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

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

Dear readers,

The idea that data that has been generated or collected by public sector bodies or other entities should benefit society in more ways, has been part of EU policy for a long time, but now we have a very ambitious regulation that transforms the dream to a plan.

Regulation (EU) 2022/868, the Data Governance Act of the EU, creates a harmonised framework for data exchanges and lays down requirements for data governance. This Regulation develops the borderless digital internal market and a human-centric, trustworthy and secure data society and economy.

Certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data in public databases are not made available, not even for research or innovative activities in the public interest, despite such

availability being possible in accordance with the applicable Union law. *Yes, even after the GDPR regulation.*

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

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

What is new? The European Commission has introduced common logos to easily identify trusted data intermediation service providers and data altruism organisations in the EU, which will connect data holders, both individuals and companies with data users.

Read more at number 4 below.

We have an interesting development. The US Department of Defense (DoD) announced the establishment of a generative artificial intelligence (AI) task force.

According to the DoD, generative artificial intelligence (Al) capabilities such as Large Language Models (LLMs) are growing in popularity, capability, and impact around the globe. These capabilities are trained on massive datasets to generate content at a near-instantaneous speed to a level of detail and apparent coherence which would have previously required human authorship.

These capabilities unlock new opportunities, just as they pose significant new and enduring risks. The DoD must explore the use of this technology to take advantage of these models' scale, speed, and interactive capabilities to improve the Department's mission effectiveness while identifying proper

protection measures, including safeguarding individuals' privacy and civil liberties, and mitigating risks.

The Chief Digital and Artificial Intelligence Officer (CDAO) Generative AI and LLM Task Force, Task Force Lima, will focus the Department's exploration and responsible fielding of generative AI capabilities within and across the DoD, providing guidance and making recommendations for the relevant policy-making bodies to address.

This is an interesting development. I remember the Final Report from the US National Security Commission on Artificial Intelligence (756 pages!) in 2021. According to the report, no comfortable historical reference captures the impact of artificial intelligence (AI) on national security.

AI is not a single technology breakthrough, like a bat-wing stealth bomber. The race for AI supremacy is not like the space race to the moon. AI is not even comparable to a general-purpose technology like electricity.

However, what Thomas Edison said of electricity encapsulates the AI future: “It is a field of fields … it holds the secrets which will reorganize the life of the world.”

Edison’s astounding assessment came from humility. All that he discovered was “very little in comparison with the possibilities that appear.”

Read more at number 8 below.

In Switzerland, according to the Swiss National Cybersecurity Centre (NCSC), cybercriminals have come up with a variety of fake support scams that are aimed at installing a remote access tool on the victim's computer and then making credit card payments or e-banking transactions.

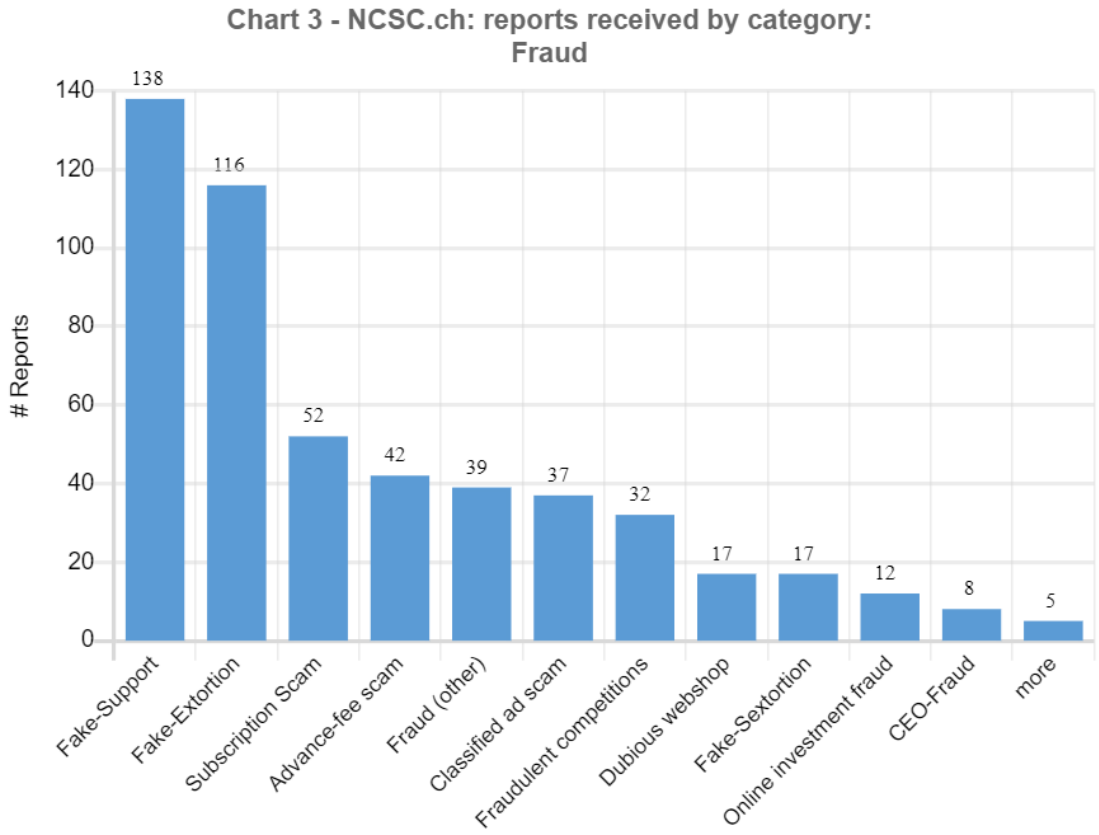
Callers pretending to be an employee of an IT company, and claiming that the victim's computer is infected and needs to be repaired, have been around for some time.

The fake support callers phone people at random. They have no idea how the computers of the people they are calling are configured.

The attackers' main objective is to persuade the victims to download a program (remote access tool) that allows them to access the computer, which provides them with a gateway for further criminal activity.

Recent months have seen the arrival of two new variants, which ultimately turn out to also be fake support scams.

Perhaps the original IT support scam is not as lucrative as it used to be, or the victims have become more sceptical and thus more careful, so the perpetrators are trying other tactics.



Fake invoices

In the first variant, the fraudsters claim that the victim has bought something, and send them a fake invoice. In most cases, the supposed purchase involves a subscription for an antivirus program. The invoice in the mail appears to show that the victim has already paid the bill.

The recipient is told to contact the invoicing party if they do not agree with the payment. A phone number is given as the only way of contacting the invoicing party. In order to ensure that the victim does not get suspicious, the numbers given are usually Swiss numbers.

If the victim calls the number, they are connected to a call centre employee who promises to solve the problem immediately.

The customer is told to install a remote access tool on their computer, so that the "employee" can cancel the payment.

Once the remote access tool is installed, the customer is supposed to enter their access credentials for the e-banking portal or their credit card details.

The fraudsters then make various payments in the background.

Norton

--- AUFTRAGSEINGANG ---

Lieber Kunde,

Kunden-ID:
Referenznummer:

Rechnungsnummer	
Datum der Rechnung	JULI 27, 2023
Rechnungsbedingungen	Fällig bei Erhalt
Fälligkeitsdatum	JULI 27, 2023

Beschreibung	Menge	Einheitspreis	Betrag
1 Jahr Jahresplan (AMC)	1	€ 267.54	€ 267.54
Hinweis für den Empfänger (s)		Zwischensumme	€ 267.54
Danke für Ihr Interesse			
		Insgesamt	€ 267.54

- Die Transaktion wurde von Ihrem autorisierten Bankkonto abgebucht und sollte innerhalb von 48 Stunden erscheinen.
- Bitte kontaktieren Sie unseren Kundendienst unter +41 (225) wenn Sie diese Zahlung nicht geleistet haben oder wenn Sie zusätzliche Hilfe benötigen.

Herzliche Grüße,
Norton-Team

Betrug / Fraude / Frode / Fraud

In the above image, we see a fake invoice, apparently from Norton. It claims that the transaction has already been debited from the bank account and will show up in the victim's e-banking account in 48 hours.

Fake calls from the police

Since the end of June, the NCSC has been receiving a large number of reports about the second variant. This starts with an apparent phone call from the police. A computer-generated voice informs the victim that their personal banking data has been brought into connection with a crime. For further information, the call recipient should press 1.

The modus operandi was initially unclear, but the reports by members of the public indicate that in the case of a call back, the victim is told to download a remote access tool and grant the attackers access to their computer.

Here too, the fraudsters try to persuade the victim to grant access to their e-banking account. Once the fraudsters have obtained access, they use the remote access tool to make payments in the background.

Advice from the Swiss National Cybersecurity Centre (NCSC):

- End such phone calls immediately.

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

- If you made a payment, immediately contact the bank through which you made it. They may be able to stop the payment.

- Do not give anyone remote access to your computer. If you granted remote access, there is a possibility that your computer has been infected.

The first step is to uninstall the remote access program. If you suspect an infection, have your computer examined immediately by a specialist and cleaned if necessary. The safest option is to completely reinstall the computer. However, do not forget to back up all personal data beforehand.

Welcome to our monthly newsletter.

Best regards,

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

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

Number 1 (Page 10)

NIST CSWP 29 (Initial Public Draft)
The NIST Cybersecurity Framework 2.0

Number 2 (Page 12)

CISA, NSA, FBI and International Partners Issue Advisory on the Top Routinely Exploited Vulnerabilities in 2022

Number 3 (Page 14)

Irish Data Protection Commission announces €345 million fine of TikTok

Number 4 (Page 17)

Data Governance Act: common logos to easily identify trusted EU data intermediaries and data altruism organisations to re-use data

Number 5 (Page 19)

Attorney General Bonta Announces $93 Million Settlement Regarding Google's Location-Privacy Practices

Number 6 (Page 21)

NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers

Three new algorithms are expected to be ready for use in 2024. Others will follow.

Number 7 (Page 23)

Voices from DARPA Episode 71: The Quantum Mechanic

Number 8 (Page 25)

DOD Announces Establishment of Generative AI Task Force

Number 9 (Page 28)

Ransomware, extortion and the cyber crime ecosystem

A white paper from the NCSC and the National Crime Agency (NCA)

Number 10 (Page 31)

Security Incident

Number 11 (Page 33)

Supervisory cooperation in the fight against financial crime is improving

Number 12 (Page 36)

Seeking Legitimacy: Considerations for Strategic Communications in the Digital Age

Number 13 (Page 39)

From the Finnish Customs website tulli.fi

Contents of the Piilopuoti web server seized by Finnish Customs – major breakthrough in the anonymous Tor network

Number 14 (Page 41)

What's Wrong With This Picture? NIST Face Analysis Program Helps to Find Answers

Number 15 (Page 44)

Director of National Intelligence Avril D. Haines Releases the 2023 National Intelligence Strategy for the Intelligence Community

Number 1

NIST CSWP 29 (Initial Public Draft)
The NIST Cybersecurity Framework 2.0

Date Published: August 8, 2023
Comments Due: November 5, 2023

This is the public draft of the NIST Cybersecurity Framework (CSF or Framework) 2.0.

The Framework has been used widely to reduce cybersecurity risks since its initial publication in 2014. Many organizations have told NIST that CSF 1.1 remains an effective framework for addressing cybersecurity risks.

There is also widespread agreement that changes are warranted to address current and future cybersecurity challenges and to make it easier for organizations to use the Framework.

NIST is working with the community to ensure that CSF 2.0 is effective for the future while fulfilling the CSF's original goals and objectives.

NIST seeks feedback on whether this draft revision addresses organizations' current and anticipated future cybersecurity challenges, is aligned with leading practices and guidance resources, and reflects comments received so far.

In addition, NIST requests ideas on the best way to present the modifications from CSF 1.1 to CSF 2.0 to support transition.

NIST encourages concrete suggestions for improvements to the draft, including revisions to the narrative and Core.

This draft includes an updated version of the CSF Core, reflecting feedback on the April discussion draft.

This publication does not contain Implementation Examples or Informative References of the CSF 2.0 Core, given the need to frequently update them. Draft, initial Implementation Examples have been released under separate cover for public comment.

NIST seeks feedback on what types of Examples would be most beneficial to Framework users, as well as what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks, for example). NIST also seeks feedback on how

often Implementation Examples should be updated and whether and how to accept Implementation Examples developed by the community.

21 **Table of Contents**

As the CSF 2.0 is finalized, the updated Implementation Examples and Informative References will be maintained online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT).

Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

To read more: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

Number 2

CISA, NSA, FBI and International Partners Issue Advisory on the Top Routinely Exploited Vulnerabilities in 2022

The following cybersecurity agencies coauthored this joint Cybersecurity Advisory (CSA):

- United States: The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI).
- Australia: Australian Signals Directorate's Australian Cyber Security Centre (ACSC).
- Canada: Canadian Centre for Cyber Security (CCCS).
- New Zealand: New Zealand National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team New Zealand (CERT NZ).
- United Kingdom: National Cyber Security Centre (NCSC-UK).

This advisory provides details on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2022 and the associated Common Weakness Enumeration(s) (CWE).

In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems.

Key Findings

In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems.

Proof of concept (PoC) code was publicly available for many of the software vulnerabilities or vulnerability chains, likely facilitating exploitation by a broader range of malicious cyber actors.

Malicious cyber actors generally have the most success exploiting known vulnerabilities within the first two years of public disclosure—the value of such vulnerabilities gradually decreases as software is patched or upgraded.

Timely patching reduces the effectiveness of known, exploitable vulnerabilities, possibly decreasing the pace of malicious cyber actor

operations and forcing pursuit of more costly and time-consuming methods (such as developing zero-day exploits or conducting software supply chain operations).

Malicious cyber actors likely prioritize developing exploits for severe and globally prevalent CVEs.

While sophisticated actors also develop tools to exploit other vulnerabilities, developing exploits for critical, wide-spread, and publicly known vulnerabilities gives actors low-cost, high-impact tools they can use for several years.

Additionally, cyber actors likely give higher priority to vulnerabilities that are more prevalent in their specific targets' networks.

Multiple CVE or CVE chains require the actor to send a malicious web request to the vulnerable device, which often includes unique signatures that can be detected through deep packet inspection.

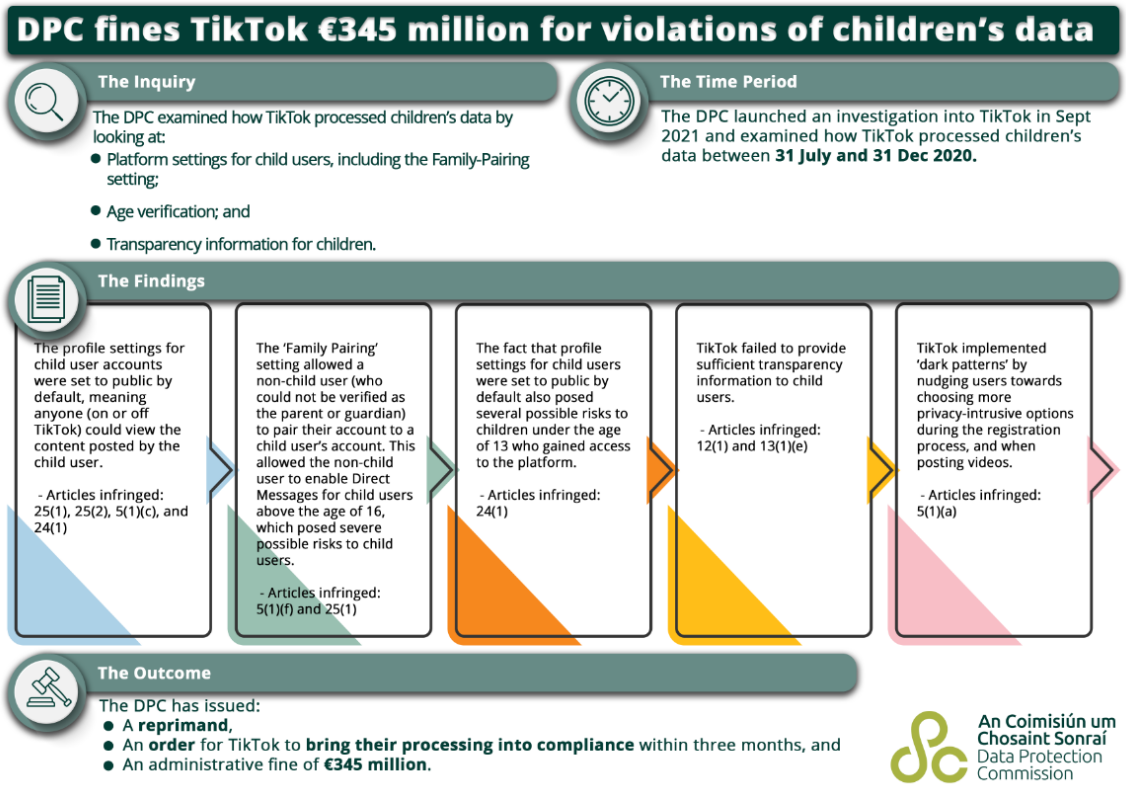
To read more: https://media.defense.gov/2023/Aug/03/2003273618/-1/-1/0/JOINT-CSA-2022-TOP-ROUTINELY-EXPLOITED-VULNERABILITIES.PDF

Number 3

Irish Data Protection Commission announces €345 million fine of TikTok

An Coimisiún um Chosaint Sonraí
Data Protection Commission

The Data Protection Commission (DPC) adopted its final decision regarding its inquiry into TikTok Technology Limited (TTL) on 1 September 2023.



This own-volition inquiry sought to examine the extent to which, during the period between 31 July 2020 and 31 December 2020 (the Relevant Period), TTL complied with its obligations under the GDPR in relation to its processing of personal data relating to child users of the TikTok platform in the context of:

1. Certain TikTok platform settings, including public-by-default settings as well as the settings associated with the 'Family Pairing' feature; and

2. Age verification as part of the registration process.

As part of the inquiry, the DPC also examined certain of TTL's transparency obligations, including the extent of information provided to child users in relation to default settings.

At the conclusion of its investigation, the DPC submitted a draft decision to all Supervisory Authorities Concerned (CSAs), for the purpose of Article 60(3) GDPR, on 13 September 2022. The DPC's draft decision proposed findings of infringement of Articles 5(1)(c), 5(1)(f), 24(1), 25(1), 25(2), 12(1) and 13(1)(e) GDPR, in relation to the above processing.

While there was broad consensus on the DPC's proposed findings, objections to the draft decision were raised by the Supervisory Authorities (each an SA, collectively SAs) of Italy and Berlin (acting on behalf of itself and the Baden-Württemberg SA).

The objection raised by the Berlin SA sought the inclusion of an additional finding of infringement of the Article 5(1)(a) GDPR principle of fairness as regards 'dark patterns' while the objection raised by the Italian SA sought to reverse the DPC's proposed finding of compliance with Article 25 GDPR, as regards TTL's approach to age verification during the Relevant Period.

The DPC was unable to reach consensus with the CSAs on the subject-matter of the objections and, in the circumstances, decided to refer the objections to the EDPB for determination pursuant to the Article 65 GDPR dispute resolution mechanism.

The European Data Protection Board adopted its binding decision on the subject matter of the objections on 2 August 2023 with a direction that the DPC must amend its draft decision to include a new finding of infringement of the Article 5(1)(a) GDPR principle of fairness, further to the objection raised by the Berlin SA, and to extend the scope of the existing order to bring processing into compliance, to include reference to the remedial work required to address this new finding of infringement.

The DPC's decision, which was adopted on 1 September 2023, records findings of infringement of Articles 5(1)(c), 5(1)(f), 24(1), 25(1), 25(2), 12(1), 13(1)(e) and 5(1)(a) GDPR. The decision further exercises the following corrective powers:

- A reprimand;
- An order requiring TTL to bring its processing into compliance by taking the action specified within a period of three months from the date on which the DPC's decision is notified to TTL; and
- Administrative fines totalling €345 million.

For more information, the EDPB has published the Article 65 decision and the final decision on its website. You may visit: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en

To read more: https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok

Number 4

Data Governance Act: common logos to easily identify trusted EU data intermediaries and data altruism organisations to re-use data

The Commission has introduced common logos to easily identify trusted data intermediation service providers and data altruism organisations in the EU, which will connect data holders, both individuals and companies with data users.

Identifying trusted data intermediation services and data altruism organisations is part of the implementation of the Data Governance Act.

The data intermediation services and data altruism organisations that satisfy the conditions enshrined in the Data Governance Act and opt for the use of the logos, will have to display the logo clearly on every online and offline publication.

The use of these logos at EU level will differentiate the recognised trusted services from other services, contributing to transparency in the data market.

The logo for data altruism organisations recognised in the EU must be accompanied by a QR code with a link to the EU public register of recognised data altruism organisations, which will be available as of 24 September 2023.

The logos have been adopted through an Implementing Regulation and will be registered as trademarks, to protect them from improper use.

Data is a powerful resource that can fuel innovation across Europe's industrial ecosystems.

The Data Governance Act aims to make more data available by increasing trust in data-sharing and tackling technical barriers.

To learn more: https://digital-strategy.ec.europa.eu/en/news/data-governance-act-common-logos-easily-identify-trusted-eu-data-intermediaries-and-data-altruism

https://digital-strategy.ec.europa.eu/en/library/data-governance-act-implementing-regulation

Number 5

Attorney General Bonta Announces $93 Million Settlement Regarding Google's Location-Privacy Practices

California Attorney General Rob Bonta announced a $93 million settlement with Google resolving allegations that its location-privacy practices violated California consumer protection laws.

The settlement follows a multi-year investigation by the California Department of Justice that determined Google was deceiving users by collecting, storing, and using their location data for consumer profiling and advertising purposes without informed consent.

In addition to paying $93 million, Google has agreed to accept strong injunctive terms to deter future misconduct.

"Our investigation revealed that Google was telling its users one thing – that it would no longer track their location once they opted out – but doing the opposite and continuing to track its users' movements for its own commercial gain. That's unacceptable, and we're holding Google accountable with today's settlement," said Attorney General Bonta. "I want to thank my Consumer Protection Section for their work on this matter and for securing important privacy safeguards on behalf of all Californians."

Based in Mountain View, California, Google generates the majority of its revenue from advertising, and location-based advertising (or geotargeted advertising) is a critical feature of Google's advertising platform because advertisers want the ability to market to users based on their geographical locations. Google also uses their location data to build behavioral profiles of users to help determine which ads to serve users.

In a complaint filed with the proposed stipulated judgment, Attorney General Bonta alleges that Google deceived users in numerous ways regarding how it collected, stored, and used a person's location data.

For example, the complaint alleges that Google falsely told users that if they turned off the "Location History" setting, then Google would not store their location data. However, according to the complaint, even when a user turned Location History off, Google continued to collect and store that user's location data through other sources. The complaint also alleges that

Google deceived users about their ability to opt out of advertisements targeted to their location.

Under the settlement, Google must pay the state $93 million and be subject to a number of injunctive terms that will protect the privacy interests of California users, including requirements that Google:

- Show additional information to users when enabling location-related account settings.
- Provide more transparency about location tracking.
- Provide users with detailed information about the location data that Google collects and how it is used through a "Location Technologies" webpage.
- Disclose to users that their location information may be used for ads personalization.
- Disclose to users before using Location History data to build ad targeting profiles for users.
- Obtain review by Google's internal Privacy Working Group and document approval for all material changes to location-setting and ads personalization disclosures that will have a material impact on privacy.

A copy of the complaint and proposed stipulated judgment, which details the aforementioned settlement terms and remains subject to court approval, can be found at:
https://oag.ca.gov/system/files/attachments/press-docs/Filed%20stamped%20Google%20Complaint.pdf

https://oag.ca.gov/system/files/attachments/press-docs/Google%20Proposed%20Order%20FINAL%20%283%29.pdf

To read more: https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-93-million-settlement-regarding-google%E2%80%99s

Number 6

NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers

Three new algorithms are expected to be ready for use in 2024. Others will follow.

Last year, the National Institute of Standards and Technology (NIST) selected four algorithms designed to withstand attack by quantum computers. Now the agency has begun the process of standardizing these algorithms — the final step before making these mathematical tools available so that organizations around the world can integrate them into their encryption infrastructure.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium , FALCON and SPHINCS+ (read as "Sphincs plus"). Reviewers noted the high efficiency of the first two, and NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but it is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections.

Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions. The additional four algorithms still under consideration are designed for general encryption and do not use structured lattices or hash functions in their approaches.

While the standard is in development, NIST encourages security experts to explore the new algorithms and consider how their applications will use them, but not to bake them into their systems yet, as the algorithms could change slightly before the standard is finalized.

NIST released draft standards for three of the four algorithms it selected in 2022. A draft standard for FALCON, the fourth algorithm, will be released in about a year.

NIST is calling on the worldwide cryptographic community to provide feedback on the draft standards until Nov. 22, 2023.

"We're getting close to the light at the end of the tunnel, where people will have standards they can use in practice," said Dustin Moody, a NIST mathematician and leader of the project. "For the moment, we are requesting feedback on the drafts. Do we need to change anything, and have we missed anything?"

Sensitive electronic information, such as email and bank transfers, is currently protected using public-key encryption techniques, which are based on math problems a conventional computer cannot readily solve.

Quantum computers are still in their infancy, but a sufficiently powerful one could solve these problems, defeating the encryption. The new standards, once completed, will provide the world with its first tools to protect sensitive information from this new kind of threat.

To read more: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

Number 7

Voices from DARPA Episode 71: The Quantum Mechanic

In popular culture, quantum is a descriptive term often added to various technical topics and projects to make them sound cool.

But what is quantum mechanics, really, and how do we know whether quantum technologies will transform computing, communications, sensing, and a host of other fields?

To find answers, join us for a new episode of the Voices from DARPA podcast series, where we hear from Dr. Joe Altepeter, a quantum physicist in DARPA's Defense Sciences Office (DSO).

Altepeter helps clarify what for most of us is a complicated subject, providing a basic understanding of quantum and describing his two DARPA programs focused on quantum computing.

The first program, called Quantum Benchmarking, aims to estimate the long-term utility of quantum computers by creating new benchmarks, or yardsticks, that quantitatively measure how useful a quantum computer would be at solving problems we care about.

The second related program, Underexplored Systems for Utility-Scale Quantum Computing (US2QC), seeks to determine if an underexplored approach to quantum computing is capable of achieving utility-scale operation (i.e., its computational value exceeds its cost) much faster than conventional predictions.

Buckle up and tune in for a fast-paced tutorial from DARPA's quantum mechanic!

Dr. Joe Altepeter, Defense Sciences Office (DSO), Program Manager

Dr. Joe Altepeter joined DARPA in the Defense Sciences Office in September 2019. His interests include quantum and quantum-inspired technologies, novel sensors and imaging systems, hyperspectral awareness, and the visualization of useful data from complex physical systems.

Prior to joining DARPA as a program manager, Altepeter was an associate at Berberian & Company, LLC, where he acted as a scientific and technical consultant for DARPA and the Intelligence Advanced Research Projects Agency, IARPA. Before his consulting work at DARPA, he was an assistant research professor in Northwestern University's Electrical Engineering &

Computer Science Department, an intelligence community postdoctoral fellow, a National Science Foundation graduate research fellow, and a Fulbright Scholar. Altepeter received his Bachelor of Science in physics from Washington University in Saint Louis, and his doctorate in physics from the University of Illinois at Urbana-Champaign.

Blubrry (podcast host): https://blubrry.com/voices_from_darpa/115097241/episode-71-the-quantum-mechanic/

YouTube: https://www.youtube.com/watch?v=_aJEw8dU0tg

iTunes: https://podcasts.apple.com/us/podcast/voices-from-darpa/id1163190520

To read more: https://www.darpa.mil/news-events/2023-08-18

Number 8

DOD Announces Establishment of Generative AI Task Force

U.S. Department of Defense

The Department of Defense (DoD) announced the establishment of a generative artificial intelligence (AI) task force, an initiative that reflects the DoD's commitment to harnessing the power of artificial intelligence in a responsible and strategic manner.

Deputy Secretary of Defense Dr. Kathleen Hicks directed the organization of Task Force Lima; it will play a pivotal role in analyzing and integrating generative AI tools, such as large language models (LLMs), across the DoD.

"The establishment of Task Force Lima underlines the Department of Defense's unwavering commitment to leading the charge in AI innovation," Hicks said.

"As we navigate the transformative power of generative AI, our focus remains steadfast on ensuring national security, minimizing risks, and responsibly integrating these technologies. The future of defense is not just about adopting cutting-edge technologies, but doing so with foresight, responsibility, and a deep understanding of the broader implications for our nation."

Led by the Chief Digital and Artificial Intelligence Office (CDAO), Task Force Lima will assess, synchronize, and employ generative AI capabilities across the DoD, ensuring the Department remains at the forefront of cutting-edge technologies while safeguarding national security.

CDAO

Chief Digital & Artificial Intelligence Office
9010 DEFENSE PENTAGON, ROOM 3A268
WASHINGTON, D.C. 20301-1600

Generative Artificial Intelligence Coordination and Governance Plan

Generative artificial intelligence (AI) capabilities such as Large-Language Models (LLMs) are growing in popularity, capability, and impact around the globe. These capabilities are trained on massive datasets to generate content to a level of detail and semantic coherence that mimics human authorship. These capabilities unlock new opportunities, just as they pose significant new and enduring risks. Within this rapidly evolving space, it will be critical to coordinate experimentation, findings, guidance, and messaging across the Department. The Chief Digital and Artificial Intelligence Officer (CDAO) Council will serve as the focal point for Department of Defense (DoD)-wide coordination and synchronization of generative AI related materiel and non-materiel issues. The Council will guide and prioritize the activities of Task Force Lima and disseminate Task Force findings related to technical integration and use. Recognizing the rapid innovation in foundational and multi-modal models, the CDAO Council's oversight, as well as experiments organized by Task Force Lima, will maintain a broad technical approach in their evaluation of generative AI capabilities and applications. It will not focus exclusively on LLMs.

"The DoD has an imperative to responsibly pursue the adoption of generative AI models while identifying proper protective measures and mitigating national security risks that may result from issues such as poorly managed training data," said Dr. Craig Martell, the DoD Chief Digital and Artificial Intelligence Officer.

"We must also consider the extent to which our adversaries will employ this technology and seek to disrupt our own use of AI-based solutions."

Leveraging partnerships across the Department, Intelligence Community and other government agencies, the task force will help minimize risk and redundancy while pursuing generative AI initiatives across the Department.

Artificial intelligence has emerged as a transformative technology with the potential to revolutionize various sectors, including defense. By leveraging generative AI models, which can use vast datasets to train algorithms and generate products efficiently, the Department aims to enhance its operations in areas such as warfighting, business affairs, health, readiness, and policy.

"The adoption of artificial intelligence in defense is not solely about innovative technology but also about enhancing national security," said U.S. Navy Capt. M. Xavier Lugo, Task Force Lima mission commander and member of the CDAO's Algorithmic Warfare Directorate.

"The DoD recognizes the potential of generative AI to significantly improve intelligence, operational planning, and administrative and business processes. However, responsible implementation is key to managing associated risks effectively."

The CDAO became operational in June 2022 and is dedicated to integrating and optimizing artificial intelligence capabilities across the DoD.

The office is responsible for accelerating the DoD's adoption of data, analytics, and AI, enabling the Department's digital infrastructure and policy adoption to deliver scalable AI-driven solutions for enterprise and joint use cases, safeguarding the nation against current and emerging threats.

For more information about Task Force Lima, please visit the CDAO website at ai.mil. You can also connect with the CDAO on LinkedIn (@ DoD Chief Digital and Artificial Intelligence Office) and Twitter (@dodcdao). Additional updates and news can be found on the CDAO Unit Page on DVIDS.

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 10 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Establishment of Chief Digital and Artificial Intelligence Officer Generative Artificial Intelligence and Large Language Models Task Force, Task Force Lima

Dr. Craig Martell
Chief Digital and Artificial Intelligence Officer

Ms. Margie Palmieri
Deputy Chief Digital and Artificial Intelligence Officer

To read more: https://media.defense.gov/2023/Aug/10/2003279040/-1/-1/1/ESTABLISHMENT_OF_CDAO_GENERATIVE_AI_AND_LARGE_LANGUAGE_MODELS_TASK_FORCE_TASK_FORCE_LIMA_OSD006491-23_RES_FINAL.PDF

Number 9

Ransomware, extortion and the cyber crime ecosystem

A white paper from the NCSC and the National Crime Agency (NCA)

National Cyber Security Centre

The cyber crime ecosystem

Most of the serious cyber attacks have traditionally been carried out by OCGs such as EvilCorp, which comprise highly organised criminals operating much like legitimate businesses with offices, salaries, holiday and sick pay, and other benefits.

There's also a number of smaller, less-organised criminal groups and criminal microservices traded on illicit forums and marketplaces, all supporting each other.

While cyber crime exists in most countries around the world, the major threat to the UK emanates from the Russian-speaking community that have benefited from the larger OCGs helping shape the forums where these services are traded.

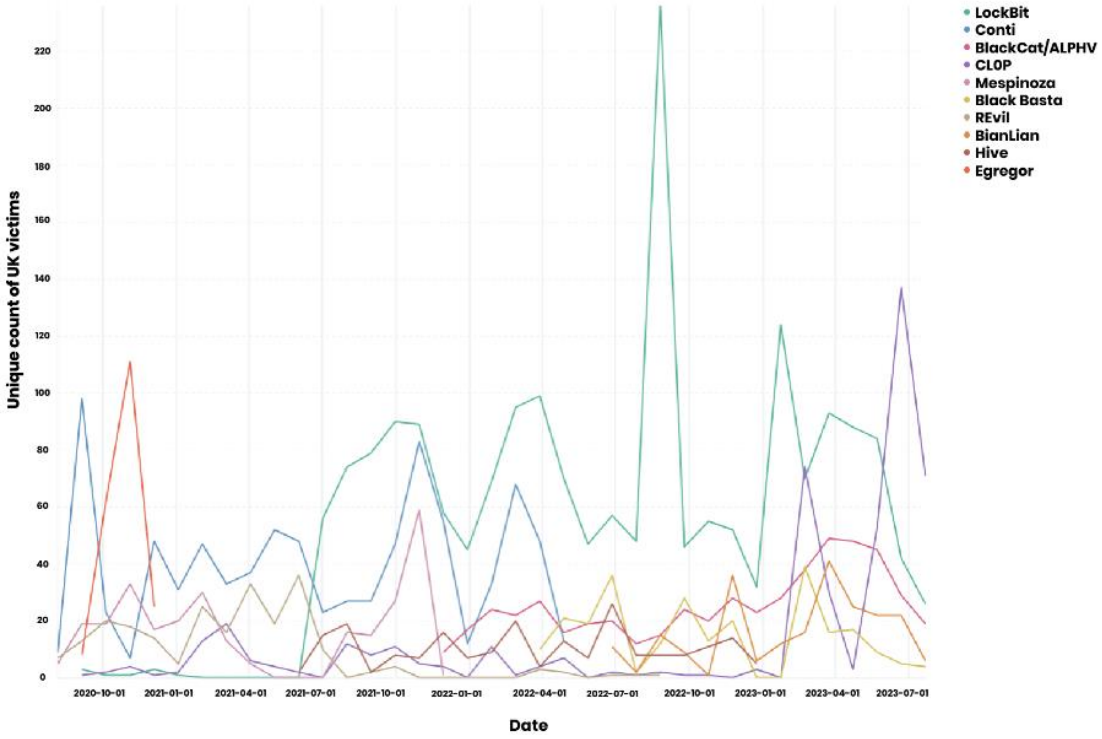


FIGURE 1. DATA LEAK VICTIMS BY LEAK SITE BRAND. SOURCE: SECUREWORKS

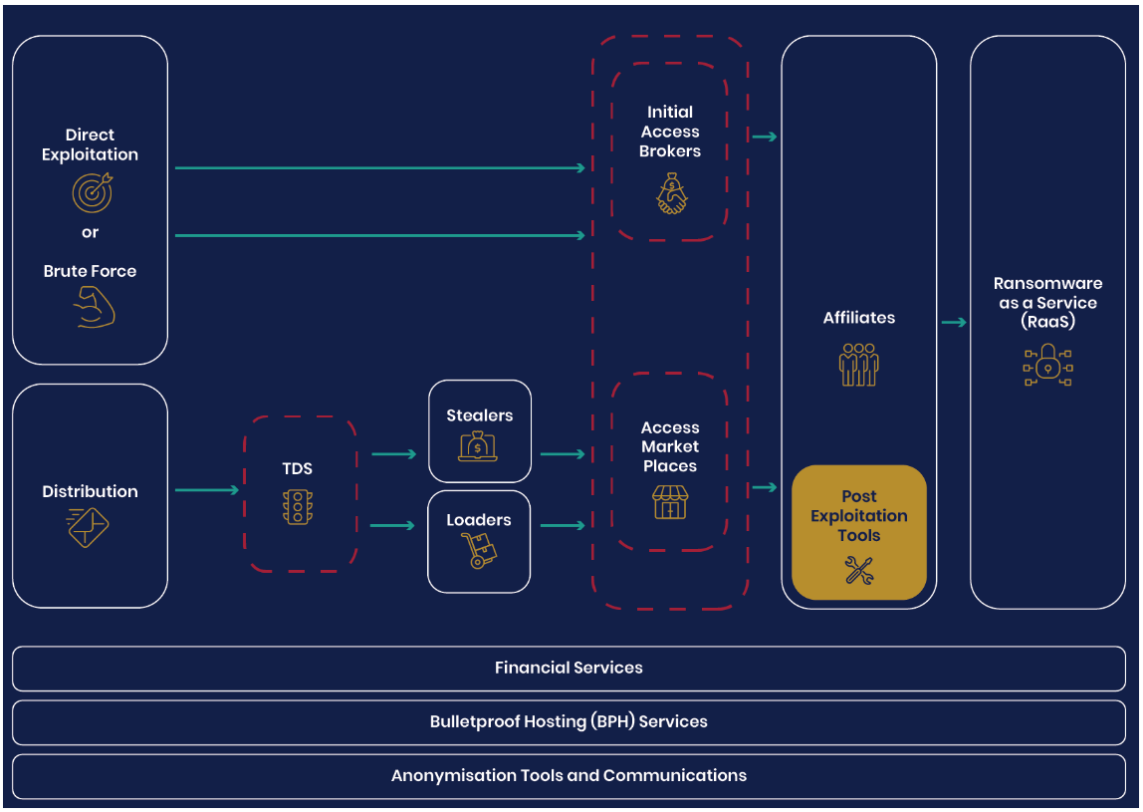
Like other criminal services, ransomware has been adapting to this marketplace to become more accessible and scalable through groups selling ransomware as a service (RaaS).

The resulting increase in criminals adopting ransomware and extortion tactics means that smaller criminal groups, working together, can make a large impact.

Sanctions, indictments and rewards levied on the likes of EvilCorp (and the group behind Conti) has seen them draw on the wider ecosystem to distance themselves from the larger OCG branding.

Figure 1 is an estimate of the number of UK victims from the top 10 ransomware variants over the last 3 years. It shows that over time, some of the previously dominant groups (such as Conti and Egregor) have disappeared while more brands of 'as a service' data leak sites (such as ALPHV, Lockbit and Hive) have become available.

The numbers here can only be taken as an indication of the true volume, as any victims that paid the ransom will not appear on the leak sites (and some ransomware variants do not adopt data leak tactics).



Despite the variety of criminal services available, there is a high level attack path for ransomware that can be broken into functions delivered by different malicious actors (Figure 2).

The chronological flow of an attack is typically left to right, starting with an initial interaction with the victim on the left, and increasing in impact

moving towards the right. In many cases, organisations are not aware that they have become a victim until the very end of this process.

It's worth noting that:

- each function can be conducted by a different threat actor and sold to each other as a service
- malicious actors can execute more than one function themselves as fits their working methods, skills and capabilities
- some of these functions are also optional, such as TDS (Traffic Distribution Systems), which is used in some malware delivery, but not others.

This attack path is supported by a wide range of services, including criminal forums for discussing and exchanging services, anonymisation tools and malicious 'bulletproof' hosting that claim to provide infrastructure services that are resilient to takedown from law enforcement.

Each of these underpinning services are necessary for the ecosystem to function but are outside the scope of this document.

CONTENTS

To read more: https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem

Number 10

Security Incident

We were recently informed that on Saturday, August 19, 2023, a cyber threat actor targeted a T-Mobile US., Inc. account belonging to a Kroll employee in a highly sophisticated "SIM swapping" attack.

Specifically, T-Mobile, without any authority from or contact with Kroll or its employee, transferred that employee's phone number to the threat actor's phone at their request.

As a result, it appears the threat actor gained access to certain files containing personal information of bankruptcy claimants in the matters of BlockFi, FTX and Genesis.

Immediate actions were taken to secure the three affected accounts.

Affected individuals have been notified by email.

We are cooperating with the FBI and a full investigation is underway. We have no evidence to suggest other Kroll systems or accounts were impacted.

Please be advised that Kroll Restructuring Administration will never ask or require you to do any of the following in connection with the processing of bankruptcy claims or the distribution of assets:

1. Link a cryptocurrency wallet to a website or application
2. Provide your seed phrase or private keys
3. Download any software or use a particular wallet application
4. Provide your password over email, text message or over the phone
5. Provide personal identifying information, such as your birthday or social security number, over email, social media or in any manner other than as described in a Court-approved process posted to Kroll Restructuring Administration's case website or the Court's docket

Across our firm, we continue to prioritize data security and information protection.

We deeply regret any inconvenience or concern this situation may have caused and we will continue to prioritize the safety and trust of our clients, partners and community.

To read more: https://www.kroll.com/en/about-us/news/security-incident

Number II

Supervisory cooperation in the fight against financial crime is improving

The European Banking Authority (EBA) published its third Report on the functioning of anti-money laundering and countering the financing of terrorism (AML/CFT) colleges.

The Report finds that competent authorities had taken important steps to improve the functioning of AML/CFT colleges. Nevertheless, many colleges had not reached full maturity.

The Report highlights good practices that will be useful for competent authorities to further improve the effectiveness of AML/CFT colleges and of supervisory outcomes.

AML/CFT colleges are permanent structures that serve to enhance cooperation between different supervisors involved in the supervision of cross-border institutions.

As of 31 December 2022, competent authorities had reported 229 fully operating colleges to the EBA. An additional 54 colleges had yet to hold their first meeting.

This Report sets out findings and observations from the monitoring of AML/CFT colleges in 2022 done by EBA staff. This suggests that college members had taken important steps to improve the effectiveness of AML/CFT colleges.

More specifically, members were approaching the organisation of AML/CFT colleges in a more structured manner, which contributed to the exchange of more substantive and actionable information than was the case in the previous years.

Prudential supervisors and financial intelligence units (FIUs) participated in a greater number of colleges. As a result, supervisors had access to more relevant information that could timely inform their approach to the supervision of institutions operating on a cross-border basis. In some colleges, members had taken steps to identify common issues and address these issues in a coordinated manner.

Despite these notable achievements, AML/CFT colleges had not yet reached full maturity. Competent authorities reported that approximately 50 colleges had not yet held their first meeting. In some colleges the sharing of relevant information remained insufficient. Lastly, the onboarding of third country authorities was still a challenge and only a few of them could participate in college meetings.

The Report highlights good practices that could be useful for competent authorities to overcome these challenges and further improve the effectiveness of AML/CFT colleges going forward.

Figure 1.: Number of AML/CFT colleges established between 01/01/2022 and 31/12/2022 per country and per sector

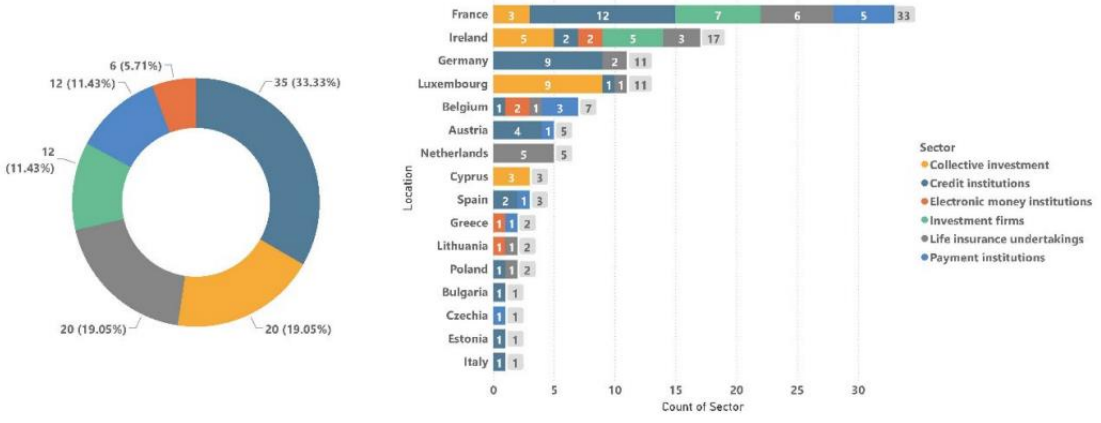
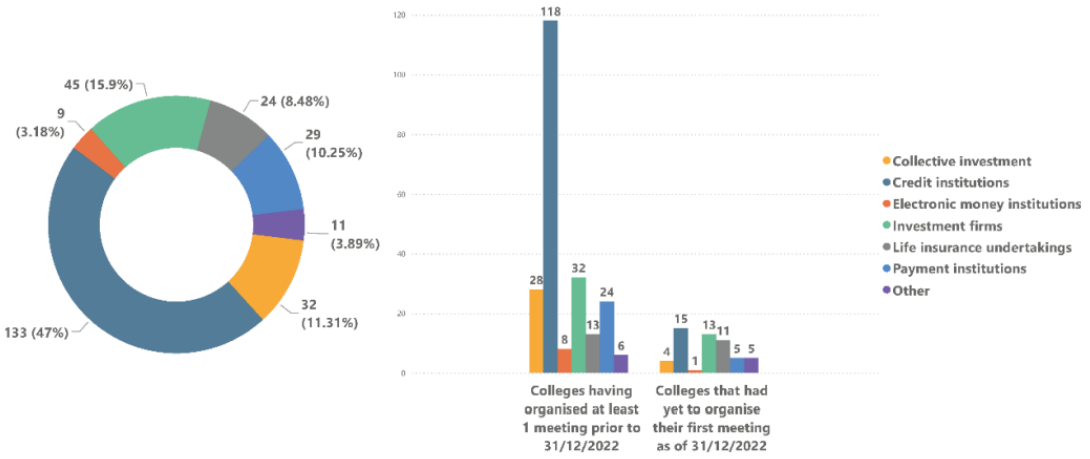


Figure 2.: Total number of AML/CFT colleges per sector



To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1061535/Report%20on%20the%20functioning%20of%20AMLCFT%20colleges%20in%202022.pdf

Number 12

Seeking Legitimacy: Considerations for Strategic Communications in the Digital Age

While the Soviet Union in particular developed well-honed strategies for propaganda during the Cold War, the last ten years have seen an explosion in the speed and reach of a new breed of disinformation.

Messages now travel far and wide on social media at the speed of thought, as people look to Twitter and TikTok for news.

Governments find themselves attempting to sort out which stories will pass and which stories will stick, as they struggle to bet limited resources against emerging problems.

Democracies are particularly vulnerable to disinformation because laws are designed to protect free speech, not to protect the state from speech.

Propaganda spreads easily across borders in the digital age.

One recently uncovered web portal served multiple potential sympathisers in several languages; it provided pro-Kremlin activists from many countries with templates for letters opposing the destruction of Soviet monuments, including offers to help write and translate the letters into English and French.

By one estimate, dozens of well-crafted pieces of pro-Kremlin disinformation appear every week—more than any country can handle alone.

Tactical response to specific pieces of information is difficult. Doing it well requires rapid attribution of the disinformation, agile crafting of a response, and a clear grasp of what is legally permissible for that government.

Teamwork across national borders can only help with the daunting task of anticipation and agility. Even if governments choose not to mix it up in the melee of hand-to-hand information combat, with its attendant risks, most seek to create more resilient populations with media literacy programmes. Further, all NATO allies seek legitimacy when speaking publicly about

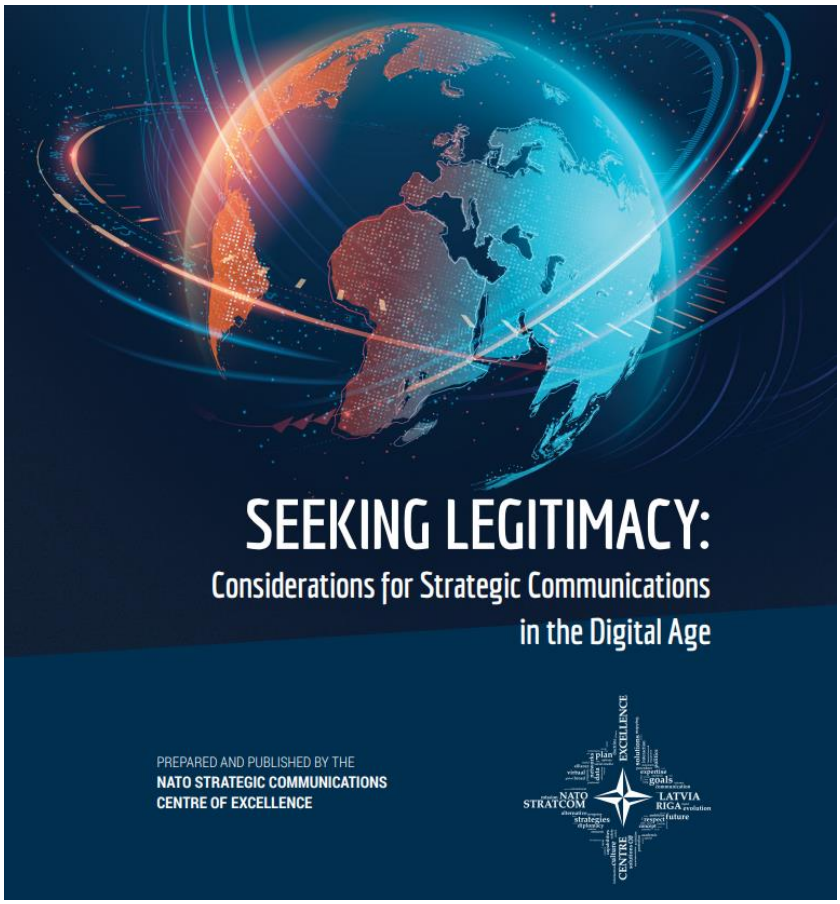
national and NATO priorities, in particular countering negative NATO narratives.

Each nation will face its own calculus on which stories to engage and which to dismiss, but they would do well to remember that, just as disinformation travels across borders, so can government messages, often reaching audiences far removed from the intended recipients and unintentionally clashing with other official messages.

Indeed, artificial intelligence and machine learning (AI/ML) are already having an impact on messaging practices, and we are likely to see a near future where AI/ML can craft tailored messages in any language at scale, both for good and for ill.

Before that future becomes the present, governments must find ways to align messaging whenever possible to have a fighting chance against smart and scalable disinformation campaigns.

To read more: https://stratcomcoe.org/publications/seeking-legitimacy-considerations-for-strategic-communications-in-the-digital-age/289



CONTENTS

Number 13

From the Finnish Customs website tulli.fi

Contents of the Piilopuoti web server seized by Finnish Customs – major breakthrough in the anonymous Tor network

TULLI

Finnish Customs has seized the “Piilopuoti” web server in cooperation with foreign authorities, and seized the contents of the server. The web server was operational in the Tor network since 2022.

The Finnish-language website that sold narcotics opened on 18 May 2022. The site operated as a hidden service in the encrypted Tor network.

The site has been used in anonymous criminal activities such as narcotics trade. As a rule, the narcotics sold on the site were smuggled to Finland from abroad.

During the preliminary investigation into the case, Finnish Customs has conducted extensive cooperation with German and Lithuanian authorities, as well as Europol, the European Union Agency for Criminal Justice Cooperation (Eurojust), authorities of other countries, and various police units in Finland.

The criminal investigation is still underway. At this point, Finnish Customs and our international cooperation partners will not provide any further information on the matter.

To read more: https://tulli.fi/en/-/contents-of-the-piilopuoti-web-server-seized-by-finnish-customs-major-breakthrough-in-the-anonymous-tor-network

Number 14

What's Wrong With This Picture? NIST Face Analysis Program Helps to Find Answers

Face recognition software is commonly used as a gatekeeper for accessing secure websites and electronic devices, but what if someone can defeat it by simply wearing a mask resembling another person's face?

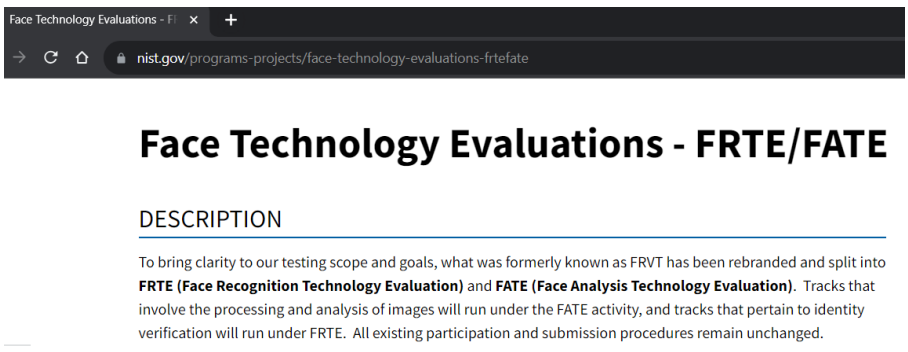
Newly published research from the National Institute of Standards and Technology (NIST) reveals the current state of the art for software designed to detect this sort of spoof attack.

The new study appears together with another that evaluates software's ability to call out potential problems with a photograph or digital face image, such as one captured for use in a passport.

Together, the two NIST publications provide insight into how effectively modern image-processing software performs an increasingly significant task: face analysis.

Face analysis is distinct from face recognition, which may be a more familiar term. Broadly speaking, face recognition aims to identify a person based on an image, while face analysis is concerned with image characterization, such as flagging images that are themselves problematic — whether because of nefarious intent or simply due to mistakes in the photo's capture.

The two publications are the first on the subject to appear since NIST divided its Face Recognition Vendor Test (FRVT) program into two tracks, Face Recognition Technology Evaluation (FRTE) and Face Analysis Technology Evaluation (FATE). You may visit: https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate



Efforts involving the processing and analysis of images, as the two new publications do, now are categorized under the FATE track.

Technology tests on both tracks are meant to provide information on the capabilities of algorithms to inform developers, end users, standards processes, and policy and decision makers.

“Can a given software algorithm tell you whether there’s something wrong with a face image?” said Mei Ngan, a NIST computer scientist. “For example, are the person’s eyes closed? Is the image blurry? Is the image actually a mask that looks like another person’s face? These are the sort of defects that some developers claim their software can detect, and the FATE track is concerned with evaluating these claims.”

Ngan is an author of the first study, Face Analysis Technology Evaluation (FATE) Part 10: Performance of Passive, Software-Based Presentation Attack Detection (PAD) Algorithms, which evaluated the ability of face analysis algorithms to detect whether these issues constituted evidence of a spoofing attack, referred to as PAD.

The research team evaluated 82 software algorithms submitted voluntarily by 45 unique developers. The researchers challenged the software with two different scenarios: impersonation, or trying to look like another specific person; and evasion, or trying to avoid looking like oneself.

The team evaluated the algorithms with nine types of presentation attacks, with examples including a person wearing a sophisticated mask designed to mimic another person’s face and other simpler attacks such as holding a photo of another person up to the camera or wearing an N95 mask that hid some of the wearer’s face.

The results varied widely among PAD algorithms, and Ngan noted one thing: Some developers’ algorithms worked well at detecting a given type of presentation attack in the images, but none could detect all attack types tested.

“Only a small percentage of developers could realistically claim to detect certain presentation attacks using software,” she said. “Some developers’ algorithms could catch two or three types, but none caught them all.”

Among the other findings was that even the top-performing PAD algorithms worked better in tandem.

“We asked if it would lower the error rate if you combined the results from different algorithms. It turns out that can be a good idea,” Ngan said. “When we chose four of the top performing algorithms on the

impersonation test and fused their results, we found the group did better than any one of them alone."

To read more: https://www.nist.gov/news-events/news/2023/09/whats-wrong-picture-nist-face-analysis-program-helps-find-answers

Number 15

Director of National Intelligence Avril D. Haines Releases the 2023 National Intelligence Strategy for the Intelligence Community

The Director of National Intelligence Avril D. Haines released the 2023 National Intelligence Strategy (NIS), which provides strategic direction for the Intelligence Community (IC) over the next four years.

“The National Intelligence Strategy articulates what the Intelligence Community will need to cultivate to be effective in the future: an information and technological edge, a broad array of partnerships, and a talented and diverse workforce as we pursue our vision of an IC that embodies America’s values,” said Director of National Intelligence Avril Haines.

“It also highlights the expanding role of the IC in supporting the resilience of our national critical infrastructure and that of our allies and partners.”

The six goals outlined in this NIS reflect key elements of the current strategic environment: the centrality of strategic competition between the United States and the People’s Republic of China (PRC) and the Russian Federation; the growing importance of emerging technologies, supply chains, and economic statecraft to national security; the increasing influence of sub-national and non-state actors; and the challenges stemming from the convergence of shared global challenges, such as climate change and health security.

The NIS is a foundational document for the IC and reflects the input of leaders from each of the 18 intelligence elements, as it directs the operations, investments, and priorities of the collective.

Additional IC leaders shared the following statements on the strategy’s announcement.

Director Bill Burns, Central Intelligence Agency: “Today’s world is increasingly complicated and contested, and one in which humanity faces both peril and promise. We are in a transformative era marked by strategic competition, rapid technological change, and increasingly worrisome transnational threats. To meet this moment, we in the Intelligence Community must be agile and innovative.

The National Intelligence Strategy lays out how we must approach the transforming world in order to provide needed and timely insights by emphasizing the importance of investing in partnerships, technological innovation, diverse talent, and expertise to address issues from competition with China to climate change and global food insecurity."

General Paul Nakasone, Director, National Security Agency: "Our efforts to better understand the PRC's intents and actions require the combined efforts of the IC, our allies, and partners. Together, we are developing capacity, capability, and resiliency to meet the pacing challenges of our nation and partners. The 2023 National Intelligence Strategy is geared toward making this process a robust reality.

The NIS recognizes a growing competition between democracies and autocracies. Competition spurs innovation, fresh thinking, and, when necessary, action. The NIS identifies six priority goals that will protect not only our nation but also our partners in the years ahead."

The IC is Comprised of the Following 18 Elements:

TWO INDEPENDENT AGENCIES

1. The Office of the Director of National Intelligence (ODNI)
2. The Central Intelligence Agency (CIA)

NINE DEPARTMENT OF DEFENSE ELEMENTS

The following elements also receive guidance and oversight from the Under Secretary of Defense for Intelligence and Security (USD I&S)—

1. The Defense Intelligence Agency (DIA)
2. The National Security Agency (NSA)
3. The National Geospatial-Intelligence Agency (NGA)
4. The National Reconnaissance Office (NRO)
5. U.S. Air Force Intelligence
6. U.S. Navy Intelligence
7. U.S. Army Intelligence
8. U.S. Marine Corps Intelligence
9. U.S. Space Force Intelligence

SEVEN ELEMENTS OF OTHER DEPARTMENTS AND AGENCIES

1. The Department of Energy's Office of Intelligence and Counterintelligence
2. The Department of Homeland Security's Office of Intelligence and Analysis and
3. The intelligence and counterintelligence elements of the U.S. Coast Guard
4. The Department of Justice's Federal Bureau of Investigation and
5. The Drug Enforcement Administration's Office of National Security Intelligence
6. The Department of State's Bureau of Intelligence and Research
7. The Department of the Treasury's Office of Intelligence and Analysis

Director Chris Wray, Federal Bureau of Investigation: "The FBI and our Intelligence Community partners are constantly working to anticipate new

threats to our national security and how to counter those challenges. The new National Intelligence Strategy is a vital guide for all members of the IC.

We face an ever-growing list of challenges and threats to the Homeland, including China's determined efforts to reshape the international order and threaten democratic ideals, cyberattacks and supply chain disruptions by hostile foreign nations and cyber criminals, and narcotics trafficking. As the strategy recognizes, partnerships, innovation, and building and retaining a talented and diverse workforce are the key to successfully answering the threats we face now and in the future."

United as a Community, the 18 intelligence elements will work together to ensure the IC is sufficiently agile, integrated, innovative, and resilient to inform national security and foreign policy decisions, resulting in a Nation that is secure and prosperous.

To read more:
https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf

Cyber Risk GmbH

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

Online Training

Recorded on-demand training and live webinars.

More »

In-house Training

Engaging training classes and workshops.

More »

Social Engineering

Developing the human perimeter to deal with cyber threats.

More »

For the Board

Short and comprehensive briefings for the board of directors.

More »

Assessments

Open source intelligence (OSINT) reports and recommendations.

More »

High Value Targets

They have the most skilled adversaries. We can help.

More »

Cyber security training

Overview

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

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

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

Duration

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

Our Education Method

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

Our Instructors

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

Our websites include:

a. Sectors and Industries.

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

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

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

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

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

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

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

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

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

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

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

b. Understanding Cybersecurity.

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

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

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

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

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

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

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

c. Understanding Cybersecurity in the European Union.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

You may contact:

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

Disclaimer

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

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

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

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

This information:

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

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

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

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

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

- is in no way constitutive of interpretative;

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

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

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

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

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