

Schweizer Radio Und Fernsehen (SRF), “Social Engineers und ihr Lieblingsnetzwerk”, with Christina Lekati (47 minutes). You may visit: <https://www.srf.ch/audio/digital-podcast/social-engineers-und-ihr-lieblingsnetzwerk?id=12484536>

Cyber Risk and Compliance News and Alerts, November 2023

Every problem has perhaps one or more solutions, but every solution is the source of new problems. In IT, every line of code that solves a problem is a new risk.

Leonardo da Vinci believed that *learning never exhausts the mind*. I am not sure he would still believe that today. I have just read an article with the title “*Can Math Secure Mixed Reality Systems from Attack?*” (you will find more at numbers 9 and 10 below). It took me some time to understand the terms and concepts described in this article.



But what is **mixed reality**? According to Microsoft, mixed reality is a blend of physical and digital worlds, unlocking natural and intuitive 3D human, computer, and environmental interactions. This new reality is based on advancements in computer vision, graphical processing, display technologies, input systems, and cloud computing.

Mixed reality is the **next wave** in computing following mainframes, PCs, and smartphones. It blends physical and digital worlds. These two realities mark the polar ends of a spectrum known as the **virtuality continuum**. We refer to this spectrum of realities as the mixed reality spectrum. On one end of the spectrum, we have the physical reality that we as humans exist. On the other end of the spectrum, we have the corresponding digital reality.

According to the Johns Hopkins University Applied Physics Laboratory, **cognitive engineering** is a multidisciplinary endeavour concerned with the analysis, design, and evaluation of complex systems of people and technology. It combines knowledge and experience from cognitive science, human factors, human-computer interaction design, and systems engineering.

Situation awareness (SA) is increasingly using cognitive engineering. It addresses the state or character of an operator's (like a pilot's) engagement with his/her operational environment, within the context of a task.

Cyberspace has become both, **the battlefield and the object of a battle**. In Information Warfare, acting against information systems (and their associated communications assets) is necessary, in order to affect an adversary's ability to interpret, understand, and act. And here comes cybersecurity.

Read more at number 9 and 10 below.

In their first-ever joint public appearance, leaders of the Five Eyes intelligence partnership (the United States, the United Kingdom, Canada, Australia, and New Zealand) travelled to the U.S. at the invitation of FBI Director Christopher Wray and launched the first Emerging Technology and Securing Innovation Security Summit in Palo Alto, California.

The heads of the Australian Security Intelligence Organisation (ASIO), the Canadian Security Intelligence Service (CSIS), the Federal Bureau of Investigations (FBI), MI5, and the New Zealand Security Intelligence Service (NZSIS) unveiled **five principles** which **businesses** can adopt to help keep their staff and their information safe and secure.

What are the five Principles of Secure Innovation?

1. Know the Threats

Understand the way state-backed and hostile actors could try and get hold of your technology.

2. Secure your Environment

Create an effective system for security risk management, incorporating risk ownership, identification, assessment, and mitigation.

3. Secure your Products

Build security into your products from the start, and actively protect and manage your intellectual assets.

4. Secure your Partnerships

Manage the risks that partnerships with investors, suppliers, and collaborators can bring.

5. Secure your Growth

As your company grows, manage the security risks from entering new markets and expanding your workforce.

FIVE PRINCIPLES TO SECURE INNOVATION

- 1. KNOW THE THREATS**
 We want to support you to innovate and collaborate in a way that keeps your organization safe and secure.
 There are many ways a state-backed or hostile actor could try to get hold of innovations or technologies:
 - Insider
 - Cyber
 - Physical
 - International Travel
 - Investment
 - Overseas jurisdictions
 - Supply chain
- 2. SECURE YOUR BUSINESS ENVIRONMENT**
 Effective protective security requires management of the security risks a business faces.
 Ownership: Appoint a board-level security lead who factors security into business decisions and initiates a security dialogue within the business.
 Identification: Identify your business-critical assets and the threats to them.
 Assessment: Assess security risks alongside other risks to your business.
 Mitigation: Protect your critical assets using physical and virtual barriers, access controls and detection and plan your response should something go wrong.
- 3. SECURE YOUR PRODUCTS**
 You should ensure the products and services your business is developing are secure, and that you are actively protecting and managing your intellectual assets and expertise.
 Secure by default: Embed security in your products and services to keep your customers safe and develop a more secure society.
 IP management: Identifying and actively managing intellectual assets, property and your business's expertise will help maintain the novelty and commercial value of your business's innovation.
- 4. SECURE YOUR PARTNERSHIPS**
 To operate securely, your company should manage the risks that partnerships with investors, suppliers and collaborators bring.
 Background checks: Your business should know who you are working with.
 Share with intent: Take a strategic approach to what you are sharing with partners, investors and potential investors.
 Legal protections: Include protections for assets and data within contracts.
- 5. SECURE YOUR GROWTH**
 As your company grows, additional security risks arise which need to be managed.
 Entering new markets: As you enter international markets, you will need to consider export controls, jurisdiction risk and travel security.
 Expanding workforce: Growing companies will need to introduce pre-employment screening and security training, and work on developing or maintaining your security culture as your organization changes.

The Five Eyes coalition grew from the 1946 BRUSA agreement, shortly after the end of World War II, to share intelligence and coordinate security efforts. The five member countries have a long history of trust and cooperation, and they share a commitment to common values.

The partnership has played a significant role in global security over the past seven decades, strengthening intelligence-sharing and cooperation among its member countries in order to protect their national security and common interests.

The security services are focused on countering a range of threats, including terrorism, cybersecurity, weapons proliferation, organized crime, and state-backed espionage and interference.

Read more at number 20 below.

This is a very good definition: “Resolution is the process of managing a financial institution in failure, with the purpose to minimise the impact on the financial system and the public purse.

The objective of an effective resolution regime is to make the resolution of financial institutions feasible without severe systemic disruption and

without exposing taxpayers to loss. A resolution must maintain vital economic functions through mechanisms which make it possible for shareholders and unsecured and uninsured creditors to absorb losses in a manner that respects the hierarchy of claims in liquidation.”

This is part of the paper “2023 Bank Failures - Preliminary lessons learnt for resolution” from the Financial Stability Board (FSB).

The paper also covers another area of concern: *Non-Global Systemically Important Banks (non-G-SIBs) resolution and the US bank failures*.

The failures of Silicon Valley Bank (SVB), Signature Bank and First Republic Bank showed that banks not identified as G-SIBs can still be systemically significant or critical upon failure.

For instance, the failure of such institutions could give rise to customer and counterparty behaviour that adversely impacts other institutions perceived by the market as peers.

The three US regional banks were effectively resolved without bailing out shareholders and unsecured creditors. This was done using existing powers and tools such as the set-up of bridge banks and use of the systemic risk exception (the latter tool only for SVB and Signature Bank) as well as the set-up of a new, temporary bank term funding program by the Federal Reserve.

The speed of recent runs is a major observation and challenge to emerge from some of the recent cases. The [ubiquity of social media and mobile banking](#) may mean that bank runs (which are more likely in cases of high concentration of uninsured deposits), when they happen, happen faster.

Whilst the core problems of the banks themselves may be different (e.g., poor management practices, asset quality, etc.), once a bank run has gathered pace, it becomes extremely challenging to halt outflows.

Considering how firms (and authorities) can maintain credibility in the face of such a run should be a key consideration going forward. The [role of social media](#) in the SVB depositor run illustrates the dynamics that can arise.

[Social media posts advised depositors to withdraw](#) funds from SVB, and many uninsured depositors did so all at once.

The concentration of these large deposits in technology firms and individuals who appear to have been part of closely overlapping virtual communities may have contributed to the synchronised nature of the deposit outflows.

Furthermore, the brevity of the runway period for both SVB and Signature Bank challenged the FDIC's abilities to complete all pre-failure marketing preparations, which are meant to prevent contagion and preserve franchise value.

Authorities may experience similar challenges in the future, especially with the continued innovation of payment systems and information sharing technologies.

Similar observations were made with regard to **Credit Suisse's** most severe liquidity outflow periods in October 2022 and March 2023. The ease of using 24/7 available digital banking applications allowed depositors to withdraw funds even during weekends.

The associated dynamics made predictions of liquidity movements more difficult and allowed for very large deposit withdrawals within hours.

Ovid believed that "minds that are ill at ease, are agitated by both hope and fear". The social media have changed the game.

Read more at number 5 below.

I find some parts of the new executive order very interesting.

On October 30, 2023, the US President Joe Biden signed the first Executive Order (EO) focusing on safe, secure and trustworthy **Artificial Intelligence**.

According to the EO, the term "**crime forecasting**" means the use of analytical techniques to attempt to predict future crimes or crime-related information. It can include machine-generated predictions that use algorithms to analyze large volumes of data, as well as other forecasts that are generated **without** machines and based on statistics, such as historical crime statistics.

The term "**commercially available information**" means any information or data about an individual or group of individuals, including an individual's or group of individuals' device or location, that is made available or **obtainable** and sold, leased, or licensed to the general public or to governmental or non-governmental entities.

The term "**synthetic biology**" means a field of science that involves **redesigning** organisms, or the biomolecules of organisms, at the genetic level to give them new characteristics. Synthetic nucleic acids are a type of biomolecule redesigned through synthetic-biology methods.

According to the EO, the Secretary of Homeland Security shall establish an **Artificial Intelligence Safety and Security Board** as an advisory committee.

The Advisory Committee shall include AI experts from the private sector, academia, and government, as appropriate, and provide to the Secretary of Homeland Security and the Federal Government's critical infrastructure community advice, information, or recommendations for improving **security, resilience, and incident response** related to AI usage in critical infrastructure.

You can find more at: <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>

The same time, we have the G7 Leaders' Statement on the *Hiroshima AI Process* about International Guiding Principles for Organizations Developing Advanced AI Systems. We read:

“We, the Leaders of the Group of Seven (G7), stress the innovative opportunities and transformative potential of advanced Artificial Intelligence (AI) systems, in particular, foundation models and generative AI. We also recognize the need to manage risks and to protect individuals, society, and our shared principles including the rule of law and democratic values, keeping humankind at the center.”

Read more at number 7, 8, 11 below.

In Switzerland, we have an excellent post from the Swiss National Cyber Security Centre (NCSC). The NCSC is the Confederation's competence centre for cybersecurity and thus the first contact point for businesses, public administrations, educational institutions and the general public for cyber related issues.

A number of **phishing** cases were reported to the NCSC. Fraudsters continue to target customers of parcel, telephony and transport service providers very frequently. But there are also two **less common** phishing scams.

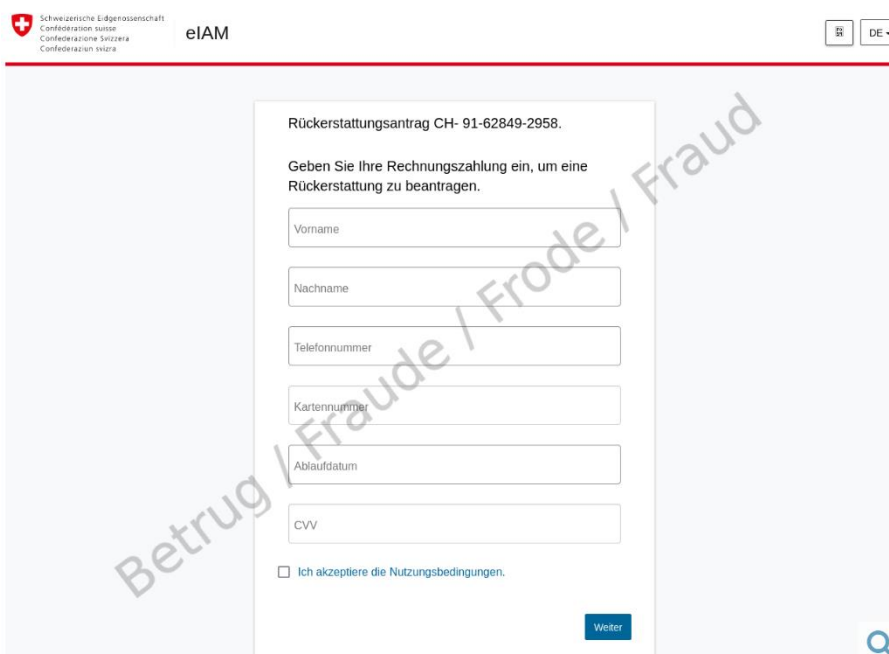
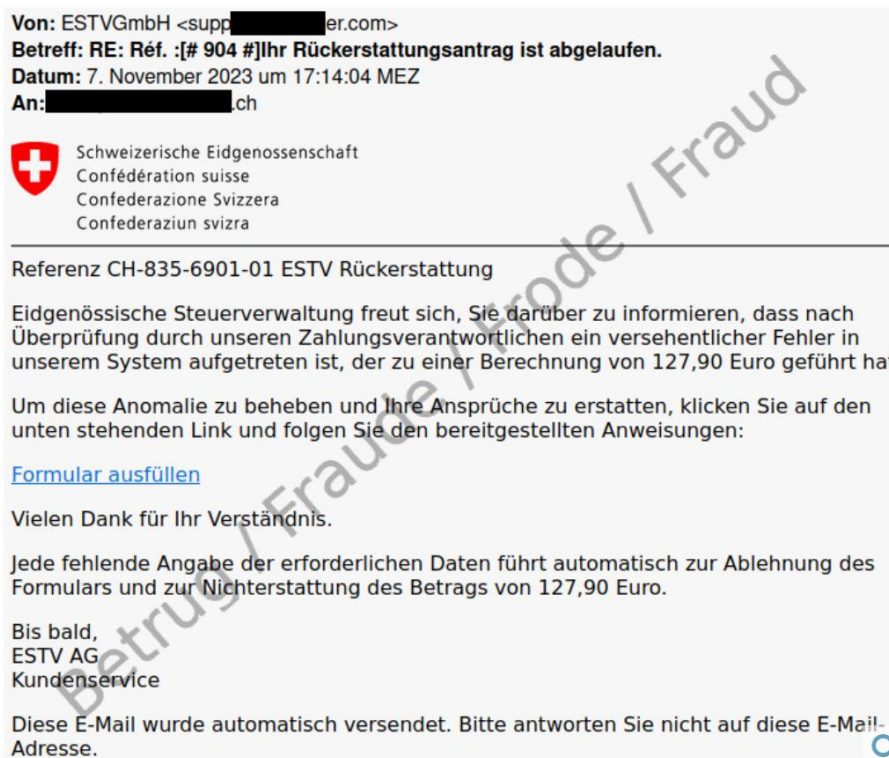
Purported tax refund

An email claims that the recipient is entitled to a credit note (refund) from the Federal Tax Administration (FTA). The following image shows such an email. However, the sender, which does not look at all like it is the FTA, is enough to make anyone suspicious. Even if you do not know the exact domain of the FTA, federal services and websites are **always found at admin.ch, never at *.com**.

If you move the mouse over the link (without clicking), the URL to which the link would lead is displayed. Here too, the URL/target domain have no connection with the FTA. Even just one of these features alone (sender or URL) indicates that this is a fraud attempt.

If you take a closer look at the email, you will notice that the fraudsters have made a number of mistakes:

- The FTA is not a GmbH or AG.
- Any tax refunds would be made in Swiss francs and not in euros.
- The language used in the email does not reflect that of an official notification from the authorities.



But what happens if you are tempted to click on the link? A page opens that imitates the eIAM service. eIAM is the Federal Administration's central access and authorisation system for web applications.

However, this is only an intermediate step. Once you have entered an email address, a screen for entering credit card details appears. The real eIAM service would require authentication with at least a password.

To continue with the fraudulent process, it is sufficient to enter the credit card number and the CVV code – this shows the fraudsters' intentions.

Further alarm bells should ring for the potential victim at this point at the latest: for a standard refund, a credit card number is of course never requested, but rather an IBAN (account number).

The fraudsters then try to go one step further.

To be able to debit the card, they need confirmation from the card owner, which is often sent to the legitimate owner's mobile phone by text message.

They immediately ask for this code.

CH-LOGIN
& bring your own identity
eGovernment

Mobile Verifizierung

Um die Rückerstattung zu bestätigen, geben Sie bitte das an Ihre Mobiltelefonnummer gesendete OTP ein.

Geben Sie hier OTP ein

Der über OTP erhaltene Betrag wird umgehend zurückerstattet.

Verifizieren

If the victim enters all this data, the attackers can take control of the credit card and make purchases in the victim's name.

Crypto wallet phishing

The NCSC has also received emails in the name of the financial services provider Swissquote doing the rounds. A link was sent with a request to connect crypto wallets to the financial institution, allegedly for security reasons.

A quick look at the URL again reveals that the link does not lead to Swissquote. Clicking on the "Connect" button opens a menu with a selection of crypto service providers.

Here, the aim of the fraudsters is to gain access to the contents of the user's wallet.

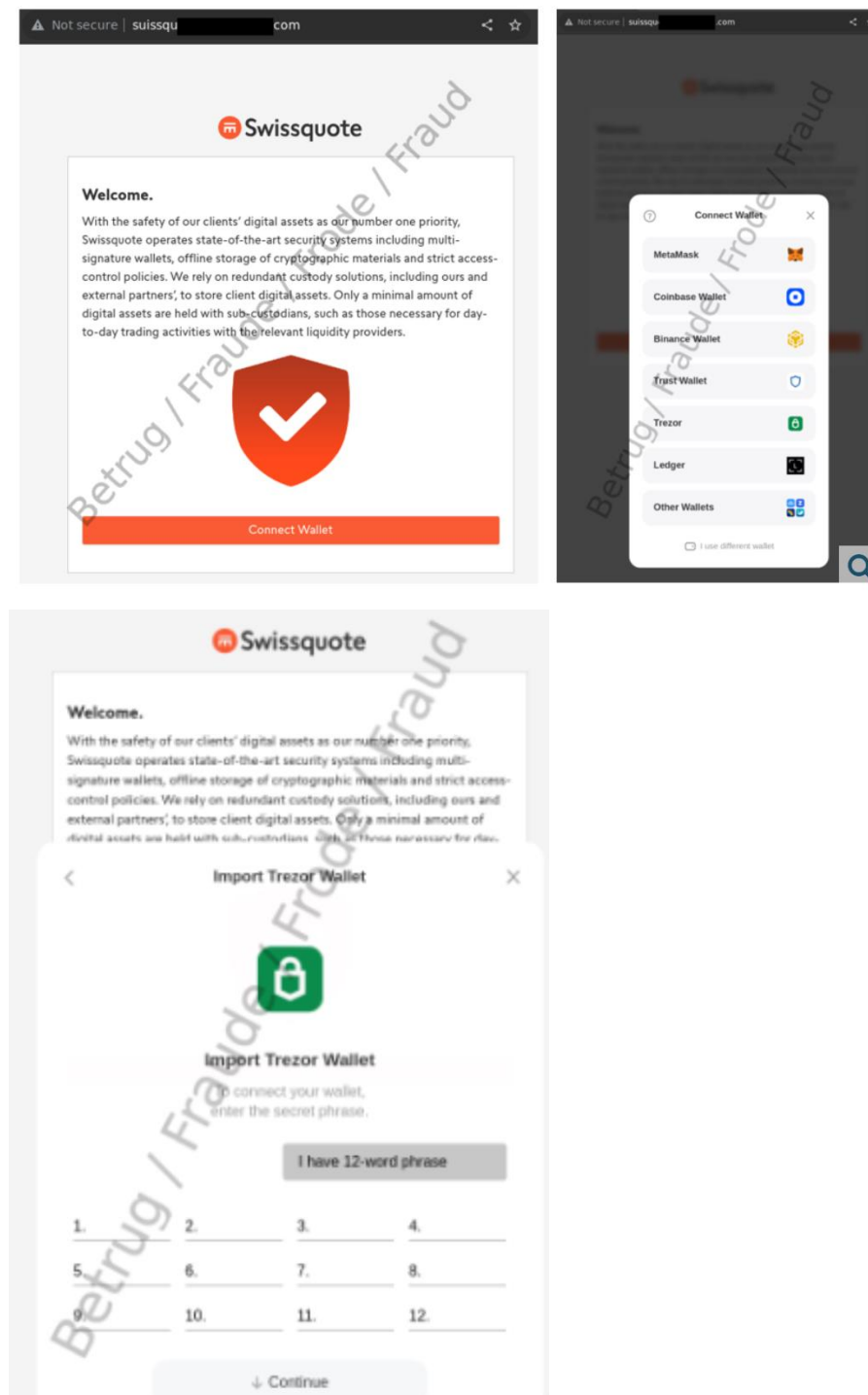
For this purpose, the so-called "seed phrase" is requested, also known as the

"recovery phrase".

This is a sequence of 12 or 24 random words that enables access to the user's wallet if the user's private key is lost.

Therefore, this seed phrase should be kept safe and not given to anyone.

Fraudsters can use a user's seed phrase to take over the victim's wallet and thus their cryptocurrencies.



NCSC tips on recognising phishing messages

As a general rule: never enter passwords, codes or credit card details on a site that you have opened via a link in an email or text message.

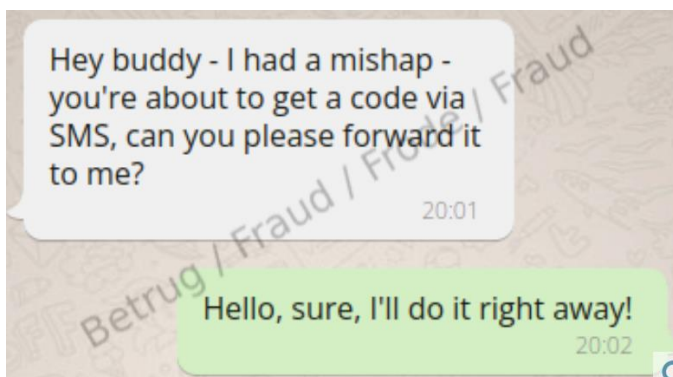
It is usually enough to focus on the typical features of a email to recognise phishing. Paying a little attention will unmask a phishing email in seconds:

1. The sender's address: unfortunately, this can be easily faked. In legitimate emails, the email address domain in the sender field must match the contact details, which are usually given at the end of the email.
2. The phishing link: the display name can be deceptive. If you move the mouse pointer over the link (without clicking), you can see where the link would actually lead. If it is a domain that is clearly not related to the sender, do not click on the link.
3. Language and graphics: inappropriately used or incorrect logos, strange salutations and greetings, possibly a mix of languages and stylistic uncertainties – all of these indicate that the sender's intentions are not legitimate.

Further NCSC tips:

1. Check the message for the three points mentioned above;
2. Never enter passwords, codes or credit card details on a page that you have opened via a link in an email or text message;
3. Never forward codes that you have received by text message;
4. If someone wants to legitimately transfer money to you, you will be asked for your IBAN, not your credit card number;
5. If in doubt, ask the service provider in question directly what the enquiry is about. Do not use a telephone number given in an e-mail or text message, instead look up the correct number online;
6. Phishing emails can be reported to the NCSC (<https://www.report.ncsc.admin.ch/>);
7. If you have provided credit card details, contact your credit card service provider immediately so that they can block your card;
8. In the event of financial loss, report the matter to the cantonal police.

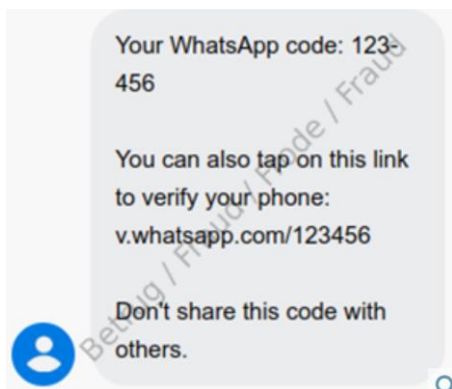
Don't trust every message you get from a contact



The NCSC is once again observing a rise in reports on the following phenomenon: one of your contacts gets in touch via WhatsApp and asks you for help with an **urgent** problem. All you have to do is forward a code.

At first glance, everything seems fine, but unfortunately the forwarding causes your WhatsApp account to be blocked. How does that happen, and what can you do to prevent it?

The code arrives almost simultaneously, via text message:



Forwarding a code costs nothing. But it doesn't take long for the rude awakening: the victim can **no longer access** their own WhatsApp account or send and receive messages. What has happened?

In this case, the contact's account has already been compromised and taken over by a hacker, who now has access to the contacts list and is going through it and trying to take over those accounts too.

To do this, **the hacker can simply** enter a contact's phone number in WhatsApp and take over the account, provided they are able to confirm that the number really belongs to them. This requires them to know and enter the 6-digit code that is sent to the real owner's device.

For this, the hacker needs a ruse to obtain the code. As soon as the code is in their possession, they can **complete the takeover** of the account – at least in most cases. Unless the owner has taken precautions. But more about that later.

Now **the game starts all over again: each new compromised account brings more contacts with it**, which the attacker now also tries to take over.

Motivation

A hacked WhatsApp account does not only allow scammers to take over other accounts. The hackers can also:

- blackmail the user by demanding money to release the account;
- **send spam**, e.g. with **links to phishing websites** or adverts for investment scams. **Since the message comes from a contact, it looks all the more trustworthy;**
- misuse the account as a contact for small ad fraud – this is especially useful if a scammer is operating from abroad but wants to look Swiss.

Countermeasures

However, users of WhatsApp or other chat services are not entirely powerless against this tactic. You can protect yourself better in just a few steps:

- As a general rule, you should never share any code you receive. If in doubt, you can always call the person who is apparently requesting the code, to ask what is going on.
- You should definitely activate two-factor authentication (on Android, for example: Settings à Account à 2-Step Verification). This issues a one-time 6-digit code. Without this code, the account cannot be transferred to another device. Of course, you should never share this code either.
- Please also read the NCSC review on WhatsApp hacking via voicemail: to prevent this scam, protect your voicemail appropriately, or deactivate it. You may visit: https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2023/wochenrueckblick_32.html

You must frequently visit the Swiss National Cyber Security Centre (NCSC) at: <https://www.ncsc.admin.ch/ncsc/en/home.html>

Information for



Individuals



Companies



Authorities



IT Specialists

Report



an incident



a vulnerability

Welcome to our monthly newsletter.

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

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



Number 1 (Page 18)

Beyond 2040 - EDA analysis warns on future warfare trends and technology imperatives for European defence

*Number 2 (Page 22)*

PHISHING GUIDANCE: STOPPING THE ATTACK CYCLE AT PHASE ONE



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Number 3 (Page 24)

ENISA Threat Landscape 2023

*Number 4 (Page 27)*

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction

Microsoft Incident Response, Microsoft Threat Intelligence

*Number 5 (Page 30)*

2023 Bank Failures - Preliminary lessons learnt for resolution

*Number 6 (Page 34)*

Acting on our commitment to safe and secure AI

Bug bounty program specific to generative AI, and new ways to support open source security for AI supply chains



Number 7 (Page 37)

Hiroshima Process - International Guiding Principles for Organizations Developing Advanced AI Systems



Number 8 (Page 41)

G7 Leaders' Statement on the Hiroshima AI Process

THE WHITE HOUSE



Number 9 (Page 42)

Understanding Cognitive Security



Number 10 (Page 45)

Can Math Secure Mixed Reality Systems from Attack



Number 11 (Page 48)

The European Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence



Number 12 (Page 50)

Answering the Call to Build the Nation's Cyber Workforce

Kemba Walden, Acting National Cyber Director in the Office of the National Cyber Director

THE WHITE HOUSE



Number 13 (Page 55)

Revisiting Connected Device Security
Secure Your Drone

**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

*Number 14 (Page 57)*

Minister Anand announces a ban on the use of WeChat and Kaspersky suite of applications on government mobile devices



Government
of Canada

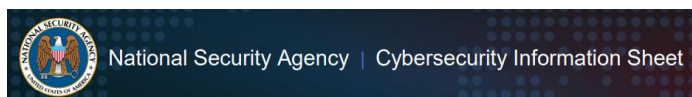
Gouvernement
du Canada

Number 15 (Page 59)

The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023

*Number 16 (Page 63)*

Advancing Zero Trust Maturity Throughout the Device Pillar

*Number 17 (Page 66)*

Cross-Sector Cybersecurity Performance Goals

A common set of protections that all critical infrastructure entities - from large to small - should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.

**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

*Number 18 (Page 68)*

Former NSA Employee Pleads Guilty to Attempted Espionage

*Number 19 (Page 70)*

UK-US data bridge: explainer



Number 20 (Page 74)

Five Eyes intelligence partners launch outreach drive to secure innovation



Number 21 (Page 77)

Protect Yourself: Commercial Surveillance Tools



Number 22 (Page 79)

NIST Seeks Collaborators for Consortium Supporting Artificial Intelligence Safety

The AI Safety Institute Consortium will help develop tools to measure and improve AI safety and trustworthiness.



Number 23 (Page 82)

NIST's Responsibilities Under the October 30, 2023 Executive Order



Number 24 (Page 85)

The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement



*Number 1***Beyond 2040 - EDA analysis warns on future warfare trends and technology imperatives for European defence**

The European Defence Agency (EDA), has published an in-depth analysis on the impact of long-term global, capability and technology trends in defence.

“Enhancing EU Military Capabilities beyond 2040” identifies key future trends that will shape capability requirements and technology advances within the next 20 years and beyond.



Developed in cooperation with experts from EU Member States, EDA has identified a series of long-term capability trends that are crucial to maintaining military advantage over potential adversaries.

The analysis informs part of the EU’s Capability Development Priorities, which EDA will present to EU Ministers of Defence on 14 November 2023.

The main identified trends from the 2023 Long-term Assessment of the Capability Development Plan include multi-domain connectivity; cognitive superiority that allows enhanced situational awareness in near real time; the ability to counter future weapon systems and a greater reliance on space based enabling and operational assets.

The adaptability of armed forces to use both analogue and digital defence mindsets to accommodate legacy military platforms with technological developments is also highlighted as a key trend.

CONTINUED RISE OF EMERGING DISRUPTIVE TECHNOLOGIES (EDTS)

EDTs will play a primary role in shaping 2040 military requirements. EDA identifies nine key EDTs and examines them from the capability development perspective, to describe possible military applications and challenges to be considered as part of the future battlespace.

Systems emerging from EDTs, as well as their combinations, are likely to have multiple applications in the military context.

Autonomous systems are a valuable example in that regard, already being rapidly incorporated into military capabilities, and expected to accelerate in the coming years.

Novel disruptive weapons, such as hypersonic and directed energy weapons, will bring new opportunities and challenges for armed forces.

EDA Chief Executive, Jiří Šedivý said: “As we try to envisage what threats we might face in the next decades, one thing is certain: maintaining technological supremacy, through defence innovation is a strategic necessity.

By working together to develop stronger and more credible military capabilities, the EU can be proactive in safeguarding its security, asserting its autonomy, and ensuring the safety and well-being of its citizens.”

FUTURE MILITARY CAPABILITY AREAS

The EDA’s analysis finds that the impact of fast-paced technology and the identified capability trends will also shape requirements across all military capability areas, for instance in;

- Information and cognitive superiority as a key aspect in the future operational environment, with command-and-inform capabilities paramount to future requirements.
- A need for new generation of weapons and platforms to produce significant shifts in engagement and protective capabilities.
- Future deployments activities that will be highly impacted by AI and autonomous systems. The operational environment in 2040 and beyond will call for improved and more solid military sustainment and logistics.

GLOBAL FUTURE STRATEGIC FACTORS

An analysis of the main factors that will shape the strategic context in 2040 and beyond was conducted, identifying the trends regarding strategic factors, where persistent digitalisation will significantly affect the character of war.

Climate change and its impact will reshape future operational environments. While growing global competition, spread of misinformation, ageing population,

cyber threats, and economic factors have been identified as key elements impacting the future of EU security.

EDA TECHNOLOGY FORESIGHT PROJECT FINDINGS PUBLISHED

EDA Technology Watch & Foresight activities were used as basis to develop fictitious scenarios of analysis concerning possible future operational environments, together with official reference on long-term macro trends.

This R&T reference helped to frame specific possible elements of capabilities to face in 20+ years ahead with a consistent assessment on the expected levels of technology maturity, to avoid ineffective science fiction effects.

In that regard, EDA has also published the summary of its ‘Technology Foresight Exercise’, which provides a high-level long-term vision on multiple possible futures for defence, with a special focus of the impact of technologies. EDA’s Foresight Exercise looks up to 20 years into the future, to provide this strategic vision of the possible impact of technologies in defence in 2040+.

To facilitate outside-the-box thinking, different activities took place within the exercise, and it was open to high-level experts from different technological and non-technological domains, as well as from non-governmental bodies, academia, industry, and civil society.

For instance, the widespread digitalisation of the battlefield with developments related to the use of Artificial Intelligence, 5G communication networks, software-based battlefield vision, and pervasive use of unmanned systems was identified as a key opportunity and threat for the future defence capabilities.

BACKGROUND – METHODOLOGY

EDA Enhancing EU Military Capabilities beyond 2040 is elaborated with the participation of capability planners, technology experts and foresight analysts from EU Member States, EDA, EU Military Committee, EU Military Staff and NATO.

Firstly, the analysis regroups the main factors that will shape the strategic context in 20 years and beyond, such as climate and demographic changes, technological advances and growing global competitiveness, together with EDA Technology Foresight analysis to assess technology impact on future capability landscape.

Secondly, possible long-term operational scenarios were developed, considering future threats, long-term strategic factors, and technological leaps.

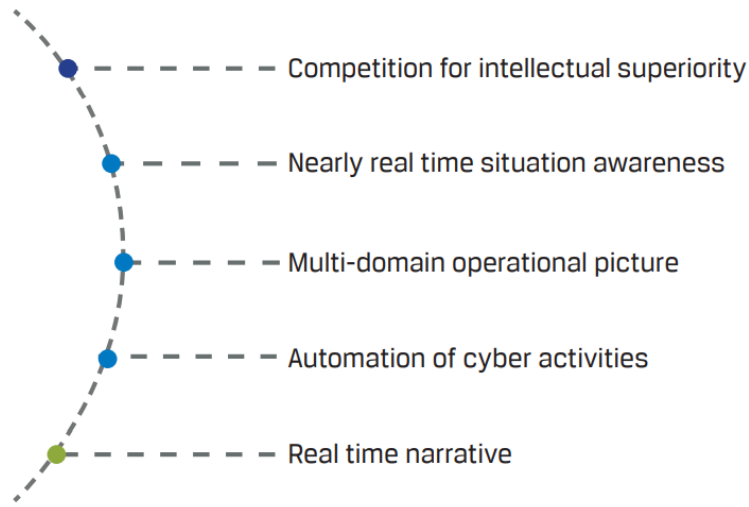
Finally, two tabletop exercises (TTX), comprising fictitious scenarios, were conducted to extract preliminary defence capability requirements findings.

Experts in military planning, research and technology and foresight analysis from Member States, EDA, EU Military Staff and NATO delivered a deep analysis of

the possible implications for future capabilities based on injections of fictitious but realistic groups of events in a given scenario.

The analysis of all findings from both Tabletop Exercises delivered a robust Long-Term Capability Assessment to inform the current CDP revision, as well as the future update of Research and Technology activities.

FIGHT FOR COGNITIVE SUPERIORITY



To read more: <https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf>



THE CAPABILITY DEVELOPMENT PLAN.....1



GLOBAL FUTURE STRATEGIC FACTORS.....5



LONG-TERM CAPABILITY TRENDS.....15



TECHNOLOGY IMPACT ON FUTURE MILITARY CAPABILITIES.....25



REQUIREMENTS FOR FUTURE MILITARY CAPABILITY AREAS.....37

Number 2

PHISHING GUIDANCE: STOPPING THE ATTACK CYCLE AT PHASE ONE



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Social engineering is the attempt to trick someone into revealing information (e.g., a password) or taking an action that can be used to compromise systems or networks.

Phishing is a form of social engineering where malicious actors lure victims (typically via email) to visit a malicious site or deceive them into providing login credentials.

Malicious actors primarily leverage phishing for:

- *Obtaining login credentials.* Malicious actors conduct phishing campaigns to steal login credentials for initial network access.
- *Malware deployment.* Malicious actors commonly conduct phishing campaigns to deploy malware for follow-on activity, such as interrupting or damaging systems, escalating user privileges, and maintaining persistence on compromised systems.

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint guide to outline phishing techniques malicious actors commonly use and to provide guidance for both network defenders and software manufacturers.

This will help to reduce the impact of phishing attacks in obtaining credentials and deploying malware.

The guidance for network defenders is applicable to all organizations but may not be feasible for organizations with limited resources.

Therefore, this guide includes a section of tailored recommendations for small- and medium-sized businesses that may not have the resources to hire IT staff dedicated to a constant defense against phishing threats.

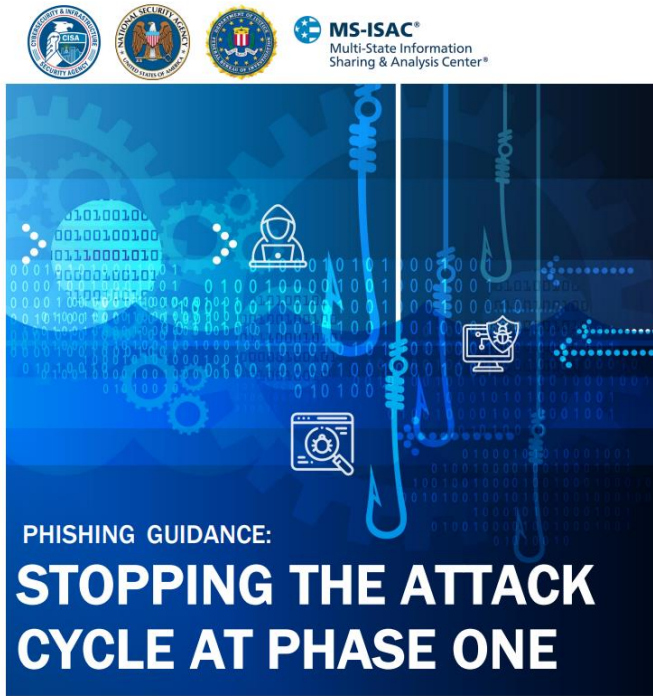
The guidance for software manufacturers focuses on secure-by-design and -default tactics and techniques.

Manufacturers should develop and supply software that is secure against the most prevalent phishing threats, thereby increasing the cybersecurity posture of their customers.

TABLE OF CONTENTS

OVERVIEW.....3
PHISHING TO OBTAIN LOGIN CREDENTIALS4
MALWARE-BASED PHISHING.....5
MITIGATIONS5
INCIDENT RESPONSE 11
REPORTING 12
CISA SERVICES 12
RESOURCES 13
ACKNOWLEDGEMENTS 14
DISCLAIMER 14
REFERENCES..... 14

To read more: <https://media.defense.gov/2023/Oct/18/2003322402/-1/-1/o/CSI-PHISHING-GUIDANCE.PDF>



Number 3

ENISA Threat Landscape 2023



The ENISA Threat Landscape (ETL) report, now in its eleventh edition, plays a crucial role in understanding the current state of cybersecurity mainly within the European Union (EU).

It provides valuable insights into emerging trends in terms of cybersecurity threats, threat actors' activities as well as vulnerabilities and cybersecurity incidents.

Accordingly, the ETL aims at informing decisions, priorities and recommendations in the field of cybersecurity.

It identifies the top threats and their particularities, threat actors' motivations and attack techniques, as well as provides a deep-dive insight on particular sectors along with a relevant impact analysis.

The work has been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

In the latter part of 2022 and the first half of 2023, the cybersecurity landscape witnessed a significant increase in both the variety and quantity of cyberattacks and their consequences.

The ongoing war of aggression against Ukraine continued to influence the landscape.

Hactivism has expanded with the emergence of new groups, while ransomware incidents surged in the first half of 2023 and showed no signs of slowing down.

The prime threats identified and analysed include:

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats against availability: Denial of Service
- Threat against availability: Internet threats
- Information manipulation and interference

- Supply chain attacks

This is the eleventh edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape.

It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis.

It also describes relevant mitigation measures. This year's work has again been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

For each of the identified threats, we determine impact, motivation, attack techniques, tactics and procedures to map relevant trends and propose targeted mitigation measures.

During the reporting period, key findings include:

- DDoS and ransomware rank the highest among the prime threats, with social engineering, data related threats, information manipulation, supply chain, and malware following.
- A noticeable rise was observed in threat actors professionalizing their as-a-Service programs, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises.
- ETL 2023 identified public administration as the most targeted sector (~19%), followed by targeted individuals (~11%), health (~8%), digital infrastructure (~7%) and manufacturing, finance and transport.
- Information manipulation has been as a key element of Russia's war of aggression against Ukraine has become prominent.
- State-nexus groups maintain a continued interest on dual-use tools (to remain undetected) and on trojanising known software packages. Cybercriminals increasingly target cloud infrastructures, have geopolitical motivations in 2023 and increased their extortion operations, not only via ransomware but also by directly targeting users.
- Social engineering attacks grew significantly in 2023 with Artificial Intelligence (AI) and new types of techniques emerging, but phishing still remains the top attack vector



To read more: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>

Number 4

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction

Microsoft Incident Response, Microsoft Threat Intelligence



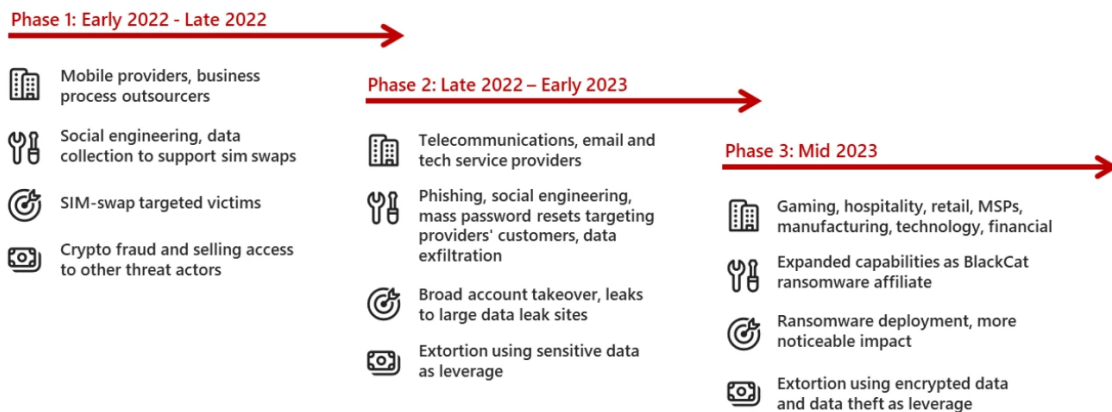
Microsoft has been tracking activity related to the financially motivated threat actor Octo Tempest, whose evolving campaigns represent a growing concern for organizations across multiple industries.

Octo Tempest leverages broad social engineering campaigns to compromise organizations across the globe with the goal of financial extortion.

With their extensive range of tactics, techniques, and procedures (TTPs), the threat actor, from our perspective, is one of the most dangerous financial criminal groups.

Octo Tempest is a financially motivated collective of native English-speaking threat actors known for launching wide-ranging campaigns that prominently feature adversary-in-the-middle (AiTM) techniques, social engineering, and SIM swapping capabilities.

 Octo Tempest: Evolving targeting, actions, outcomes, and monetization of attacks



Octo Tempest, which overlaps with research associated with oktapus, Scattered Spider, and UNC3944, was initially seen in early 2022, targeting mobile telecommunications and business process outsourcing organizations to initiate phone number ports (also known as SIM swaps).

Octo Tempest monetized their intrusions in 2022 by selling SIM swaps to other criminals and performing account takeovers of high-net-worth individuals to steal their cryptocurrency.

Building on their initial success, Octo Tempest harnessed their experience and acquired data to progressively advance their motives, targeting, and techniques, adopting an increasingly aggressive approach.

In late 2022 to early 2023, Octo Tempest expanded their targeting to include cable telecommunications, email, and technology organizations.

During this period, Octo Tempest started monetizing intrusions by extorting victim organizations for data stolen during their intrusion operations and in some cases even resorting to physical threats.

In mid-2023, Octo Tempest became an affiliate of ALPHV/BlackCat, a human-operated ransomware as a service (RaaS) operation, and initial victims were extorted for data theft (with no ransomware deployment) using ALPHV Collections leak site.

This is notable in that, historically, Eastern European ransomware groups refused to do business with native English-speaking criminals.

By June 2023, Octo Tempest started deploying ALPHV/BlackCat ransomware payloads (both Windows and Linux versions) to victims and lately has focused their deployments primarily on VMWare ESXi servers.

Octo Tempest progressively broadened the scope of industries targeted for extortion, including natural resources, gaming, hospitality, consumer products, retail, managed service providers, manufacturing, law, technology, and financial services.

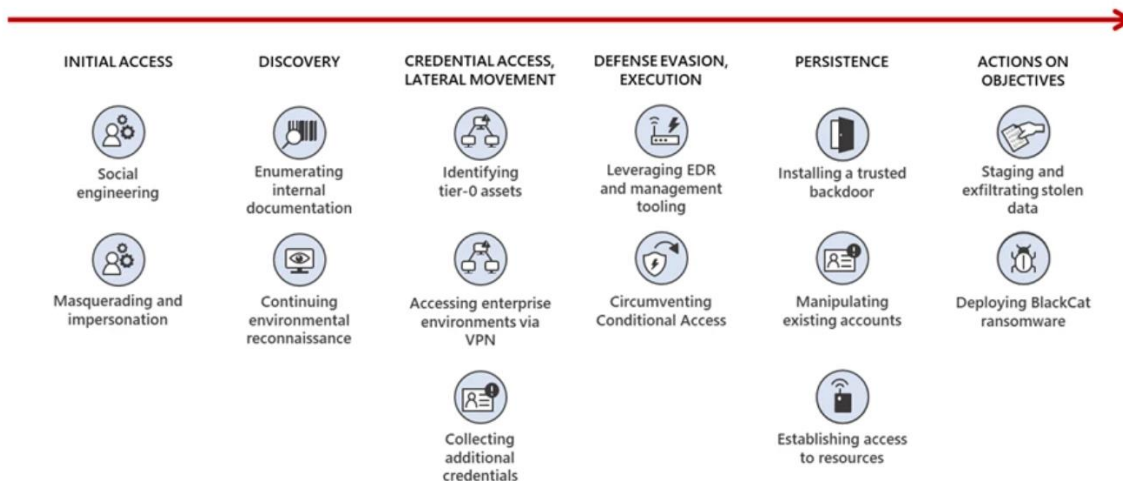
In recent campaigns, we observed Octo Tempest leverage a diverse array of TTPs to navigate complex hybrid environments, exfiltrate sensitive data, and encrypt data.

Octo Tempest leverages tradecraft that many organizations don't have in their typical threat models, such as SMS phishing, SIM swapping, and advanced social engineering techniques.

This blog post aims to provide organizations with an insight into Octo Tempest's tradecraft by detailing the fluidity of their operations and to offer organizations defensive mechanisms to thwart the highly motivated financial cybercriminal group.

Analysis

The well-organized, prolific nature of Octo Tempest's attacks is indicative of extensive technical depth and multiple hands-on-keyboard operators. The succeeding sections cover the wide range of TTPs we observed being used by Octo Tempest.



Social engineering with a twist

Octo Tempest commonly launches social engineering attacks targeting technical administrators, such as support and help desk personnel, who have permissions that could enable the threat actor to gain initial access to accounts.

The threat actor performs research on the organization and identifies targets to effectively impersonate victims, mimicking idiolect on phone calls and understanding personal identifiable information to trick technical administrators into performing password resets and resetting multifactor authentication (MFA) methods.

Octo Tempest has also been observed impersonating newly hired employees in these attempts to blend into normal on-hire processes.

To read more: <https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/>

*Number 5***2023 Bank Failures - Preliminary lessons learnt for resolution***Executive summary*

The bank failures of the first quarter of 2023 constitute the first real test at a larger scale of the international resolution framework established by the Key Attributes of Effective Resolution Regimes for Financial Institutions (“Key Attributes”) in the aftermath of the Global Financial Crisis.

The Financial Stability Board (FSB) announced publicly that it would review the lessons to be learnt from the recent actions taken by the authorities to resolve financial institutions for the operation of the international resolution framework.

**2023 Bank Failures****Preliminary lessons learnt for resolution**

Over the period between March and September 2023, the FSB has reviewed the recent events in Switzerland, the United States (US), and the United Kingdom (UK) and assessed potential implications for the FSB’s resolution framework as set out in the FSB Key Attributes.

This report identifies preliminary lessons learnt regarding the FSB Key Attributes’ framework for

- (i) resolving a global systemically important bank (G-SIB), drawing on an analysis of the Credit Suisse case; and
- (ii) the resolution of systemically important banks more broadly, drawing on the recent bank failure episodes in the US.

Introduction.....	4
1. Preliminary lessons learnt from the Credit Suisse case for G-SIB resolution and resolution planning.....	5
1.1. Background on the Credit Suisse case.....	5
1.2. Implications of the Credit Suisse episode for the FSB Resolution Framework....	10
1.3. Strengths of the existing framework	11
1.4. Challenges of the Credit Suisse case.....	13
2. Preliminary lessons learnt from the US bank failures for deposit insurance and systemic importance of non-G-SIBs.....	18
2.1. Background on the US bank failures.....	18
2.2. Implications of the US episode.....	21
2.3. Strengths of the existing framework	23
2.4. Challenges of the US cases.....	23
3. Issues to be further explored.....	27
3.1. Effective public sector backstop funding mechanisms to support resolution and restore market confidence.....	28
3.2. Choice of resolution strategies and optionality of resolution tools.....	28
3.3. Communications, coordination, and speed of bank runs	29
3.4. Operationalisation of bail-in.....	30
3.5. Post-stabilisation restructuring	31
3.6. Resolution of banks that could be systemic in failure	31
3.7. Uninsured deposits and the role of deposit insurance in resolution	31
Annex: Overview of the Key Attributes.....	33
Abbreviations.....	34

G-SIB resolution and the Credit Suisse case

Following long-standing difficulties and extreme episodes of liquidity stress in October 2022 and March 2023, Credit Suisse was acquired by UBS, supported by ample liquidity facilities including a public liquidity backstop, a second-loss guarantee from the Swiss government, and a write-down of Additional Tier 1 (AT1) bonds.

The actions by the Swiss authorities to facilitate a commercial transaction outside of resolution supported financial stability and the global operations of Credit Suisse. At the same time, it raises the question why resolution was not the chosen path despite it being an executable alternative at that time in light of preparations made.

The Swiss authorities had concerns about the ability of the prepared resolution strategy to address the crisis of confidence at Credit Suisse.

This report seeks to set out a clear understanding of the Swiss authorities' actions with a view to drawing lessons for the international resolution framework.

Since the summer of 2022, the Swiss Financial Market Supervisory Authority (FINMA) had initiated intensive meetings of the Crisis Management Group (CMG), which included home and key host authorities of Credit Suisse.

In collaboration with the CMG, FINMA had conducted two valuations for the purpose of bail-in resolution (in November 2022 and March 2023), suggesting that if FINMA had pursued a full bail-in, Credit Suisse would have reopened with a consolidated Common Equity Tier 1 (CET1) ratio of about 44% of risk weighted assets (RWAs).

It was also established that Credit Suisse did not have any known retail Total Loss-Absorbing Capacity (TLAC) bond holders. FINMA had addressed, in good cooperation with the Bank of England (BoE), Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC) and Securities and Exchange Commission (SEC), several technical issues to prepare for resolution.

CMG members worked on recognition aspects, as applicable, and the near-final draft documents were distributed to the CMG members.

Based on the review conducted by the FSB, it appears that the resolution planning work of the past decade, the availability of loss-absorbing resources, the collaboration that took place within the CMG in the months leading up to the failure of Credit Suisse, and the efforts of Swiss and host authorities to address remaining obstacles had put authorities in a position to conduct a single point-of-entry (SPE) resolution, if desired.

Indeed, the host authorities involved confirmed their readiness to support the execution of the SPE resolution and their confidence that resolution could be undertaken.

At the same time, the Credit Suisse case highlighted a number of important issues for the effective implementation of the international resolution framework that merit further attention as part of the future work of the FSB. Among these are the need for an effective public sector liquidity backstop and operational readiness of banks to access it as a last resort. In addition, firms and authorities need to:

- (i) address the legal issues identified in the execution of bail-in across borders in the course of resolution planning,
- (ii) better operationalise a range of resolution options such as transfer and sale of business tools alone or in combination with bail-in, and
- (iii) understand the impact of bail-in on financial markets.

Additionally, the Credit Suisse case shows that authorities should continue to prioritise testing and simulating effective decision making and execution at domestic and international levels.

They should also extend their communication and coordination efforts outside of the core CMG.

This review reaches the conclusion that recent events demonstrate the soundness of the international resolution framework in that it provided the Swiss authorities with an executable alternative to the solution that they deemed preferable in this particular case.

While the report identifies several areas for further analysis and improvements in the operationalisation and implementation of the G-SIB resolution framework, this review upholds the appropriateness and feasibility of the framework, rather than presenting issues that would question the substance of the Key Attributes themselves.

To read more: <https://www.fsb.org/wp-content/uploads/P101023.pdf>

Number 6

Acting on our commitment to safe and secure AI

Bug bounty program specific to generative AI, and new ways to support open source security for AI supply chains



Cyberthreats evolve quickly and some of the biggest vulnerabilities aren't discovered by companies or product manufacturers — but by outside security researchers. That's why we have a long history of supporting collective security through our Vulnerability Rewards Program (VRP), Project Zero and in the field of Open Source software security. It's also why we joined other leading AI companies at the White House earlier this year to commit to advancing the discovery of vulnerabilities in AI systems.

Welcome to Bug Hunter University

Here you'll find all you need to sharpen your ability, whether you're an advanced hunter or just starting out.

Today, we're expanding our VRP to reward for attack scenarios specific to generative AI. We believe this will incentivize research around AI safety and security, and bring potential issues to light that will ultimately make AI safer for everyone. We're also expanding our open source security work to make information about AI supply chain security universally discoverable and verifiable.

New technology requires new vulnerability reporting guidelines

As part of expanding VRP for AI, we're taking a fresh look at how bugs should be categorized and reported.

Category	Attack Scenario	Guidance
Prompt Attacks: Crafting adversarial prompts that allow an adversary to influence the behavior of the model, and hence the output in ways that were not intended by the application.	Prompt injections that are invisible to victims and change the state of the victim's account or or any of their assets.	In Scope
	Prompt injections into any tools in which the response is used to make decisions that directly affect victim users.	In Scope
	Prompt or preamble extraction in which a user is able to extract the initial prompt used to prime the model only when sensitive information is present in the extracted preamble.	In Scope
	Using a product to generate violative, misleading, or factually incorrect content in your own session: e.g. 'jailbreaks'. This includes 'hallucinations' and factually inaccurate responses. Google's generative AI products already have a dedicated reporting channel for these types of content issues.	Out of Scope

Generative AI raises new and different concerns than traditional digital security, such as the potential for unfair bias, model manipulation or misinterpretations of data (hallucinations).

As we continue to integrate generative AI into more products and features, our Trust and Safety teams are leveraging decades of experience and taking a comprehensive approach to better anticipate and test for these potential risks. But we understand that outside security researchers can help us find, and address, novel vulnerabilities that will in turn make our generative AI products even safer and more secure.

In August, we joined the White House and industry peers to enable thousands of third-party security researchers to find potential issues at DEF CON's largest-ever public Generative AI Red Team event.

Now, since we are expanding the bug bounty program and releasing additional guidelines for what we'd like security researchers to hunt, we're sharing those guidelines so that anyone can see what's "in scope." We expect this will spur security researchers to submit more bugs and accelerate the goal of a safer and more secure generative AI.

Two new ways to strengthen the AI Supply Chain

We introduced our Secure AI Framework (SAIF) — to support the industry in creating trustworthy applications — and have encouraged implementation through AI red teaming.

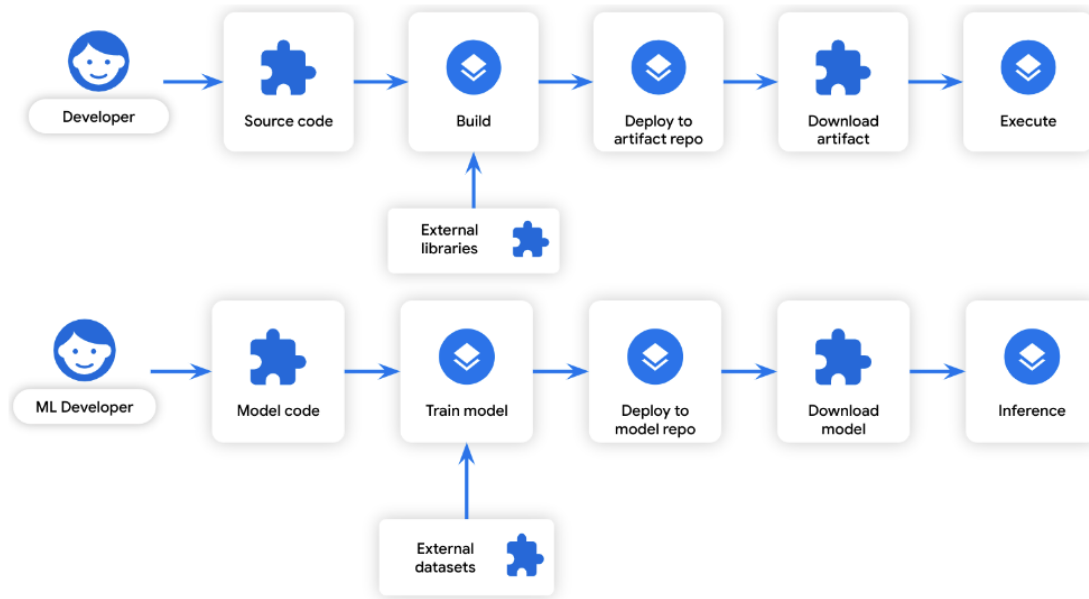
The first principle of SAIF is to ensure that the AI ecosystem has strong security foundations, and that means securing the critical supply chain components that enable machine learning (ML) against threats like model tampering, data poisoning, and the production of harmful content.

Today, to further protect against machine learning supply chain attacks, we're expanding our open source security work and building upon our prior collaboration with the Open Source Security Foundation.

The Google Open Source Security Team (GOSST) is leveraging SLSA and Sigstore to protect the overall integrity of AI supply chains.

SLSA involves a set of standards and controls to improve resiliency in supply chains, while Sigstore helps verify that software in the supply chain is what it claims to be. To get started, today we announced the availability of the first prototypes for model signing with Sigstore and attestation verification with SLSA.

These are early steps toward ensuring the safe and secure development of generative AI — and we know the work is just getting started. Our hope is that by incentivizing more security research while applying supply chain security to AI, we'll spark even more collaboration with the open source security community and others in industry, and ultimately help make AI safer for everyone.



Similarities between software development and ML model development

To read more: <https://blog.google/technology/safety-security/google-ai-security-expansion/>

*Number 7***Hiroshima Process - International Guiding Principles for Organizations Developing Advanced AI Systems**

The Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems aims to promote safe, secure, and trustworthy AI worldwide and will provide guidance for organizations developing and using the most advanced AI systems, including the most advanced foundation models and generative AI systems (henceforth "advanced AI systems").

Organizations may include, among others, entities from academia, civil society, the private sector, and the public sector.

This non-exhaustive list of guiding principles is discussed and elaborated as a living document to build on the existing OECD AI Principles in response to recent developments in advanced AI systems and are meant to help seize the benefits and address the risks and challenges brought by these technologies.

These principles should apply to all AI actors, when and as applicable to cover the design, development, deployment and use of advanced AI systems.

We look forward to developing these principles further as part of the comprehensive policy framework, with input from other nations and wider stakeholders in academia, business and civil society.

We also reiterate our commitment to elaborate an international code of conduct for organizations developing advanced AI systems based on the guiding principles below.

Different jurisdictions may take their own unique approaches to implementing these guiding principles in different ways.

We call on organizations in consultation with other relevant stakeholders to follow these actions, in line with a risk-based approach, while governments develop more enduring and/or detailed governance and regulatory approaches.

We also commit to develop proposals, in consultation with the OECD, GPAI and other stakeholders, to introduce monitoring tools and mechanisms to help organizations stay accountable for the implementation of these actions.

We encourage organizations to support the development of effective monitoring mechanisms, which we may explore to develop, by contributing best practices.

While harnessing the opportunities of innovation, organizations should respect the rule of law, human rights, due process, diversity, fairness and non-discrimination, democracy, and humancentricity, in the design, development and deployment of advanced AI systems.

Organizations should not develop or deploy advanced AI systems in a way that undermines democratic values, are particularly harmful to individuals or communities, facilitate terrorism, enable criminal misuse, or pose substantial risks to safety, security, and human rights, and are thus not acceptable.

States must abide by their obligations under international human rights law to promote that human rights are fully respected and protected, while private sector activities should be in line with international frameworks such as the United Nations Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises.

Specifically, we call on organizations to abide by the following principles, commensurate to the risks:

1. Take appropriate measures throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and mitigate risks across the AI lifecycle.

This includes employing diverse internal and independent external testing measures, through a combination of methods such as red-teaming, and implementing appropriate mitigation to address identified risks and vulnerabilities.

Testing and mitigation measures should for example, seek to ensure the trustworthiness, safety and security of systems throughout their entire lifecycle so that they do not pose unreasonable risks.

In support of such testing, developers should seek to enable traceability, in relation to datasets, processes, and decisions made during system development.

2. Identify and mitigate vulnerabilities, and, where appropriate, incidents and patterns of misuse, after deployment including placement on the market.

Organizations should use, as and when appropriate commensurate to the level of risk, AI systems as intended and monitor for vulnerabilities, incidents, emerging risks and misuse after deployment, and take appropriate action to address these.

Organizations are encouraged to consider, for example, facilitating third-party and user discovery and reporting of issues and vulnerabilities after deployment.

Organizations are further encouraged to maintain appropriate documentation of reported incidents and to mitigate the identified risks and vulnerabilities, in collaboration with other stakeholders.

Mechanisms to report vulnerabilities, where appropriate, should be accessible to a diverse set of stakeholders.

3. Publicly report advanced AI systems' capabilities, limitations and domains of appropriate and inappropriate use, to support ensuring sufficient transparency, thereby contributing to increase accountability.

This should include publishing transparency reports containing meaningful information for all new significant releases of advanced AI systems. Organizations should make the information in the transparency reports sufficiently clear and understandable to enable deployers and users as appropriate and relevant to interpret the model/system's output and to enable users to use it appropriately, and that transparency reporting should be supported and informed by robust documentation processes.

4. Work towards responsible information sharing and reporting of incidents among organizations developing advanced AI systems including with industry, governments, civil society, and academia.

This includes responsibly sharing information, as appropriate, including, but not limited to evaluation reports, information on security and safety risks, dangerous intended or unintended capabilities, and attempts by AI actors to circumvent safeguards across the AI lifecycle.

5. Develop, implement and disclose AI governance and risk management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures, in particular for organizations developing advanced AI systems.

This includes disclosing where appropriate privacy policies, including for personal data, user prompts and advanced AI system outputs.

Organizations are expected to establish and disclose their AI governance policies and organizational mechanisms to implement these policies in accordance with a risk-based approach.

This should include accountability and governance processes to evaluate and mitigate risks, where feasible throughout the AI lifecycle.

6. Invest in and implement robust security controls, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle.

These may include securing model weights and algorithms, servers, and datasets, such as through operational security measures for information security and appropriate cyber/physical access controls.

7. Develop and deploy reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques to enable users to identify AI-generated content.

This includes, where appropriate and technically feasible, content authentication such provenance mechanisms for content created with an organization's advanced AI system.

The provenance data should include an identifier of the service or model that created the content, but need not include user information.

Organizations should also endeavor to develop tools or APIs to allow users to determine if particular content was created with their advanced AI system such as via watermarks.

Organizations are further encouraged to implement other mechanisms such as labeling or disclaimers to enable users, where possible and appropriate, to know when they are interacting with an AI system.

8. Prioritize research to mitigate societal, safety and security risks and prioritize investment in effective mitigation measures.

This includes conducting, collaborating on and investing in research that supports the advancement of AI safety, security and trust, and addressing key risks, as well as investing in developing appropriate mitigation tools.

9. Prioritize the development of advanced AI systems to address the world's greatest challenges, notably but not limited to the climate crisis, global health and education.

These efforts are undertaken in support of progress on the United Nations Sustainable Development Goals, and to encourage AI development for global benefit. Organizations should prioritize responsible stewardship of trustworthy and human-centric AI and also support digital literacy initiatives.

10. Advance the development of and, where appropriate, adoption of international technical standards.

This includes contributing to the development and, where appropriate, use of international technical standards and best practices, including for watermarking, and working with Standards Development Organizations (SDOs).

11. Implement appropriate data input measures and protections for personal data and intellectual property.

Organizations are encouraged to take appropriate measures to manage data quality, including training data and data collection, to mitigate against harmful biases.

Appropriate transparency of training datasets should also be supported and organizations should comply with applicable legal frameworks.

To read more:

<https://www.mofa.go.jp/files/100573471.pdf>

*Number 8***G7 Leaders' Statement on the Hiroshima AI Process**

THE WHITE HOUSE



We, the Leaders of the Group of Seven (G7), stress the innovative opportunities and transformative potential of advanced Artificial Intelligence (AI) systems, in particular, foundation models and generative AI.

We also recognize the need to manage risks and to protect individuals, society, and our shared principles including the rule of law and democratic values, keeping humankind at the center.

We affirm that meeting those challenges requires shaping an inclusive governance for artificial intelligence.

Building on the progress made by relevant ministers on the Hiroshima AI Process, including the G7 Digital & Tech Ministers' Statement issued on September 7, 2023, we welcome the Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems and the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems (https://www.mofa.go.jp/ecm/ec/page5e_000076.html).

In order to ensure both documents remain fit for purpose and responsive to this rapidly evolving technology, they will be reviewed and updated as necessary, including through ongoing inclusive multistakeholder consultations. We call on organizations developing advanced AI systems to commit to the application of the International Code of Conduct.

We instruct relevant ministers to accelerate the process toward developing the Hiroshima AI Process Comprehensive Policy Framework, which includes project based cooperation, by the end of this year, in cooperation with the Global Partnership for Artificial Intelligence (GPAI) and the Organisation for Economic Co-operation and Development (OECD), and to conduct multi-stakeholder outreach and consultation, including with governments, academia, civil society, and the private sector, not only those in the G7 but also in the economies beyond, including developing and emerging economies.

We also ask relevant ministers to develop a work plan by the end of the year for further advancing the Hiroshima AI Process. We believe that our joint efforts through the Hiroshima AI Process will foster an open and enabling environment where safe, secure, and trustworthy AI systems are designed, developed, deployed, and used to maximize the benefits of the technology while mitigating its risks, for the common good worldwide, including in developing and emerging economies with a view to closing digital divides and achieving digital inclusion. We also look forward to the UK's AI Safety Summit on November 1 and 2.

To read more: <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/>

Number 9

Understanding Cognitive Security



Cognitive security is maintaining rational decision-making under adversarial conditions. It entails generally accepting the same shared reality and rules of the game to come to a decision, resisting/mitigating emotional manipulation and protecting individuals and societies to enable collective action to solve problems.

Risks to cognitive security include the following:

- Manipulating human decision-making
- Hacking the "human" of the human-machine team
- Person-to-group behavior manipulation
- How to get information to the human (symbiotic human-computer interface)
- Expanding beyond HMI to HME (human-machine environment or human-machine ecosystem)
- Narrative weaponization
- Politicized and monetized information environments

Our research aims to develop new tools and methodologies to protect decision-making in the face of persistent social-cyber adversarial conditions and environments.

We seek to define and detect attacks against individuals, society, etc. meant to confuse, delay, and degrade action, while researching and developing novel tools and methodologies to assess the information space, at all levels (e.g., operational, strategic) and phases (e.g., competition, conflict) of conflict.

Finally, our research investigates and explores over the horizon at emerging and future threats to cognitive security. Some example research lab outputs include developing and maintaining customized social-cyber analysis and analytic capabilities, as well as advising on mitigating/countering/monitoring/etc. social-cyber threats.

Cyber modeling and simulation (M&S) allows the exploration of complex interrelation between humans, software, and hardware systems and how they can lead to vulnerabilities or resilience. The ACI's Cyber Modeling and Simulation Research Lab (CMSRL) enables the exploration of cyber modeling and simulation in decision making and provides context and understanding of cyber risk, allowing for the development of methods and tooling to identify and mitigate

vulnerabilities in systems. By creating abstractions of the physical world and using cutting edge tools to support multiple-domain operations, we can examine these interactions and changes in the system overtime and create scalable solutions.



The next-generation battlefield will be populated with a vast number of interconnected, heterogeneous and sometimes autonomous agents including devices, networks, software, and humans.

Defending such complex and/or autonomous systems will be impossible for humans to do alone, making our research key in defending such system.

In response to the challenges facing the Cyber and Information Domain, our research directly supports the Army, Department of Defense, Intelligence Community, and Nation in the research, design, development, experimentation, testing, evaluation and operationalization of computationally intelligent, assured (secure, resilient, robust, trusted), and distributed decision-support models, tools, and systems for autonomous cyber operations in highly-contested, complex battlefield environments.

To build, assess and deploy smart, autonomous cyber-systems that enable intelligent, assured and federated decision-making, our research explores the science of information, computation, learning, and fusion for adaptive, collaborative pattern discovery, reasoning, perception, action and decision-making given heterogenous, complex, disparate data spanning devices, networks, software, and humans.

Our research aims to develop models and tools for collective intelligence, likely augmented by interacting with human cyber analysts and decision-makers. In conducting basic and applied research in the areas of data science, operations research, artificial intelligence, cognitive science, scientific computing and advanced analytics, our research seeks to tackle a multitude of challenges in infrastructure and architecture engineering, individual and collective decision-making, stealth and resilience, as well as society.

Specifically, our research aims to provide new capabilities to:

- Shift emphasis from sensing to information awareness
- Understand the underpinning of autonomy
- Relieve human cognitive overload in dealing with the data deluge problem
- Enhance human-machine interface in information processing
- Cope with various complex disparate data/information types
- Integrate a diversity of unique reasoning and learning components collaborating simultaneously
- Bridge correlational with causal discovery
- Determine solutions or obstructions to local-to-global data fusion problems
- Mechanize reasoning/learning and computing in the same computational environment
- Yield provably efficient procedures to enable or facilitate advanced data analytics
- Deal with high-dimensional and massive datasets with provably guaranteed performance

To read more: <https://cyber.army.mil/Research/Research-Labs/Cognitive-Security/>

Number 10

Can Math Secure Mixed Reality Systems from Attack



DARPA's Intrinsic Cognitive Security program seeks proposals to develop computational science that protects Defense Department systems from potential adversary exploits

The increasing use of mixed reality systems could become a new potential vulnerability.

Mixed reality (MR) merges real and virtual worlds in real time. Adversaries could exploit the intimate connection between users and their MR equipment through various techniques targeting cognition. Examples include:

- Information flooding to induce motion sickness;
- Planting real-world objects to clutter displays;
- Injecting virtual data to distract personnel;
- Using real-world objects to overwhelm the user with confusing false alarms, etc.

Commercial MR systems apply **cognitive engineering** principles during system development, but today's methods do not ensure that systems operate safely when facing an adversary intent on interfering with a mission.

Cognitive effects that have been demonstrated in virtual settings include manipulating emotion, inducing cybersickness, causing confusion or anxiety, and reducing trust in equipment.

To fulfill its mission to prevent technological surprise, DARPA intends to get in front of this issue before military personnel widely rely on MR for their missions.

The agency recently launched the Intrinsic Cognitive Security (ICS) program to explore and validate mathematical approaches, known as formal methods, to provide guarantees that MR system designs mitigate potential cognitive attacks.

Formal methods have not been widely used to protect MR users, but the cognitive engineering field provides principles to help formulate models and guarantees. ICS aims to prove guarantees relevant to MR user attacks and protections based on models applicable to MR system use.

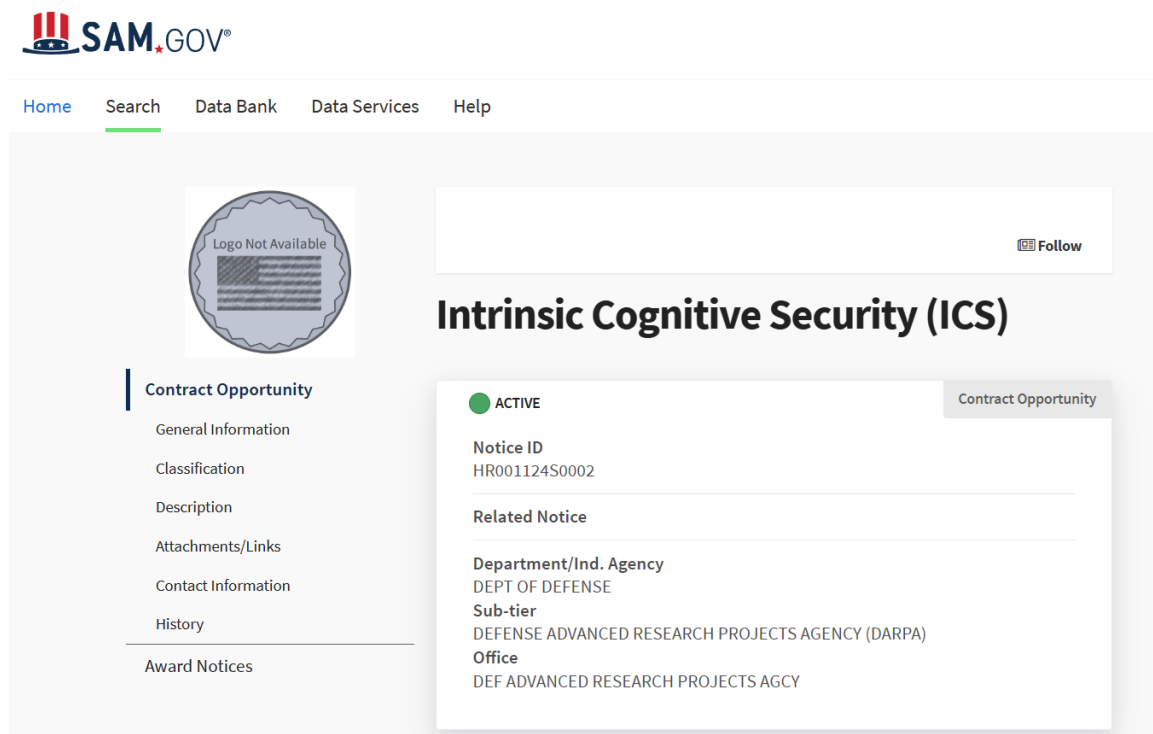
“We need to develop methods to protect mixed reality systems before systems lacking protections are pervasive,” said Dr. Matthew Wilding, DARPA's ICS program manager. “This program will show how to protect personnel using rigorous, math-based development practices that enable MR adoption plans in DOD organizations.”

Wilding says modeling user behavior in the MR domain will also help formalize an understanding of how people behave when using immersive systems. ICS does not have a sole MR system in mind. Instead, proposers will work with various commercial technologies performing different MR-related tasks.

ICS is a 36-month effort divided into two phases. Phase 1 focuses on developing proved guarantees to describe desirable properties of mixed reality systems and supporting models to enable proofs of the guarantees, including cognitive models. Building off Phase 1 results, Phase 2 will validate the usefulness of the guarantees in mixed reality systems. Performers will develop prototypes to demonstrate how guarantees can lessen vulnerabilities using commercially available hardware and software.

For technical details and proposal instructions visit the ICS broad agency announcement at SAM.gov:

<https://sam.gov/opp/cfaf7a3e51fc4f62ae412of88d52f418/view>



The screenshot shows the SAM.gov website interface. At the top, there is a navigation bar with links for Home, Search, Data Bank, Data Services, and Help. Below this, a circular logo placeholder indicates 'Logo Not Available'. The main content area features a large heading for 'Intrinsic Cognitive Security (ICS)' and a 'Follow' button. A sidebar on the left lists various contract details: Contract Opportunity, General Information, Classification, Description, Attachments/Links, Contact Information, History, and Award Notices. The main content area displays the contract's status as 'ACTIVE' and provides the following details:

- Notice ID:** HR001124S0002
- Related Notice:**
- Department/Ind. Agency:** DEPT OF DEFENSE
- Sub-tier:** DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)
- Office:** DEF ADVANCED RESEARCH PROJECTS AGCY

Abstracts are due Nov. 2, 2023, by noon ET. Abstracts are strongly encouraged, but are not required to submit a full proposal. Proposals are due Dec. 20, 2023, by noon ET.

Information from the program's Proposers Day is available on YouTube:

<https://www.youtube.com/watch?v=aCkMzorzHdk>

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

YouTube GR Search

DARPA Vision: Extend formal methods with cognitive guarantees and models

Formal methods are rigorous, mathematics-based approaches that provide guarantees about computational systems

Formal methods use
(1) guarantees expressed as mathematical conjectures
(2) models supporting guarantee proofs

Hardware design
Example: aggressive optimization
Guarantee Tool-optimized hardware operates as designed
Models Binary decision diagram (BDD) logic

Cloud computing
Example: secure private clouds
Guarantee Unauthorized cloud access blocked
Models Satisfiability Modulo Theory (SMT) network configs, software representations

System engineering
Example: cyber resilient vehicles
Guarantee Proper separation of shared vehicle components
Models Higher-order logic (HOL) separation, system interfaces

Mixed reality
Types of cognitive guarantees and models
Status
Confidence
Attention
Perception
Physiology

Needed
Guarantees that protect users of mixed reality systems
Models of cognition for reasoning about users of mixed reality systems

Distribution A. Approved for public release: distribution unlimited. 31

Intrinsic Cognitive Security - Proposers Day Program Overview

To read more: <https://www.darpa.mil/news-events/2023-10-24>

Number 11

The European Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence



The Commission welcomes the agreement by G7 leaders on International Guiding Principles on Artificial Intelligence (AI) and a voluntary Code of Conduct for AI developers under the Hiroshima AI process.

These principles and the voluntary Code of Conduct will complement, at international level, the legally binding rules that the EU co-legislators are currently finalising under the EU AI Act.

President of the European Commission, Ursula von der Leyen, was among those who subscribed to the G7 leaders' statement issued by the 2023 Japan G7 presidency.

President von der Leyen, said: “The potential benefits of Artificial Intelligence for citizens and the economy are huge. However, the acceleration in the capacity of AI also brings new challenges. Already a regulatory frontrunner with the AI Act, the EU is also contributing to AI guardrails and governance at global level. I am pleased to welcome the G7 international Guiding Principles and the voluntary Code of Conduct, reflecting EU values to promote trustworthy AI. I call on AI developers to sign and implement this Code of Conduct as soon as possible.”

Ensuring safety and trustworthiness of the technology

The eleven Guiding Principles adopted by the leaders of the seven countries and the EU, which make up the G7, provide guidance for organisations developing, deploying and using advanced AI systems, such as foundation models and generative AI, to promote safety and trustworthiness of the technology.

They include commitments to mitigate risks and misuse and identify vulnerabilities, to encourage responsible information sharing, reporting of incidents, and investment in cybersecurity as well as a labelling system to enable users to identify AI-generated content.

Informed by the results of a stakeholder survey, these principles have been jointly developed by the EU with the other G7 members, under the Hiroshima Artificial Intelligence Process.

The Guiding Principles have in turn served as the basis to compile a Code of Conduct, which will provide detailed and practical guidance for organisations developing AI.

The voluntary Code of Conduct will also promote responsible governance of AI globally.

Both documents will be reviewed and updated as necessary, including through inclusive multistakeholder consultations, to ensure they remain fit for purpose and responsive to this rapidly evolving technology.

The G7 leaders have called on organisations developing advanced AI systems to commit to the application of the International Code of Conduct.

The first signatories will be announced in the near future.

Background

The G7 Hiroshima Artificial Intelligence Process was established at the G7 Summit on 19 May 2023 to promote guardrails for advanced AI systems on a global level.

The initiative is part of a wider range of international discussions on guardrails for AI, including at the OECD, the Global Partnership on Artificial Intelligence (GPAI) and in the context of the EU-U.S. Trade and Technology Council and the EU's Digital Partnerships.

Since first announcing its intention to work on a Code of Conduct at the TTC Ministerial of 31 May 2023, the European Commission actively worked with key international partners in the G7 to develop the principles and the Code of Conduct on AI.

These international commitments are consistent with the legally binding rules currently being negotiated as part of the more comprehensive Artificial Intelligence Act (EU AI Act), which will apply in the EU.

The proposal for the EU AI Act will guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU.

The AI Act will provide risk-based, legally binding rules for AI systems that are placed on the market or put into service in the Union market.

To read more:

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5379

*Number 12***Answering the Call to Build the Nation's Cyber Workforce**

Kemba Walden, Acting National Cyber Director in the Office of the National Cyber Director

THE WHITE HOUSE



At the start of Cybersecurity Awareness Month I issued a call to action – asking organizations to join us building a cyber workforce that meets the challenges of our digital age. As October draws to a close, I'm impressed by the commitments that have been made by organizations across the nation to help us meet the growing demand for cybersecurity talent to build more secure, resilient and defensible cyberspace that is aligned with our values.

whitehouse.gov/oncd/briefing-room/2023/09/29/a-call-to-action-building-the-cyber-workforce-the-nation-needs/

WHITE HOUSE



SEPTEMBER 29, 2023

A Call To Action: Building the Cyber Workforce the Nation Needs

I'm grateful to every organization which heeded the call since the release of the National Cybersecurity Workforce and Education Strategy in July. To date, more than 50 organizations have made commitments in support of the strategy and we have secured over \$280 million dollars towards equipping Americans with foundational cyber skills, transforming cyber education, expanding the national cyber workforce, and strengthening the federal cyber workforce.

whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%e2%81%a0harris-administration-announces-national-cyber-workforce-and-education

THE WHITE HOUSE



JULY 31, 2023

FACT SHEET: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America's Cyber Talent

In October alone, some of the nation's largest companies have stepped up to accelerate and expand training and apprenticeship programs, committing to

Cyber Risk GmbH, CHE-244.099.341, Dammstrasse 16, 8810 Horgen, Switzerland - www.cyber-risk-gmbh.com

reach up to 225,000 people, and have built cybersecurity competitions to challenge new expertise and bring talent into leading cybersecurity companies.

As the President often reminds us, “We’ve never set our mind to a project we haven’t accomplished if we do it together.” That’s because American workers have shown time and time again that, if given an opportunity, they are dynamic, adaptable and up to any challenge. In the face of rapid technological change and the great promise that comes with leading the digital economy, now is the time to redouble our efforts and ensure American workers have the opportunity to join this important mission to create a secure, resilient and defensible cyberspace.

And, addressing this need is not only a national security imperative, but a massive economic opportunity. Together we’re charting a path to ensure more Americans can obtain good-paying, middle-class jobs in cybersecurity – building an economy of resilience from the bottom up and the middle out.

We are appreciative of the commitments made by big technology companies like Cisco Systems and Palo Alto Networks, by manufacturers like Boeing, financial institutions like Visa, non-profits like ISC2, partnerships between groups like Siemens Energy, the SANS Institute and ICS Village, and statewide ecosystems like the Ohio Cyber Range Institute-Regional Programming center Ecosystem (OCRI-RPC).

Together, commitments made by all of these institutions will build the pipeline of cyber talent and foster our ability to create a secure, resilient and defensible cyberspace.

These are just some of the great activities happening across the country. For a full list of our commitments made to date and to learn more about how your organization can join our effort, visit www.whitehouse.gov/cyberworkforce

I’m pleased to welcome the energy, commitment and efforts of each organization joining the effort. Let’s keep the momentum and great partnerships going.

Boeing

The digital revolution has created new demands for technical skills to align with a digital future of work. The Boeing Technical Apprenticeship Program (BTAP) is an accelerated, on-the-job, earn as you learn registered apprenticeship development program for those interested in gaining new job-ready technical skills for emerging and in demand roles.

BTAP participants receive paid, relevant work experience and are mentored by industry leaders, while acquiring the skills and on the job experiences that are valued. After a successful pilot program produced high quality and diverse employees in seven states, the BTAP is planning to expand the next round of apprenticeships up to 20 people to directly support Boeing as well as expand with industry partners to allow employees to be prepared for jobs in Information Systems Security, Architecture and Cloud Security, Incident Response, and/or Product Security Engineering.

Cisco Systems

To ensure that U.S. organizations receive the certification-driven, skills-based training they need to develop their cybersecurity teams and achieve cybersecurity readiness, Cisco committed to training 200,000 people with cybersecurity skills in the U.S. by July 2025 through the Cisco Networking Academy.

Cisco has also announced new Multicloud Certifications focused on connectivity and security to ensure IT professionals have the skills to protect companies from future cyber-attacks.

In addition to providing security products and solutions, Cisco is addressing the critical need to close the cybersecurity skills gap at all levels by offering a continuum of learning through Cisco Networking Academy and Cisco U.

Further, Cisco recently released a new Ethical Hacker course to prepare individuals for cyber offensive roles like Ethical Hacker and Penetration Tester.

For tech professionals who want to reskill or upskill, Cisco Learning & Certifications, including the Cisco U. platform prepares learners for professional-level certifications up to expert-level bootcamps and role-based skills training. Cisco offers an industry-leading portfolio of technology innovations, with networking, security, collaboration, cloud management, and more.

The Ohio Cyber Range Institute-Regional Programming Center Ecosystem (OCRI-RPC)

The OCRI-RPC Ecosystem is committed to expanding its skills-based training on a secure cyber range to all 88 counties in Ohio.

Housed at and administered by the University of Cincinnati on behalf of the state, the OCRI-RPC Ecosystem knits together 24 other Ohio universities, colleges, and non-profit organizations through a regional programming center system to deliver cyber range services to cybersecurity professionals and students across Ohio.

The OCRI-RPC Ecosystem has supported, to date, over 20,000 distinct Ohio-based users through 314 K-12 classes, 668 higher education courses, and delivering 105 cyber camps, exercises, and bootcamps, the latter involving 1000 citizens seeking industry recognized cybersecurity credentials.

ICS Village, SANS Institute, Siemens Energy

ICS Village (a non-profit organization to advance security awareness and education of industrial control systems (ICS)), SANS Institute (a non-profit organization to advance security awareness and education of industrial control systems, Siemens Energy (a Siemens business that supports companies and countries to reduce emissions across the energy landscape for a more sustainable energy system), and their partners plan to launch the Cybersecurity & Industrial Infrastructure Security Apprenticeship Program (CIISAp) as a Registered

Apprenticeship to develop the next generation of cyber defenders protecting the digitally connected systems such as energy assets, wastewater treatment facilities, advanced manufacturing, and transportation systems.

The initial goal is to fill the pipeline with 100 candidates with a focus on veterans and transitioning military members. This four-year program would enable apprentices to apply their technical industrial cybersecurity education with moderate computer skills, and gain the hands-on experience and knowledge needed to fill existing cybersecurity vacancies that currently pay above \$90,000 per year. Apprentices would gain job experience at a rotation of employers while receiving technical training, as well as completing hands-on exercises and industry certifications.

(ISC)2 (International Information Systems Security Consortium)

ISC2, an organization that provides training and certifications for cybersecurity professionals, will provide a minimum of 25,000 individuals working in Advanced Manufacturing with its foundational Certified in Cybersecurity certification exam and training for free to help address the sector's critical cybersecurity skills gap. ISC2 will also introduce a series of 10 virtual forums over the next 2 years to explore solutions to the cybersecurity workforce challenges impacting the nation's advanced manufacturing sector.

Palo Alto Networks

Palo Alto Networks kicked off its 2023-2024 Secure the Future competition, which challenges 100 students enrolled in community and four-year colleges and universities throughout the country to identify and address cyber threats in vulnerable industries.

To date, Palo Alto Networks has hired seven participants from the competition. The top three finalists are awarded cash prizes of \$10,000, \$5,000, and \$2,500, respectively.

The company also invests in educating and training a new cohort of early talent professionals and interns as members of its Systems Engineering (SE) Academy. It is one of several accelerated onboarding programs offered by Palo Alto Networks to help develop and diversify the cyber workforce and arm recent college graduates with hands-on labs and facilitated training with industry experts.

As full-time members of the Palo Alto Networks workforce, program participants help organizations optimize their security posture. Palo Alto Networks recently welcomed a new cohort of systems engineers and is actively recruiting for 2024.

VISA

Credit card company Visa, a world leader in digital payment technology, has launched the Visa Payments Learning Program to diversify entry paths into the workforce with an initial focus on payments cybersecurity. Through its learning

courses and certifications, Visa seeks to upskill underutilized talent, such as returning-to-workforce, early-in-career, second career, and military talent – thereby broadening the industry’s talent marketplace.

Visa’s initial introductory Payments Cybersecurity training courses and certifications will be offered to three groups: students via partner institutions, Visa clients, and Visa employees, apprentices and interns. Visa has welcomed an initial cohort of apprentices, who have undergone 16-weeks of specialist training and have recently embarked on a one-year apprenticeship. Visa also plans to develop intermediate and advanced level courses and certifications in 2024, and ultimately provide educational pathways to both local communities and to the broader payments industry.

To read more: <https://www.whitehouse.gov/oncd/briefing-room/2023/11/03/answering-the-call-to-build-the-nations-cyber-workforce/>

Number 13

Revisiting Connected Device Security Secure Your Drone



Drones are quickly becoming integrated into our everyday lives, similar to our smartphones and computers.

As drones grow in popularity, they could become easy targets for those who want to exploit the vulnerabilities of connected devices to compromise our individual privacy.

This security guidance presents options for drone users to protect their data and minimize privacy risks.

What is a Connected Device?

Connected devices are physical objects that connect and exchange data with other devices and systems via the internet.

Across the country, individuals and organizations use connected devices and systems daily. Connected devices include laptops, smartphones, tablets, smart home systems, cars, and drones.

As connected devices, drones are often connected to the internet and other devices via Bluetooth. As a result, they take on many of the vulnerabilities of these connections and are susceptible to cyberattacks and privacy violations.

- Flight Controller**
 Transmits commands to the receiver via electronic signals to perform functions such as controlling speed.
- Global Positioning System (GPS)**
 Processes geographical information from satellites which enables positioning hold, autonomous flight, flight elevation of below 400ft, and waypoint navigation.
- Ground Control Station (GCS)**
 Includes software applications that allow for the display of the controller's commands and additional functions, including live video monitoring and the communication of flight parameters while the drone is operating.
- Software/Firmware**
 Synchronizes all components of drone operation by sending commands received from the controller to various physical components of the drone. In most cases, the operator must update software and firmware via Wi-Fi to operate the drone reliably.
- Camera**
 Enables first-person view for real-time and advanced image processing via analog wireless transmission.

PRE-FLIGHT

Ensuring your drone's security begins before your purchase is even complete. Consider the following recommendations before purchasing a drone and during set-up to protect your data privacy.

Buying your drone

Beware: Using a drone and critical components manufactured and developed by foreign countries carries an increased risk of a foreign adversary gaining unauthorized access to your personal information.

Consider:

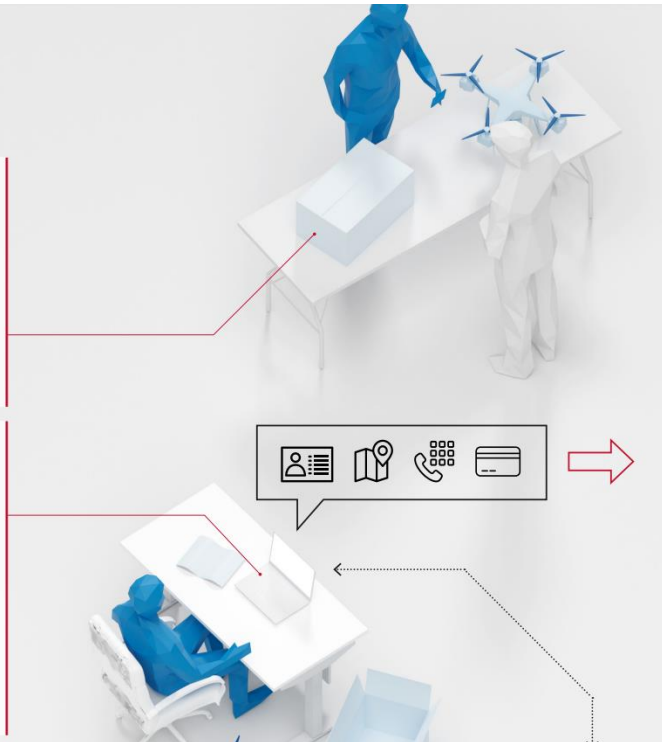
- Understanding where your drone is manufactured.
- Taking time to understand the manufacturer's privacy policy before purchasing, including how and where your data will be stored and shared.

Setting up your drone account

Beware: When signing up on applications, your personal information, including credit card information, may be stored and shared with the manufacturer.

Consider:

- Looking into the manufacturer's registration requirements and determining what information you can opt out of sharing.
- Using strong passwords for accounts and/or changing any default passwords.
- Setting up two-factor authentication, if possible.
 - A code is sent to your mobile phone or computer when your drone is used. Without entering the correct code, your drone cannot be used.



To read more: https://www.cisa.gov/sites/default/files/2023-01/FINAL_508%20Compliant_Secure%20Your%20Drone_Privacy%20and%20Data%20Protection%20Guidance_24JAN2023.pdf

Number 14

Minister Anand announces a ban on the use of WeChat and Kaspersky suite of applications on government mobile devices



Government
of Canada

Gouvernement
du Canada

The President of the Treasury Board, Anita Anand, announced a ban on the use of the WeChat and Kaspersky suite of applications on government-issued mobile devices.

The Government of Canada is committed to keeping government information and networks secure. We regularly monitor potential threats and take immediate action to address risks.

Effective October 30, 2023, the WeChat and Kaspersky suite of applications will be removed from government-issued mobile devices. Users of these devices will also be blocked from downloading the applications in the future.

The Chief Information Officer of Canada determined that WeChat and Kaspersky suite of applications present an unacceptable level of risk to privacy and security. On a mobile device, the WeChat and Kaspersky applications data collection methods provide considerable access to the device's contents.

The decision to remove and block the WeChat and the Kaspersky applications was made to ensure that Government of Canada networks and data remain secure and protected and are in line with the approach of our international partners.

While the risks of using these applications are clear, we have no evidence that government information has been compromised.

For the broader public, the decision to use a social media application or mobile platform is a personal choice. However, the Communications Security Establishment's Canadian Centre for Cyber Security (Cyber Centre) provides advice and guidance regarding the use of personal social media and on security considerations that should be made when using social media in an organization. You may visit: <https://www.cyber.gc.ca/en/guidance/protect-how-you-connect>



Communications
Security Establishment

Centre de la sécurité
des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR
CYBER SECURITY

Use of personal social media in the workplace

To read more: <https://www.canada.ca/en/treasury-board-secretariat/news/2023/10/minister-anand-announces-a-ban-on-the-use-of-wechat-and-kaspersky-suite-of-applications-on-government-mobile-devices.html>

IS INSTANT MESSAGING SECURE?

IM applications are used in the workplace as quick and easy ways to communicate with coworkers, whether working in the office or remotely. However, IM applications are not entirely safe or private. Threat actors can gain access to the information you are transmitting; always be cautious of the sensitivity level of the data that you are sending through these applications.

Some IM applications are linked to your social media accounts. If you use your social media account credentials to log in to an IM application, you are connecting the applications. Many social media and IM applications are owned by the same company, which allows the company to collect and share your data between your associated accounts. Threat actors who successfully hack into one of your accounts can also access your data that is associated with other connected applications.

IS END-TO-END ENCRYPTION SECURE?

End-to-end encryption is a confidentiality service that encrypts the sender's data (e.g. converts information to hide its contents and prevent unauthorized access) and only allows the receiver to decrypt it. Many IM applications use end-to-end encryption to secure your information and messages. Although this seems like a high level of security when sending and receiving information, you should not rely entirely on end-to-end encryption to protect your data. Threat actors can compromise your devices to retrieve the encrypted data either in the hopes of decrypting at a later time, or by compromising your unencrypted data. It is important to take these points into consideration before sending a message with a higher level of sensitivity.

WHAT ARE THE RISKS INVOLVED IN USING IM?

There are many risks that should be considered when using IM as a form of communication. Threat actors can obtain your information through some of the following methods:

- Gaining access to your log-in credentials (e.g. unprotected passwords).
- Obtaining credentials for other accounts that are connected to the IM application.
- Exposing sensitive information that you have sent to them by sharing it with others (e.g. through a screenshot).
- Collecting personal information from shared accounts (e.g. exposing your personal information online [birthdate, address] can lead to potential password hacks).
- Stealing information through an infected device (e.g. open applications being exposed to spyware).
 - Encrypted messages are unreadable until attackers gain the credentials to decrypt them.

Even if you are using a legitimate and safe IM application, threat actors can take advantage of unknown loopholes and vulnerabilities in the applications. These vulnerabilities put your sensitive information at risk of being placed in the wrong hands.



THREATS TO YOUR IDENTITY

Any personal information shared online is at risk of being compromised or stolen. Some main threats to your digital identity include the following examples:



PHISHING

A scammer calls, texts, or emails you, or uses social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information.



SOCIAL ENGINEERING

A scammer uses a more personalized phishing attack to target you specifically. Social engineering attacks often include personal details about you or your organization to trick you into sharing further personal details.



DEEPFAKES

A threat actor uses synthetic media (e.g. video, audio, photos) to impersonate you or your organization, as a form of authentication (e.g. biometrics) or misrepresentation, to steal sensitive information or spread misinformation.



THIRD-PARTY DATA BREACHES

Your vendor's network and sensitive data is compromised by threat actors. External networks and information (e.g. client data, credentials) handled by the compromised vendor are at risk. Compromised credentials may be used to access other accounts, further spreading the attack.

*Number 15***The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023**

Artificial Intelligence (AI) presents enormous global opportunities: it has the potential to transform and enhance human wellbeing, peace and prosperity.

To realise this, we affirm that, for the good of all, AI should be designed, developed, deployed, and used, in a manner that is safe, in such a way as to be human-centric, trustworthy and responsible.

We welcome the international community's efforts so far to cooperate on AI to promote inclusive economic growth, sustainable development and innovation, to protect human rights and fundamental freedoms, and to foster public trust and confidence in AI systems to fully realise their potential.

AI systems are already deployed across many domains of daily life including housing, employment, transport, education, health, accessibility, and justice, and their use is likely to increase.

We recognise that this is therefore a unique moment to act and affirm the need for the safe development of AI and for the transformative opportunities of AI to be used for good and for all, in an inclusive manner in our countries and globally.

This includes for public services such as health and education, food security, in science, clean energy, biodiversity, and climate, to realise the enjoyment of human rights, and to strengthen efforts towards the achievement of the United Nations Sustainable Development Goals.

Alongside these opportunities, AI also poses significant risks, including in those domains of daily life.

To that end, we welcome relevant international efforts to examine and address the potential impact of AI systems in existing fora and other relevant initiatives, and the recognition that the protection of human rights, transparency and explainability, fairness, accountability, regulation, safety, appropriate human oversight, ethics, bias mitigation, privacy and data protection needs to be addressed.

We also note the potential for unforeseen risks stemming from the capability to manipulate content or generate deceptive content. All of these issues are critically important and we affirm the necessity and urgency of addressing them.

Particular safety risks arise at the 'frontier' of AI, understood as being those highly capable general-purpose AI models, including foundation models, that could perform a wide variety of tasks - as well as relevant specific narrow AI that could exhibit capabilities that cause harm - which match or exceed the

capabilities present in today's most advanced models. Substantial risks may arise from potential intentional misuse or unintended issues of control relating to alignment with human intent.

These issues are in part because those capabilities are not fully understood and are therefore hard to predict.

We are especially concerned by such risks in domains such as cybersecurity and biotechnology, as well as where frontier AI systems may amplify risks such as disinformation.

There is potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models.

Given the rapid and uncertain rate of change of AI, and in the context of the acceleration of investment in technology, we affirm that deepening our understanding of these potential risks and of actions to address them is especially urgent.

Many risks arising from AI are inherently international in nature, and so are best addressed through international cooperation.

We resolve to work together in an inclusive manner to ensure human-centric, trustworthy and responsible AI that is safe, and supports the good of all through existing international fora and other relevant initiatives, to promote cooperation to address the broad range of risks posed by AI.

In doing so, we recognise that countries should consider the importance of a pro-innovation and proportionate governance and regulatory approach that maximises the benefits and takes into account the risks associated with AI.

This could include making, where appropriate, classifications and categorisations of risk based on national circumstances and applicable legal frameworks. We also note the relevance of cooperation, where appropriate, on approaches such as common principles and codes of conduct.

With regard to the specific risks most likely found in relation to frontier AI, we resolve to intensify and sustain our cooperation, and broaden it with further countries, to identify, understand and as appropriate act, through existing international fora and other relevant initiatives, including future international AI Safety Summits.

All actors have a role to play in ensuring the safety of AI: nations, international fora and other initiatives, companies, civil society and academia will need to work together.

Noting the importance of inclusive AI and bridging the digital divide, we reaffirm that international collaboration should endeavour to engage and involve a broad range of partners as appropriate, and welcome development-orientated

approaches and policies that could help developing countries strengthen AI capacity building and leverage the enabling role of AI to support sustainable growth and address the development gap.

We affirm that, whilst safety must be considered across the AI lifecycle, actors developing frontier AI capabilities, in particular those AI systems which are unusually powerful and potentially harmful, have a particularly strong responsibility for ensuring the safety of these AI systems, including through systems for safety testing, through evaluations, and by other appropriate measures.

We encourage all relevant actors to provide context-appropriate transparency and accountability on their plans to measure, monitor and mitigate potentially harmful capabilities and the associated effects that may emerge, in particular to prevent misuse and issues of control, and the amplification of other risks.

In the context of our cooperation, and to inform action at the national and international levels, our agenda for addressing frontier AI risk will focus on:

- identifying AI safety risks of shared concern, building a shared scientific and evidence-based understanding of these risks, and sustaining that understanding as capabilities continue to increase, in the context of a wider global approach to understanding the impact of AI in our societies.
- building respective risk-based policies across our countries to ensure safety in light of such risks, collaborating as appropriate while recognising our approaches may differ based on national circumstances and applicable legal frameworks.

This includes, alongside increased transparency by private actors developing frontier AI capabilities, appropriate evaluation metrics, tools for safety testing, and developing relevant public sector capability and scientific research.

In furtherance of this agenda, we resolve to support an internationally inclusive network of scientific research on frontier AI safety that encompasses and complements existing and new multilateral, plurilateral and bilateral collaboration, including through existing international fora and other relevant initiatives, to facilitate the provision of the best science available for policy making and the public good.

In recognition of the transformative positive potential of AI, and as part of ensuring wider international cooperation on AI, we resolve to sustain an inclusive global dialogue that engages existing international fora and other relevant initiatives and contributes in an open manner to broader international discussions, and to continue research on frontier AI safety to ensure that the benefits of the technology can be harnessed responsibly for good and for all.

We look forward to meeting again in 2024.

Agreement

The countries represented were:

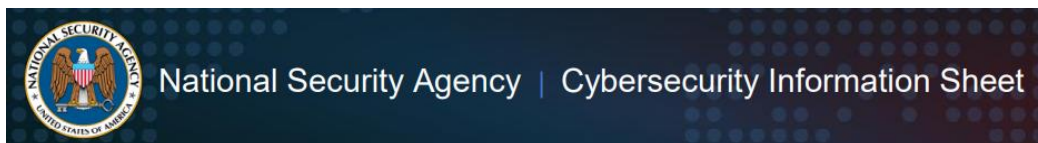
- Australia
- Brazil
- Canada
- Chile
- China
- European Union
- France
- Germany
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Kenya
- Kingdom of Saudi Arabia
- Netherlands
- Nigeria
- The Philippines
- Republic of Korea
- Rwanda
- Singapore
- Spain
- Switzerland
- Türkiye
- Ukraine
- United Arab Emirates
- United Kingdom of Great Britain and Northern Ireland
- United States of America

References to ‘governments’ and ‘countries’ include international organisations acting in accordance with their legislative or executive competences.

To read more: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>

Number 16

Advancing Zero Trust Maturity Throughout the Device Pillar



Continued cyber incidents have called attention to the immense challenges of ensuring effective cybersecurity across the federal government, as with many large enterprises, and demonstrate that “business as usual” approaches are no longer sufficient to defend the nation from cyber threats.

The government can no longer depend only on traditional strategies and defenses to protect critical systems and data.

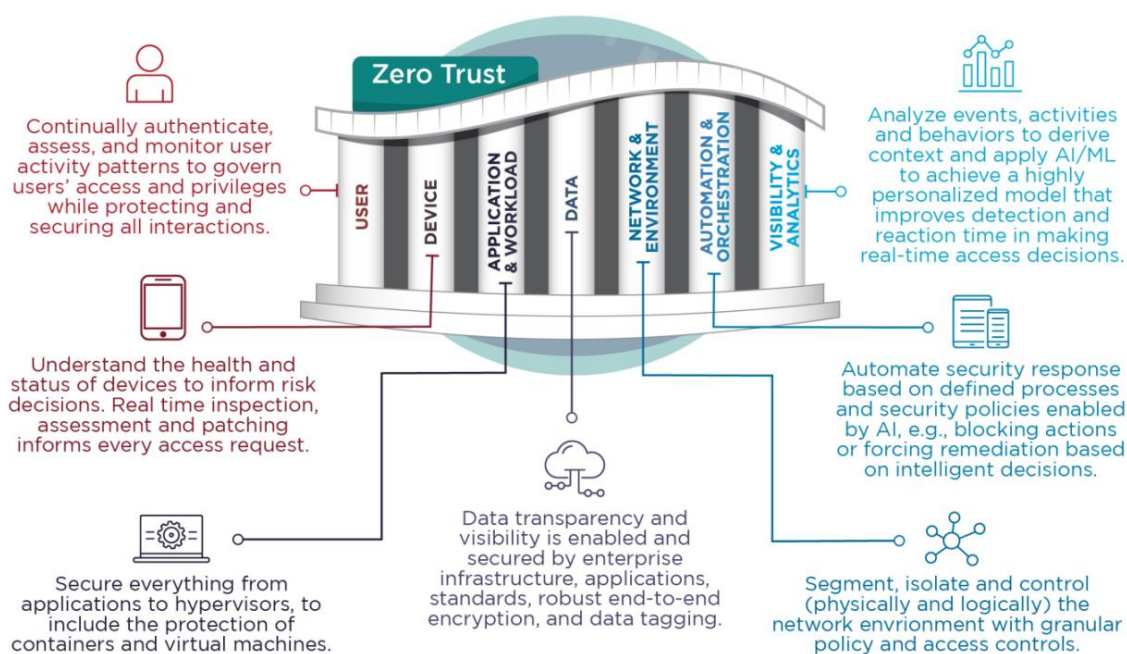


Figure 1: Description of the seven pillars of Zero Trust

A modernized cybersecurity framework—Zero Trust—integrates visibility from multiple vantage points, makes risk-aware access decisions, and automates detection and response.

Implementing this framework places network defenders in a better position to secure sensitive data, systems, applications, and services.

This cybersecurity information sheet (CSI) provides recommendations for maturing devices—the Zero Trust device pillar—to effectively ensure all devices seeking access earn trust based on device metadata and continual

checks to determine if the device meets the organization's minimum bar for access.

Contents

Executive summary	1
Introduction	3
Audience	4
Background	4
Device pillar	5
Device inventory	7
Device detection and compliance	8
Device authorization with real time inspection	10
Remote access protection	10
Automated vulnerability and patch management	12
Centralized device management	13
Endpoint threat detection and response	14
Summary of guidance	16
Further guidance	17
Works cited	17

The primary capabilities of the device pillar are:

- identification, inventory, and authentication
- detection of unknown devices and configuration compliance checks of known ones
- device authorization using real time inspections
- remote access protections
- hardware updates and software patches
- device management capabilities
- endpoint detection and response for threat detection and mitigation

This CSI further discusses how these capabilities integrate into a comprehensive Zero Trust (ZT) framework, as described in Embracing a Zero Trust Security Model.

National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) owners and operators should use this and complementary guidance to understand how to take concrete steps for maturing device security by implementing the outlined capabilities.

To read more: <https://media.defense.gov/2023/Oct/19/2003323562/-1/-1/o/CSI-DEVICE-PILLAR-ZERO-TRUST.PDF>

Number 17

Cross-Sector Cybersecurity Performance Goals

A common set of protections that all critical infrastructure entities - from large to small - should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.



CISA's Cybersecurity Performance Goals (CPGs) are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people.

These voluntary CPGs strive to help small- and medium-sized organizations kickstart their cybersecurity efforts by prioritizing investment in a limited number of essential actions with high-impact security outcomes.

The CPGs are intended to be:

- A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
- A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
- A combination of recommended practices for information technology (IT) and operational technology (OT) owners, including a prioritized set of security practices.
- Unique from other control frameworks as they consider not only the practices that address risk to individual entities, but also the aggregate risk to the nation.

CISA's CPGs have been organized to align to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) functions:

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that we impaired due to a cybersecurity event.

IDENTIFY (1)				
1.A Asset Inventory	ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: \$\$\$ IMPACT: HIGH COMPLEXITY: MEDIUM TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED: Hardware Additions (T1200) Exploit Public-Facing Application (TO819, ICS TO819) Internet-accessible device (ICS TO883)		DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	DATE: <input type="text"/> <input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	
RECOMMENDED ACTION: Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.				
FREE SERVICES AND REFERENCES: Cyber Hygiene Services , "Stuff Off Search" Guide or email vulnerability@cisa.dhs.gov				



To read more: <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf

Number 18

Former NSA Employee Pleads Guilty to Attempted Espionage



Defendant Admits to Attempting to Transmit National Defense Information to an Agent of a Foreign Government

Jareh Sebastian Dalke, 31, of Colorado Springs, pleaded guilty today to six counts of attempting to transmit classified National Defense Information (NDI) to an agent of the Russian Federation (Russia).

According to court documents, from June 6, 2022, to July 1, 2022, Dalke was an employee of the National Security Agency (NSA) where he served as an Information Systems Security Designer.

Dalke admitted that between August and September 2022, in order to demonstrate both his “legitimate access and willingness to share,” he used an encrypted email account to transmit excerpts of three classified documents to an individual he believed to be a Russian agent.

In actuality, that person was an FBI online covert employee. All three documents from which the excerpts were taken contain NDI, are classified as Top Secret//Sensitive Compartmented Information (SCI) and were obtained by Dalke during his employment with the NSA.

On or about Aug. 26, 2022, Dalke requested \$85,000 in return for all the information in his possession. Dalke claimed the information would be of value to Russia and told the FBI online covert employee that he would share more information in the future, once he returned to the Washington, D.C., area.

Dalke subsequently arranged to transfer additional classified information in his possession to the purported Russian agent at Union Station in downtown Denver. Using a laptop computer and the instructions provided by the FBI online covert employee, Dalke transferred five files, four of which contain Top Secret NDI.

The other file was a letter, which begins (in Russian and Cyrillic characters) “My friends!” and states, in part, “I am very happy to finally provide this information to you. . . . I look forward to our friendship and shared benefit. Please let me know if there are desired documents to find and I will try when I return to my main office.” The FBI arrested Dalke on Sept. 28, moments after he transmitted the files.

As part of his plea agreement, Dalke admitted that he willfully transmitted files to the FBI online covert employee with the intent and reason to believe the information would be used to injure the United States and to benefit Russia.

Dalke faces a maximum penalty of up to life in prison. Sentencing is scheduled for April 26, 2024. A U.S. district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division, U.S. Attorney Cole Finegan for the District of Colorado and Executive Assistant Director Larissa L. Knapp of the FBI's National Security Branch made the announcement.

The FBI Washington and Denver Field Offices are investigating the case.

Assistant U.S. Attorneys Julia K. Martinez and Jena R. Neuscheler for the District of Colorado and Trial Attorneys Christina A. Clark and Adam L. Small of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

DALKE Emailed National Defense Information to the OCE

On or about August 6, 2022, DALKE emailed excerpts ("Excerpt 1," "Excerpt 2," and "Excerpt 3") of three classified documents ("Classified Document 1," "Classified Document 2," and "Classified Document 3") to the OCE. All three of the documents from which the excerpts were taken are classified as Top Secret//SCI and contain National Defense Information. In addition, the excerpts themselves each contain classified National Defense Information. DALKE stated that he was providing the excerpts to demonstrate both his "legitimate access and willingness to share," and further noted that the excerpts were just a "small sample to what is possible."

Classified Document 1 is a 22-page threat assessment of Foreign Government-1's military offensive capabilities. DALKE accessed and printed Classified Document 1 on or about June 17, 2022, during his employment with NSA. Excerpt 1 is the cover page and

To read more:

<https://www.justice.gov/media/1320846/dl?inline>

<https://www.justice.gov/opa/pr/former-nsa-employee-pleads-guilty-attempted-espionage>

Number 19

UK-US data bridge: explainer



The UK Secretary of State for Science, Innovation, and Technology the Rt Hon Michelle Donelan MP took the decision to establish the UK-US data bridge and lay adequacy regulations in Parliament to this effect.

The Secretary of State took this decision, under Section 17A of the Data Protection Act 2018, to establish a data bridge with the United States of America through the UK Extension to the EU-US Data Privacy Framework.

The Secretary of State has determined that the UK Extension to the EU-US Data Privacy Framework does not undermine the level of data protection for UK data subjects when their data is transferred to the US.

This decision was based on their determination that the framework maintains high standards of privacy for UK personal data.

Adequacy regulations have been laid in Parliament today (21 September 2023) to give effect to this decision. UK businesses and organisations will be able to make use of this data bridge to safely and securely transfer personal data to certified organisations in the US, once the regulations come into force from the 12 October.

Supporting this decision, the US Attorney General, on the 18 September, designated the UK as a 'qualifying state' under Executive Order 14086.

This will allow all UK individuals whose personal data has been transferred to the US under any transfer mechanisms (i.e. including those set out under UK GDPR Articles 46 and 49) access to the newly established redress mechanism in the event that they believe that their personal data has been accessed unlawfully by US authorities for national security purposes.

The laying of the SI today follows on from an announcement earlier in the year which highlighted the data bridge as a key deliverable for 2023 under the UK-US Comprehensive Dialogue on Technology and Data.

A commitment in principle to establish the data bridge was also announced by the Prime Minister and President Biden in June this year as part of the Atlantic Declaration.

Data bridges

1. The term 'data bridge' is our preferred public terminology for 'adequacy', and describes the decision to **permit the flow of personal data from the UK to another country without the need for further safeguards**. It symbolises the connection between destinations that is established by these decisions

and encapsulates the UK's collaborative approach with our international partners.

2. Data bridges are not reciprocal, therefore they do not allow the free flow of data from other countries to the UK. Instead, a data bridge ensures that the level of protection for UK individuals' personal data under UK GDPR is maintained.
3. A data bridge assessment takes into account, amongst other things, the protection the country provides for personal data, the rule of law, respect for human rights and fundamental freedoms, and the existence and effective functioning of a regulator.
4. Data bridges secure the free and safe exchange of personal data across borders, from the UK to another country. They unlock growth for businesses, allow us to share crucial information for life-saving research, and encourage science and innovation across borders.

Reducing barriers to data sharing also makes things better for consumers, opening up opportunities for higher-quality services and lower prices on things they pay for.

Data Privacy Framework

1. The EU-US Data Privacy Framework is a bespoke, opt-in certification scheme for US companies, enforced by the Federal Trade Commission (FTC) and Department of Transportation (DoT), and administered by the Department of Commerce (DoC).
2. The Data Privacy Framework includes a set of enforceable principles and requirements that must be certified to, and complied with, in order for US organisations to be able to join the Data Privacy Framework. These principles take the form of commitments to data protection and govern how an organisation uses, collects and discloses personal data.
3. This replaces the previous Privacy Shield framework, established in 2016 to provide a legal basis for companies to comply with EU data protection requirements when transferring personal data to the US.
4. The UK has established a data bridge for the "UK Extension to the Data Privacy Framework" that allows certified US companies to sign-up to be able to receive UK personal data through the framework.
5. We will continue to monitor the Data Privacy Framework to ensure that it functions as intended, as part of the Department for Science, Innovation and Technology (DSIT's) requirement to monitor data bridges.
6. The US 'designation' of the UK relates to the US Executive Order 14086 ("Enhancing Safeguards for United States Signals Intelligence Activities") which created an independent and binding redress mechanism which can

- be accessed by individuals whose personal data is transferred from qualifying states.
7. The UK's designation as a qualifying state therefore allows UK individuals to seek redress if they believe their personal data was collected or processed through US signals intelligence in a manner that violated applicable US law.
 8. This is a new and important safeguard that the US introduced to address the concerns raised in the 2020 Schrems II judgment, in preparation for the operationalisation of the new Data Privacy Framework.
 9. Designation by the US of the UK was an important factor that led to the data bridge assessment being successful, providing increased safeguards and redress mechanisms for UK individuals.

Privacy

1. A data bridge ensures high protection for UK individuals when their data is transferred to another country. As discussed above, the US has introduced new rules and practices relating to government access to data which the UK has access to as a designated country.
2. In establishing this data bridge, we have taken steps to ensure the level of protection people in the UK enjoy under the UK GDPR is not undermined.

That includes closely assessing the level of protection of personal data under the Data Privacy Framework, as well as the wider legal and regulatory system.

The US data bridge will ensure that high standards of protection for personal data are maintained when the data is sent to certified US organisations.

Any US company that elects to receive UK data under the data bridge will be required to maintain those standards.

3. Protecting individuals' privacy – particularly when it comes to their most sensitive information – is paramount. Under the data bridge, the level of protection your personal data has within UK GDPR will be maintained.
4. The data bridge will not remove the obligations of UK companies under UK data protection law to ensure that data, especially sensitive health data, is properly protected and the rights of data subjects upheld, including when they make decisions about transferring data to other organisations.

The data bridge will ensure that these high standards of protection and privacy travel with the data when it leaves the UK to reach certified US organisations.



Headlines

From **12 October 2023**, businesses in the UK can start to transfer personal data to US organisations certified to the “UK Extension to the EU-US Data Privacy Framework” (UK Extension) under Article 45 of the UK GDPR without the need for further safeguards such as those set out in Articles 46 and 49 of the UK GDPR. UK organisations should be mindful of the need to update privacy policies and document their own processing activities as necessary to reflect any changes in how they transfer personal data to the US.

The EU-US Data Privacy Framework (DPF) is a bespoke, opt-in certification scheme for US organisations, enforced by the Federal Trade Commission (FTC) and Department of Transportation (DoT), and administered by the Department of Commerce (DoC).



To read more: <https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-explainer>

https://assets.publishing.service.gov.uk/media/650c4c7efbd7bc000de54786/factsheet_for_uk_organisations.pdf

Number 20

Five Eyes intelligence partners launch outreach drive to secure innovation



The heads of the Five Eyes domestic intelligence agencies launched new advice to help organisations protect themselves against the security threats posed by **nation states**.

Sharing a public stage for the first time, the heads of:

- the Australian Security Intelligence Organisation (ASIO),
- the Canadian Security Intelligence Service (CSIS),
- the Federal Bureau of Investigations (FBI),
- MI5, and
- the New Zealand Security Intelligence Service (NZSIS)

unveiled **five principles** which businesses can adopt to help keep their staff and their information safe and secure.

You may visit: <https://www.npsa.gov.uk/blog/five-eyes-launches-five-principles-secure-innovation>

FIVE PRINCIPLES TO SECURE INNOVATION

- 1. KNOW THE THREATS**
 We want to support you to innovate and collaborate in a way that keeps your organization safe and secure.
 There are many ways a state-backed or hostile actor could try to get hold of innovations or technologies:
 Insider
 Cyber
 Physical
 International Travel
 Investment
 Overseas jurisdictions
 Supply chain
- 2. SECURE YOUR BUSINESS ENVIRONMENT**
 Effective protective security requires management of the security risks a business faces.
 Ownership: Appoint a board-level security lead who factors security into business decisions and initiates a security dialogue within the business.
 Identification: Identify your business-critical assets and the threats to them.
 Assessment: Assess security risks alongside other risks to your business.
 Mitigation: Protect your critical assets using physical and virtual barriers, access controls and detection and plan your response should something go wrong.
- 3. SECURE YOUR PRODUCTS**
 You should ensure the products and services your business is developing are secure, and that you are actively protecting and managing your intellectual assets and expertise.
 Secure by default: Embed security in your products and services to keep your customers safe and develop a more secure society.
 IP management: Identifying and actively managing intellectual assets, property and your business's expertise will help maintain the novelty and commercial value of your business's innovation.
- 4. SECURE YOUR PARTNERSHIPS**
 To operate securely, your company should manage the risks that partnerships with investors, suppliers and collaborators bring.
 Background checks: Your business should know who you are working with.
 Share with intent: Take a strategic approach to what you are sharing with partners, investors and potential investors.
 Legal protections: Include protections for assets and data within contracts.
- 5. SECURE YOUR GROWTH**
 As your company grows, additional security risks arise which need to be managed.
 Entering new markets: As you enter international markets, you will need to consider export controls, jurisdiction risk and travel security.
 Expanding workforce: Growing companies will need to introduce pre-employment screening and security training, and work on developing or maintaining your security culture as your organization changes.

Logos of ASIO, CSIS, FBI, MI5, and NZSIS are displayed at the bottom right of the infographic.

At an event hosted by the Hoover Institution at Stanford University and the FBI, the agency heads warned that states were seeking to steal businesses' intellectual property in order to fast track their own technological and military capabilities and undermine others' competitive edge.

hoover.org/events/emerging-threats-innovation-and-security

Events Student Opportunities

 **HOOVER**
INSTITUTION About Hoover

EVENTS | 

Emerging Threats, Innovation, And Security

Secretary Condoleezza Rice & FBI Director
Christopher Wray talk about **Emerging Threats,
Innovation, and Security** on **Tuesday, October 17,
2023** at **10:30 AM PT.**

MI5 Director General, Ken McCallum said:

“The Five Eyes is the world’s oldest and most significant intelligence alliance. The strength of our partnership saves lives in our countries and around the world.

Across all five of our countries we are seeing a sharp rise in aggressive attempts by other states to steal competitive advantage.

This contest is particularly acute on emerging technologies; states which lead the way in areas like artificial intelligence, quantum computing and synthetic biology will have the power to shape all our futures.

We all need to be aware, and respond, before it’s too late.

So today we’ve jointly bolstered security across our five nations by offering practical steps organisations can take to keep themselves safe. At the same time, in the UK, we are launching NPSA’s Secure Innovation guidance.”

To coincide with the event, **new guidance** has been published in the UK by the National Protective Security Authority (NPSA), the protective security arm of MI5 and the National Cyber Security Centre (NCSC), part of GCHQ.

This is the first public campaign launched since NPSA was created in March this year.

You may visit: <https://www.npsa.gov.uk/secure-innovation>

SECURE INNOVATION

The security threat to the UK emerging tech industry is growing.
But many such businesses remain vulnerable to attack.

This campaign provides security advice that can help startups protect their innovation. Take the first steps to establish strong security practices below.



Download the Quick Start Guide



Play campaign video



To read more: <https://www.mi5.gov.uk/news/five-eyes-launch-drive-to-secure-innovation>

Number 21

Protect Yourself: Commercial Surveillance Tools



Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes.

Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections.

In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device.

These surveillance tools can:

- Record audio, including phone calls.
- Track phone's location.
- Access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history.

Below are common cybersecurity practices that may mitigate some risks:

- Regularly update device operating systems and mobile applications.
- Be suspicious of content from unfamiliar senders, especially those which contain links or attachments.
- Don't click on suspicious links or suspicious emails and attachments.
- Check URLs before clicking links, or go to websites directly.
- Regularly restart mobile devices, which may help damage or remove malware implants.
- Encrypt and password protect your device.
- Maintain physical control of your device when possible.
- Use trusted Virtual Private Networks.
- Disable geo-location options and cover camera on devices.
- While these steps mitigate risks, they don't eliminate them. It's always safest to behave as if the device is compromised, so be mindful of sensitive content.

To read more:

https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FI_NAL_Jan-7-2022_Protect_Yourself_Commercial_Surveillance_Tools.pdf



*Number 22***NIST Seeks Collaborators for Consortium Supporting Artificial Intelligence Safety**

The AI Safety Institute Consortium will help develop tools to measure and improve AI safety and trustworthiness.



The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) is calling for participants in a **new consortium** supporting development of innovative methods for evaluating artificial intelligence (AI) systems to improve the rapidly growing technology's safety and trustworthiness. This consortium is a core element of the new NIST-led U.S. AI Safety Institute announced yesterday at the U.K.'s AI Safety Summit 2023, in which U.S. Secretary of Commerce Gina Raimondo participated. You may visit: <https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute>

Artificial Intelligence Safety Institute Consortium**Overview**

Building upon its long track record of working with the private and public sectors and its history of reliable and practical measurement and standards-oriented solutions, NIST seeks research collaborators who can support this vital undertaking. Specifically, NIST looks to:

- Create a convening space for collaborators to have an informed dialogue and enable sharing of information and knowledge
- Engage in collaborative research and development through shared projects
- Enable assessment and evaluation of test systems and prototypes to inform future AI measurement efforts

To create a lasting approach for continued joint research and development, NIST will engage stakeholders via this consortium. The work of the consortium will be open and transparent and provide a hub for interested parties to work together in building and maturing a measurement science for trustworthy and responsible AI.

The institute and its consortium are part of NIST's response to the recently released Executive Order on Safe, Secure, and Trustworthy Development and Use of AI.

THE WHITE HOUSE



Administration | Priorities | The Record

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

BRIEFING ROOM | PRESIDENTIAL ACTIONS

The EO tasks NIST with a number of responsibilities, including development of a companion resource to the AI Risk Management Framework (AI RMF) focused on generative AI, guidance on authenticating content created by humans and

watermarking AI-generated content, a new initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, and creation of test environments for AI systems. NIST will rely heavily on engagement with industry and relevant stakeholders in carrying out these assignments. The new institute and consortium are central to those efforts.

“The U.S. AI Safety Institute Consortium will enable close collaboration among government agencies, companies and impacted communities to help ensure that AI systems are safe and trustworthy,” said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. “Together we can develop ways to test and evaluate AI systems so that we can benefit from AI’s potential while also protecting safety and privacy.”

The U.S. AI Safety Institute will harness work already underway by NIST and others to build the foundation for trustworthy AI systems, supporting use of the AI RMF, which NIST released in January 2023. The framework offers a voluntary resource to help organizations manage the risks of their AI systems and make them more trustworthy and responsible. The institute aims to measurably improve organizations’ ability to evaluate and validate AI systems, as detailed in the AI RMF Roadmap.

“The institute's collaborative research will strengthen the scientific underpinnings of AI measurement so that extraordinary innovations in artificial intelligence can benefit all people in a safe and equitable way,” said NIST’s Elham Tabassi, federal AI standards coordinator and a member of the National AI Research Resource Task Force.

Building on its long track record of working with the private and public sectors as well as its history of measurement and standards-oriented solutions, NIST is seeking collaborators from across society to join the consortium.

The consortium will function as a convening space for an informed dialogue and the sharing of information and insights. It will be a vehicle to support collaborative research and development through shared projects, and will promote the assessment and evaluation of test systems and prototypes to inform future AI measurement efforts.

“Participation in the consortium is open to all organizations interested in AI safety that can contribute through combinations of expertise, products, data and models,” said Jacob Taylor, NIST’s senior advisor for critical and emerging technologies. “NIST is responsible for helping industry understand how to manage the risks inherent in AI products. To do so, NIST intends to work with stakeholders at the intersection of the technical and the applied. We want the U.S. AI Safety Institute to be highly interactive because the technology is emerging so quickly, and the consortium can help ensure that the community’s approach to safety evolves alongside.”

In particular, NIST is soliciting responses from all organizations with relevant expertise and capabilities to enter into a consortium cooperative research and

development agreement (CRADA) to support and demonstrate pathways to enable safe and trustworthy AI. Members would be expected to contribute:

- Expertise in one or more of several specific areas, including AI metrology, responsible AI, AI system design and development, human-AI teaming and interaction, socio-technical methodologies, AI explainability and interpretability, and economic analysis;
- Models, data and/or products to support and demonstrate pathways to enable safe and trustworthy AI systems through the AI RMF;
- Infrastructure support for consortium projects; and
- Facility space and handling of hosting consortium researchers, workshops and conferences.

Interested organizations with relevant technical capabilities should submit a letter of interest by Dec. 2, 2023. More details on NIST's request for collaborators are available in the Federal Register. NIST plans to host a workshop on Nov. 17, 2023, for those interested in learning more about the consortium and engaging in the conversation about AI safety.

The U.S. AI Safety Institute will partner with other U.S. government agencies on evaluating AI capabilities, limitations, risks and impacts and coordinate on building testbeds. The institute will also work with organizations in ally and partner countries to share best practices, align capability evaluation, and red-team guidance and benchmarks.

To read more: <https://www.nist.gov/news-events/news/2023/11/nist-seeks-collaborators-consortium-supporting-artificial-intelligence>

*Number 23***NIST's Responsibilities Under the October 30, 2023 Executive Order**

The President's Executive Order (EO) on Safe, Secure, and Trustworthy Artificial Intelligence issued on October 30, 2023, charges multiple agencies – including NIST – with producing guidelines and taking other actions to advance the safe, secure, and trustworthy development and use of Artificial Intelligence (AI).

The EO directs NIST to develop guidelines and best practices to promote consensus industry standards that help ensure the development and deployment of safe, secure, and trustworthy AI systems. Specifically, NIST is to:

1. Develop a companion resource to the AI Risk Management Framework focused on generative AI
2. Develop a companion resource to the Secure Software Development Framework to incorporate secure-development practices for generative AI and dual-use foundation models
3. Launch a new initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities that could cause harm
4. Establish guidelines and processes – except for AI used as a component of a national security system – to enable developers of generative AI, especially dual-use foundation models, to conduct AI red-teaming tests for deployment of safe, secure, and trustworthy systems. This includes:
 - 4.1. Coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models and related to privacy-preserving machine learning
 - 4.2. In coordination with the Secretary of Energy and the Director of the National Science Foundation (NSF), developing and helping to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies, as well as support the design, development, and deployment of associated privacy-enhancing technologies (PETs)
5. Engage with industry and relevant stakeholders to develop and refine (for possible use by synthetic nucleic acid sequence providers):
 - 5.1. Specifications for effective nucleic acid synthesis procurement screening
 - 5.2. Best practices, including security and access controls, for managing sequence-of-concern databases to support such screening
 - 5.3. Technical implementation guides for effective screening

5.4. Conformity assessment best practices and mechanisms

6. Develop a report to the Director of OMB identifying existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for:

6.1. Authenticating content and tracking its provenance

6.2. Labeling synthetic content (e.g., watermarking)

6.3. Detecting synthetic content

6.4. Preventing generative AI from producing Child Sexual Abuse Material or producing non-consensual intimate imagery of real individuals

6.5. Testing software used for the above purposes

6.6. Auditing and maintaining synthetic content

7. Create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI.

8. Develop guidelines, tools, and practices to support agencies' implementation of minimum risk-management practices.

9. Assist the Secretary of Commerce in coordinating with key international partners and standards development organizations to drive the development and implementation of AI-related consensus standards, cooperation, and information sharing.

Then the Secretary of Commerce (coordinating with the Secretary of State and heads of other Federal agencies) will establish a plan for global engagement to promote and develop AI standards.

These efforts are to be guided by principles set out in the NIST AI Risk Management Framework and the US Government National Standards Strategy for Critical and Emerging Technology, which is led by NIST.

In some assignments, NIST will be working on behalf of the Secretary of Commerce.

NIST is to consult with other agencies in producing some of its guidance; in turn, several of those agencies are directed to consult NIST (directly or through the Secretary of Commerce) in accomplishing their actions under the EO.

Most of the EO tasks to NIST have a 270 day deadline.

In addition to working with government agencies, NIST intends to engage with the private sector, academia, and civil society as it produces guidance called for by the EO.

NIST will build and expand on current efforts in several of these areas.

That includes the Generative AI Public Working Group established in June 2023.

To read more: <https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence>

*Number 24***The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement**

Quantum computing and quantum technologies hold significant potential to improve a wide range of applications and tasks.

At the same time, recent technological progress in this field, also referred to as the ‘Second Quantum Revolution’, is threatening to break the encryption we use to keep our most sensitive information safe.

The purpose of this report is to provide a forward-looking assessment of the impact of quantum computing and quantum technologies from the law enforcement perspective.

In offering an extensive look at the wide range of potential applications in this context, this report is the first of its kind.

The report is the result of a collaborative effort of the European Commission’s Joint Research Centre (JRC), Europol’s European Cybercrime Centre (EC3), and the Europol Innovation Lab.

Area	Law enforcement	Criminals
General	Raise awareness on the threat of quantum computers and stay abreast of technological developments to combat risks at the earliest stage possible. Ensure law enforcement is leveraging the latest technology.	Reconsider their current <i>modi operandi</i> and identify potential to abuse availability of quantum computers.
Store now, decrypt later	Hold on to currently inaccessible encrypted data resulting from criminal investigations with a view to later decryption.	Accumulate and store encrypted information (for instance obtained from data breaches) with a view to later decryption.
Quantum password guessing	Significantly improve their technical ability to access password-protected data and devices from criminal investigations.	Be pushed to find alternative solutions for secure communications or increase operational security by using stronger passwords and multi-factor authentication. More easily hack into password-protected data and devices.
Digital forensics	Use new side-channel attacks and fault injection vulnerabilities to improve ability to gain access to criminal devices.	Employ counter measures or identify alternative technological solutions to increase operational security.
Post-quantum cryptography	Put into place transition plans to post-quantum cryptography for own data storage.	Switch to quantum-safe solutions.

It aims to inform decision-makers, policy-makers, and practitioners on the benefits and threats stemming from quantum computing and quantum technologies.

Metrology & sensors



PRECISION
FORENSICS



IMPROVED
SURVEILLANCE &
DETECTION



REAL-TIME
DECISION MAKING

The report provides an update on the current state-of-play, and offers concrete recommendations to better prepare for the future.

Quantum computing and quantum technologies have the potential to revolutionise the work of law enforcement.

One of the most immediately significant areas quantum computers will impact is cryptography. As such, a large part of the cryptographic protocols currently used are threatened by the arrival of quantum computers. This includes both symmetric and asymmetric cryptography.

While symmetric cryptography can be relatively easily patched, widely used asymmetric cryptography would collapse entirely if subjected to this process.

The realisation that quantum computers pose a significant threat to currently used cryptography has led to post-quantum cryptography, which aims to keep sensitive information secure from this emerging threat.

From the perspective of law enforcement, post-quantum cryptography has two major areas of impact.

First, law enforcement agencies need to prepare already to ensure that sensitive information and systems are protected adequately.

Second, the transition to post-quantum cryptography might reveal new vulnerabilities that could be exploited in the future.

At the same time, the impact of quantum computing in this field offers numerous potential advantages for law enforcement.

As such, quantum computers can support the investigation of cold cases, improve password guessing, and allow for new digital forensics techniques.



In addition to the impact quantum computing will have on cryptography, the overall field of quantum technologies is expected to bring significant advancements across several other areas.

This includes improvements in data analysis, machine learning and artificial intelligence, which may benefit from quantum algorithms to process large amounts of data at scale.

Quantum communications can enable the establishment of highly secure communications channels through which sensitive law enforcement data can be transmitted.

Finally, quantum sensors can improve the reliability of evidence, decrease the chance of wrongful convictions, and improve the surveillance and detection of objects.

In order for law enforcement to better prepare for the future of quantum computing and quantum technologies, five key recommendations have been identified.

While the development of universal quantum computers is still a future scenario, important steps can and should already be taken today to ensure better preparedness.

Quantum computing and quantum technologies have the potential to revolutionise the work of law enforcement.

At the same time, these technologies are likely to pose criminal threats that will need to be mitigated.

Only by understanding this impact and taking relevant action, can law enforcement agencies fully leverage these opportunities.

This report aims to provide the first step in this endeavour.

To read more: <https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement>

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 prejudice the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudice the interpretation that the Courts might place on the matters at issue.

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

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

General Terms and Conditions for all visitors to the Cyber Risk GmbH websites, and all legal transactions made through the Cyber Risk GmbH websites:

<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



[ABOUT](#) [TRAINING](#) [FOR THE BOARD](#) [ASSESSMENT](#) [READING ROOM](#) [CONTACT](#) [CYBER RISK LINKS](#) [IMPRESSUM](#)



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=SfBjOxnd_XI



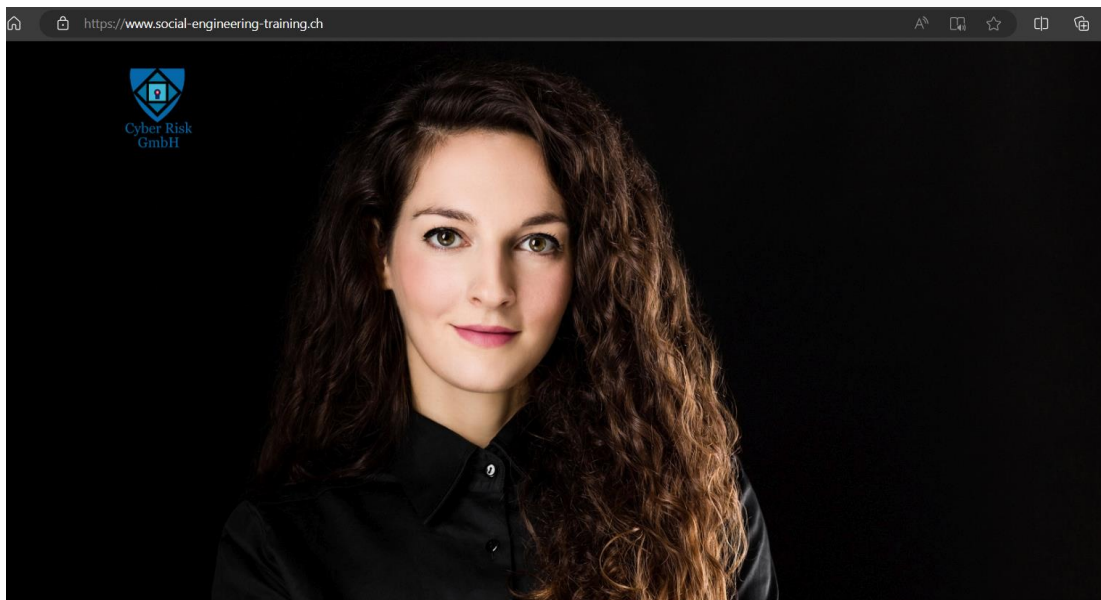
Our websites include:

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>

Cyber Risk GmbH, CHE-244.099.341, Dammstrasse 16, 8810 Horgen, Switzerland - www.cyber-risk-gmbh.com

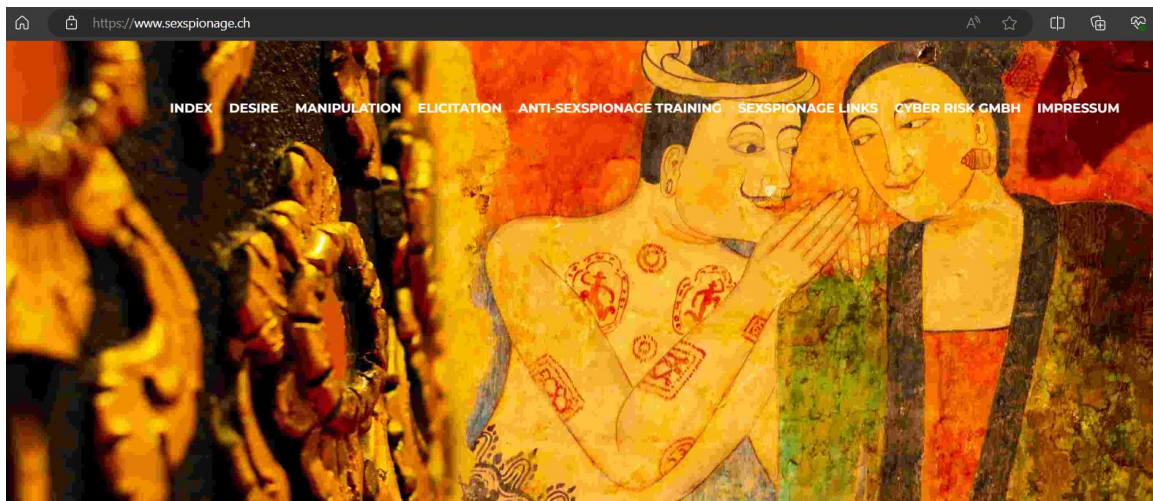
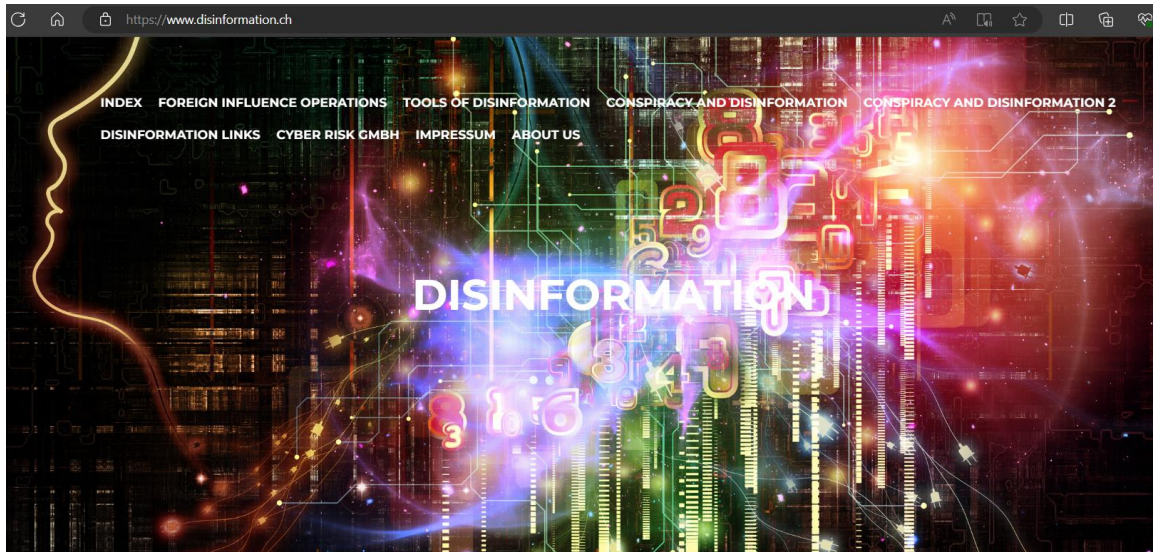
8. Electricity Cybersecurity - <https://www.electricity-cybersecurity.com>
9. Gas Cybersecurity - <https://www.gas-cybersecurity.com>
10. Hydrogen Cybersecurity - <https://www.hydrogen-cybersecurity.com>
11. Transport Cybersecurity - <https://www.transport-cybersecurity.com>
12. Transport Cybersecurity 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.

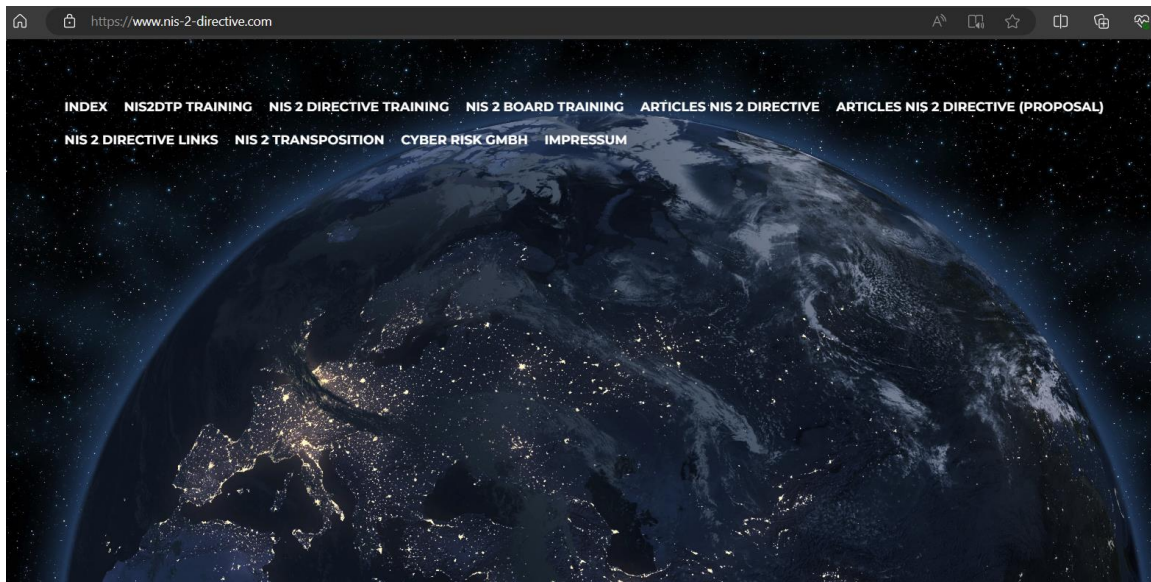
1. What is Disinformation? - <https://www.disinformation.ch>
2. What is Steganography? - <https://www.steganography.ch>
3. What is Cyberbiosecurity? - <https://www.cyberbiosecurity.ch>
4. What is Synthetic Identity Fraud? - <https://www.synthetic-identity-fraud.com>
5. What is a Romance Scam? - <https://www.romance-scams.ch>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



c. Understanding Cybersecurity in the European Union.

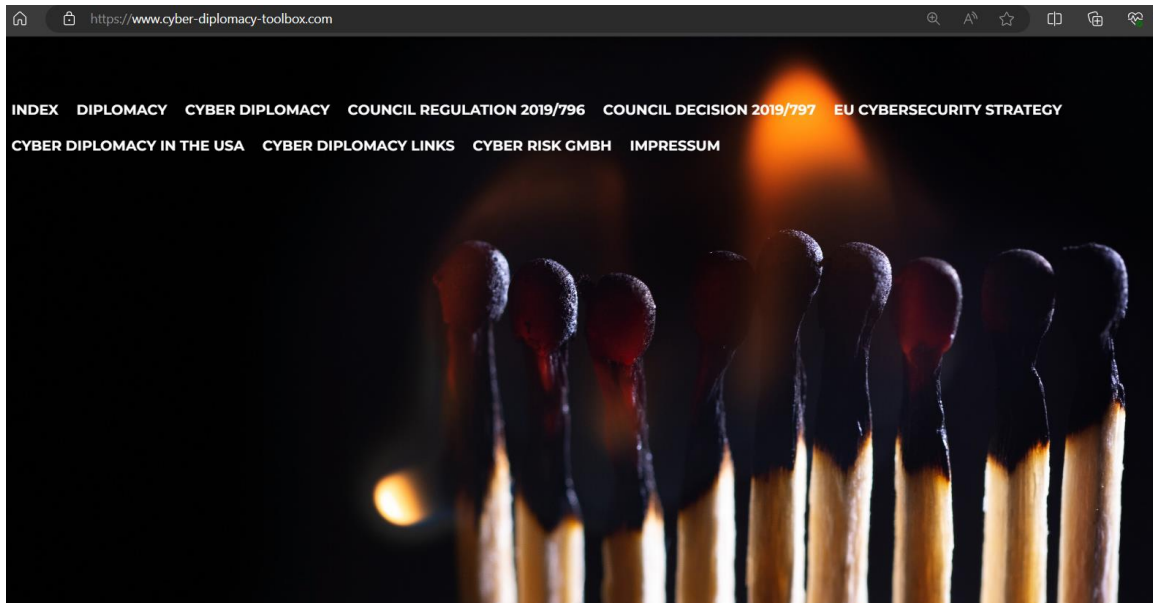
1. The NIS 2 Directive - <https://www.nis-2-directive.com>
2. The European Cyber Resilience Act - <https://www.european-cyber-resilience-act.com>
3. The Digital Operational Resilience Act (DORA) - <https://www.digital-operational-resilience-act.com>
4. The Critical Entities Resilience Directive (CER) - <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>



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

