIST SP 800-55v1 ipd

Measurement Guide for Information Security

Volume 1 — Identifying and Selecting Measures

To read more: https://csrc.nist.gov/pubs/sp/800/55/v1/ipd

Number 2

PCAOB Staff Outline 2024 Inspection Priorities with Focus on Driving Improvements in Audit Quality

The staff report includes key risks and considerations auditors should focus on, along with questions for audit committees and more.

Public Company Accounting Oversight Board (PCAOB) inspectors outlined their priorities for 2024 inspections in a PCAOB staff report. The report highlights key risks, like high interest rates, and other considerations, like audit areas with recurring deficiencies, that auditors should be focused on when planning and performing audit procedures. It notes that the PCAOB will continue to prioritize inspections of financial-services sector audits, digital assets, and more.

The report also includes suggested questions for audit committees to hold firms accountable to high standards when hiring and overseeing the audit process.

“Our inspection priorities Spotlight provides firms with important insights to help them plan and perform high-quality audits investors deserve,” said PCAOB Chair Erica Y. Williams. “We encourage firms and audit committees to make use of this important tool to help improve audit quality.”

The report also reiterates the inspection staff’s commitment to enhancements to our inspection program, such as increasing the number of engagements reviewed and improving the timeliness of inspection reports.

Among the PCAOB’s inspection enhancements in 2024 will be the creation of a PCAOB team that will evaluate culture across the largest domestic audit firms. This initiative will include interviewing firm personnel and evaluating other documentation, with the aim of using this information to enhance the PCAOB’s understanding of how audit firm cultures may be affecting audit quality.

Overall Business Risk Considerations:

Our 2024 inspection program will consider overall business risks present in the audits inspected. A few of these business risks include:

1. Persistent high interest rates, tightening of credit availability, and/or inflationary challenges.

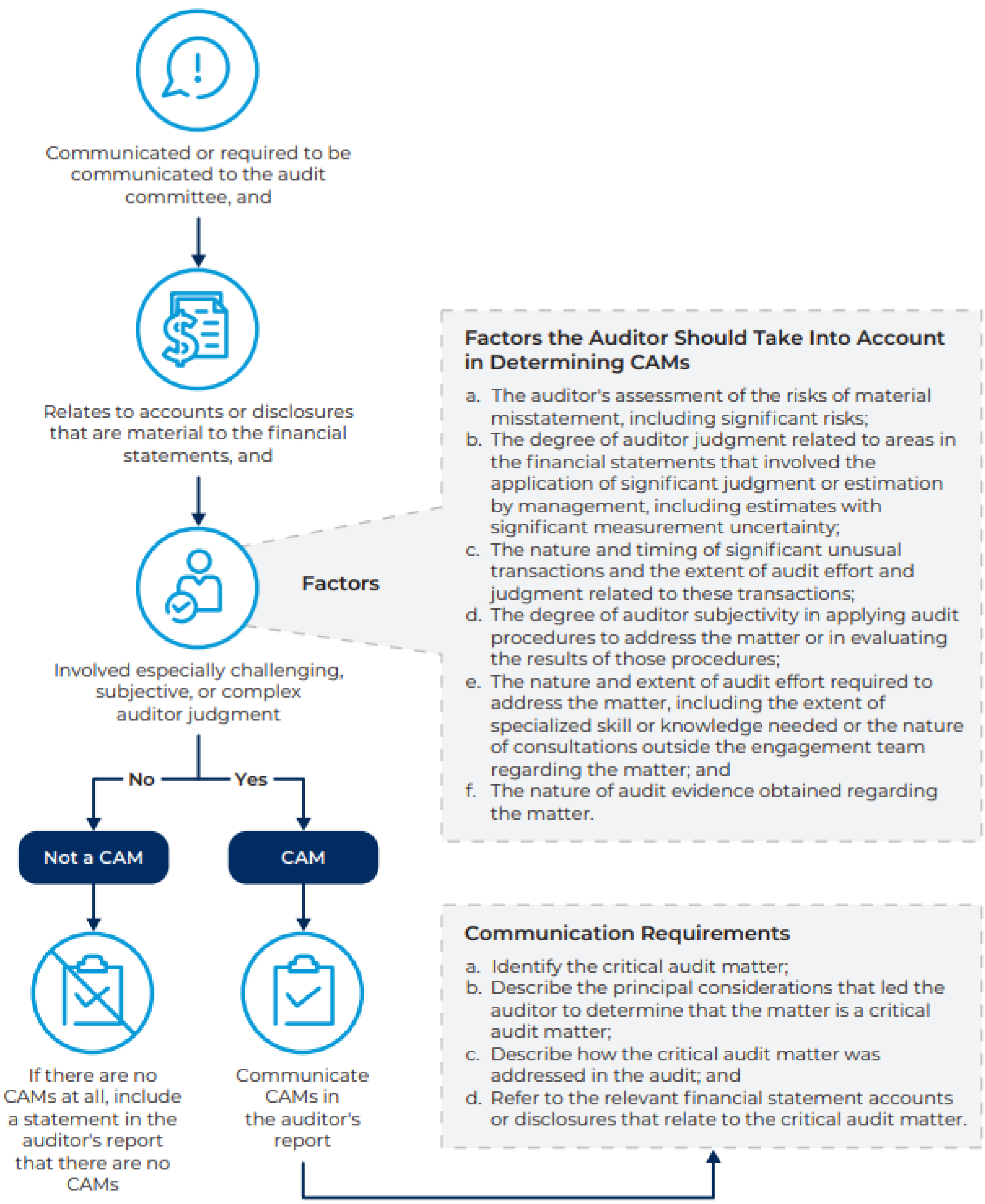
2. Disruptions in the supply chain and rising costs.

3. Business models that are significantly impacted by rapidly changing technology.

4. Geopolitical conflicts.

5. Financial statements that include areas with a higher inherent risk of fraud, estimates involving complex models or processes, and/or presentation and disclosures that may be impacted by complexities in the public company's activities.

Determining and Communicating Critical Audit Matters (CAMs)


Communicated or required to be communicated to the audit committee, and
Relates to accounts or disclosures that are material to the financial statements, and
Factors
Involved especially challenging, subjective, or complex auditor judgment
No
Yes
Not a CAM
CAM
If there are no CAMs at all, include a statement in the auditor's report that there are no CAMs
Communicate CAMs in the auditor's report

Factors the Auditor Should Take Into Account in Determining CAMs

a. The auditor's assessment of the risks of material misstatement, including significant risks;
b. The degree of auditor judgment related to areas in the financial statements that involved the application of significant judgment or estimation by management, including estimates with significant measurement uncertainty;
c. The nature and timing of significant unusual transactions and the extent of audit effort and judgment related to these transactions;
d. The degree of auditor subjectivity in applying audit procedures to address the matter or in evaluating the results of those procedures;
e. The nature and extent of audit effort required to address the matter, including the extent of specialized skill or knowledge needed or the nature of consultations outside the engagement team regarding the matter; and
f. The nature of audit evidence obtained regarding the matter.

Communication Requirements

a. Identify the critical audit matter;
b. Describe the principal considerations that led the auditor to determine that the matter is a critical audit matter;
c. Describe how the critical audit matter was addressed in the audit; and
d. Refer to the relevant financial statement accounts or disclosures that relate to the critical audit matter.

Prioritized Sectors/Industries:

In 2024, in addition to continuing to select some engagements for review based on risk and some randomly, we will do the following:

1. Continue our emphasis on selecting audits of companies engaging in merger and acquisition activities or business combinations.

2. Continue our emphasis on selecting audits of broker-dealers that file compliance reports and others that provide customers with various investment opportunities, such as introducing brokers.

3. Continue to select non-traditional audit areas to inspect.

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

SPOTLIGHT

Staff Priorities for 2024 Inspections and Interactions With Audit Committees

Inspections Considerations:

The report also discusses a range of considerations that should be important for auditors when planning and performing risk assessments and audit procedures.

These considerations include:

1. Challenges and Recurring Deficiencies We Have Observed in Our Inspections of Auditors of Broker-Dealers

2. Recurring Deficiencies

3. Evaluating Audit Evidence

4. Understanding the Company and Its Environment

5. Use of Other Auditors

6. Going Concern
7. Critical Audit Matters (CAMs)
8. Digital Assets
9. Cybersecurity
10. Use of Data and Technology

To read more: https://assets.pcaobus.org/pcaob-dev/docs/default-source/documents/2024-priorities-spotlight.pdf?sfvrsn=7c595fae_2

Number 3

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access.

Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our Secure Future Initiative (SFI), we are sharing this update.

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents.

The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed.

The attack was not the result of a vulnerability in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required.

This attack does highlight the continued risk posed to all organizations from well-resourced nation-state threat actors like Midnight Blizzard.

As we said late last year when we announced Secure Future Initiative (SFI), given the reality of threat actors that are resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk – the traditional sort of calculus is simply no longer sufficient.

For Microsoft, this incident has highlighted the urgent need to move even faster. We will act immediately to apply our current security standards to Microsoft-owned legacy systems and internal business processes, even when these changes might cause disruption to existing business processes.

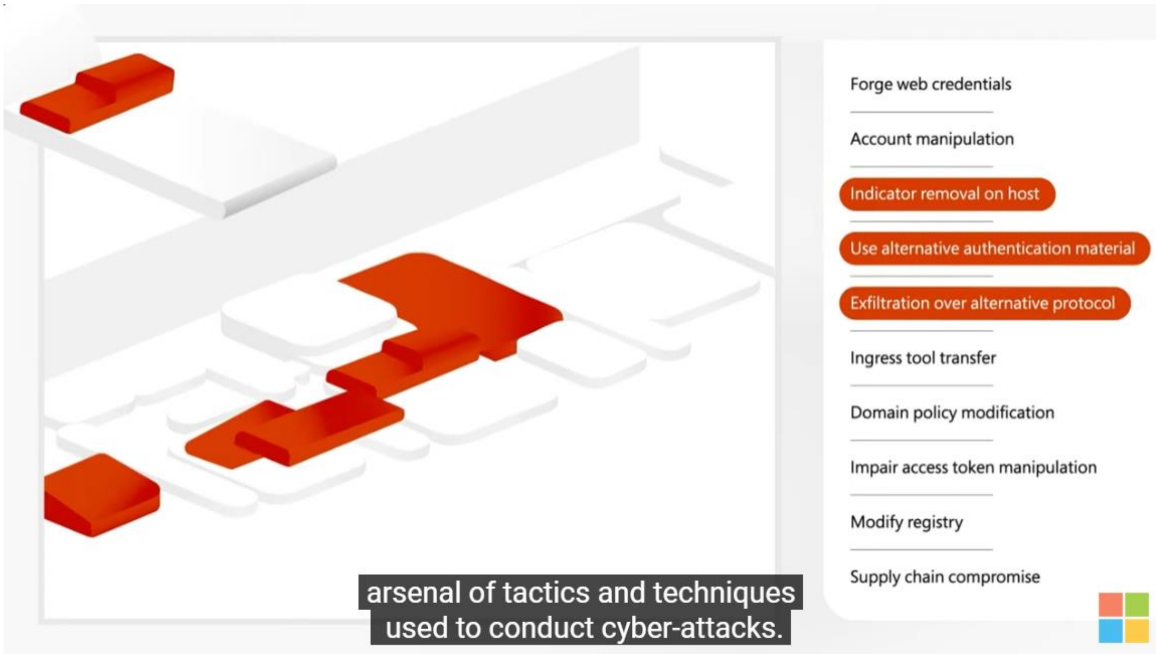
This will likely cause some level of disruption while we adapt to this new reality, but this is a necessary step, and only the first of several we will be taking to embrace this philosophy.

We are continuing our investigation and will take additional actions based on the outcomes of this investigation and will continue working with law enforcement and appropriate regulators.

We are deeply committed to sharing more information and our learnings, so that the community can benefit from both our experience and observations about the threat actor. We will provide additional details as appropriate.

To read more: https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

https://www.youtube.com/watch?v=wFtGD7p58cQ



Forge web credentials

Account manipulation

Indicator removal on host

Use alternative authentication material

Exfiltration over alternative protocol

Ingress tool transfer

Domain policy modification

Impair access token manipulation

Modify registry

Supply chain compromise

arsenal of tactics and techniques used to conduct cyber-attacks.

Number 4

Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021

While publicly reported and patched in October 2023, Mandiant and VMware Product Security have found UNC3886, a highly advanced China-nexus espionage group, has been exploiting CVE-2023-34048 as far back as late 2021.

These findings stem from Mandiant's continued research of the novel attack paths used by UNC3886, which historically focuses on technologies that are unable to have EDR deployed to them. UNC3886 has a track record of utilizing zero-day vulnerabilities to complete their mission without being detected, and this latest example further demonstrates their capabilities.

When covering the discovery of CVE-2023-20867 in VMware's tools, the attack path in Figure 1 was presented describing the flow of attacker activity within the VMware ecosystem (i.e. vCenter, ESXi Hypervisors, Virtualized Guest Machines). At the time, with the evidence available, Mandiant continued researching how backdoors were being deployed to vCenter systems.

To read more: https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021

Number 5

Operationalising the Framework for Evaluating Capability against Information Influence Operations

A Case Study of the Psychological Defence Agency's Courses

Evaluation is a crucial step in decision-making and strategic planning in most contemporary organisations. This should also be the case for the development of capability in countering information influence operations (IIO).

Different actors, ranging from governments to the private sector, have varying approaches to address these issues, as well as different evaluation norms and standards. However, evaluation of capabilities for countering IIO is a relatively new concept.

IIO capabilities, in a civilian context, include several functions and activities that need to be performed in a coordinated manner, by multiple actors and units, and over different timeframes.

It is therefore not always easy to know what kind of strategy and method should be used for assessment; often it differs depending on what is being assessed, the purpose of the assessment, and for whom it is made.

Still, without evaluating these capabilities an organisation might not use its resources efficiently or might not be working towards the required capability level.

Evaluation is therefore an important and necessary part of quality assurance, and a means for improving the work of the community as a whole.

An initial step was taken in 2022 to establish a common framework for evaluating capability in countering different threats in the information environment through the paper A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence and Foreign Interference written by James Pamment and published by the NATO Strategic Communications Centre of Excellence.

For this follow-up report, we focus on education and training to represent a starting point for applying the framework. Education and training are crucial components in developing a prepared and capable organisation.

The benefits of improving education and training capabilities are scalable across society. These benefits often reach beyond the specific area of focus, as individuals gain valuable skills and knowledge that can be applied in other areas of their personal and professional lives.

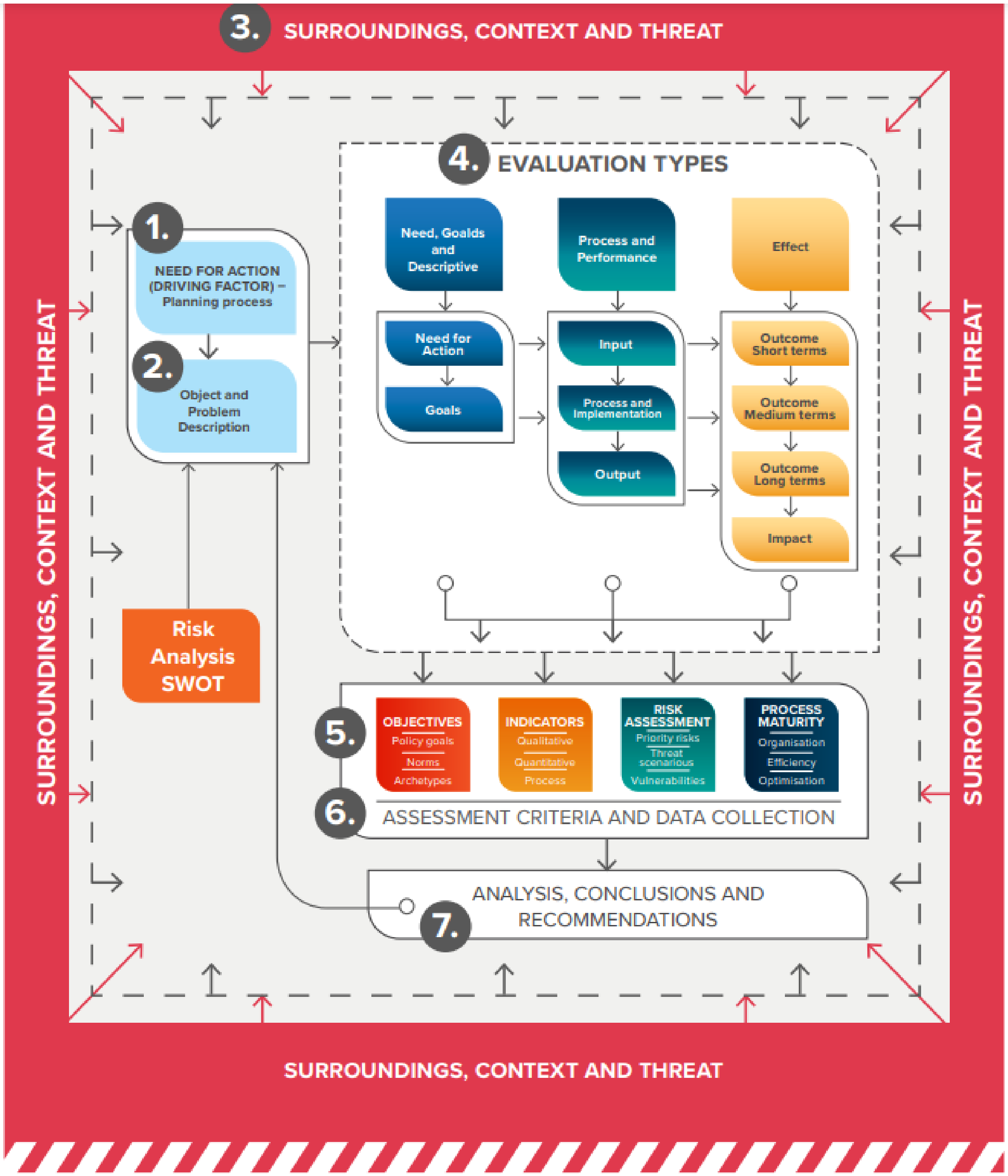


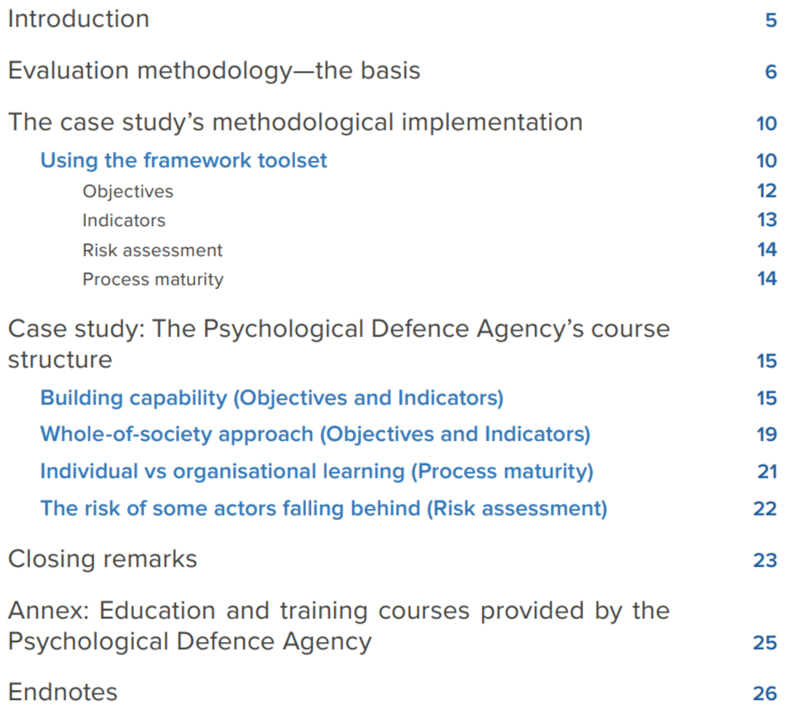
FIGURE 2. An example of an evaluation map that described the basis of evaluation methodology.

Improving education and training in one area of a community or part of the public can have a ripple effect on the entire society, making it a vital component to address.

This report presents an evaluation of the education and course structure of the Swedish Psychological Defence Agency (Myndigheten för psykologiskt försvar, MPF), in effect applying the framework to a concrete example.

The MPF was founded with the main objective of coordinating and developing the advancement of Sweden's psychological defence in partnership with public institutions and other stakeholders in society.

The aim of the report is to offer advice on how to deploy the evaluation methodology using the previous framework and also some best practice guidance on how to use the framework toolset in the evaluation process.



To read more: https://stratcomcoe.org/publications/operationalising-the-framework-for-evaluating-capability-against-information-influence-operations-a-case-study-of-the-psychological-defence-agencys-courses/295

Number 6

Pioneering a New National Security

GCHQ

Britain today is a digital nation, leading and shaping events across a world inextricably linked through cyberspace. Now and into the future, the value of our economy, our way of life, and our global influence will be built on our advanced digital infrastructure, capabilities and knowledge.

Artificial Intelligence – a form of software that can learn to solve problems at a scale and speed impossible for humans – is increasingly essential to the way we live. It is already transforming sectors as diverse as healthcare, telecommunications, and manufacturing.

AI software informs our satnavs, guides our internet searches, and protects us every time we make an electronic purchase, or open an app on our smartphone. In the century since it was founded, GCHQ has been at the forefront of innovation in national security.

Generations of brilliant analysts, with their diverse mix of minds, have used their technical ingenuity, cutting-edge technology and wide-ranging partnerships to identify, analyse and disrupt threats to our nation.

Today, as technological change continues to accelerate, we are pioneering new approaches to understanding the complex and interconnected world around us. We have long championed the responsible use of data science and believe that AI will be at the heart of our organisation's future.

Thinking about AI encourages us to think about ourselves, and what it means to be human: our preferred way of life, our guiding values and our common beliefs.

The field of AI ethics has emerged over the last decade to help organisations turn these ethical principles into practical guidance for software developers – helping to embed our core values within our computers and software.

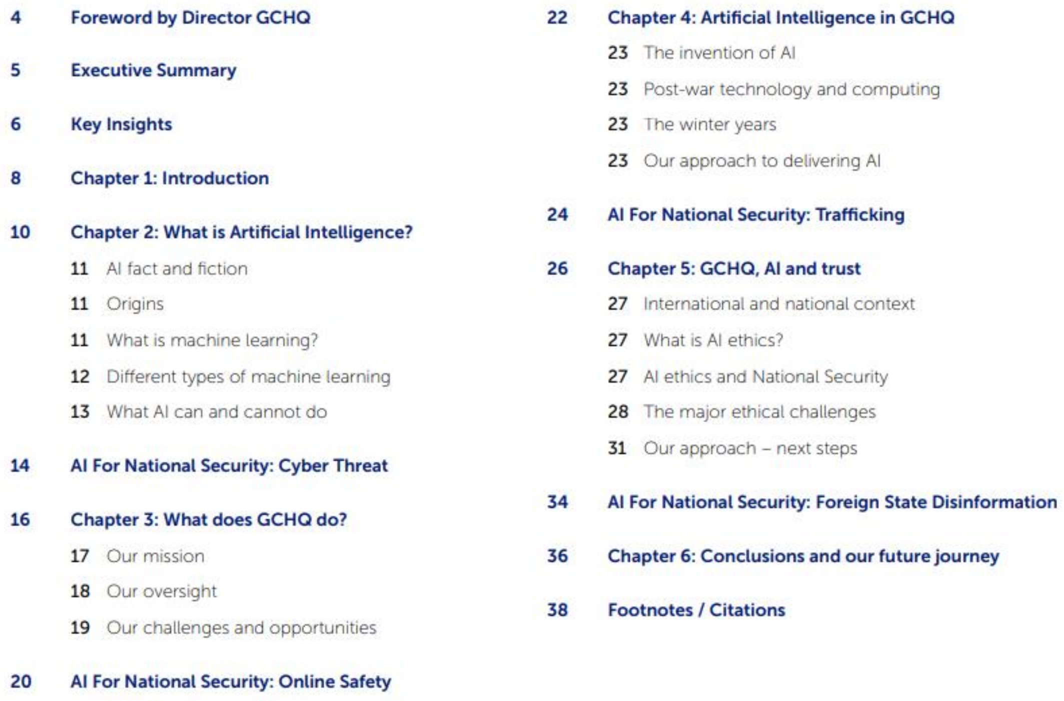
We won't pretend that there are not challenges ahead of us. In using AI we will strive to minimise and where possible eliminate biases, whether around gender, race, class or religion. We know that individuals pioneering this technology are shaped by their own personal experiences and backgrounds.

Acknowledging this is only the first step – we must go further and draw on a diverse mix of minds to develop, apply and govern our use of AI. Left unmanaged, our use of AI incorporates and reflects the beliefs and assumptions of its creators – AI systems are no better or no worse than the human beings that create them.

Our society is learning and growing: the Alan Turing Institute and similar bodies are helping to show us how we might build and use AI in a more ethical, responsible manner. GCHQ is committed to creating and using AI in a way that supports fairness, empowerment, transparency and accountability – and to protecting the nation from AI-enabled security threats pursued by our adversaries.

We believe that, by working together with our partners across Britain and beyond, we can deliver this vision.

This paper describes the digital Britain of today, and our values-led approach for the spaces where people, information and technology meet. It lays out GCHQ's AI and Data Ethics Framework, and how we intend to use AI in our operations. It forms part of our commitment to inclusion, debate and openness.



To read more: https://www.gchq.gov.uk/files/GCHQAIPaper.pdf

Number 7

NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

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

1. AI systems can malfunction when exposed to untrustworthy data, and attackers are exploiting this issue.

2. New guidance documents the types of these attacks, along with mitigation approaches.

3. No foolproof method exists as yet for protecting AI from misdirection, and AI developers and users should be wary of any who claim otherwise.

Adversaries can deliberately confuse or even "poison" artificial intelligence (AI) systems to make them malfunction — and there's no foolproof defense that their developers can employ. Computer scientists from the National Institute of Standards and Technology (NIST) and their collaborators identify these and other vulnerabilities of AI and machine learning (ML) in a new publication.

Their work, titled Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (NIST.AI.100-2), is part of NIST's broader effort to support the development of trustworthy AI, and it can help put NIST's AI Risk Management Framework into practice. The publication, a collaboration among government, academia and industry, is intended to help AI developers and users get a handle on the types of attacks they might expect along with approaches to mitigate them — with the understanding that there is no silver bullet.

"We are providing an overview of attack techniques and methodologies that consider all types of AI systems," said NIST computer scientist Apostol Vassilev, one of the publication's authors. "We also describe current mitigation strategies reported in the literature, but these available defenses currently lack robust assurances that they fully mitigate the risks. We are encouraging the community to come up with better defenses."

AI systems have permeated modern society, working in capacities ranging from driving vehicles to helping doctors diagnose illnesses to interacting with customers as online chatbots. To learn to perform these tasks, they are trained on vast quantities of data: An autonomous vehicle might be shown images of highways and streets with road signs, for example, while a chatbot based on a large language model (LLM) might be exposed to records of online conversations. This data helps the AI predict how to respond in a given situation.

One major issue is that the data itself may not be trustworthy. Its sources may be websites and interactions with the public. There are many opportunities for bad actors to corrupt this data — both during an AI system's training period and afterward, while the AI continues to refine its behaviors by interacting with the physical world. This can cause the AI to perform in an undesirable manner.

Chatbots, for example, might learn to respond with abusive or racist language when their guardrails get circumvented by carefully crafted malicious prompts.

“For the most part, software developers need more people to use their product so it can get better with exposure,” Vassilev said. “But there is no guarantee the exposure will be good. A chatbot can spew out bad or toxic information when prompted with carefully designed language.”

In part because the datasets used to train an AI are far too large for people to successfully monitor and filter, there is no foolproof way as yet to protect AI from misdirection. To assist the developer community, the new report offers an overview of the sorts of attacks its AI products might suffer and corresponding approaches to reduce the damage.

The report considers the four major types of attacks: evasion, poisoning, privacy and abuse attacks. It also classifies them according to multiple criteria such as the attacker’s goals and objectives, capabilities, and knowledge.

Evasion attacks, which occur after an AI system is deployed, attempt to alter an input to change how the system responds to it. Examples would include adding markings to stop signs to make an autonomous vehicle misinterpret them as speed limit signs or creating confusing lane markings to make the vehicle veer off the road.

Poisoning attacks occur in the training phase by introducing corrupted data. An example would be slipping numerous instances of inappropriate language into conversation records, so that a chatbot interprets these instances as common enough parlance to use in its own customer interactions.

Privacy attacks, which occur during deployment, are attempts to learn sensitive information about the AI or the data it was trained on in order to misuse it. An adversary can ask a chatbot numerous legitimate questions, and then use the answers to reverse engineer the model so as to find its weak spots — or guess at its sources. Adding undesired examples to those online sources could make the AI behave inappropriately, and making the AI unlearn those specific undesired examples after the fact can be difficult.

Abuse attacks involve the insertion of incorrect information into a source, such as a webpage or online document, that an AI then absorbs. Unlike the aforementioned poisoning attacks, abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source to repurpose the AI system’s intended use.

“Most of these attacks are fairly easy to mount and require minimum knowledge of the AI system and limited adversarial capabilities,” said co-author Alina Oprea, a professor at Northeastern University. “Poisoning attacks, for example, can be mounted by controlling a few dozen training samples, which would be a very small percentage of the entire training set.”

The authors — who also included Robust Intelligence Inc. researchers Alie Fordyce and Hyrum Anderson — break down each of these classes of attacks into subcategories and add approaches for mitigating them, though the publication acknowledges that the defenses AI experts have devised for adversarial attacks thus far are incomplete at best. Awareness of these limitations is important for developers and organizations looking to deploy and use AI technology, Vassilev said.

“Despite the significant progress AI and machine learning have made, these technologies are vulnerable to attacks that can cause spectacular failures with dire consequences,” he said. “There are theoretical problems with securing AI algorithms that simply haven’t been solved yet. If anyone says differently, they are selling snake oil.”

To read more: https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

Number 8

Testing the cognitive limits of large language models

Fernando Perez-Cruz and Hyun Song Shin

Key takeaways

1. When posed with a logical puzzle that demands reasoning about the knowledge of others and about counterfactuals, large language models (LLMs) display a distinctive and revealing pattern of failure.

2. The LLM performs flawlessly when presented with the original wording of the puzzle available on the internet but performs poorly when incidental details are changed, suggestive of a lack of true understanding of the underlying logic.

3. Our findings do not detract from the considerable progress in central bank applications of machine learning to data management, macro analysis and regulation/supervision. They do, however, suggest that caution should be exercised in deploying LLMs in contexts that demand rigorous reasoning in economic analysis.

The dazzling virtuosity of large language models (LLMs) has stirred the public imagination.

Generative pretrained transformer (GPT) and similar LLMs have demonstrated an impressive array of capabilities, ranging from generating computer code and images to solving complex mathematical problems.

However, even as users are dazzled by the virtuosity of large language models, a question that often crops up is whether they “know” or “understand” what they are saying, or – as argued by Bender and Koller (2020) – they are merely parroting text that they encountered on the internet during their extensive training routine.

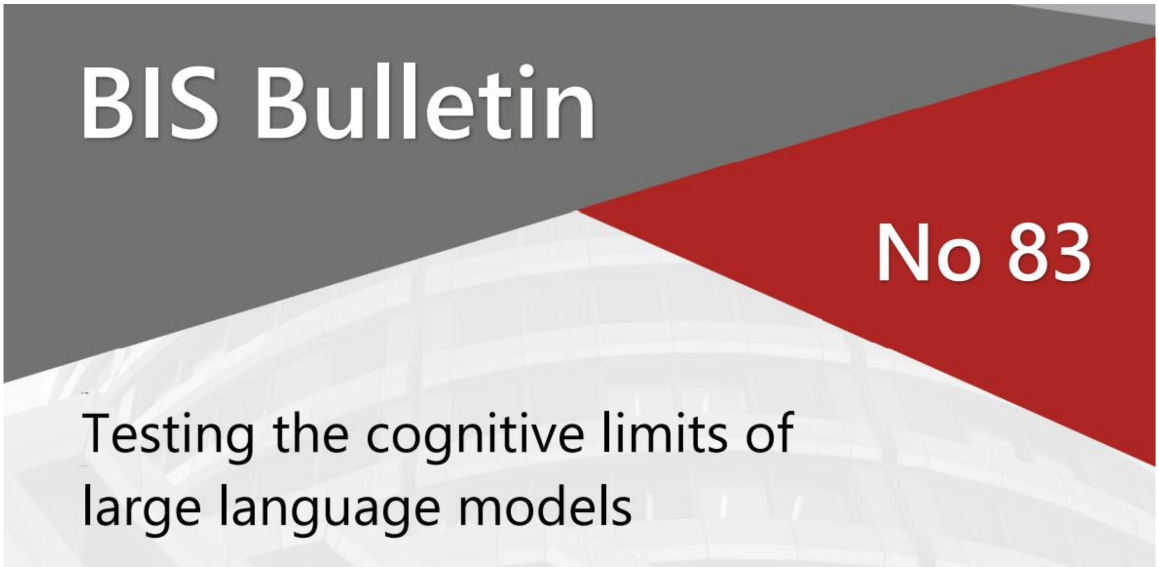
These questions are not only important in terms of the philosophy of knowledge but are likely to be crucial in assessing the eventual economic impact of LLMs.

Devising a test for self-awareness is not easy, but some questions can only be answered through the mastery of reasoning needed for situational awareness. In this spirit, we quizzed GPT-4 (Achiam et al (2023)) with the so-called Cheryl’s birthday puzzle.

This is a well-known logic puzzle which went viral in 2015 and has its own Wikipedia page.

Given the extensive online discussion, the latest LLMs will have encountered the puzzle and its solution as part of their extensive corpus of training text.

The solution to the puzzle necessitates reasoning about knowledge (both about one's own knowledge and that of others), as well as sophistication in counterfactual reasoning of the form: "p is false, but if it were true, then q would also be true."



BIS Bulletin

No 83

Testing the cognitive limits of large language models

To read more: https://www.bis.org/publ/bisbull83.pdf

https://www.bis.org/publ/bisbull83_annex.pdf

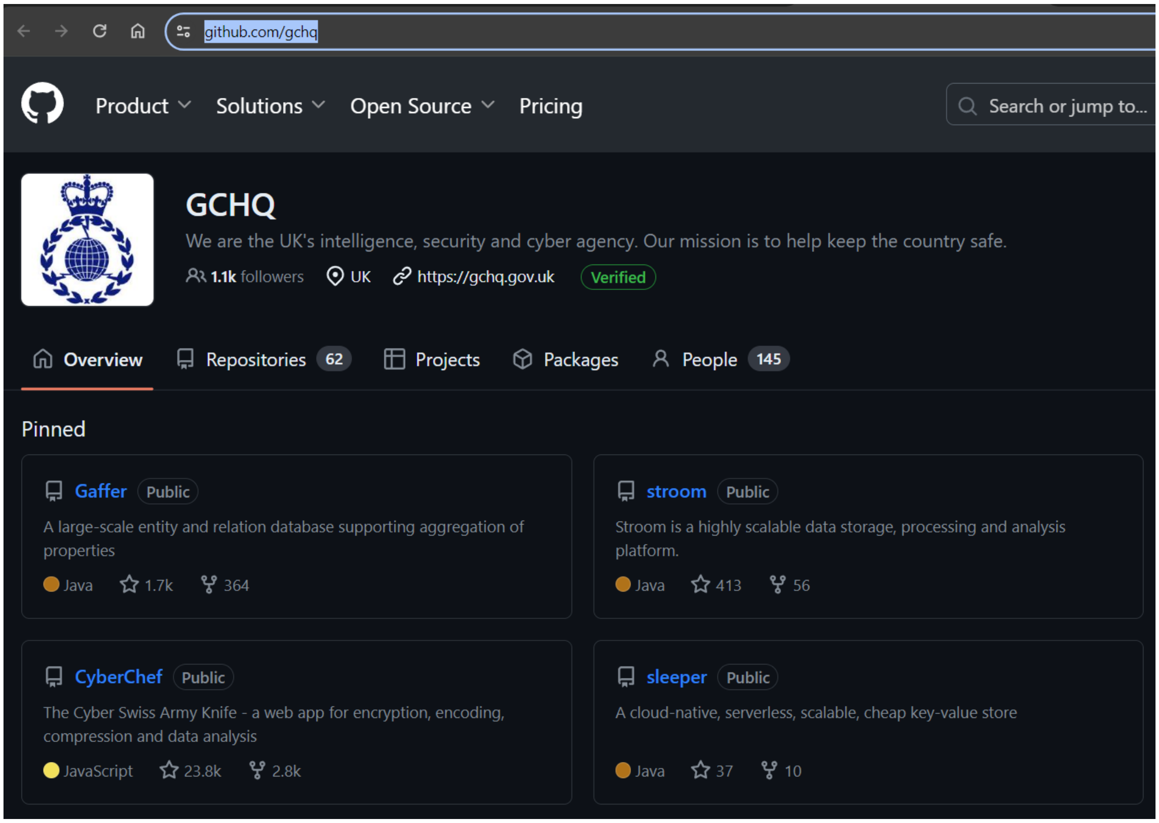
Number 9

GCHQ software and apps

GCHQ is a world-leading intelligence, cyber and security agency with a mission to keep the UK safe

Our software engineers have cooked up several open-source software packages and put them on #GitHub!

You can use for a whole range of technical tasks - from data analysis to encryption.



GCHQ

We are the UK's intelligence, security and cyber agency. Our mission is to help keep the country safe.

1.1k followers · UK · https://gchq.gov.uk · Verified

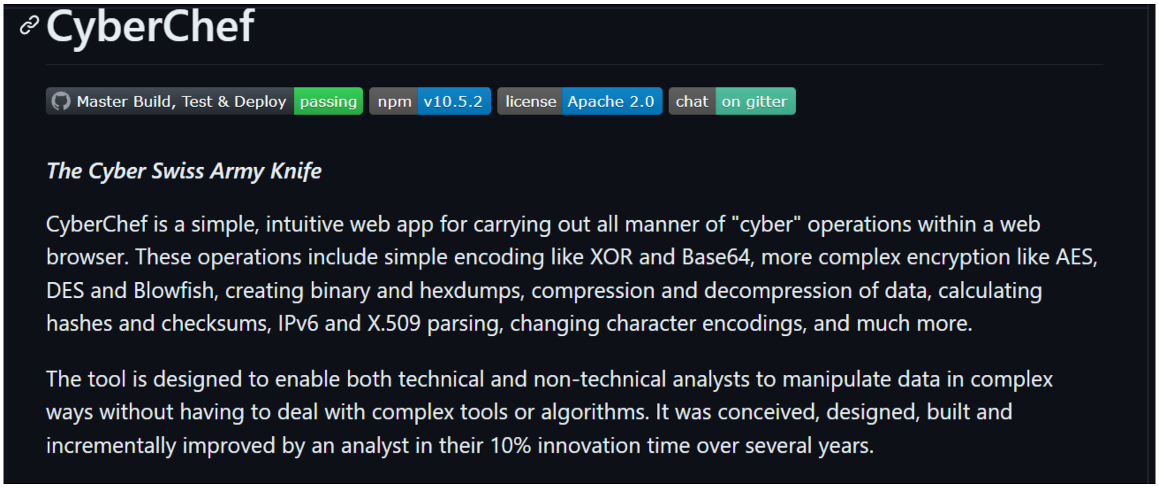
Pinned

Gaffer (Public) — A large-scale entity and relation database supporting aggregation of properties — Java, 1.7k stars, 364 forks

stroom (Public) — Stroom is a highly scalable data storage, processing and analysis platform. — Java, 413 stars, 56 forks

CyberChef (Public) — The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis — JavaScript, 23.8k stars, 2.8k forks

sleeper (Public) — A cloud-native, serverless, scalable, cheap key-value store — Java, 37 stars, 10 forks

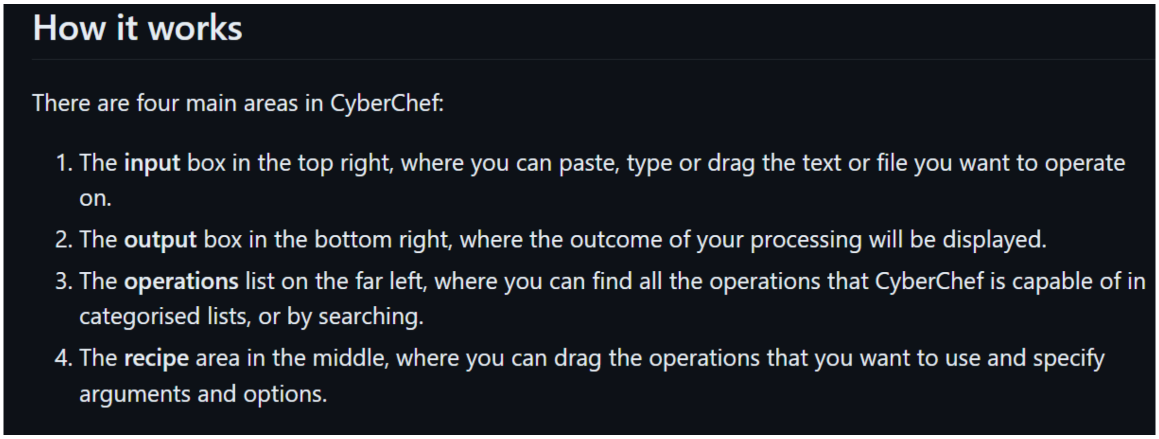


CyberChef

The Cyber Swiss Army Knife

CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser. These operations include simple encoding like XOR and Base64, more complex encryption like AES, DES and Blowfish, creating binary and hexdumps, compression and decompression of data, calculating hashes and checksums, IPv6 and X.509 parsing, changing character encodings, and much more.

The tool is designed to enable both technical and non-technical analysts to manipulate data in complex ways without having to deal with complex tools or algorithms. It was conceived, designed, built and incrementally improved by an analyst in their 10% innovation time over several years.



How it works

There are four main areas in CyberChef:

1. The **input** box in the top right, where you can paste, type or drag the text or file you want to operate on.
2. The **output** box in the bottom right, where the outcome of your processing will be displayed.
3. The **operations** list on the far left, where you can find all the operations that CyberChef is capable of in categorised lists, or by searching.
4. The **recipe** area in the middle, where you can drag the operations that you want to use and specify arguments and options.

You may visit: https://github.com/gchq

Number 10

2023 National Security Agency (NSA) Cybersecurity

NSA's new AI Security Center, housed at the Cybersecurity Collaboration Center will promote the secure development, integration, and adoption of AI capabilities within national security systems and the Defense Industrial Base (DIB).

This center will also leverage NSA's unique foreign signals intelligence insights to help industry understand how adversaries use and target AI.

By engaging leaders from U.S. industry, national labs, academia, in concert with the Intelligence Community, the DoD, and foreign partners, the AI Security Center will help develop AI security best practices and guidance.

NSA Cybersecurity protects and defends:

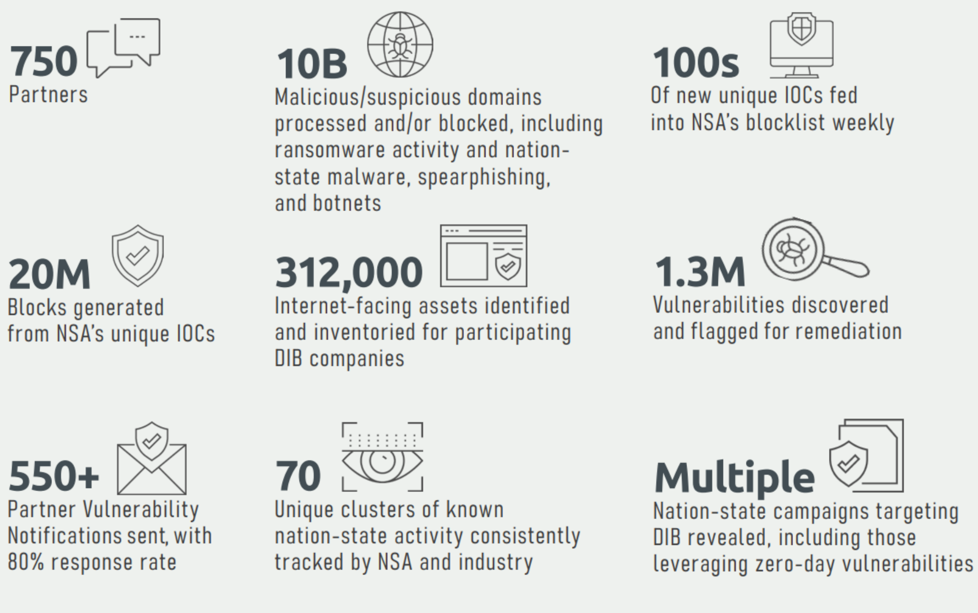
• National Security Systems (NSS): Networks that contain classified information or are otherwise critical to United States military and intelligence activities. It is vital that these networks remain secure to ensure U.S. warfighting capabilities are mission-ready and to protect the nation's most sensitive information.

• The Department of Defense (DoD): U.S. Military services and combatant commands as well as U.S. government agencies and departments related to national security.

• The Defense Industrial Base (DIB): The ever-growing group of companies that design, develop, operate, and maintain the Department of Defense's critical systems, platforms, and technologies required to defend the nation. Their products, services, and capabilities are vital to the security of the U.S. and our allies.

In an effort to be more transparent, NSA publishes an annual year in review sharing information regarding cybersecurity efforts that better equipped U.S. defenses against high priority cyber threats.

NSA's efforts to help secure the nation's most sensitive systems also help your cybersecurity because NSA cascades these solutions through public guidance and engages with key technology providers to help them bolster the security of their products and services.



750
Partners

10B
Malicious/suspicious domains processed and/or blocked, including ransomware activity and nation-state malware, spearphishing, and botnets

100s
Of new unique IOCs fed into NSA's blocklist weekly

20M
Blocks generated from NSA's unique IOCs

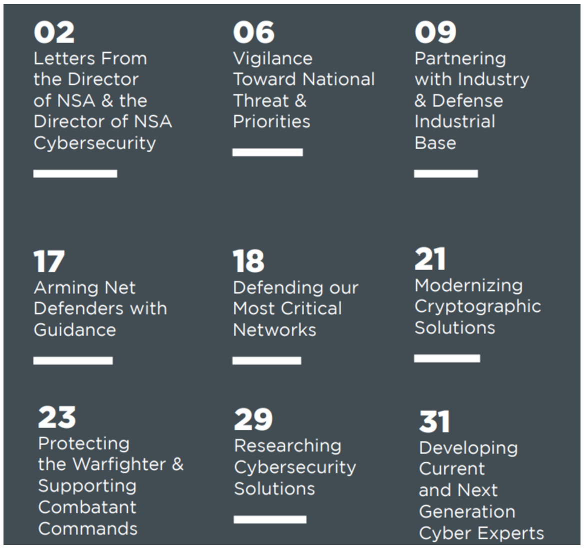
312,000
Internet-facing assets identified and inventoried for participating DIB companies

1.3M
Vulnerabilities discovered and flagged for remediation

550+
Partner Vulnerability Notifications sent, with 80% response rate

70
Unique clusters of known nation-state activity consistently tracked by NSA and industry

Multiple
Nation-state campaigns targeting DIB revealed, including those leveraging zero-day vulnerabilities



02 Letters From the Director of NSA & the Director of NSA Cybersecurity

06 Vigilance Toward National Threat & Priorities

09 Partnering with Industry & Defense Industrial Base

17 Arming Net Defenders with Guidance

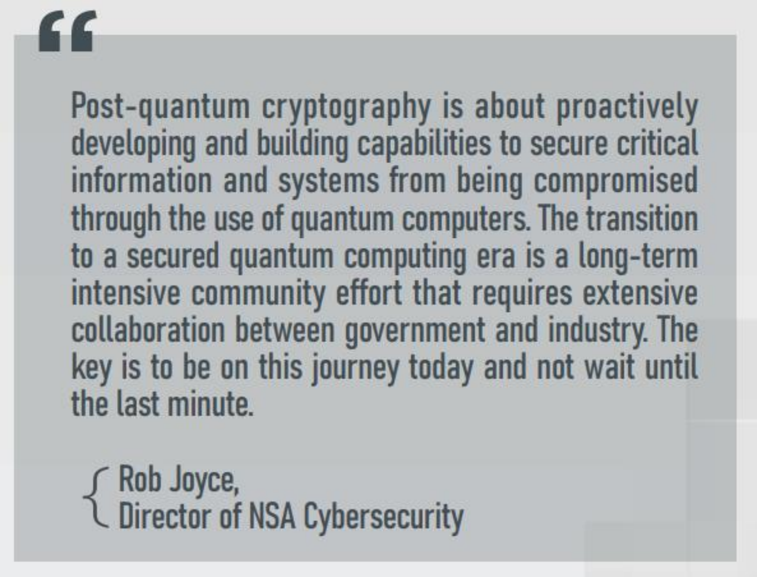
18 Defending our Most Critical Networks

21 Modernizing Cryptographic Solutions

23 Protecting the Warfighter & Supporting Combatant Commands

29 Researching Cybersecurity Solutions

31 Developing Current and Next Generation Cyber Experts



> Post-quantum cryptography is about proactively developing and building capabilities to secure critical information and systems from being compromised through the use of quantum computers. The transition to a secured quantum computing era is a long-term intensive community effort that requires extensive collaboration between government and industry. The key is to be on this journey today and not wait until the last minute.
>
> Rob Joyce,
> Director of NSA Cybersecurity

To read more: https://media.defense.gov/2023/Dec/19/2003362479/-1/-1/0/NSA%202023%20Cybersecurity%20Year%20In%20Review.PDF

Number 11

US Allies Offensive Cyber: Entrapment Risk or Entanglement Nuisance

Major Mikkel Storm Jensen, Ph.D.

THE CYBER DEFENSE REVIEW

Putin's threat to escalate the war in Ukraine in response to external interference presents a timely reason to reconsider who has the military means to trigger escalation and perhaps draw allies into the conflict.

In 1984, Glenn H. Snyder wrote an analysis of states' dilemmas in alliances with this issue at its core that has demonstrably had excellent explanatory and predictive power.

In the Cold War's technological strategic context of nuclear and conventional military means, he found that: "In general, entrapment is a more serious concern for the lesser allies than for the superpowers [...] because the superpowers have a much greater capacity for taking initiatives (notably nuclear initiatives)."

In NATO, the US controls much of the alliance's conventional military capabilities and most of its nuclear weapons. Applying Snyder's analysis, this vests the US with a sufficient level of control over NATO's crisis management, to minimize the US' risk of entrapment in conflicts.

Emergence of cyberspace as a new venue for military operations changes the US strategic environment. The US was initially NATO's only declared actor in cyberspace, but over the last decade more than half of NATO's members have begun developing offensive cyberspace operations (OCO) capabilities.

Based on Snyder's analysis, should the US add proliferation amongst friends and allies to its concerns over OCO proliferation amongst foes? The theoretical answer is "yes." Any increase in allies' potential for independent initiatives decreases US ability to control escalation, increasing the risk of entrapment.

The real-world answer depends on the degree to which OCO has the potential for strategic impact. The counterargument is that OCO's potential military impact even in a crisis would be insignificant, thereby rendering allies' independent deployment of OCO a manageable risk insofar as entangling an otherwise involuntary US.

Hence, the question is the relative magnitude of the entrapment threat from US allies' OCO: Do US allies' growing OCO capabilities constitute a credible risk for entrapment, or are they a mere entanglement nuisance? US' strategies do not provide an answer.
Since 2018, they have signaled a more active role for US OCO capabilities to serve as a deterrent, both above and below the threshold of armed conflict. As yet,

however, no guidance has been forthcoming as to how allies' OCO capabilities fit this intent.

Nor does the academic literature inform this subject, a void this article seeks to begin filling. Following a brief review of pertinent academic literature, this article presents the theoretical tools deployed.

After introducing mainly Snyder's analysis of alliance dilemmas, the theories are applied to the case of the US dominant position in NATO. The analysis then investigates OCO's influence on the outcomes of Snyder's analysis on entrapment by analyzing how the technical and operational attributes of military cyber capabilities effects differ from conventional and nuclear means.

It demonstrates how OCO are, in some respects, reasonable to analyze on par with nuclear weapons. The article then reviews the US-published statements and policies on her own and allies' OCO capabilities and compares with US policies during the late 1950s potential proliferation of nuclear weapons amongst NATO members.

To read more:
https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Fall/CDR_V8N3_Fall_2023_r3.pdf

THE CYBER DEFENSE REVIEW

Coalition Strategic Cyber Campaigns: Functional Engagement as Cyber Doctrine for Middle Power Statecraft
Joseph Szeman and Christian Leuprecht

Weaponizing Words: Using Technology to Proliferate Information Warfare
Dr. Craig Douglas Albert, Samantha Mullaney, Lt. Col. Joseph Huitt, Dr. Lance Y. Hunter, Lydia Snider

The Ukrainian Information and Cyber War
Dr. Chris Bronk, Gabriel Collins (J.D.), Prof. Dan Wallach

U.S. Allies Offensive Cyber: Entrapment Risk or Entanglement Nuisance
Maj. Mikkel Storm Jensen, Ph.D.

Risks to Zero Trust in a Federated Mission Partner Environment
Keith Strandell and Dr. Sudip Mittal

Competitive Advantage in the Russo-Ukraine War: Technological Potential Against a Kremlin Goliath
Capt. Melissa Vargas

Beyond "Bigger, Faster, Better:" Assessing Thinking About Artificial Intelligence and Cyber Conflict
Dr. Christopher Whyte

Number 12

ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

CISA has observed widespread and active exploitation of vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure solutions, hereafter referred to as "affected products."

Successful exploitation of the vulnerabilities in these affected products allows a malicious threat actor to move laterally, perform data exfiltration, and establish persistent system access, resulting in full compromise of target information systems.

CISA has determined these conditions pose an unacceptable risk to Federal Civilian Executive Branch (FCEB) agencies and require emergency action.

This determination is based on widespread exploitation of vulnerabilities by multiple threat actors, the prevalence of the affected products in the federal enterprise, the high potential for a compromise of agency information systems, the impact of a successful compromise, and the complexity of the proposed mitigations.

To read more: https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities

Number 13

FBI, Human Trafficking Prevention Month

Human trafficking is the illegal exploitation of a person. Anyone can be a victim of human trafficking, and it can occur in any U.S. community—cities, suburbs, and even rural areas. The FBI works human trafficking cases under its Crimes Against Children and Human Trafficking program. We take a trauma informed, victim-centered approach in investigating these cases.

In the United States, both U.S. residents and foreign nationals are being bought and sold like modern-day slaves. Traffickers use violence, manipulation, or false promises of well-paying jobs or romantic relationships to exploit victims. Victims are forced to work as prostitutes or to take jobs as migrant, domestic, restaurant, or factory workers with little or no pay. Human trafficking is a heinous crime that exploits the most vulnerable in society.

Under the human trafficking program, the FBI investigates:

1. Sex trafficking: When individuals are compelled by force, fraud, or coercion to engage in commercial sex acts. Sex trafficking of a minor occurs when the victim is under the age of 18. For cases involving minors, it is not necessary to prove force, fraud, or coercion.

2. Labor trafficking: When individuals are compelled by force, threats, or fraud to perform labor or service.

3. Domestic servitude: When individuals within a household appear to be nannies, housekeepers, or other types of domestic workers, but they are being controlled and exploited.

Human Trafficking Task Forces

The most effective way to investigate human trafficking is through a collaborative, multi-agency approach with our federal, state, local, and tribal partners.

1. FBI Child Exploitation and Human Trafficking Task Forces operate within nearly every FBI field office. The ultimate goal of these task forces is to recover victims and investigate traffickers at the state and federal level.

2. The Anti-Trafficking Coordination Team Initiative builds human trafficking enforcement efforts and enhances access to specialized human trafficking subject matter experts, leads, and intelligence. Each team

develops and implements a strategic action plan, which leads to high-impact federal investigations and prosecutions.

The initiative is a collaborative effort among the FBI, the Department of Justice, Department of Homeland Security, and Department of Labor. Twelve FBI field offices participate in the initiative, including Atlanta, Boston, Cleveland, El Paso, Kansas City, Los Angeles, Memphis, Miami, Minneapolis, Newark, Portland, and Sacramento.

3. The Enhanced Collaborative Model Human Trafficking Program is a multi-agency task force initiative funded through the Department of Justice's Office for Victims of Crime and Bureau of Justice Assistance.

   This program supports the development and enhancement of multi-disciplinary human trafficking task forces that implement collaborative approaches to combat all forms of human trafficking.

   These multi-disciplinary task forces include members from the U.S. Attorney's Office, local prosecutor's office, federal law enforcement, state/local law enforcement, and a community service provider, with the goal of proactively identifying and recovering victims of human trafficking.

To read more: https://www.fbi.gov/investigate/violent-crime/human-trafficking

Number 14

CISA and ENISA enhance their Cooperation

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Geopolitics have shaped the cyber threat landscape, bringing like-minded partners closer together in the wake of common cyber challenges and advances in digital technologies.

At the EU-US Cyber Dialogue, ENISA and CISA announced the signing of their Working Arrangement as an important milestone in the overall cooperation between the United States and the European Union in the field of cybersecurity, also following the Joint Statement of European Commissioner Thierry Breton and U.S. Secretary for Homeland Security Alejandro Mayorkas of January 2023.

CISA AND ENISA TO ENHANCE THEIR COOPERATION
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

ENISA’s International Strategy directs the Agency to be selective in engaging with international partners and to limit its overall approach in international cooperation to those areas and activities that will have high and measurable added value in achieving the Agency’s strategic objectives.

CISA is a key partner to ENISA in achieving these objectives and by extension the EU in achieving a higher common level of cybersecurity.

The Working Arrangement is both a consolidation of present areas of cooperation, as well as opening the door to new ones.

Current examples are the organisation and promotion of the International Cybersecurity Challenge (ICC), exchanging best practices in the area of incident reporting or ad hoc information exchanges on basic cyber threats.

This arrangement is broad in nature and covers both short-term structured cooperation actions, as well as paving the way for longer-term cooperation in cybersecurity policies and implementation approaches.

Cooperation will be sought in the areas of:

1. Cyber Awareness & Capacity Building to enhance cyber resilience: including facilitating the participation as third country representatives in specific EU-wide cybersecurity exercises or trainings and the sharing and promotion of cyber awareness tools and programmes.

2. Best practice exchange in the implementation of cyber legislation; including on key cyber legislation implementation such as the NIS Directive, incident reporting, vulnerabilities management and the approach to sectors such as telecommunications and energy.

3. Knowledge and information sharing to increase common situational awareness: including a more systematic sharing of knowledge and information in relation to the cybersecurity threat landscape to increase the common situational awareness to the stakeholders and communities and in full respect of data protection requirements.

A work plan will operationalise the Working Arrangement and regular reporting at the EU-US Cyber Dialogues is foreseen.

To read more: https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation

Number 15

Voices from DARPA

Podcast Episode 75: The Metamaterial Visionary

Program manager in DARPA’s Defense Sciences Office highlights fascinating optics programs made possible by novel engineered materials

We usually think of materials based on our experience in the natural world. For example, something that’s light is usually fragile (like a feather) or something heavy is usually strong (like a brick).

But what if we could engineer a material that had completely new characteristics that defied properties found in nature?

Engineered materials, also known as metamaterials, allow us to do just that. DARPA Program Manager Dr. Rohith Chandrasekar in DARPA’s Defense Sciences Office has led programs designing metamaterials that revolutionize how light interacts with matter.

His programs are enabling new concepts for improving Warfighter effectiveness and health on the battlefield with new optics and materials.

In this episode, Dr. Chandrasekar discusses several of these programs including Enhanced Night Vision in Eyeglass Form (ENVision), which has developed metamaterials to replace heavy and bulky binocular-like night-vision goggles lenses with lightweight lenses providing more infrared information and near eyesight field of view, in a form factor like a pair of glasses.

He also discusses his Coded Visibility program, which focused on developing novel obscurants (aka smoke) used on the battlefield to provide friendly forces with visibility of the environment, while simultaneously hiding them from detection by an adversary.

The catch, however, is that the smoke particles needed to be safe to breathe and potentially even tunable using active sources. Finally, he talks about the Accelerating discovery of Tunable Optical Materials (ATOM) program.

This effort seeks to identify new materials whose properties could be rapidly changed to enable different functions.

Imagine a massive telephoto camera on the sideline of a sporting event replaced with a planar imaging system that could zoom, or a thin filter that can rapidly collect critical data across infrared bands for spectroscopy, all with no moving parts.

Sounds like magic, but it’s not! Enjoy listening to DARPA’s Metamaterial Visionary.

To find more: https://www.youtube.com/watch?v=FK15MTLfY5w

Number 16

Ghidra

You can download NSA's reverse engineering tool that helps cybersecurity professionals analyze malicious code and malware like viruses and gives them a better understanding of potential vulnerabilities in their networks and systems.

Ghidra is one of many open-source software (OSS) projects developed within the National Security Agency. Complete source code for Ghidra along with build instructions have been added to the repository. Please read the updated CONTRIBUTING guide to find out more about how you can join the community.

To read more: https://www.nsa.gov/Cybersecurity/Cybersecurity-Products-Services/

Disclaimer

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

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

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

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

This information:

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

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

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

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

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

- is in no way constitutive of interpretative;

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

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

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

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

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

Cyber Risk GmbH

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

Cyber Risk GmbH offers:

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

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

Instructor-led training in Baur au Lac, Zurich

BAUR AU LAC

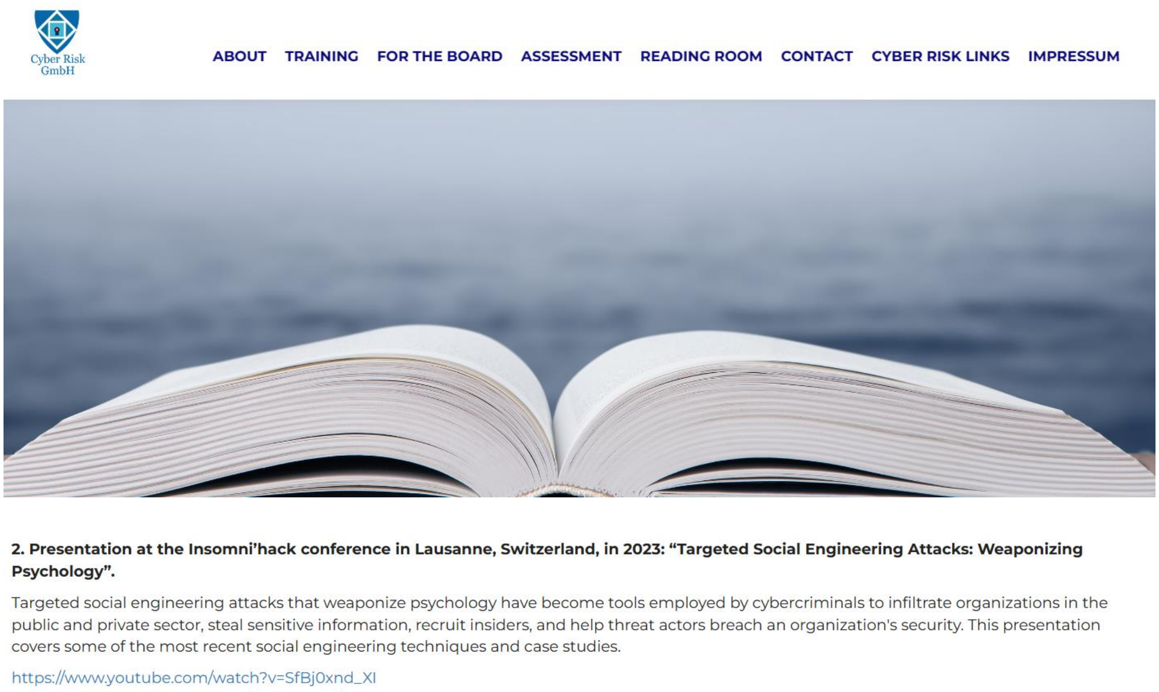
- Great training, exceptional venues.
- Presentations for the Board and the C-Suite.

CEO Briefings in Baur au Lac, Zurich

BAUR AU LAC

- CEO Briefings, answering the questions of the CEO.

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



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

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

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

Our websites include:

a. Sectors and Industries.

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

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

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

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

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

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

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

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

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

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

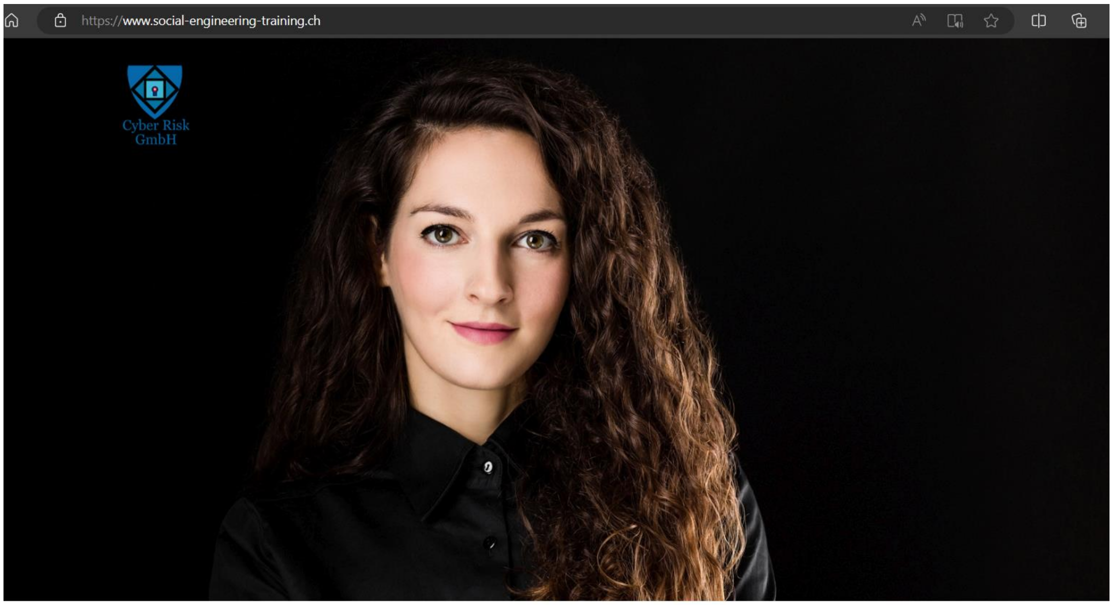
11. Transport Cybersecurity - https://www.transport-cybersecurity.com

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

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

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

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



b. Understanding Cybersecurity.

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

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

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

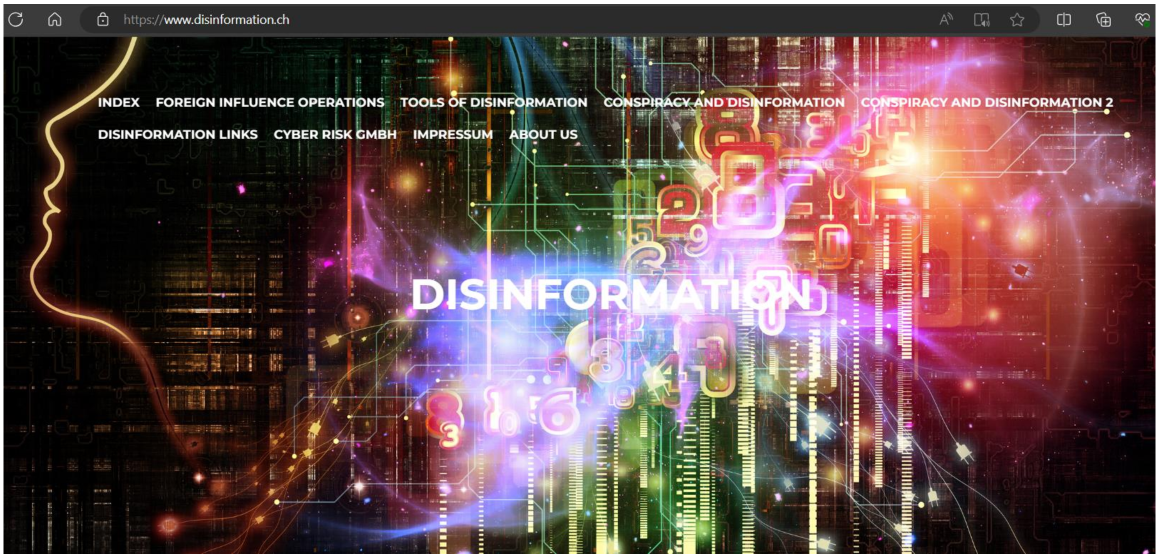
4. What is Synthetic Identity Fraud? - https://www.synthetic-identity-fraud.com

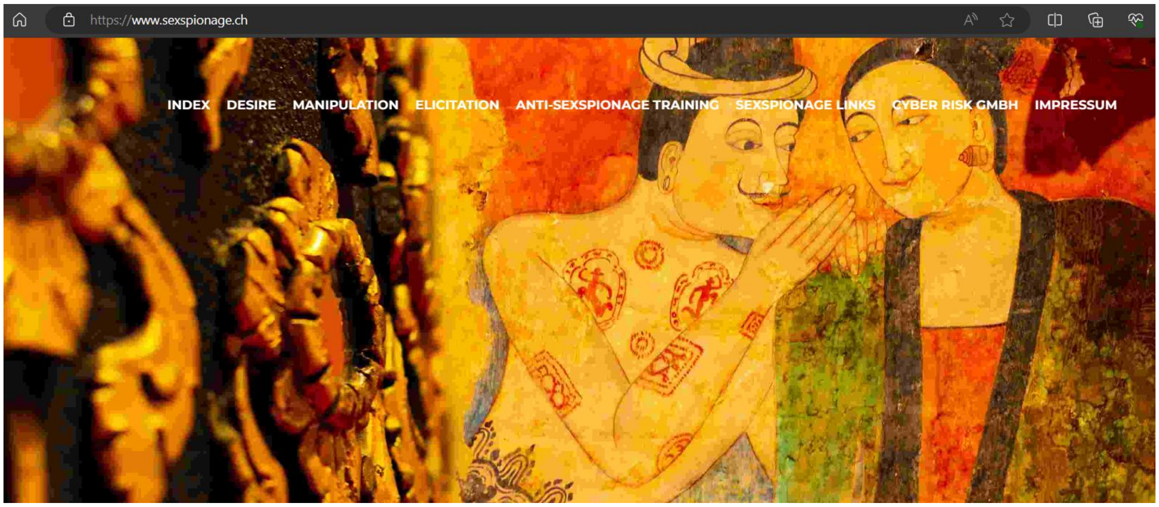
5. What is a Romance Scam? - https://www.romance-scams.ch

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

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

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


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



c. Understanding Cybersecurity in the European Union.

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

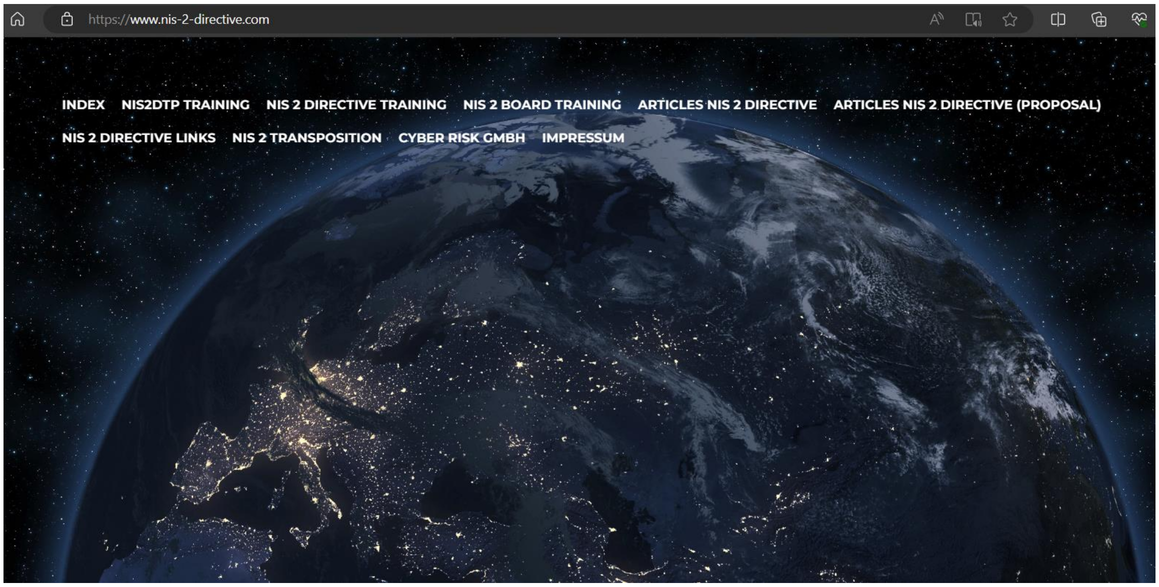
2. The European Cyber Resilience Act - https://www.european-cyber-resilience-act.com

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

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

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

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



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

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

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

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

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

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

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

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

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

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

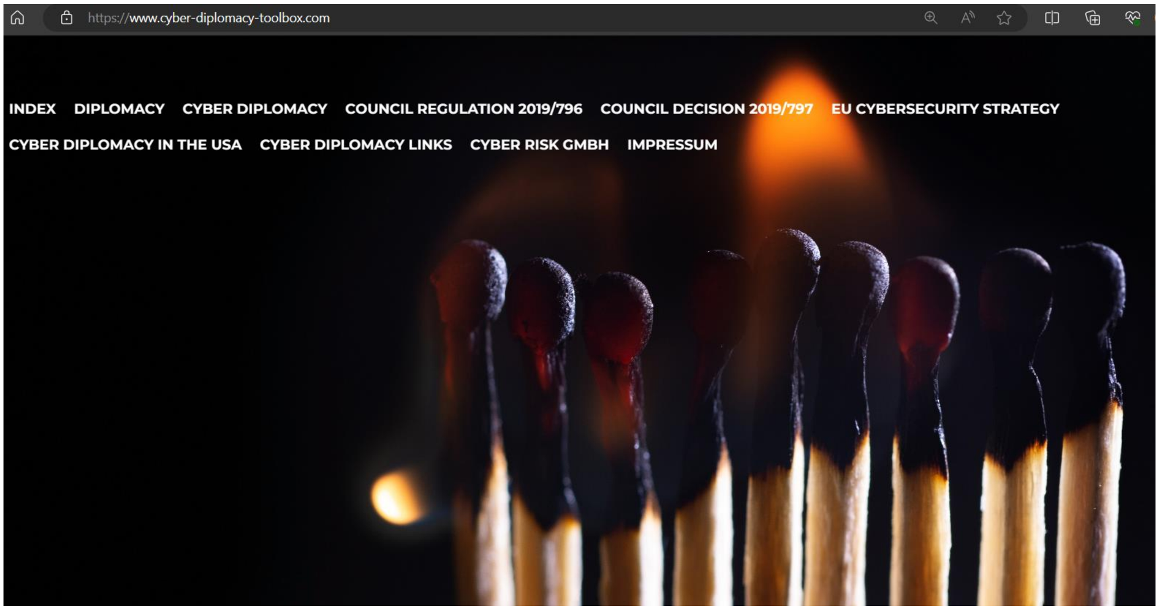
17. The European Digital Identity Regulation - https://www.european-digital-identity-regulation.com

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

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

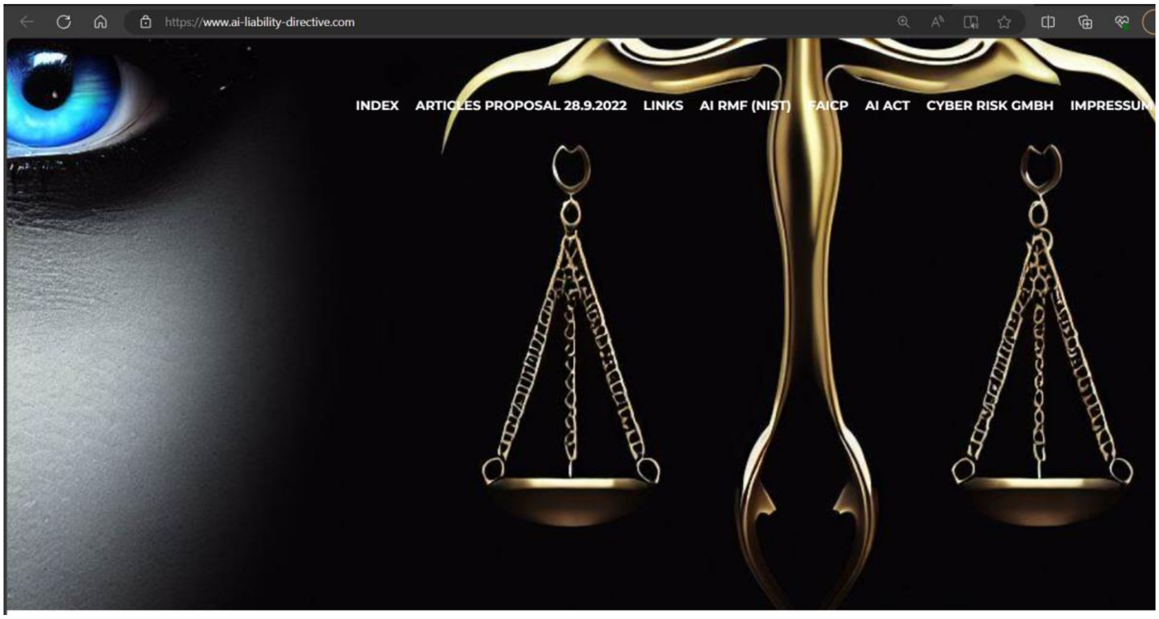
20. The Strategic Compass of the European Union https://www.strategic-compass-european-union.com

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


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

You may contact:

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


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