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

November 2022, top cyber risk and compliance related local news stories and world events

Dear readers,

We carefully consider the consequences of the new Executive Order on *Enhancing Safeguards for United States Signals Intelligence Activities*.

This is a very important development, as it is the US response to a decision of the European Court of Justice (ECJ). On July 16, 2020, the ECJ decided that the *EU-U.S. Privacy Shield framework* (Privacy Shield) was *invalid*. The ECJ upheld the EU Standard Contractual Clauses (SCCs), but decided that before any transfer of data from the EU to the USA, companies and organizations must verify that the parties can provide the level of protection required by the EU law. This is a major challenge for companies and organizations.

The European Court of Justice based its decision on two main grounds:
a. The Privacy Shield did not adequately protect personal data, as a result of the disclosures of personal data to the U.S. intelligence entities.

b. The mechanism created by the Privacy Shield to address complaints by EU citizens, lacked the independence and authority to adopt decisions binding the American *intelligence agencies*.

This is why this executive order is named *"Enhancing Safeguards For United States Signals Intelligence Activities"*.

We all know the difficulties after the EU General Data Protection Regulation (GDPR), that restricts how companies transfer personal data outside the European Union. Only when the EU decides that a particular country provides an adequate level of protection for personal data (there is a formal adequacy decision), the EU allows personal data to flow freely between the EU and the particular country, without the need to rely on additional transfer measures and contractual clauses.

What is next - the European Commission, after consultation with the European Data Protection Board (EDPB), will assess the developments in the USA, to determine whether there is a level of protection in the USA equivalent with the one in the EU.

Well, if you wonder what I believe about the decision of the European Commission, I will remind you what Descartes has said: *"An optimist may see a light where there is none, but why must the pessimist always run to blow it out?"*

What has happened before this executive order?

In March 2022, the European Commission and the United States announced that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the Schrems II decision of July 2020.

The new Framework marked an unprecedented commitment on the U.S. side to implement reforms that will strengthen the privacy and civil liberties protections applicable to U.S. signals intelligence activities.

Under the Trans-Atlantic Data Privacy Framework, the United States is to put in place new safeguards to ensure that *signals surveillance activities* are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities.

The Trans-Atlantic Data Privacy Framework reflected more than a year of detailed negotiations between the U.S. and E.U. led by Secretary of Commerce Gina Raimondo and Commissioner for Justice Didier Reynders. It will provide a basis for trans-Atlantic data flows, which are critical to protecting citizens' rights and enabling trans-Atlantic commerce in all sectors of the economy, including for small and medium enterprises.

Read more at number 2 and 3 below. Welcome to the Top 10 list.

I have heard that *diplomacy* is the art of saying *nice doggie* until you can find a rock.

Well, the Council of the European Union has probably found the rock, and the EU has had enough: Cyber attacks, disinformation, lies, election interference, hybrid war. The Council of the EU is not using diplomatic language anymore. Forget the polite words and the legal complex terms. They do not use the phrase *"we are concerned"*. Look at what they say in the June 2022 Council conclusions on a Framework for a coordinated EU response to *hybrid campaigns* (*they* use the capital letters):

THE COUNCIL OF THE EUROPEAN UNION,

"ACKNOWLEDGES that state and non-state actors are increasingly using hybrid tactics, posing a growing threat to the security of the EU, its Member States and its partners.

RECOGNISES that, for some actors applying such tactics, peacetime is a period for covert malign activities, when a conflict can continue or be prepared for in a less open form.

EMPHASISES that state actors and non-state actors also use information manipulation and other tactics to interfere in democratic processes and to mislead and deceive citizens.

NOTES that Russia's armed aggression against Ukraine is showing the readiness to use the highest level of military force, regardless of legal or humanitarian considerations, combined with hybrid tactics, cyberattacks, foreign information manipulation and interference, economic and energy coercion and an aggressive nuclear rhetoric, and

ACKNOWLEDGES the related risks of potential spillover effects in EU neighbourhoods that could harm the interests of the EU."

"EMPHASISES that when the perpetrator of a hybrid campaign can be identified with a high degree of certainty, asymmetric and proportionate

measures in line with international law may be taken – including forms of diplomatic, political, military, economic or strategic communication – to prevent or respond to a hybrid campaign, including in the event of malicious activities that are not classified as internationally unlawful acts but are considered unfriendly acts."

"STRESSES the need to further develop in 2022 both the EU Hybrid Toolbox and the Foreign Information Manipulation and Interference Toolbox (FIMI toolbox), in line with the guidance given by the Strategic Compass."

What is the *EU Hybrid Toolbox?* Well, the "Strategic Compass of the European Union", approved by the Council in March 2022, covers all the aspects of the security and defence policy in the EU, and is structured around *four pillars*: act, invest, partner and secure.

In the SECURE pillar, we read:

"We need to enhance our ability to anticipate threats, guarantee secure access to strategic domains and protect our citizens. To that end, we will:

- Boost our intelligence capacities, such as the EU Single Intelligence and Analysis Capacity (SIAC) framework to enhance our situational awareness and strategic foresight;

- Create an EU Hybrid Toolbox that brings together different instruments to detect and respond to a broad range of hybrid threats. In this context, we will develop a dedicated toolbox to address foreign information manipulation and interference;

- Further develop the EU Cyber Defence Policy to be better prepared for and respond to cyberattacks; strengthen our actions in the maritime, air and space domains, notably by expanding the Coordinated Maritime Presences to other areas, starting with the IndoPacific, and by developing an EU Space Strategy for security and defence."

Read more at number 22 below.

In 2021, the European Central Bank published a paper with title: "The risk management approach to *macro-prudential* policy". I really liked how the paper started:

"The Stoic philosopher Seneca once observed that *when pleasures have corrupted both mind and body, nothing seems tolerable – not because the suffering is hard, but because the sufferer is soft*.

The quote nicely encapsulates a common view of macro-prudential policy: Make the financial system strong (hard) enough to withstand adverse shocks, taking advantage of good times to build up buffers and increase fortitude."

Seneca has also said that *true happiness is… to enjoy the present, without anxious dependence upon the future,* but you cannot introduce macro-prudential policies with quotes like that.

According to the European Central Bank, the objective of *macro-prudential* policy is to make the financial system strong enough to withstand adverse shocks, taking advantage of good times to increase capital and liquidity buffers.

According to this view, macro-prudential measures are recommended in case *medium-term* downside risks to the economy are deemed too severe.

Such measures, however, can have *short-term* costs in terms of upside potential, or expected growth, of the economy.

In this newsletter, we have the new *Risk Dashboard,* based on Solvency II data from the second quarter of 2022, from the European Insurance and Occupational Pensions Authority (EIOPA). We read:

"*Macro-related risks remain significant* for the insurance sector. Forecasted GDP growth at global level further decreased, and CPI forecasts remained at high level for main geographical areas. Unemployment rate for main geographical areas remained at low level. Weighted average of 10 years swap rates increased. Central banks continue the normalization of their monetary policy."

Read more in Number 9 below.

I loved this name: *Project Tourbillon*.

Project Tourbillon has been launched by the Innovation Hub's Swiss Centre (Bank for International Settlements), and explores how to improve cyber resiliency, scalability and privacy in a prototype Central Bank Digital Currency (CBDC).

In 1801, Abraham-Louis Breguet earned the rights for the *"Tourbillon"* patent. Watches have tourbillons to address the problems with *gravity* that creates a drag on watch's movement.

Breguet had the idea of installing the entire escapement (the balance and spring, the lever and the escape-wheel) inside a mobile carriage that performs a complete rotation each minute.

Project Tourbillon, dealing with a prototype Central Bank Digital Currency (CBDC), is a smart innovative solution that, instead of the problem of gravity, solves the problems that have to so with cyber security and privacy.

A CBDC can offer opportunities that are not possible with cash. A convenient and accessible CBDC could serve as an alternative to potentially unsafe forms of private money, offer users privacy, reduce illegal activity, facilitate fiscal transfers and/or enable "programmable money".

Introducing a CBDC could have financial stability implications that would need to be assessed and managed carefully. These include:

- the potential for *digital bank runs* in times of stress,
- longer-term consequences for bank funding.

Any assessment of the materiality of these sources of financial stability risk, and the effectiveness of possible mitigants, would depend on the specific design of a CBDC and the structure of the financial system in which it might exist. Given designs and systems will *differ* by jurisdiction, so will the broad financial system structural effects and risks, which will require significant research by a central bank to completely understand.

Read more at number 14 below.

We have the new and *very interesting* semi-annual report of the Swiss National Cybersecurity Centre (NCSC), that deals with the most important cyber incidents of the first half of 2022, both in Switzerland and internationally.

The focus topic concerns cyberspace and armed conflicts. We read:

"*Cyberspace and armed conflicts*.

Armed conflicts are increasingly being conducted with the help of cyberattacks. Such attacks can be perpetrated not only by state players, but also by non-state attackers such as hacktivists or criminal groups. The Ukraine conflict in particular shows where cyberattacks can be used as a tool. This multi-faceted issue is the focus topic of this report, which explores it from a variety of angles.

Huge increase in threatening emails

In the first half of 2022, the NCSC saw a huge increase in reports from the general public. By the end of June, the NCSC had received 17,186 reports,

which was around 70% more than in the previous half-year period, when 10,234 reports were received. This considerable increase was driven primarily by reports on threatening emails supposedly from the police, so-called fake extortion emails.

Fraud still leading the pack nationally

During the period under review, most of the reports to the NCSC concerned various forms of fraud (10,447 reports). About half of these were reports concerning fake extortion emails (5,872 reports). Other types of fraud included advance-fee fraud (1,834), fake sextortion (615) and classified ad fraud (419). Reports on phishing and malware remained at the same level as in the previous half-year period.

Heavy losses in investment fraud and business email compromise

Aside from ransomware, the NCSC saw the greatest potential for damage for companies in the phenomenon of business email compromise. In the first half of 2022, the NCSC received 47 reports in this regard, with total losses amounting to CHF 2.3 million. Investment fraud is one of the crimes with the highest losses, especially among private individuals. In the first half of 2022, cases with total losses exceeding CHF 3 million were reported to the NCSC.

Slight decrease in ransomware reports

Although ransomware reports edged down from 91 to 83 relative to the previous half-year period, this form of attack is still the most acute cyberthreat facing organisations in Switzerland. Since the start of the year, various organisations in Switzerland from different sectors have been the target of ransomware attacks.

Spoofing on the rise

The NCSC also saw a dramatic increase in reports concerning falsified (spoofed) telephone numbers. In this case, dubious call centres spoof the caller ID and display the telephone numbers of private individuals, thereby luring the person being contacted into taking the call.

The NCSC received 319 reports in the first half of 2022, whereas there were only 17 reports in the 2021 reporting period."

Read more at number 1 below.

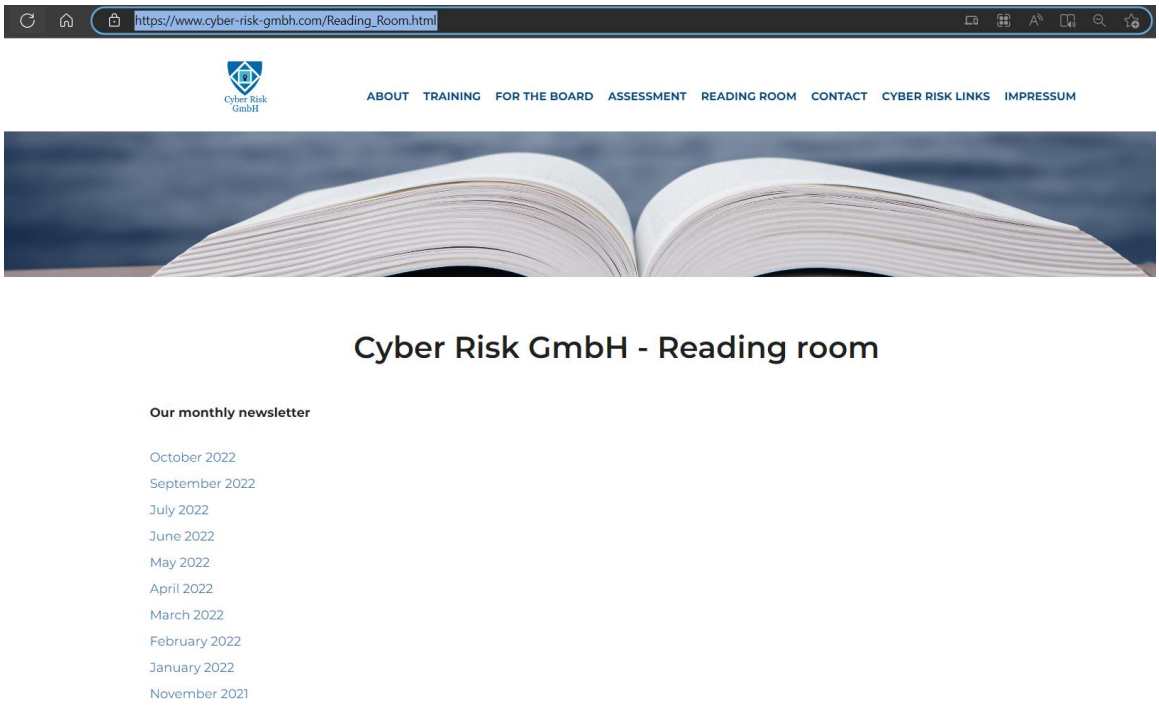
Welcome to our monthly newsletter.

Best regards,

George Lekatis

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

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



Visit our Reading Room at:
https://www.cyber-risk-gmbh.com/Reading_Room.html

Number 1 (Page 13)

NCSC semi-annual report with focus on cyberspace and armed conflicts

Swiss National Cybersecurity Centre NCSC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

National Cyber Security Centre
NCSC

Number 2 (Page 15)

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

THE WHITE HOUSE

Number 3 (Page 35)

Court of Justice of the European Union, the Schrems II decision

The court declared that the Privacy Shield, the EU-US personal data transfer mechanism, was no longer lawful.

COURT OF JUSTICE
OF THE EUROPEAN UNION

Number 4 (Page 40)

Post-Quantum Cryptography, Integration study

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Number 5 (Page 44)

Aurum: a two-tier retail CBDC system

The BIS Innovation Hub and the Hong Kong Monetary Authority have completed a retail CBDC technology prototype.

BIS

HONG KONG MONETARY AUTHORITY
香港金融管理局

Number 6 (Page 47)

Defenders beware: A case for post-ransomware investigations

Microsoft Detection and Response Team (DART)

Microsoft

Number 7 (Page 49)

So long and thanks for all the bits

Ian Levy, the NCSC's departing Technical Director, discusses life, the universe, and everything.

Number 8 (Page 52)

First phase of new supercomputer installed at Los Alamos National Laboratory

Number 9 (Page 54)

Risk Dashboard indicates overall resilience among insurers even amid high macro and market risks

Number 10 (Page 58)

ENISA Threat Landscape 2022

Number 11 (Page 61)

Dozens Charged in $250 Million COVID Fraud Scheme

FBI investigation alleges massive misuse of money meant to feed children during pandemic

Number 12 (Page 64)

National Security Memorandum on Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security

THE WHITE HOUSE

Number 13 (Page 69)

Privacy Policy

TikTok

Number 14 (Page 73)

Project Tourbillon

Launched by the BIS Innovation Hub's Swiss Centre, explores how to improve cyber resiliency, scalability and privacy in a prototype Central Bank Digital Currency (CBDC).

BIS

Number 15 (Page 76)

DEV-0569 finds new ways to deliver Royal ransomware, various payloads - Microsoft Security Threat Intelligence

Microsoft

Number 16 (Page 79)

CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Number 17 (Page 81)

How we handled a recent phishing incident that targeted Dropbox

Dropbox.Tech

Number 18 (Page 84)

NIST's Superconducting Hardware Could Scale Up Brain-Inspired Computing

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Number 19 (Page 87)

31 arrested for stealing cars by hacking keyless tech

EUROPOL

Number 20 (Page 89)

International Regulation of Crypto-asset Activities - Questions for consultation

FSB FINANCIAL STABILITY BOARD

Number 21 (Page 92)

Cybersecurity threats in the health care sector

OFFICE OF SEN. MARK R. WARNER
Cybersecurity is Patient Safety
POLICY OPTIONS IN THE HEALTH CARE SECTOR

Mark R. Warner

NOVEMBER 2022

Number 22 (Page 94)

Council conclusions on a Framework for a coordinated EU response to hybrid campaigns

European Council
Council of the European Union

Number 1

NCSC semi-annual report with focus on cyberspace and armed conflicts

Swiss National Cybersecurity Centre NCSC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

National Cyber Security Centre
NCSC

The latest semi-annual report of the National Cybersecurity Centre NCSC deals with the most important cyberincidents of the first half of 2022 both in Switzerland and internationally.

3.3 Non-state aggressors on both sides

Following the Russian offensive of 24 February 2022, numerous non-state actors (hacktivist organisations and criminal groups) announced their intention to participate in the war in cyberspace.

They either claim attacks as their own or threaten those who attack "their" warring party with reprisals.

In total, more than 80 such non-state groups have been identified. One of the most significant groups on the Russian side is Killnet. In response to the support given to Ukraine and the sanctions against Russia, the group has carried out numerous DDoS attacks.

In particular, websites of airports, state institutions and financial institutions of numerous European countries were affected.

The resulting damage depends heavily on how dependent the respective victims are on their internet presence and how well prepared they are for such attacks.

In most cases, DDoS attacks can be blocked or rendered harmless relatively quickly.

On the Ukrainian side, the Anonymous collective claimed numerous attacks on Russian organisations, as well as on Western companies that continued to operate in Russia.

For example, on 20 March 2022, Anonymous called on Western companies operating in Russia to withdraw from the Russian market within 48 hours.

If they failed to do so, they risked becoming a target of the group. Since then, Anonymous has carried out numerous hack-and-leak attacks:

confidential corporate and government data, mainly from Russia, has been stolen and published.

On 26 February 2022, Ukraine announced the creation of an IT Army of Ukraine and called for volunteers from all over the world to join it and carry out attacks in cyberspace in favour of Ukraine.

One of the main pillars of this group is its Telegram channel, which it uses to communicate the targets of its DDoS attacks. Despite the high frequency of attacks by non-state groups, the impact of these attacks on the course of the war appears marginal so far.

To read more: https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/ncsc-hjb-2022-1.html

Number 2

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

THE WHITE HOUSE

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose.

The United States collects signals intelligence so that its national security decisionmakers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm.

Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment, and the United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners.

At the same time, the United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information. Therefore, this order establishes safeguards for such signals intelligence activities.

Sec. 2. Signals Intelligence Activities.

(a) Principles. Signals intelligence activities shall be authorized and conducted consistent with the following principles:

(i) Signals intelligence activities shall be authorized by statute or by Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and with applicable statutes and Executive Orders, proclamations, and other Presidential directives.

(ii) Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:

(A) signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and

(B) signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(iii) Signals intelligence activities shall be subjected to rigorous oversight in order to ensure that they comport with the principles identified above.

(b) Objectives. Signals intelligence collection activities shall be conducted in pursuit of legitimate objectives.

(i) Legitimate objectives.

(A) Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives:

(1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners;

(2) understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;

(3) understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry;

(4) protecting against foreign military capabilities and activities;

(5) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(6) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(7) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(8) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(9) protecting against threats to the personnel of the United States or of its allies or partners;

(10) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (b)(i) of this section;

(11) protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and

(12) advancing collection or operational capabilities or activities in order to further a legitimate objective identified in subsection (b)(i) of this section.

(B) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that signals intelligence collection activities may be used.

The Director of National Intelligence (Director) shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(ii) Prohibited objectives.

(A) Signals intelligence collection activities shall not be conducted for the purpose of:

(1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;

(2) suppressing or restricting legitimate privacy interests;

(3) suppressing or restricting a right to legal counsel; or

(4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.

(B) It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially. The collection of such information is authorized only to protect the national security of the United States or of its allies or partners.

(iii) Validation of signals intelligence collection priorities.

(A) Under section 102A of the National Security Act of 1947, as amended (50 U.S.C. 3024), the Director must establish priorities for the Intelligence Community to ensure the timely and effective collection of national intelligence, including national intelligence collected through signals intelligence.

The Director does this through the National Intelligence Priorities Framework (NIPF), which the Director maintains and presents to the President, through the Assistant to the President for National Security Affairs, on a regular basis.

In order to ensure that signals intelligence collection activities are undertaken to advance legitimate objectives, before presenting the NIPF or any successor framework that identifies intelligence priorities to the President, the Director shall obtain from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) an assessment as to whether, with regard to anticipated signals intelligence collection activities, each of the intelligence priorities identified in the NIPF or successor framework:

(1) advances one or more of the legitimate objectives set forth in subsection (b)(i) of this section;

(2) neither was designed nor is anticipated to result in signals intelligence collection in contravention of the prohibited objectives set forth in subsection (b)(ii) of this section; and

(3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(B) If the Director disagrees with any aspect of the CLPO's assessment with respect to any of the intelligence priorities identified in the NIPF or successor framework, the Director shall include the CLPO's assessment and the Director's views when presenting the NIPF to the President.

(c) Privacy and civil liberties safeguards. The following safeguards shall fulfill the principles contained in subsections (a)(ii) and (a)(iii) of this section.

(i) Collection of signals intelligence.

(A) The United States shall conduct signals intelligence collection activities only following a determination that a specific signals intelligence collection activity, based on a reasonable assessment of all relevant factors, is necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; it could be used, for example, to ensure alternative pathways for validation or for maintaining reliable access to the same information.

In determining whether to collect signals intelligence consistent with this principle, the United States — through an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees — shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence.

(B) Signals intelligence collection activities shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, not disproportionately impact privacy and civil liberties.

Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.

(C) For purposes of subsection (c)(i) of this section, the scope of a specific signals intelligence collection activity may include, for example, a specific line of effort or target, as appropriate.

(ii) Bulk collection of signals intelligence.

(A) Targeted collection shall be prioritized. The bulk collection of signals intelligence shall be authorized only based on a determination — by an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees — that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection.

When it is determined to be necessary to engage in bulk collection in order to advance a validated intelligence priority, the element of the Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.

(B) Each element of the Intelligence Community that collects signals intelligence through bulk collection shall use such information only in pursuit of one or more of the following objectives:

(1) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(2) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(3) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(4) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(5) protecting against threats to the personnel of the United States or of its allies or partners; and

(6) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (c)(ii) of this section.

(C) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that bulk collection may be used.

The Director shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(D) In order to minimize any impact on privacy and civil liberties, a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (for example, without specific identifiers or selection terms) shall be subject to the safeguards described in this subsection, unless such data is:

(1) used only to support the initial technical phase of the targeted signals intelligence collection activity;

(2) retained for only the short period of time required to complete this phase; and

(3) thereafter deleted.

(iii) Handling of personal information collected through signals intelligence.

(A) Minimization. Each element of the Intelligence Community that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence.

(1) Dissemination. Each element of the Intelligence Community that handles personal information collected through signals intelligence:
(a) shall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended, states may be disseminated in the case of information concerning United States persons;

(b) shall not disseminate personal information collected through signals intelligence solely because of a person's nationality or country of residence;

(c) shall disseminate within the United States Government personal information collected through signals intelligence only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information;

(d) shall take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the United States Government, including to a foreign government or international organization; and

(e) shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of this order.

(2) Retention. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(a) shall retain non-United States persons' personal information collected through signals intelligence only if the retention of comparable information concerning United States persons would be permitted under applicable law and shall subject such information to the same retention periods that would apply to comparable information concerning United States persons;

(b) shall subject non-United States persons' personal information collected through signals intelligence for which no final retention determination has been made to the same temporary retention periods that would apply to comparable information concerning United States persons; and

(c) shall delete non-United States persons' personal information collected through signals intelligence that may no longer be retained in the same manner that comparable information concerning United States persons would be deleted.

(B) Data security and access. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(1) shall process and store personal information collected through signals intelligence under conditions that provide appropriate protection and prevent access by unauthorized persons, consistent with the applicable

safeguards for sensitive information contained in relevant Executive Orders, proclamations, other Presidential directives, Intelligence Community directives, and associated policies;

(2) shall limit access to such personal information to authorized personnel who have a need to know the information to perform their mission and have received appropriate training on the requirements of applicable United States law, as described in policies and procedures issued under subsection (c)(iv) of this section; and

(3) shall ensure that personal information collected through signals intelligence for which no final retention determination has been made is accessed only in order to make or support such a determination or to conduct authorized administrative, testing, development, security, or oversight functions.

(C) Data quality. Each element of the Intelligence Community that handles personal information collected through signals intelligence shall include such personal information in intelligence products only as consistent with applicable Intelligence Community standards for accuracy and objectivity, with a focus on applying standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

(D) Queries of bulk collection. Each element of the Intelligence Community that conducts queries of unminimized signals intelligence obtained by bulk collection shall do so consistent with the permissible uses of signals intelligence obtained by bulk collection identified in subsection (c)(ii)(B) of this section and according to policies and procedures issued under subsection (c)(iv) of this section, which shall appropriately take into account the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(E) Documentation. In order to facilitate the oversight processes set forth in subsection (d) of this section and the redress mechanism set forth in section 3 of this order, each element of the Intelligence Community that engages in signals intelligence collection activities shall maintain documentation to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected.

The content of any such documentation may vary based on the circumstances but shall, to the extent reasonable, provide the factual basis pursuant to which the element of the Intelligence Community, based on a reasonable assessment of all relevant factors, assesses that the signals

intelligence collection activity is necessary to advance a validated intelligence priority.

(iv) Update and publication of policies and procedures. The head of each element of the Intelligence Community:

(A) shall continue to use the policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014 (Signals Intelligence Activities) (PPD-28), until they are updated pursuant to subsection (c)(iv)(B) of this section;

(B) shall, within 1 year of the date of this order, in consultation with the Attorney General, the CLPO, and the Privacy and Civil Liberties Oversight Board (PCLOB), update those policies and procedures as necessary to implement the privacy and civil liberties safeguards in this order; and

(C) shall, within 1 year of the date of this order, release these policies and procedures publicly to the maximum extent possible, consistent with the protection of intelligence sources and methods, in order to enhance the public's understanding of, and to promote public trust in, the safeguards pursuant to which the United States conducts signals intelligence activities.

(v) Review by the PCLOB.

(A) Nature of review. Consistent with applicable law, the PCLOB is encouraged to conduct a review of the updated policies and procedures described in subsection (c)(iv)(B) of this section once they have been issued to ensure that they are consistent with the enhanced safeguards contained in this order.

(B) Consideration of review. Within 180 days of completion of any review by the PCLOB described in subsection (c)(v)(A) of this section, the head of each element of the Intelligence Community shall carefully consider and shall implement or otherwise address all recommendations contained in such review, consistent with applicable law.

(d) Subjecting signals intelligence activities to rigorous oversight. The actions directed in this subsection are designed to build on the oversight mechanisms that elements of the Intelligence Community already have in place, in order to further ensure that signals intelligence activities are subjected to rigorous oversight.

(i) Legal, oversight, and compliance officials. Each element of the Intelligence Community that collects signals intelligence:

(A) shall have in place senior-level legal, oversight, and compliance officials who conduct periodic oversight of signals intelligence activities, including an Inspector General, a Privacy and Civil Liberties Officer, and an officer or officers in a designated compliance role with the authority to conduct oversight of and ensure compliance with applicable United States law;

(B) shall provide such legal, oversight, and compliance officials access to all information pertinent to carrying out their oversight responsibilities under this subsection, consistent with the protection of intelligence sources or methods, including their oversight responsibilities to ensure that any appropriate actions are taken to remediate an incident of non-compliance with applicable United States law; and

(C) shall not take any actions designed to impede or improperly influence such legal, oversight, and compliance officials in carrying out their oversight responsibilities under this subsection.

(ii) Training. Each element of the Intelligence Community shall maintain appropriate training requirements to ensure that all employees with access to signals intelligence know and understand the requirements of this order and the policies and procedures for reporting and remediating incidents of non-compliance with applicable United States law.

(iii) Significant incidents of non-compliance.

(A) Each element of the Intelligence Community shall ensure that, if a legal, oversight, or compliance official, as described in subsection (d)(i) of this section, or any other employee, identifies a significant incident of non-compliance with applicable United States law, the incident is reported promptly to the head of the element of the Intelligence Community, the head of the executive department or agency (agency) containing the element of the Intelligence Community (to the extent relevant), and the Director.

(B) Upon receipt of such report, the head of the element of the Intelligence Community, the head of the agency containing the element of the Intelligence Community (to the extent relevant), and the Director shall ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance.

(e) Savings clause. Provided the signals intelligence collection is conducted consistent with and in the manner prescribed by this section of this order, this order does not limit any signals intelligence collection technique authorized under the National Security Act of 1947, as amended (50 U.S.C. 3001 et seq.), the Foreign Intelligence Surveillance Act of 1978,

as amended (50 U.S.C. 1801 et seq.) (FISA), Executive Order 12333, or other applicable law or Presidential directive.

Sec. 3. Signals Intelligence Redress Mechanism.

(a) Purpose. This section establishes a redress mechanism to review qualifying complaints transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation of United States law and, if necessary, appropriate remediation.

(b) Process for submission of qualifying complaints. Within 60 days of the date of this order, the Director, in consultation with the Attorney General and the heads of elements of the Intelligence Community that collect or handle personal information collected through signals intelligence, shall establish a process for the submission of qualifying complaints transmitted by the appropriate public authority in a qualifying state.

(c) Initial investigation of qualifying complaints by the CLPO.

(i) Establishment. The Director, in consultation with the Attorney General, shall establish a process that authorizes the CLPO to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints. This process shall govern how the CLPO will review qualifying complaints in a manner that protects classified or otherwise privileged or protected information and shall ensure, at a minimum, that for each qualifying complaint the CLPO shall:

(A) review information necessary to investigate the qualifying complaint;

(B) exercise its statutory and delegated authority to determine whether there was a covered violation by:

(i) taking into account both relevant national security interests and applicable privacy protections;

(ii) giving appropriate deference to any relevant determinations made by national security officials; and

(iii) applying the law impartially;

(C) determine the appropriate remediation for any covered violation;

(D) provide a classified report on information indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court (FISC) to the Assistant Attorney General for National Security, who

shall report violations to the FISC in accordance with its rules of procedure;

(E) after the review is completed, inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that:

(1) "the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation";

(2) the complainant or an element of the Intelligence Community may, as prescribed in the regulations issued by the Attorney General pursuant to section 3(d)(i) of this order, apply for review of the CLPO's determinations by the Data Protection Review Court described in subsection (d) of this section; and

(3) if either the complainant or an element of the Intelligence Community applies for review by the Data Protection Review Court, a special advocate will be selected by the Data Protection Review Court to advocate regarding the complainant's interest in the matter;

(F) maintain appropriate documentation of its review of the qualifying complaint and produce a classified decision explaining the basis for its factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation in the event there was such a violation, consistent with its statutory and delegated authority;

(G) prepare a classified ex parte record of review, which shall consist of the appropriate documentation of its review of the qualifying complaint and the classified decision described in subsection (c)(i)(F) of this section; and

(H) provide any necessary support to the Data Protection Review Court.

(ii) Binding effect. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by the CLPO to undertake appropriate remediation pursuant to subsection (c)(i)(C) of this section, subject to any contrary determination by the Data Protection Review Court.

(iii) Assistance. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the reviews described in subsection (c)(i) of this section, consistent with the protection of intelligence sources and methods, and shall not take any actions

designed to impede or improperly influence the CLPO's reviews. Privacy and civil liberties officials within elements of the Intelligence Community shall also support the CLPO as it performs the reviews described in subsection (c)(i) of this section.

(iv) Independence. The Director shall not interfere with a review by the CLPO of a qualifying complaint under subsection (c)(i) of this section; nor shall the Director remove the CLPO for any actions taken pursuant to this order, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity.

(d) Data Protection Review Court.

(i) Establishment. The Attorney General is authorized to and shall establish a process to review determinations made by the CLPO under subsection (c)(i) of this section. In exercising that authority, the Attorney General shall, within 60 days of the date of this order, promulgate regulations establishing a Data Protection Review Court to exercise the Attorney General's authority to review such determinations. These regulations shall, at a minimum, provide that:

(A) The Attorney General, in consultation with the Secretary of Commerce, the Director, and the PCLOB, shall appoint individuals to serve as judges on the Data Protection Review Court, who shall be legal practitioners with appropriate experience in the fields of data privacy and national security law, giving weight to individuals with prior judicial experience, and who shall not be, at the time of their initial appointment, employees of the United States Government.

During their term of appointment on the Data Protection Review Court, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the Data Protection Review Court.

(B) Upon receipt of an application for review filed by the complainant or an element of the Intelligence Community of a determination made by the CLPO under subsection (c) of this section, a three-judge panel of the Data Protection Review Court shall be convened to review the application. Service on the Data Protection Review Court panel shall require that the judge hold the requisite security clearances to access classified national security information.

(C) Upon being convened, the Data Protection Review Court panel shall select a special advocate through procedures prescribed in the Attorney General's regulations. The special advocate shall assist the panel in its consideration of the application for review, including by advocating

regarding the complainant's interest in the matter and ensuring that the Data Protection Review Court panel is well informed of the issues and the law with respect to the matter.

Service as a special advocate shall require that the special advocate hold the requisite security clearances to access classified national security information and to adhere to restrictions prescribed in the Attorney General's regulations on communications with the complainant to ensure the protection of classified or otherwise privileged or protected information.

(D) The Data Protection Review Court panel shall impartially review the determinations made by the CLPO with respect to whether a covered violation occurred and the appropriate remediation in the event there was such a violation. The review shall be based at a minimum on the classified ex parte record of review described in subsection (c)(i)(F) of this section and information or submissions provided by the complainant, the special advocate, or an element of the Intelligence Community.

In reviewing determinations made by the CLPO, the Data Protection Review Court panel shall be guided by relevant decisions of the United States Supreme Court in the same way as are courts established under Article III of the United States Constitution, including those decisions regarding appropriate deference to relevant determinations of national security officials.

(E) In the event that the Data Protection Review Court panel disagrees with any of the CLPO's determinations with respect to whether a covered violation occurred or the appropriate remediation in the event there was such a violation, the panel shall issue its own determinations.

(F) The Data Protection Review Court panel shall provide a classified report on information indicating a violation of any authority subject to the oversight of the FISC to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure.

(G) After the review is completed, the CLPO shall be informed of the Data Protection Review Court panel's determinations through procedures prescribed by the Attorney General's regulations.

(H) After a review is completed in response to a complainant's application for review, the Data Protection Review Court, through procedures prescribed by the Attorney General's regulations, shall inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to

United States signals intelligence activities, that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."

(ii) Binding effect. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by a Data Protection Review Court panel to undertake appropriate remediation.

(iii) Assistance. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the review described in subsection (d)(i) of this section, consistent with the protection of intelligence sources and methods, that a Data Protection Review Court panel requests from the CLPO and shall not take any actions for the purpose of impeding or improperly influencing a panel's review.

(iv) Independence. The Attorney General shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint under subsection (c)(i) of this section; nor shall the Attorney General remove any judges appointed as provided in subsection (d)(i)(A) of this section, or remove any judge from service on a Data Protection Review Court panel, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity, after taking due account of the standards in the Rules for Judicial-Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act (28 U.S.C. 351 et seq.).

(v) Record of determinations. For each qualifying complaint transmitted by the appropriate public authority in a qualifying state, the Secretary of Commerce shall:

(A) maintain a record of the complainant who submitted such complaint;

(B) not later than 5 years after the date of this order and no less than every 5 years thereafter, contact the relevant element or elements of the Intelligence Community regarding whether information pertaining to the review of such complaint by the CLPO has been declassified and whether information pertaining to the review of any application for review submitted to the Data Protection Review Court has been declassified, including whether an element of the Intelligence Community filed an application for review with the Data Protection Review Court; and

(C) if informed that such information has been declassified, notify the complainant, through the appropriate public authority in a qualifying state, that information pertaining to the review of their complaint by the CLPO or

to the review of any application for review submitted to the Data Protection Review Court may be available under applicable law.

Sec. 4. Definitions. For purposes of this order:

(a) "Appropriate remediation" means lawful measures designed to fully redress an identified covered violation regarding a specific complainant and limited to measures designed to address that specific complainant's complaint, taking into account the ways that a violation of the kind identified have customarily been addressed.

Such measures may include, depending on the specific covered violation at issue, curing through administrative measures violations found to have been procedural or technical errors relating to otherwise lawful access to or handling of data, terminating acquisition of data where collection is not lawfully authorized, deleting data that had been acquired without lawful authorization, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to those appropriately trained, or recalling intelligence reports containing data acquired without lawful authorization or that were otherwise disseminated in a manner inconsistent with United States law.

Appropriate remediation shall be narrowly tailored to redress the covered violation and to minimize adverse impacts on the operations of the Intelligence Community and the national security of the United States.

(b) "Bulk collection" means the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms).

(c) "Counterintelligence" shall have the same meaning as it has in Executive Order 12333.

(d) "Covered violation" means a violation that:

(i) arises from signals intelligence activities conducted after the date of this order regarding data transferred to the United States from a qualifying state after the effective date of the Attorney General's designation for such state, as provided in section 3(f)(i) of this order;

(ii) adversely affects the complainant's individual privacy and civil liberties interests; and

(iii) violates one or more of the following:

(A) the United States Constitution;

(B) the applicable sections of FISA or any applicable FISC-approved procedures;

(C) Executive Order 12333 or any applicable agency procedures pursuant to Executive Order 12333;

(D) this order or any applicable agency policies and procedures issued or updated pursuant to this order (or the policies and procedures identified in section 2(c)(iv)(A) of this order before they are updated pursuant to section 2(c)(iv)(B) of this order);

(E) any successor statute, order, policies, or procedures to those identified in section 4(d)(iii)(B)-(D) of this order; or

(F) any other statute, order, policies, or procedures adopted after the date of this order that provides privacy and civil liberties safeguards with respect to United States signals intelligence activities within the scope of this order, as identified in a list published and updated by the Attorney General, in consultation with the Director of National Intelligence.

(e) "Foreign intelligence" shall have the same meaning as it has in Executive Order 12333.

(f) "Intelligence" shall have the same meaning as it has in Executive Order 12333.

(g) "Intelligence Community" and "elements of the Intelligence Community" shall have the same meaning as they have in Executive Order 12333.

(h) "National security" shall have the same meaning as it has in Executive Order 13526 of December 29, 2009 (Classified National Security Information).

(i) "Non-United States person" means a person who is not a United States person.

(j) "Personnel of the United States or of its allies or partners" means any current or former member of the Armed Forces of the United States, any current or former official of the United States Government, and any other person currently or formerly employed by or working on behalf of the United States Government, as well as any current or former member of the military, current or former official, or other person currently or formerly employed by or working on behalf of an ally or partner.

(k) "Qualifying complaint" means a complaint, submitted in writing, that:

(i) alleges a covered violation has occurred that pertains to personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the United States from a qualifying state after the effective date of the Attorney General's designation for such state, as provided in section 3(f)(i) of this order;

(ii) includes the following basic information to enable a review: information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant's data has in fact been subject to United States signals intelligence activities; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the United States; the identities of the United States Government entities believed to be involved in the alleged violation (if known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures;

(iii) is not frivolous, vexatious, or made in bad faith;

(iv) is brought on behalf of the complainant, acting on that person's own behalf, and not as a representative of a governmental, nongovernmental, or intergovernmental organization; and

(v) is transmitted by the appropriate public authority in a qualifying state, after it has verified the identity of the complainant and that the complaint satisfies the conditions of section 5(k)(i)-(iv) of this order.

(l) "Significant incident of non-compliance" shall mean a systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned.

(m) "United States person" shall have the same meaning as it has in Executive Order 12333.

(n) "Validated intelligence priority" shall mean, for most United States signals intelligence collection activities, a priority validated under the process described in section 2(b)(iii) of this order; or, in narrow circumstances (for example, when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), shall mean a priority set by the President or the head of an element of the

Intelligence Community in accordance with the criteria described in section 2(b)(iii)(A)(1)-(3) of this order to the extent feasible.

(o) "Weapons of mass destruction" shall have the same meaning as it has in Executive Order 13526.

To read more: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

Number 3

Court of Justice of the European Union, the Schrems II decision

The court declared that the Privacy Shield, the EU-US personal data transfer mechanism, was no longer lawful.

COURT OF JUSTICE
OF THE EUROPEAN UNION

JUDGMENT OF THE COURT (Grand Chamber)

Data Protection Commissioner
vs.
Facebook Ireland Ltd,
Maximillian Schrems,

intervening parties:
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance Inc.,
Digitaleurope,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P.G. Xuereb, L.S. Rossi and I. Jarukaitis, Presidents of Chambers, M. Ilešič, T. von Danwitz (Rapporteur), and D. Šváby, Judges,

Advocate General: H. Saugmandsgaard Øe,

Registrar: C. Strömholm, Administrator,

having regard to the written procedure and further to the hearing on 9 July 2019,

after considering the observations submitted on behalf of:

– the Data Protection Commissioner, by D. Young, Solicitor, B. Murray and M. Collins, Senior Counsel, and C. Donnelly, Barrister-at-Law,

– Facebook Ireland Ltd, by P. Gallagher and N. Hyland, Senior Counsel, A. Mulligan and F. Kieran, Barristers-at-Law, and P. Nolan, C. Monaghan, C. O'Neill and R. Woulfe, Solicitors,

– Mr Schrems, by H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty and S. O'Sullivan, Senior Counsel, and G. Rudden, Solicitor,

– the United States of America, by E. Barrington, Senior Counsel, S. Kingston, Barrister-at-Law, S. Barton and B. Walsh, Solicitors,

– the Electronic Privacy Information Centre, by S. Lucey, Solicitor, G. Gilmore and A. Butler, Barristers-at-Law, and C. O'Dwyer, Senior Counsel,

– BSA Business Software Alliance Inc., by B. Van Vooren and K. Van Quathem, advocaten,

– Digitaleurope, by N. Cahill, Barrister, J. Cahir, Solicitor, and M. Cush, Senior Counsel,

– Ireland, by A. Joyce and M. Browne, acting as Agents, and D. Fennelly, Barrister-at-Law,

– the Belgian Government, by J.-C. Halleux and P. Cottin, acting as Agents,

– the Czech Government, by M. Smolek, J. Vláčil, O. Serdula and A. Kasalická, acting as Agents,

– the German Government, by J. Möller, D. Klebs and T. Henze, acting as Agents,

– the French Government, by A.-L. Desjonquères, acting as Agent,

– the Netherlands Government, by C.S. Schillemans, M.K. Bulterman and M. Noort, acting as Agents,

– the Austrian Government, by J. Schmoll and G. Kunnert, acting as Agents,

– the Polish Government, by B. Majczyna, acting as Agent,

– the Portuguese Government, by L. Inez Fernandes, A. Pimenta and C. Vieira Guerra, acting as Agents,

– the United Kingdom Government, by S. Brandon, acting as Agent, and J. Holmes QC, and C. Knight, Barrister,

– the European Parliament, by M.J. Martínez Iglesias and A. Caiola, acting as Agents,

– the European Commission, by D. Nardi, H. Krämer and H. Kranenborg, acting as Agents,

– the European Data Protection Board (EDPB), by A. Jelinek and K. Behn, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 19 December 2019,

gives the following Judgment

1 This reference for a preliminary ruling, in essence, concerns:

– the interpretation of the first indent of Article 3(2), Articles 25 and 26 and Article 28(3) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), read in the light of Article 4(2) TEU and of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ('the Charter');

– the interpretation and validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100) ('the SCC Decision'); and

– the interpretation and validity of Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1; 'the Privacy Shield Decision').

2 The request has been made in proceedings between the Data Protection Commissioner (Ireland) ('the Commissioner'), on the one hand, and Facebook Ireland Ltd and Maximillian Schrems, on the other, concerning a complaint brought by Mr Schrems concerning the transfer of his personal data by Facebook Ireland to Facebook Inc. in the United States.

…

On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 2(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes

by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.

2. Article 46(1) and Article 46(2)(c) of Regulation 2016/679 must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union.

To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

3. Article 58(2)(f) and (j) of Regulation 2016/679 must be interpreted as meaning that, unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

4. Examination of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EU of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision.

5. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid.

To read more:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en

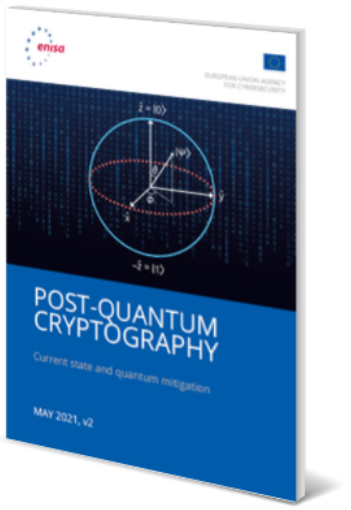
Number 4

Post-Quantum Cryptography, Integration study

With this report ENISA seeks to give insight on post-standardisation challenges. A follow-up to ENISA's 2021 Post-Quantum Cryptography: Current state and quantum mitigation study.

Post-Quantum Cryptography: Current state and quantum mitigation

This study provides an overview of the current state of affairs on the standardization process of Post-Quantum Cryptography (PQC). It presents the 5 main families of PQ algorithms; viz. code-based, isogeny-based, hash-based, lattice-based and multivariate-based. It also describes the NIST Round 3 finalists for encryption and signature schemes, as well as the alternative candidate schemes. Given that the NIST process will still run for a few years, the last chapter offers 2 proposals that system owners can implement now in order to protect the confidentiality of their data against a quantum capable attacker; namely hybrid implementations that use a combination of pre-quantum and post-quantum schemes, and the mixing of pre-shared keys into all keys established via public-key cryptography.



Download
PDF document, 1.05 MB

You may visit: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

The new report elaborates on the topic to address the following points:

- Integrating post-quantum systems into existing protocols
- New protocols designed around post-quantum systems
- Double encryption and double signatures using post-quantum systems
- Seccurity proofs in the presence of quantum attackers

• Standardisation efforts for post-quantum enabled protocols

The 2021 study provided an overview of the current state of play on the standardisation process of Post-Quantum Cryptography (PQC).

It introduced a framework for analysing existing PQC proposals, presented the five (5) main families of PQC algorithms, and the NIST Round 3 finalists for encryption and signature schemes.

It also sketched two proposals that proactive system owners can implement right now – before a standard is published – in order to protect the confidentiality of their data against a quantum capable attacker.

While agreeing on PQC cryptoalgorithms for encryption and signing is an important milestone, by itself it is not enough. Any new cryptoalgorithm will need to interplay with existing protocols or even require entirely new protocols to be designed and implemented.

Furthermore, PQC proposals are a solution to a still unrealised vulnerability – there are currently no publicly known quantum computers, strong enough to break encryption, and not all scientists believe this will ever be the case.

Whether we should implement protections against a threat that might not materialise would be a moot question if said implementations were cost free. However, PQC algorithms are often more costly, e.g. in terms of size and computations.

In addition, changing to a new cryptographic paradigm might provide new opportunities for software bugs and our understanding of the security of the PQC algorithms is often less mature.

Introduction

Cryptography is a crucial tool for the security of our digital society and is used virtually everywhere. For example, it secures our online communications, keeps the data on our devices secret even if we lose them, and protects the integrity and authenticity of digital records.

The security of cryptographic solutions deployed today is threatened by the development of quantum computers. To counter this threat, the area of post-quantum cryptography was initiated.

Post-quantum cryptography studies cryptosystems under the assumption that the attacker has access to a quantum computer, while the user is

supposed to be a regular user of today's systems with no quantum capabilities.

Several classes of problems exist that are conjectured to withstand even attacks using quantum computers. At this point the US National Institute for Standards and Technology (NIST) is running a selection process to select such systems for standardisation.

Given the success of NIST standards in the area of cryptography, it is likely that the systems selected by NIST will become the international standard for large parts of the world, including the European Union.

An overview of the process and the systems under consideration can be found in the recent Post-Quantum Cryptography: Current state and quantum mitigation study by ENISA.

In July 2022, NIST announced four candidates to be standardised, plus the four fourth round candidate Key-Establishment Mechanisms (KEMs).

In addition, NIST plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022.

One might expect that with the end of this process, i.e. the publication of the standards, everything will have been solved. We simply replace the schemes that we are using today with the new systems and be done.

This unfortunately is not the case at all. Many challenges need to be overcome before our data and our systems are secured against attacks using quantum computers.

One challenge is the size of the artifacts produced by post-quantum cryptography. The reason that today's cryptographic systems are so efficient is also the reason why they are vulnerable to quantum computers – these problems are highly structured.

Systems secure against quantum attacks have far less structure and hence a less compact description. As a consequence, keys, ciphertexts and signatures are larger for post-quantum systems than for matching pre-quantum systems.

This poses challenges to higher-level protocols. Protocol messages do not meet the size limitations of underlying protocols anymore, which at least leads to fragmentation, additional round-trips, and a more complicated state-machine if not treated carefully.

As a consequence, latency and data traffic increase. A related aspect is a decrease in the speed of some algorithms. This can significantly hurt the performance of protocols if not taken into consideration.

Both aspects can be dealt with by designing new protocols that take the new performance characteristics into account. However, this comes of course with all the challenges of designing new cryptographic protocols from assessing their security to standardising them.

The paper: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

Number 5

Aurum: a two-tier retail CBDC system

The BIS Innovation Hub and the Hong Kong Monetary Authority have completed a retail CBDC technology prototype.

BIS HONG KONG MONETARY AUTHORITY 香港金融管理局

Aurum is a full-stack (front-end and back-end) *central bank digital currency (CBDC)* system comprising a wholesale interbank system and a retail e-wallet system.

The aim was to bring to life two very different types of tokens: intermediated CBDC and stablecoins backed by CBDC in the interbank system.

The latter is unique in the study of CBDC to date. Privacy, safety and flexibility are core to the system.

The system is accompanied by technical manuals totalling over 250 pages that, together with the source code, are made accessible to all BIS member central banks on BIS Open Tech to help catalyse and inspire the global quest for the most suitable retail CBDC architecture.

Project Aurum

A Prototype for Two-tier
Central Bank Digital Currency (CBDC)

October 2022

In the era of digitisation, central banks stand before a choice: does retail central bank money need to go digital and, if so, how?

Jointly embarking on the challenge to design a full-stack central bank digital currency (CBDC) system, the Bank for International Settlements (BIS) Innovation Hub Hong Kong Centre and the Hong Kong Monetary Authority (HKMA) dubbed the project "Aurum", the Latin word for gold, reflecting our starting premise that digital currency issued under the auspices of a central bank must be as robust and trustworthy as gold.

Through the creation of a technology stack comprised of:

(1) a wholesale interbank system in which the wholesale CBDC (wCBDC) is issued to banks for onward distribution to retail users, and

(2) a retail e-wallet system in which the retail CBDC (rCBDC) circulates among retail users, we set a goal to bring to life two very different types of retail tokens:

(a) intermediated CBDC, also referred to herein as CBDC-tokens, and

(b) CBDC-backed stablecoins, or in short, stablecoins.

Given the complexity of the endeavour, the project was executed in partnership with the Hong Kong Applied Science and Technology Research Institute (ASTRI).

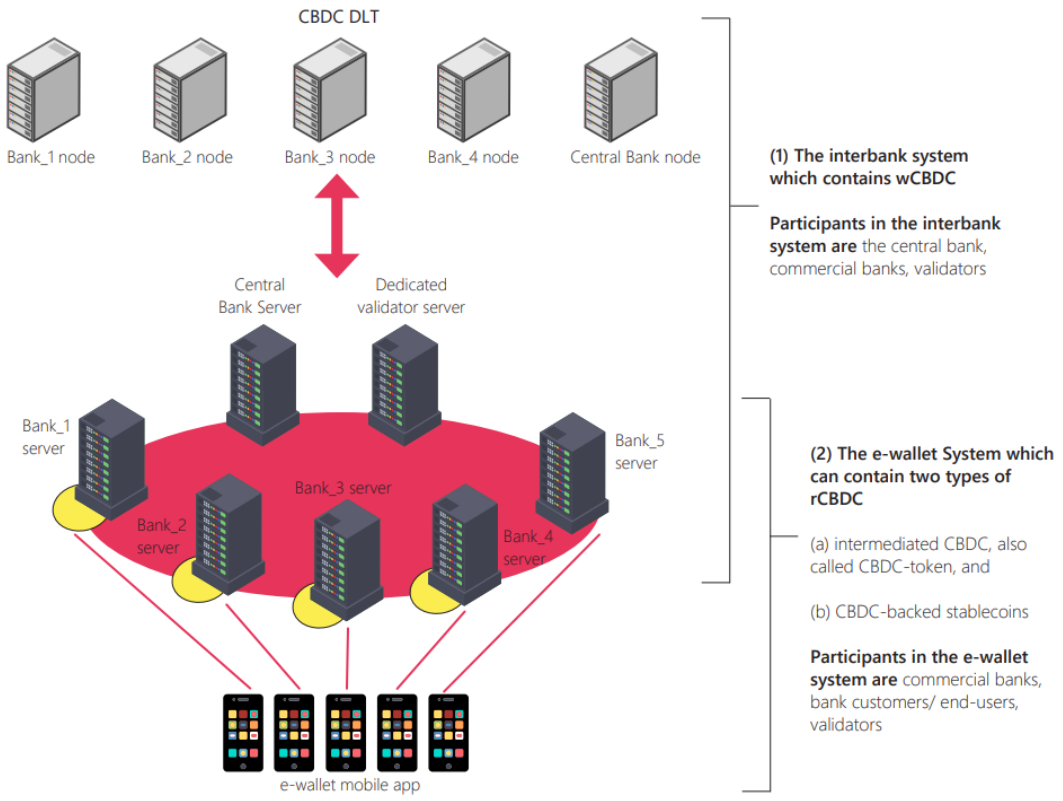
We are glad to report that after a year of development, the prototype system was successfully completed.

The present report provides an overview of the Aurum technology architecture. It is presented at a more technical level, supplemented by user interface visualisations, and should best be read in conjunction with the three e-HKD papers, as well as with the extensive body of foundational research issued by the BIS.

The Aurum system is accompanied by technical manuals totalling over 250 pages that, together with the source code, are made accessible to all BIS central bank members on BIS Open Tech to serve as a public good that furthers the study of rCBDC architectures.

The Aurum prototype also provides a solid basis for furthering the exploration and testing of e-HKD design in Hong Kong. Against this backdrop, we have no doubt that the Aurum prototype will catalyse and inspire the global quest for the most suitable rCBDC architecture.

Figure 6: High-level architecture of Aurum



To learn more: https://www.bis.org/publ/othp57.htm

https://www.bis.org/publ/othp57.pdf

Number 6

Defenders beware: A case for post-ransomware investigations

Microsoft Detection and Response Team (DART)

Microsoft

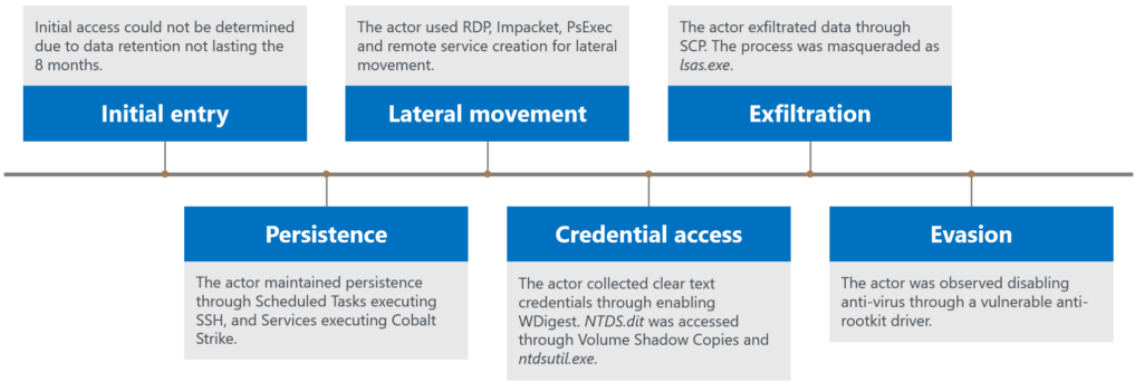
Ransomware is one of the most pervasive threats that Microsoft Detection and Response Team (DART) responds to today. The groups behind these attacks continue to add sophistication to their tactics, techniques, and procedures (TTPs) as most network security postures increase.

In this blog, we detail a recent ransomware incident in which the attacker used a collection of commodity tools and techniques, such as using living-off-the-land binaries, to launch their malicious code. Cobalt Strike was used for persistence on the network with NT AUTHORITY/SYSTEM (local SYSTEM) privileges to maintain access to the network after password resets of compromised accounts.

This incident highlights an attacker's ability to have a longstanding dwell time on a network before deploying ransomware. We will also discuss the various techniques used as well as the recommended detections and defense techniques that customers can use to increase protection against these types of attacks.

Microsoft recommends hunting proactively for pre-ransomware behaviors and hardening your network to prevent impact.

Refer to https://aka.ms/ransomware-as-a-service for more information about defending against ransomware-related incidents.



Initial access

DART was unable to determine the initial entry vector of this attack due to the age of this compromise and limited retention of security solutions,

along with encrypted devices being reimaged before analysis. The earliest observed activity showed the actor with domain administrator credentials.

Persistence

In DART's post ransomware investigation of this engagement, the team found multiple instances of scheduled tasks and services being created by the attack for persistence after they had gained access to highly privileged credentials. Services and Scheduled Tasks have the option to run as NT AUTHORITY\System, allowing their malicious code to run with highly privileged access.

Because the actor created those tasks and services on a domain controller, the Local SYSTEM access allowed them to easily access domain administrator accounts. The deployment of a backdoor to a domain controller can help an actor bypass common incident response recovery activity, such as resetting compromised accounts, in the hope of staying resident on the network.

Service: Cobalt Strike

Cobalt Strike was seen on a large scale across the network, on domain controllers, servers, and administrator workstations. The actor created Windows services to persist their payload executing rundll32 to load the Cobalt Strike DLL through invoking the "AllocConsole" exported function of a variation of the Termite family of malware.

These services were observed to execute with a combination of SYSTEM and domain administrator credentials. Termite malware is often used by crimeware groups to load Cobalt Strike while bypassing antivirus detections. Further information on the Termite malware family can be found in this blog: https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware

To read more: https://www.microsoft.com/en-us/security/blog/2022/10/18/defenders-beware-a-case-for-post-ransomware-investigations/

Number 7

So long and thanks for all the bits

Ian Levy, the NCSC's departing Technical Director, discusses life, the universe, and everything.

It's with a heavy heart that I'm announcing that I'm leaving the NCSC, GCHQ and Crown Service.

Being Technical Director of the NCSC has been the best job in the world, and truly an honour. I've spent more than two decades in GCHQ, with the last decade in this role (and its prior incarnations).

I've met and worked with some of the most amazing people, including some of the brightest people on the planet, and learned an awful lot.

I've got to give a special mention to everyone in the NCSC and wider GCHQ because they're just awesome. And I've also had the pleasure of working with vendors, regulators, wider industry, academia, international partners and a whole bunch of others.

I like to think I've done some good in this role, and I know I couldn't have accomplished half as much without them.

Regardless, there's a lot left to do. So, I thought I'd leave by sharing ten things I've learned and one idea for the future. This post is long and a bit self-indulgent, but it's my leaving blog, so suck it up

Standards are really boring, but really, really important

The globalisation I've just mentioned is driven by standards that govern how tech works in the real world. These standards are why we could all still communicate during the pandemic, regardless of what country we were in, what machine we used, what video calling software we preferred, or what ISP we used.

These standards are why your mobile phone will work in almost every country on the planet. These standards are why you can use any browser on any device to access any website hosted anywhere in the world.

These standards are incredibly detailed and technical and are developed over many years by groups of companies, governments, civil society groups and individuals coming together in things called Standard Development Organisations (SDOs).

Most people that go to standards meetings have an agenda, and it's usually to get something into a standard for commercial reasons. Many standards include technology that's patented by the contributors and these Standard Essential Patents are critical to making money out of standards, so companies want to get their patented technologies into standards.

This means that, for big global standards like 5G, many companies from around the world own the patents in the standard, and you need a licence from them to build a product. That includes Chinese companies, and this gives us a weird interdependency (and not an insignificant amount of national security risk) when you actually try to implement.

This is also why standards bodies are becoming a tool of great power competition – control the standards and you can stack the deck to make your technology more likely to be implemented. Sometimes that's just about money, but sometimes there could be other reasons.

It's interesting that Chinese people or Chinese companies hold leadership positions in more than 80% of key working groups in the main telecoms SDOs. Just saying.

The other thing we've seen happen is individuals and companies making standards reflect their values in a narrow field, without much thought about what else could go wrong.

Two examples here would be DNS-over-HTTPS (DOH) and the MASQUE protocols that underpin things like Apple Private Relay. Both of these were defined by the Internet Engineering Task Force, the organisation that sets the standards for the internet, which it does through humming.

They were intended to provide more privacy to users from all sorts of parties, but mainly government and big tech companies. The problem is that DOH makes enterprise cyber security very hard and also damages things like ISP parental controls, and some filtering for child sexual abuse images.

Apple Private Relay makes law enforcement's life much harder when looking at who's visiting certain dodgy websites, but also potentially reduces the resilience of mobile networks because it messes with the caching strategies in place today and makes diagnosing problems harder.

It also makes it impossible for those networks not to charge for certain data traffic because they can't see which sites a phone is trying to visit.

In both cases, we've got third parties affecting our national security and our ability to do cyber security, driven by other intents. In the case of a great power competition being played out in the SDOs, we need to find a way to make sure we can still have the technology we want and need that also meets our vision of security without completely balkanising the internet, since it's not clear we'd win in that case (remember the market-shaping stuff above).

In the case of companies and individuals, we need to have a more widely accepted understanding of the balance between all the different characteristics we expect on the internet. I don't want to start off a whole privacy-versus-security screaming match; we can (and should) have both. But neither should one axiomatically trump the other.

We need to reassess the design goals that we want for the future services we'll want and make sure they're vested to the relevant standards' bodies. The alternative is that things like NewIP will dominate and then we're all in the brown and smelly stuff.

To read more: https://www.ncsc.gov.uk/blog-post/so-long-thanks-for-all-the-bits

Number 8

First phase of new supercomputer installed at Los Alamos National Laboratory

The critical first phase of Los Alamos National Laboratory's newest supercomputer, Crossroads, has been successfully installed.

Called Tycho, this machine is a stepping-stone to Crossroads, which will replace Trinity as the Laboratory's primary supercomputer in the coming year and will support next-generation weapons simulations.

"We're excited to be entering this new phase of supercomputing at the Lab," said Los Alamos' HPC Platforms Program Director Jim Lujan. "Early benchmarks indicate a four-times increase in speed over Trinity. All of the new efficiencies that are part of Tycho, and ultimately Crossroads, come together to reduce that crucial time to insight. Improving efficiencies in many areas for modeling and simulation is what this project is all about."

A Hewlett Packard Enterprise machine, based on the HPE Cray EX supercomputer, Crossroads will support critical maintenance and modernization of the U.S. nuclear stockpile, as well as other nuclear security missions.

Amanda Bonnie, project manager for Crossroads, has been with Tycho from when it was just a configuration diagram, all the way to rolling the 8,000-pound cabinets off trucks and seeing them through their installation on Los Alamos' Strategic Computing Complex floor, which is approximately the size of a football field.

"I think my favorite part of the entire process is the delivery and install week," said Bonnie. "Getting to be there and see it become something before your eyes is magical."

Tycho brings to bear emerging technologies including the first large-scale deployment of Intel's new Sapphire Rapids processor. Earlier this year, HPC tests helped Intel engineers configure the chip to best serve Laboratory-specific application performance.

Adding to overall efficiency, Solid State Drives will make up the entirety of Tycho's file system — a first for Los Alamos supercomputers. Additionally, warm water direct liquid cooling will mean significant energy savings over more traditional approaches.

Following in Trinity's footsteps, Crossroads gets its name from the second series of nuclear weapons tests conducted at Bikini Atoll in 1946.

Tycho, however, has a different origin. Key Crossroads components Tycho, Rocinante and Razorback are all named for spacecraft from The Expanse — a sci-fi TV series based on novels written by James S.A. Corey (pen name of authors Ty Franck and Daniel Abraham, both of whom have New Mexico ties).

In coming months, the Crossroads team will work to stabilize Tycho, calibrating the system's 2,600 Sapphire Rapids nodes for maximum efficiency. Software will be installed and functionality testing will take place — all in time to ensure Tycho's early use in the classified environment by the end of the year and full production status in March 2023.

This Advanced Technology System is funded by the Department of Energy's National Nuclear Security Administrations' Advanced Simulation and Computing program.

To read more: https://discover.lanl.gov/news/1020-supercomputer-tycho

Number 9

Risk Dashboard indicates overall resilience among insurers even amid high macro and market risks

The European Insurance and Occupational Pensions Authority (EIOPA) published its Risk Dashboard based on Solvency II data from the second quarter of 2022.

Risks	Level	Trend (Past 3 months)	Outlook (Next 12 months)
1. Macro risks	high	↘	↗
2. Credit risks	medium	→	↗
3. Market risks	high	↑	↗
4. Liquidity and funding risks	medium	→	→
5. Profitability and solvency	medium	↗	→
6. Interlinkages and imbalances	medium	↘	→
7. Insurance (underwriting) risks	medium	→	→
8. Market perceptions	medium	↗	→
9. ESG related risks	medium	→	↗
10. Digitalisation & Cyber risks	medium	↓	↗

The results show that insurers' exposures to macro and market risks are currently the main concern for the insurance sector.

All other risk categories, such as profitability and solvency, climate as well as digitalisation and cyber risks stay at medium levels.

Macro risks remain a key source of concern amid a further decrease in global GDP growth expectations and high CPI forecasts for the main geographical areas, even as unemployment remains low.

The weighted average of 10 year swap rates increased. Central banks continue the normalisation of their monetary policy.

Market risks are currently at a high level. Volatility in bond and equity markets continue to top last year's average.

Property prices remain at the same level. Insurers' median exposure to bonds and equity remain relatively unchanged while median exposure to property slightly increased in Q2 2022.

Credit risks remain relatively moderate. CDS spreads remain at low levels for government bonds and financial bonds while further increasing for non-financial corporate bonds in the third quarter of 2022.

Insurers' relative exposure to different bonds categories remained broadly stable while slightly decreasing for government bonds in Q2. The median average credit quality of insurers' investments remained stable.

Profitability and solvency risks remain constant with returns for insurers decreased in the second quarter of 2022 across all three return indicators (return on excess of aseets over liabilities, return on assets and return on premiums). The increase of interest rates since the beginning of 2022 may be the main driver behind insurers' high SCR ratios.

Due to the current increase of interest rates, insurers booked market to market losses on derivatives given that they are typically positioned to hedge against interest rates declines.

Regarding market perceptions, insurance life and non-life stocks underperformed. The median price-to-earnings ratio of insurance groups is largely unchanged. The median of CDS spreads of insurers further increased even as insurers' external ratings remained broadly stable since the last assessment.

On climate risks, insurers maintained their relative exposure to green bonds while the ratio of investments in green bonds over the total green bond outstanding slightly decreased. The growth of green bonds in insurers' portfolios has decreased, while the growth of green bonds outstanding is stable.

The materiality of digitalisation and cyber risks for insurance as assessed by supervisors decreased slightly. Nevertheless, cyber security issues and concerns of a hybrid geopolitical conflict remain.

The cyber negative sentiment indicates an increased concern in the third quarter of 2022 while the frequency of cyber incidents decreased compared to the same quarter last year.

Key observations:

- Risk levels for the European insurance sector remain broadly constant.

- Macro-related risks remain significant for the insurance sector. Forecasted GDP growth at global level further decreased and CPI forecasts remained at high level for main geographical areas. Unemployment rate for main geographical areas remained at low level. Weighted average of 10 years swap rates increased. Central banks continue the normalization of their monetary policy.

- Credit risks remain relatively moderate. The CDS spreads remain at low levels for government bonds and financial bonds, amid further increasing for nonfinancial corporate bonds in the third quarter of 2022. Insurers' relative exposure to different bonds categories remained broadly stable while slightly decreasing for government bonds in Q2-2022. The median average credit quality of insurers' investments remained stable.

- Market risks remain stable compared to the previous assessment. Volatility in bond and equity market remained at higher than last year average. Property prices remain at the same level. The median insurers' exposure to bonds, equity remain relatively unchanged while median exposure to property slightly increased in Q2 2022.

- Profitability and solvency risks remain at medium level. Given the decrease in returns for insurers in the second quarter of 2022, the three return indicators (return on excess of aseets over liabilities, return on assets and return on premiums) decreased. The increase of interest rates since the beginning of 2022 might be the main driver behind the high SCR ratios.

- Interlinkage and imbalance risks remain at medium level. Due to the current increase of interest rate, insurers realised market to market losses on derivatives because they are positioned to hedge interest rates declines.

- Market perceptions remain at medium level. Insurance life and non-life stocks underperformed. The median price-to-earnings ratio of insurance groups remained around the same level. The median of CDS spreads of insurers further increased. Insurers' external ratings remained broadly stable since the last assessment.

- Climate risks remain at medium level. Insurers mantained their relative exposure into green bonds, while the ratio of investments into green bonds over the total green bond outstanding slightly decreased. The growth of green bonds in insurers' portfolios has decreased, while the growth of green bonds outstanding is stable.

- Digitalisation and cyber risks are at medium level. The materiality of these risks for insurance as assessed by supervisors slightly decreased yet cyber security issues and concerns of a hybrid geopolitical conflict remain. Cyber negative sentiment indicates an increased concern in the third quarter of 2022 while the frequency of cyber incidents decreased compared to the same quarter last year

To read more:

https://www.eiopa.europa.eu/tools-and-data/statistics-and-risk-dashboards/risk-dashboard_en

https://www.eiopa.europa.eu/sites/default/files/financial_stability/risk_dashboard/october_2022_risk_dashboard.pdf

Number 10

ENISA Threat Landscape 2022

This is the tenth 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).

During the reporting period of the ETL 2022, the prime threats identified include:

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

Impact of geopolitics on the cybersecurity threat landscape

- The conflict between Russia-Ukraine reshaped the threat landscape during the reporting period. Some of the interesting changes were significant increases in hacktivist activity, cyber actors conducting operations in concert with kinetic military action, the mobilisation of hacktivists, cybercrime, and aid by nation-state groups during this conflict.

- Geopolitics continue to have stronger impact on cyber operations.

- Destructive attacks are a prominent component of the operations of state actors. During the Russia-Ukraine conflict, cyber actors were observed conducting operations in concert with kinetic military action.

- A new wave of hacktivism2 has been observed especially since the Russia-Ukraine crisis began.

- Disinformation is a tool in cyberwarfare. It was used even before the 'physical' war started as a preparatory activity for Russia's invasion of Ukraine.

Threat actors increasing their capabilities

- Resourceful threat actors have utilised 0-day exploits to achieve their operational and strategic goals. The more organisations increase the maturity of their defences and cybersecurity programmes, the more they increase the cost for adversaries, driving them to develop and/or buy 0-day exploits, since defence in depth strategies reduce the availability of exploitable vulnerabilities.

- Continuous 'retirements' and the rebranding of ransomware groups is being used to avoid law enforcement and sanctions.

- Hacker-as-a-service business model gaining traction, growing since 2021.

- Threat groups have an increased interest and exhibit an increasing capability in supply chain attacks and attacks against Managed Services Providers (MSPs).

Moreover, understanding the trends related to threat actors, their motivations and their targets greatly assists in planning cybersecurity defences and mitigation strategies.

Therefore, for the purposes of the ETL 2022, the following four categories of cybersecurity threat actors are considered again:

• State-sponsored actors
• Cybercrime actors
• Hacker-for-hire actors
• Hacktivists.

Through continuous analysis, ENISA derived trends, patterns and insights for each of the major threats presented in the ETL 2022.

The key findings and judgments in this assessment are based on multiple and publicly available resources which are provided in the references used for the development of this document.

The report is mainly targeted at strategic decision-makers and policy-makers, while also being of interest to the technical cybersecurity community.

Figure 1: ENISA Threat Landscape 2022 - Prime threats

To read more: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Number II

Dozens Charged in $250 Million COVID Fraud Scheme

FBI investigation alleges massive misuse of money meant to feed children during pandemic

Forty-seven suspects have been indicted for defrauding a federally funded child nutrition program of more than $250 million.

The funds were intended to be used as reimbursements for the costs of serving meals to children in need during the COVID-19 pandemic, but investigators believe few meals were ever provided. Instead, the defendants are accused of misusing the money to purchase cars, vacations, coastal resort properties, electronics, and other luxury items for themselves.

The scheme, as outlined in the charges, represents the largest theft of federal funds allocated to pandemic aid to date.

At the center of the investigation is a now-closed Minneapolis nonprofit called Feeding Our Future and its former founder and executive director, Aimee Bock. Bock oversaw the scheme and has been indicted on multiple fraud and bribery charges.

Feeding Our Future had served as a sponsor for numerous organizations that signed up to participate in the Federal Child Nutrition Program. The program is administered by the U.S. Department of Agriculture, with states distributing funds locally.

Under the program, local sites that seek to supply the children's meals—such as restaurants and catering services—must be sponsored by another organization. That sponsoring organization monitors the sites and prepares reimbursement claims for meals provided by the sites.

In this case, however, Feeding Our Future allegedly used its position as a sponsor to engineer a massive fraud scheme.

The charges allege that beginning in early 2020, the organization began recruiting individuals and entities to open fake Federal Child Nutrition Program sites throughout Minnesota. These sites, created and operated by the defendants and others, fraudulently claimed to be serving meals to thousands of children a day within just days or weeks of being formed

despite having few—if any—staff and little to no experience serving this volume of meals.

In exchange for sponsoring these sites' fraudulent participation in the program, Feeding Our Future received more than $18 million in administrative fees it was not entitled to.

Feeding Our Future employees also allegedly solicited and received bribes and kickbacks from the individuals and companies it sponsored. Many of these kickbacks were paid in cash or disguised as "consulting fees" that were paid to shell companies created by Feeding Our Future employees to make them appear legitimate.

In total, Feeding Our Future opened more than 250 sites throughout Minnesota between March 2020 and January 2022 and falsely claimed to have served 125 million meals.

The indictments allege a number of specific ways that the defendants perpetrated the fraud:

- Conspirators submitted a fake attendance roster listing the names of 2,040 children who attended one of the sponsor's afterschool programs, yet only 20 names matched those of children who were attending school in the district.

- One site claimed to serve 2,000 to 3,000 meals per day, seven days a week, from a restaurant that previously had only a few dozen customers a day and $500-$600 in daily sales the previous year.

- One roster was created using names from a website called listofrandomnames.com. Because the program only reimbursed for meals served to children, other defendants used an Excel formula to insert a random age between 7 and 17 into the age column of the rosters. In some expense reports submitted over a period of months, the names of the children would stay the same, but their ages would change based on the random assignment.

During a news conference announcing the charges, FBI Special Agent in Charge Michael Paul said that the FBI's forensic accountants played a key role in untangling the scheme.

"During this investigation, the FBI followed many trails—including both money trails and paper trails—filled with falsified invoices and receipts, fictitious names, and an inconceivable number of meals allegedly served, all representing an astonishing display of deceit and evidence of outright fraud," he stated.

Although the 18-month long investigation was extremely complex, Paul said the crime was quite simple: “It was just a massive fraud scheme.”

To date, the FBI and its law enforcement partners have conducted more than 100 search warrants, completed an additional 100 seizure warrants, and reviewed more than 1,000 bank accounts.

U.S. Attorney Andrew Lugar announced that the government so far has been able to recover $50 million from 60 bank accounts, 45 pieces of property, and numerous vehicles and additional items, such as electronics and high-end clothing. Additional seizures are expected.

“These indictments describe an egregious plot to steal public funds meant to care for children in need in what amounts to the largest pandemic relief fraud scheme yet,” said FBI Director Christopher Wray.

“The defendants went to great lengths to exploit a program designed to feed underserved children in Minnesota amidst the COVID-19 pandemic, fraudulently diverting millions of dollars designated for the program for their own personal gain. These charges send the message that the FBI and our law enforcement partners remain vigilant and will vigorously pursue those who attempt to enrich themselves through fraudulent means.”

To read more: https://www.fbi.gov/news/stories/dozens-charged-in-250-million-covid-fraud-scheme-092122

https://www.justice.gov/opa/pr/us-attorney-announces-federal-charges-against-47-defendants-250-million-feeding-our-future

Number 12

National Security Memorandum on Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security

THE WHITE HOUSE

It is a vital interest of the United States to prepare for, prevent, detect, respond to, and recover from biological threats at home and abroad.

The coronavirus disease 2019 (COVID-19) has highlighted that the United States and the world are vulnerable to biological threats, whether naturally occurring, accidental, or deliberate.

COVID-19 has cost millions of lives and has resulted in trillions of dollars in economic loss and major setbacks in health and economic development globally.

No sector of the United States economy or society is immune to the effects of a major biological incident.

Moreover, few other national security threats are capable of producing catastrophic and potentially existential global consequences at the scale and speed of biological threats.

Therefore, countering biological threats, advancing pandemic preparedness, and achieving global health security are top national and international security priorities for the United States.

Nearly all executive departments and agencies (agencies) contribute to the biodefense mission of the United States Government.

Moving forward, the United States must fundamentally transform its capabilities to protect our Nation from biological threats and advance pandemic preparedness and health security more broadly for the world.

Section 1. Policy.

It is the policy of the United States to preserve our health, economic, social, and national security by protecting the Nation from biological threats and promoting pandemic preparedness and global health security.

The United States Government will undertake actions at home and with partners globally to reduce the risk of naturally occurring, accidental, and deliberate biological events with the potential to significantly impact

humans, animals (domestic and wildlife), plants, and the environment, and to negatively affect health, the economy, society, and security.

The foundational policies for the United States Government's role in biodefense include: the National Biodefense Strategy for Countering Biological Threats, Enhancing Pandemic Preparedness, and Achieving Global Health Security (Biodefense Strategy) and its associated Implementation Plan, American Pandemic Preparedness: Transforming Our Capabilities, and the U.S. Global Health Security Strategy.

Agency activities in support of the Biodefense Strategy and its Implementation Plan shall be conducted consistent with the Biodefense Strategy.

Activities undertaken to implement existing Executive Orders and Presidential Directives, including but not limited to those listed in Annex IV of the Biodefense Strategy, shall be conducted consistent with the Biodefense Strategy.

Further, implementation of this memorandum shall ensure consistent integration with Presidential Directives regarding domestic response.

Sec. 2. Coordination and Governance of United States Biodefense Efforts. The policy set forth in section 1 of this memorandum shall be implemented, to the extent permitted by law and available appropriations and subject to the internal programmatic and budgetary processes of relevant agencies, as follows:

(a) The Assistant to the President for National Security Affairs (APNSA) shall serve as the lead for policy coordination and review, acting through the process described in National Security Memorandum 2 (NSM-2) of February 4, 2021 (Renewing the National Security Council System), to provide strategic input and facilitate policy integration for Federal biodefense efforts.

(b) In accordance with Executive Order 13987 of January 20, 2021 (Organizing and Mobilizing the United States Government to Provide a Unified and Effective Response to Combat COVID-19 and to Provide United States Leadership on Global Health and Security), and National Security Memorandum 1 of January 21, 2021 (United States Global Leadership to Strengthen the International COVID-19 Response and to Advance Global Health Security and Biological Preparedness), the APNSA shall coordinate the Federal Government's efforts to prepare for, prevent, detect, respond to, and recover from biological threats and to advance global health security, international pandemic preparedness, and global health resilience.

This subsection does not apply to Federal law enforcement activities, criminal investigations, or intelligence activities related to domestic incidents involving suspected terrorist threats, terrorist attacks, significant cyber incidents or other acts within the criminal jurisdiction of the United States.

(c) The heads of agencies shall:

(i) implement the Biodefense Strategy, as well as related strategies such as the U.S. Global Health Security Strategy, and include biodefense-related activities, including resourcing and achieving the goals of the Biodefense Strategy and the priorities, targets, and actions of its Implementation Plan, within their strategic planning and budgetary processes;

(ii) in the event of the determination of a nationally or internationally significant biological incident, implement Federal response efforts in accordance with Homeland Security Presidential Directive 5 of February 28, 2003 (Management of Domestic Incidents), Presidential Policy Directive 8 of March 30, 2011 (National Preparedness), Presidential Policy Directive 44 of November 7, 2016 (Enhancing Domestic Incident Response), and Federal Government response and recovery frameworks and operational plans;

(iii) coordinate their biodefense policies with other agencies that have responsibilities or capabilities pertaining to biodefense, as well as with appropriate non-Federal entities;

(iv) share information and coordinate decision-making related to the biodefense enterprise; and

(v) monitor, evaluate, and hold their respective agencies accountable for the implementation of section 3(a) of this memorandum.

(d) Heads of agencies are not required to share information on counterproliferation activities, military plans or operations, intelligence activities, or specific law enforcement activities and criminal investigations.

Sec. 3. Implementation.

(a) At least once every 3 years, in alignment with the annual budget cycle, the APNSA and the Assistant to the President and Homeland Security Advisor (APHSA), in coordination with the heads of relevant agencies, shall review and update, as necessary, biodefense priorities under the Biodefense Strategy's Implementation Plan. These updates shall be

submitted to the President through the APNSA and, to the extent permitted by and consistent with applicable law and policy, released to the public.

(b) Within 1 year of the date of this memorandum and annually thereafter, the APNSA or the APHSA, in coordination with the Director of the Office of Science and Technology Policy and the Assistant to the President for Domestic Policy, shall chair a Principals Committee Senior Officials Exercise (SOE) on a biopreparedness health emergency in coordination with the heads of relevant agencies.

The SOE shall include a detailed summary of conclusions, which shall inform the review listed in subsection (a) of this section.

The heads of relevant agencies shall, on an annual basis, submit all related SOE After Action Reports to the APNSA and the APHSA to inform the review listed in subsection (a) of this section; the Administrator of the Federal Emergency Management Agency to inform the National Exercise Program; and the heads of relevant agencies to inform biopreparedness.

(c) Within 1 year of the date of this memorandum, and annually thereafter in alignment with the annual budget cycle:

(i) the heads of relevant agencies shall include in their annual budget requests to the Office of Management and Budget (OMB) information on those activities, programs, and projects that are planned, programmed, or have been executed that advance or are expected to advance the Biodefense Strategy and its Implementation Plan; ensure that these new and existing activities are prioritized in their annual budget requests; quantify resources allocated to biodefense within their annual budget requests; make a determination on whether their budget requests are sufficient to meet priorities established in the Biodefense Strategy's Implementation Plan; and meet annually with National Security Council (NSC) staff to review their annual budget requests;

(ii) as part of the annual budget process, the Director of OMB, in consultation with the APNSA, shall conduct an analysis of Federal biodefense and pandemic preparedness programs to assess whether resources are sufficient to meet the objectives of the Biodefense Strategy's Implementation Plan; and

(iii) the APNSA, through the process described in NSM-2 and in coordination with the Director of OMB, shall convene relevant agencies to ensure that interagency budgets for programs that contribute directly to the implementation of this memorandum and additional relevant resource

requests are directed to meet the objectives of the Biodefense Strategy's Implementation Plan.

To read more: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/18/national-security-memorandum-on-countering-biological-threats-enhancing-pandemic-preparedness-and-achieving-global-health-security/

Number 13

Privacy Policy

We're updating our Privacy Policy with effect from 2 December 2022.

Introduction

This privacy policy ("Privacy Policy") applies to the personal information that TikTok processes in connection with TikTok apps, websites, software and related services (the “Platform”), that link to or reference this Privacy Policy.

Data Controller: If you live in the European Economic Area (“EEA”), the United Kingdom (“UK”), or Switzerland, TikTok Technology Limited, an Irish company (“TikTok Ireland”), and TikTok Information Technologies UK Limited (“TikTok UK”), a UK company, ("TikTok," "our," "we," or "us") are the joint controllers of your information processed in connection with this Privacy Policy.

What Information We Collect

We collect your information in three ways: Information You Provide, Automatically Collected Information, and Information From Other Sources. More detail is provided below.

Information You Provide

Profile Information. We collect information that you provide when you set up an account, such as your date of birth, username, email address and/or telephone number, and password. You can add other information to your profile, such as a bio or a profile photo.

User Content. We collect the content you create or publish through the Platform, such as photographs, videos, audio recordings, livestreams, and comments, and the associated metadata (such as when, where, and by whom the content was created).

Even if you are not a user, information about you may appear in content created or published by users on the Platform. We collect User Content through pre-loading at the time of creation, import, or upload, regardless of whether you choose to save or upload that User Content, for example, to recommend music based on the video.

We also collect content (such as text, images, and video) from your device's clipboard if you choose to copy and paste content to or from the Platform or share content between it and a third party platform. In addition, we collect location information (such as tourist attractions, shops, or other points of interest) if you choose to add the location information to your User Content.

Direct Messages. If you communicate with others using direct messages, we collect the content of the message and the associated metadata (such as the time the message was sent, received and/or read, as well as the participants in the communication). We do this to block spam, detect crime, and to safeguard our users.

Your Contacts. If you choose to import your contacts, we will collect information from your device's phone book or your social media contacts. We use this information to help you make connections, including when you are using our "Find Friends" function and to suggest accounts to you.

Purchase Information. We collect your payment card information or other third-party payment information (such as PayPal) where payment is required. We also collect your transaction and purchase history.

Surveys, Research, and Promotions. We collect information you provide if you choose to participate in a survey, research, promotion, contest, marketing campaign, or event conducted or sponsored by us.

Information When You Contact Us. When you contact us, we collect the information you send us, such as proof of identity or age, feedback or inquiries about your use of the Platform or information about possible violations of our Terms of Service (our "Terms"), Community Guidelines (our "Guidelines"), or other policies.

Automatically Collected Information

Technical Information. We collect certain device and network connection information when you access the Platform. This information includes your device model, operating system, keystroke patterns or rhythms, IP address, and system language.

We also collect service-related, diagnostic, and performance information, including crash reports and performance logs. We automatically assign you a device ID and user ID. Where you log-in from multiple devices, we use information such as your device ID and user ID to identify your activity across devices to give you a seamless log-in experience and for security purposes.

Location Information. We automatically collect information about your approximate location (e.g. country, state, or city) based on your Technical Information (such as SIM card and IP address).

Also, where you enable Location Services for the TikTok app within your device settings, we collect approximate location information from your device. Click here to learn more about how we collect Location Information.

Usage Information. We collect information about how you engage with the Platform, including information about the content you view, the duration and frequency of your use, your engagement with other users, your search history and your settings.

Content Characteristics and Features. We detect and collect characteristics and features about the videos, images, and audio recordings that are part of your User Content, for example, by identifying objects and scenery, the existence or location within an image of a face or other body parts; and the text of words spoken in your User Content. We do this, for example, for content moderation and to provide special effects (such as video filters and avatars) and captions.

Inferred Information. We infer your attributes (such as age-range and gender) and interests based on the information we have about you. We use inferences, for example, to keep the Platform safe, for content moderation and, where permitted, to serve you personalised ads based on your interests.

Cookies. We use cookies and similar tracking technologies to operate and provide the Platform. For example, we use cookies to remember your language preferences, make sure you don't see the same video more than once, and for security purposes.

We also use these technologies for marketing purposes. To learn more about our use of cookies, please see our Web Cookies Policy and Platform Cookies Policy. We will obtain your consent to our use of cookies where required by law.

Information From Other Sources

Advertising, Measurement and Data Partners. Advertisers, measurement and data partners share information with us such as mobile identifiers for advertising, hashed email addresses, and event information about the actions you've taken outside of the Platform.

Some of our advertisers and other partners enable us to collect similar information directly from their website or app by integrating our TikTok Advertiser Tools (such as TikTok Pixel).

Third Party Platforms and Partners. Third party platforms provide us with information (such as your email address, user ID, and public profile) when you choose to sign up for or log in to the Platform using sign-in features provided by those third parties. We may also receive contact information that you hold or is held about you when contact information is synced with our Platform by you or another user.

When you interact with any third party service (such as third party apps, websites or products) that integrate TikTok Developer Tools, we will receive the information necessary to provide you with features like cross-service authentication or cross-posting. For example, this will happen if you log in to another platform with your TikTok account or if you use TikTok's "share" button on a third party platform to share content from there to the Platform.

Others. We may receive information about you from others, for example, where you are included or mentioned in User Content, Direct Messages, in a complaint, appeal, request or feedback submitted by a user or third party, or if your contact information is provided to us by a user.

To read more: https://www.tiktok.com/legal/page/eea/new-privacy-policy/en

Number 14

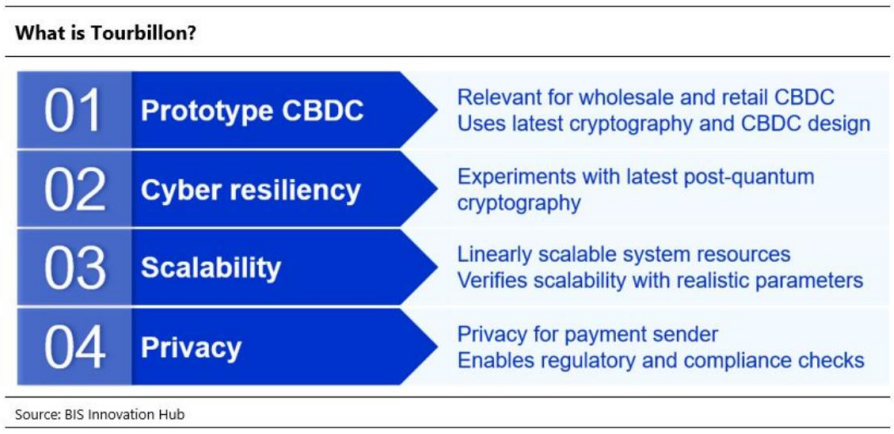
Project Tourbillon

Launched by the BIS Innovation Hub's Swiss Centre, explores how to improve cyber resiliency, scalability and privacy in a prototype Central Bank Digital Currency (CBDC).

BIS

Central banks have identified cyber resiliency, scalability and privacy as core features of CBDCs. You may visit:
https://www.bis.org/publ/othp33_summary.pdf

However, designing them involves complex trade-offs between these three elements. For example, higher resiliency against cyber-attacks, especially from quantum computers, requires additional cryptography, which can slow down payment processing. Privacy must be weighed against the need to counter money laundering, terrorism financing and other illicit payments.



Project Tourbillon aims to reconcile these trade-offs by combining proven technologies such as blind signatures and mix networks with the latest research on cryptography and CBDC design suggested by researchers David Chaum and Thomas Moser. You may visit: https://chaum.com/wp-content/uploads/2022/11/eCash_2.0_9-7-22-.pdf

Abstract: The digital cash introduced here provides better privacy than paper cash while protecting society against criminal use far better than paper money ever could. In particular, it provides each holder, though their payments are anonymous, with the ability to allow irrefutable tracing of any of their payments—and this ability is "inalienable" in that it simply cannot be given or taken away. This improved control by persons over the privacy of their own payments further allows the adoption of privacy where it might otherwise be blocked by regulation. Without such inalienability, moreover, it is believed that payment privacy intended for particular persons may be taken from them, by malware for instance, and used to protect the privacy of aggregated payments made by others. The supply of currency is completely controlled by its issuer, and the currency is provably protected against counterfeiting even by a quantum computer. Optionally, a blockchain, or individual customer choice of public blockchain, can bring the advantages of such chains, including transparency of the total amount of unspent digital cash outstanding. The design builds on several well-established cryptographic protocols, like public-key digital blind signatures and mix networks, as well as some new cryptographic techniques of its own. Its improved privacy and quantum resistance, when combined with its Visa- or PayPal-like scalability, make it an ideal candidate for central bank digital currency (CBDC).

Introduction

Most central banks are currently exploring the issuance of central bank digital currencies (CBDCs), and a recent BIS survey on the topic found

Cyber resiliency supports safe and effective digital payments infrastructures. The project achieves this by experimenting with the strongest known type of quantum-resistant cryptography.

Scalability accommodates the potential for high transaction volumes. Tourbillon achieves this by using an architecture that is compatible with, but not based on, distributed ledger technology. By making each transaction separate, the system resources scale linearly. The project seeks to verify the linear scalability of the design with realistic parameters.

Privacy is an important user requirement but at the same raises issues with regards to countering illicit activities. Tourbillon resolves this by providing privacy for the payment sender but not for the recipient. Regulatory and compliance checks will continue to apply.

The conclusions of this project will be relevant for both wholesale and retail CBDC systems. The goal is to finish the prototype by mid-2023.

> *Digital central bank money can make payments better and more inclusive. Yet delivering a CBDC involves difficult trade-offs between cyber resilience, scalability and user privacy. Project Tourbillon will build and test a prototype that reconciles these trade-offs and pushes central banks' technological frontier.*
>
> Morten Bech, Head of the BIS Innovation Hub Swiss Centre

> *Many central banks are researching CBDCs in the context of the digital asset transformation. I am proud to be a co-author with David Chaum on the eCash 2.0 paper, which is serving as the basis for this project.*
>
> Thomas Moser, Alternate Member of the Governing Board at the Swiss National Bank

> *I am thrilled to see these important advances in technology being tested out so that there is no doubt that privacy, including the more advanced type introduced here, can co-exist with the strongest type of quantum resistance and truly practical performance. This provides a better level of privacy than cash, with additional guarantees that the privacy cannot be taken from the end user.*
>
> David Chaum, inventor of eCash and creator of xx network

To read more:
https://www.bis.org/about/bisih/topics/cbdc/tourbillon.htm

Number 15

DEV-0569 finds new ways to deliver Royal ransomware, various payloads - Microsoft Security Threat Intelligence

Microsoft

Recent activity from the threat actor that Microsoft tracks as DEV-0569, known to distribute various payloads, has led to the deployment of the Royal ransomware, which first emerged in September 2022 and is being distributed by multiple threat actors.

Observed DEV-0569 attacks show a pattern of continuous innovation, with regular incorporation of new discovery techniques, defense evasion, and various post-compromise payloads, alongside increasing ransomware facilitation.

DEV-0569 notably relies on malvertising, phishing links that point to a malware downloader posing as software installers or updates embedded in spam emails, fake forum pages, and blog comments.

In the past few months, Microsoft security researchers observed the following tweaks in the group's delivery methods:

- Use of contact forms on targeted organizations' websites to deliver phishing links

- Hosting fake installer files on legitimate-looking software download sites and legitimate repositories to make malicious downloads look authentic to targets, and

- Expansion of their malvertising technique by using Google Ads in one of their campaigns, effectively blending in with normal ad traffic

These methods allow the group to potentially reach more targets and ultimately achieve their goal of deploying various post-compromise payloads. DEV-0569 activity uses signed binaries and delivers encrypted malware payloads.

The group, also known to rely heavily on defense evasion techniques, has continued to use the open-source tool Nsudo to attempt disabling antivirus solutions in recent campaigns.

In this blog we share details of DEV-0569's tactics, techniques, and procedures (TTPs) and observed behavior in recent campaigns, which show that DEV-0569 will likely continue leveraging malvertising and phishing for initial access.

We also share preventive measures that organizations can adopt to thwart DEV-0569's delivery methods involving malicious links and phishing emails using solutions like Microsoft Defender SmartScreen and Microsoft Defender for Office 365, and to reduce the impact of the group's follow-on activities. Microsoft Defender for Endpoint detects the DEV-0569 behavior discussed in this blog, including the code signing certificates in use and the attempts to disable Microsoft Defender Antivirus.

Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or developing cluster of threat activity, allowing Microsoft to track it as a unique set of information until we can reach high confidence about the origin or identity of the actor behind the activity. Once it meets defined criteria, a DEV group is converted to a named actor.

DEV-0569 attack chain: Delivery tactics tweaked

DEV-0569 has multiple methods for delivery of their initial payload. In some cases, DEV-0569 payloads are delivered via phishing campaigns run by other malicious actors that offer delivery of malware payloads as a service.

Historical observation of typical DEV-0569 attack begins with malicious links delivered to targets via malicious ads, fake forum pages, blog comments, or through phishing emails. These links lead to malicious files signed by the attacker using a legitimate certificate.

The malicious files, which are malware downloaders known as BATLOADER, pose as installers or updates for legitimate applications like Microsoft Teams or Zoom.

When launched, BATLOADER uses MSI Custom Actions to launch malicious PowerShell activity or run batch scripts to aid in disabling security solutions and lead to the delivery of various encrypted malware payloads that is decrypted and launched with PowerShell commands.

Posing as legitimate software download sites

From August to October 2022, Microsoft observed DEV-0569 activity where BATLOADER, delivered via malicious links in phishing emails, posed as legitimate installers for numerous applications like TeamViewer, Adobe Flash Player, Zoom, and AnyDesk.

BATLOADER was hosted on attacker-created domains posing as legitimate software download sites (anydeskos[.]com, for example) and on legitimate repositories like GitHub and OneDrive. Microsoft takes down verified malicious content from these repositories as they are found or reported.

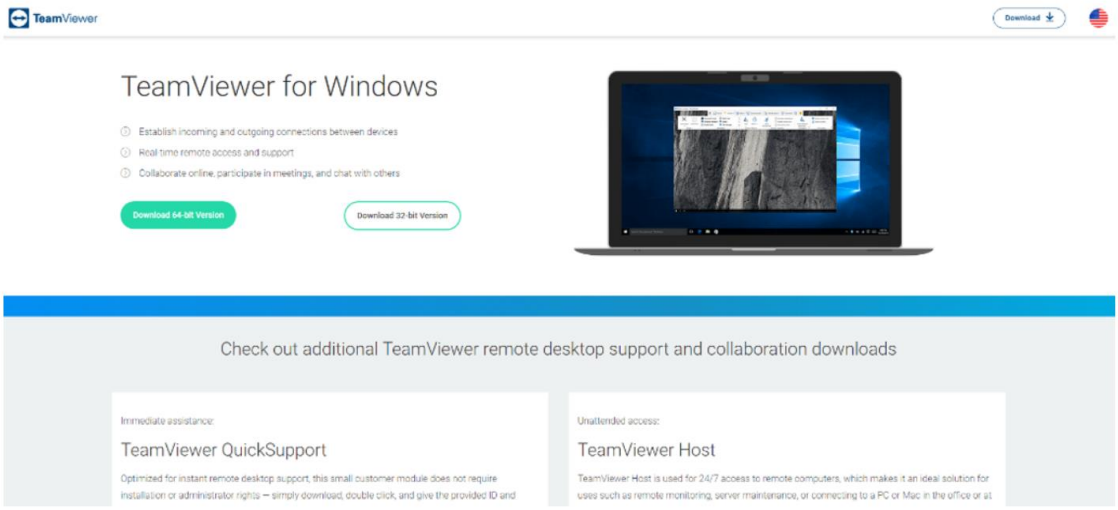


Figure 1. DEV-0569 activity seen in September 2022, where the landing site hosted BATLOADER posing as a TeamViewer installer

To read more: https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

Number 16

CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication

CISA has released two fact sheets to highlight threats against accounts and systems using certain forms of multifactor authentication (MFA).

CISA strongly urges all organizations to implement phishing-resistant MFA to protect against phishing and other known cyber threats.

If an organization using mobile push-notification-based MFA is unable to implement phishing-resistant MFA, CISA recommends using number matching to mitigate MFA fatigue.

Although number matching is not as strong as phishing-resistant MFA, it is one of best interim mitigation for organizations who may not immediately be able to implement phishing-resistant MFA.

CISA recommends users and organizations to read the fact sheets:

October 2022

OVERVIEW

This fact sheet is intended to provide for IT leaders and network defenders an improved understanding of current threats against accounts and systems that use multifactor authentication (MFA). MFA is a security control that requires a user to present a combination of two or more different authenticators (something you know, something you have, or something you are) to verify their identity for login. MFA makes it more difficult for cyber threat actors to gain access to networks and information systems if passwords or personal identification numbers (PINs) are compromised through phishing attacks or other means. With MFA enabled, if one factor, such as a password, becomes compromised, unauthorized users will be unable to access the account if they cannot also provide the second factor. This additional layer ultimately stops some of the common malicious cyber techniques, such as password spraying.

CISA has consistently urged organizations to implement MFA for all users and for all services, including email, file sharing, and financial account access. MFA is an essential practice to reduce the threat of cyber threat actors using compromised credentials to gain access to and conduct malicious activity on networks. However, not all forms of MFA are equally secure. Some forms are vulnerable to phishing, "push bombing" attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or SIM Swap attacks. These attacks, if successful, may allow a threat actor to gain access to MFA authentication credentials or bypass MFA and access the MFA-protected systems.

1. Implementing Phishing-Resistant MFA – you may visit: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

October 2022

OVERVIEW

CISA is releasing this fact sheet to highlight threats against accounts and systems using mobile push-notification-based multifactor authentication (MFA). Mobile push-notification-based MFA is a form of application-based MFA that authenticates via a mobile application notifying a user's smart phone. After receiving the prompt (aka "push" notification), the user presses "approve" on the notification to grant themselves access to their account. Cyber threat actors can gain access to systems with mobile push-notification-based MFA through using the "MFA fatigue" technique. MFA fatigue, also known as "push bombing," occurs when a cyber threat actor bombards a user with mobile application push notifications until the user either approves the request by accident or out of annoyance with the nonstop notifications.

To protect against MFA fatigue as well as other attack vectors such as phishing, CISA strongly encourages all organizations to implement phishing-resistant MFA, as detailed in CISA fact sheet Implement Phishing-Resistant MFA to Protect Against Cyber Threats. (**Note:** The Office of Management and Budget requires agencies to adopt phishing-resistant MFA methods.) If an organization that uses mobile push-notification-based MFA is unable to implement phishing-resistant MFA, CISA recommends using number matching to mitigate MFA fatigue. Although number matching is not as strong as phishing-resistant MFA, it is one of the best interim mitigation for organizations who may not immediately be able to implement phishing-resistant MFA.

2. Implementing Number Matching in MFA Applications – you may visit: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf

Number 17

How we handled a recent phishing incident that targeted Dropbox

Dropbox.Tech

We were recently the target of a phishing campaign that successfully accessed some of the code we store in GitHub.

No one's content, passwords, or payment information was accessed, and the issue was quickly resolved.

Our core apps and infrastructure were also unaffected, as access to this code is even more limited and strictly controlled. We believe the risk to customers is minimal. Because we take our commitment to security, privacy, and transparency seriously, we have notified those affected and are sharing more here.

In today's evolving threat landscape, people are inundated with messages and notifications, making phishing lures hard to detect. Threat actors have moved beyond simply harvesting usernames and passwords, to harvesting multi-factor authentication codes as well.

In September, GitHub detailed one such phishing campaign, in which a threat actor accessed GitHub accounts by impersonating the code integration and delivery platform CircleCI.

We recently learned that Dropbox was targeted by a similar campaign. On October 14, 2022, GitHub alerted us to some suspicious behavior that began the previous day. Upon further investigation, we found that a threat actor—also pretending to be CircleCI—accessed one of our GitHub accounts, too.

At no point did this threat actor have access to the contents of anyone's Dropbox account, their password, or their payment information.

To date, our investigation has found that the code accessed by this threat actor contained some credentials—primarily, API keys—used by Dropbox developers.

The code and the data around it also included a few thousand names and email addresses belonging to Dropbox employees, current and past customers, sales leads, and vendors (for context, Dropbox has more than 700 million registered users).

We take our commitment to protecting the privacy of our customers, partners, and employees seriously, and while we believe any risk to them is minimal, we have notified those affected.

At Dropbox, our number one company value is being worthy of trust. In the interest of transparency, and to contribute to the industry's understanding of these types of threats, we want to share what happened and how we responded.

What happened and our response

At Dropbox, we use GitHub to host our public repositories as well as some of our private repositories. We also use CircleCI for select internal deployments. In early October, multiple Dropboxers received phishing emails impersonating CircleCI, with the intent of targeting our GitHub accounts (a person can use their GitHub credentials to login to CircleCI).

While our systems automatically quarantined some of these emails, others landed in Dropboxers' inboxes. These legitimate-looking emails directed employees to visit a fake CircleCI login page, enter their GitHub username and password, and then use their hardware authentication key to pass a One Time Password (OTP) to the malicious site. This eventually succeeded, giving the threat actor access to one of our GitHub organizations where they proceeded to copy 130 of our code repositories.

These repositories included our own copies of third-party libraries slightly modified for use by Dropbox, internal prototypes, and some tools and configuration files used by the security team. Importantly, they did not include code for our core apps or infrastructure. Access to those repositories is even more limited and strictly controlled.

On the same day we were informed of the suspicious activity, the threat actor's access to GitHub was disabled. Our security teams took immediate action to coordinate the rotation of all exposed developer credentials, and determine what customer data—if any—was accessed or stolen. We also reviewed our logs, and found no evidence of successful abuse. To be sure, we hired outside forensic experts to verify our findings, and reported this event to the appropriate regulators and law enforcement.

What we're doing next

Our security teams work tirelessly to keep Dropbox worthy of our customer's trust. While the information accessed by this threat actor was limited, we hold ourselves to a higher standard. We're sorry we fell short, and apologize for any inconvenience. One way we hope to prevent a similar incident from occurring is by accelerating our adoption of WebAuthn.

Not all types of multi-factor authentication are created equal, and some are more vulnerable to phishing than others. While many organizations still rely on less secure forms of multi-factor authentication—such as push notifications, one-time passwords (OTP), and time-based one-time passwords (TOTP)—WebAuthn is currently the gold standard.

Prior to this incident, we were already in the process of adopting this more phishing-resistant form of multi-factor authentication. Soon, our whole environment will be secured by WebAuthn with hardware tokens or biometric factors. (We also offer WebAuthn to Dropbox customers. Visit our help center to learn how to enable this security measure on your Dropbox account.)

We know it's impossible for humans to detect every phishing lure. For many people, clicking links and opening attachments is a fundamental part of their job. Even the most skeptical, vigilant professional can fall prey to a carefully crafted message delivered in the right way at the right time. This is precisely why phishing remains so effective—and why technical controls remain the best protection against these kinds of attacks. As threats grow more sophisticated, the more important these controls become.

To read more: https://dropbox.tech/security/a-recent-phishing-campaign-targeting-dropbox

Number 18

NIST's Superconducting Hardware Could Scale Up Brain-Inspired Computing

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Scientists have long looked to the brain as an inspiration for designing computing systems. Some researchers have recently gone even further by making computer hardware with a brainlike structure.

These "neuromorphic chips" have already shown great promise, but they have used conventional digital electronics, limiting their complexity and speed.

As the chips become larger and more complex, the signals between their individual components become backed up like cars on a gridlocked highway and reduce computation to a crawl.

Now, a team at the National Institute of Standards and Technology (NIST) has demonstrated a solution to these communication challenges that may someday allow artificial neural systems to operate 100,000 times faster than the human brain.

The human brain is a network of about 86 billion cells called neurons, each of which can have thousands of connections (known as synapses) with its neighbors.

The neurons communicate with each other using short electrical pulses called spikes to create rich, time-varying activity patterns that form the basis of cognition. In neuromorphic chips, electronic components act as artificial neurons, routing spiking signals through a brainlike network.

Doing away with conventional electronic communication infrastructure, researchers have designed networks with tiny light sources at each neuron that broadcast optical signals to thousands of connections.

This scheme can be especially energy-efficient if superconducting devices are used to detect single particles of light known as photons — the smallest possible optical signal that could be used to represent a spike.

In a new Nature Electronics paper, NIST researchers have achieved for the first time a circuit that behaves much like a biological synapse yet uses just single photons to transmit and receive signals.

Such a feat is possible using superconducting single-photon detectors. The computation in the NIST circuit occurs where a single-photon detector meets a superconducting circuit element called a Josephson junction.

A Josephson junction is a sandwich of superconducting materials separated by a thin insulating film.

If the current through the sandwich exceeds a certain threshold value, the Josephson junction begins to produce small voltage pulses called fluxons.

Upon detecting a photon, the single-photon detector pushes the Josephson junction over this threshold and fluxons are accumulated as current in a superconducting loop.

Researchers can tune the amount of current added to the loop per photon by applying a bias (an external current source powering the circuits) to one of the junctions. This is called the synaptic weight.

This behavior is similar to that of biological synapses. The stored current serves as a form of short-term memory, as it provides a record of how many times the neuron produced a spike in the near past.

The duration of this memory is set by the time it takes for the electric current to decay in the superconducting loops, which the NIST team demonstrated can vary from hundreds of nanoseconds to milliseconds, and likely beyond.

This means the hardware could be matched to problems occurring at many different time scales — from high-speed industrial control systems to more leisurely conversations with humans.

The ability to set different weights by changing the bias to the Josephson junctions permits a longer-term memory that can be used to make the networks programmable so that the same network could solve many different problems.

Synapses are a crucial computational component of the brain, so this demonstration of superconducting single-photon synapses is an important milestone on the path to realizing the team's full vision of superconducting optoelectronic networks. Yet the pursuit is far from complete.

The team's next milestone will be to combine these synapses with on-chip sources of light to demonstrate full superconducting optoelectronic neurons.

General intelligence involves the integration of many sources of information into a coherent, adaptive model of the world. To design and construct hardware for general intelligence, we must consider principles of both neuroscience and very-large-scale integration. For large neural systems capable of general intelligence, the attributes of photonics for communication and electronics for computation are complementary and interdependent. Using light for communication enables high fan-out as well as low-latency signaling across large systems with no traffic-dependent bottlenecks. For computation, the inherent nonlinearities, high speed, and low power consumption of Josephson circuits are conducive to complex neural functions.

You may visit: https://aip.scitation.org/doi/10.1063/5.0040567

"We could use what we've demonstrated here to solve computational problems, but the scale would be limited," NIST project leader Jeff Shainline said. "Our next goal is to combine this advance in superconducting electronics with semiconductor light sources.

That will allow us to achieve communication between many more elements and solve large, consequential problems."

The team has already demonstrated light sources that could be used in a full system, but further work is required to integrate all the components on a single chip.

The synapses themselves could be improved by using detector materials that operate at higher temperatures than the present system, and the team is also exploring techniques to implement synaptic weighting in larger-scale neuromorphic chips.

The work was funded in part by the Defense Advanced Research Projects Agency. To read more: https://www.nist.gov/news-events/news/2022/10/nists-superconducting-hardware-could-scale-brain-inspired-computing

Number 19

31 arrested for stealing cars by hacking keyless tech

With the support of Europol and Eurojust, the French authorities in cooperation with their Spanish and Latvian counterparts have dismantled a car theft ring which used a fraudulent software to steal vehicles without using the physical key fob.

The criminals targeted vehicles with keyless entry and start systems, exploiting the technology to get into the car and drive away.

As a result of a coordinated action carried out on 10 October in the three countries involved, 31 suspects were arrested. A total of 22 locations were searched, and over EUR 1 098 500 in criminal assets seized.

The criminals targeted keyless vehicles from two French car manufacturers. A fraudulent tool – marketed as an automotive diagnostic solution, was used to replace the original software of the vehicles, allowing the doors to be opened and the ignition to be started without the actual key fob.

Among those arrested feature the software developers, its resellers and the car thieves who used this tool to steal vehicles.

The investigation was initiated by the French Gendarmerie's Cybercrime Centre (C3N). Europol has been supporting this case since March 2022 with extensive analysis and the dissemination of intelligence packages to all the countries affected by this crime.

Two operational meetings were organised at Europol's headquarters to jointly decide on the final phase of the investigation. A Europol mobile office was also deployed to France for the action day to assist the French authorities with their investigative measures.

The case was opened at Eurojust by the French authorities in September 2022. The Agency actively facilitated cross-border judicial cooperation between the national authorities involved, including the organisation of the joint action day.

The following authorities took part in the investigation:

- France: National Jurisdiction against Organised Crime (JUNALCO), National Gendarmerie (Gendarmerie Nationale)

- Latvia: State Police of Latvia

- Spain: Investigative Court num. 2 in Palma de Mallorca Balearic Islands PPO

This investigation was carried out with the financial support of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) and the Internal Security Fund (ISF) SWORD.

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime, and other serious and organised crime forms. Europol also works with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

To read more: https://www.europol.europa.eu/media-press/newsroom/news/31-arrested-for-stealing-cars-hacking-keyless-tech

Number 20

International Regulation of Crypto-asset Activities - Questions for consultation

FSB FINANCIAL STABILITY BOARD

The FSB is inviting comments on its proposed set of recommendations and on the questions set out below. Responses should be sent to fsb@fsb.org by 15 December 2022. Responses will be published on the FSB's website unless respondents expressly request otherwise.

General

1. Are the FSB's proposals sufficiently comprehensive and do they cover all crypto-asset activities that pose or potentially pose risks to financial stability?

2. Do you agree that the requirements set out in the CA Recommendations should apply to any type of crypto-asset activities, including stablecoins, whereas certain activities, in particular those undertaken by GSC, need to be subject to additional requirements?

3. Is the distinction between GSC and other types of crypto-assets sufficiently clear or should the FSB adopt a more granular categorisation of crypto-assets (if so, please explain)?

4. Do the CA Recommendations and the GSC Recommendations each address the relevant regulatory gaps and challenges that warrant multinational responses?

5. Are there any financial stability issues that remain unaddressed that should be covered in the recommendations?

Crypto-assets and markets (CA Recommendations)

6. Does the report accurately characterise the functions and activities within the crypto-ecosystem that pose or may pose financial stability risk? What, if any, functions, or activities are missing or should be assessed differently?

(The report: https://www.fsb.org/wp-content/uploads/P111022-2.pdf)

FSB FINANCIAL STABILITY BOARD

International Regulation of Crypto-asset Activities

A proposed framework – questions for consultation

7. Do you agree with the analysis of activity patterns and the associated potential risks?

8. Have the regulatory, supervisory and oversight issues and challenges as relate to financial stability been identified accurately? Are there other issues that warrant consideration at the international level?

9. Do you agree with the differentiated requirements on crypto-asset issuers and service providers in the proposed recommendations on risk management, data management and disclosure?

10. Should there be a more granular differentiation within the recommendations between different types of intermediaries or service providers in light of the risks they pose? If so, please explain.

Global stablecoins (GSC Recommendations)

11. Does the report provide an accurate analysis of recent market developments and existing stablecoins? What, if anything, is missing in the analysis or should be assessed differently?

FSB FINANCIAL STABILITY BOARD

Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements

Consultative report

(The report: https://www.fsb.org/wp-content/uploads/P111022-4.pdf)

12. Are there other changes or additions to the recommendations that should be considered?

13. Do you have comments on the key design considerations for cross-border cooperation and information sharing arrangements presented in Annex 2? Should Annex 2 be specific to GSCs, or could it be also applicable to crypto-asset activities other than GSCs?

14. Does the proposed template for common disclosure of reserve assets in Annex 3 identify the relevant information that needs to be disclosed to users and stakeholders?

15. Do you have comments on the elements that could be used to determine whether a stablecoin qualifies as a GSC presented in Annex 4?

To read more: https://www.fsb.org/2022/10/international-regulation-of-crypto-asset-activities-questions-for-consultation/

Number 21

Cybersecurity threats in the health care sector

An Increasingly Dangerous Threat

Over the past decade, the American public has witnessed increasingly brazen and disruptive attacks on its health care sector that jeopardize sensitive personal information, delay treatment, and ultimately lead to increased suffering and death.

In 2021, cybersecurity attacks on health care providers reached an all-time high, with one study indicating that more than 45 million people were affected by such attacks in 2021 – a 32 percent increase over 2020.

The health care sector is vulnerable to cyberattacks for a number of reasons, including its reliance on legacy technology, a wide and highly varied attack surface (that only grows more complex from the ever-increasing number of connected devices), a high-pressure environment where even the slightest delay can have life-or-death consequences, funding constraints, and an outdated mode of thinking that views cybersecurity as a secondary or tertiary concern.

These challenges are compounded when coupled with the incredibly alluring target that the health care sector presents to cybercriminals.

Personal health information is more valuable on the black market than even credit card information, as hackers can sell stolen medical records for anywhere from $10 to $1,000 per record.

These attacks are also costly, with the health care industry seeing the highest cost per breach of any industry, according to IBM's annual Cost of a Data Breach report.

Although these cybersecurity vulnerabilities certainly leave health care organizations exposed to patient data theft, they often have far-reaching, and more serious, impacts beyond privacy concerns.

Cyberattacks can be detrimental to patient safety, as they can lock physicians out of treatment tools, shut down hospital equipment used for care, and create backlogs that delay appointments and treatment.

When it comes to cyberattacks affecting patient care, the question is no longer a matter of if or when, but how often and how catastrophic the consequences.

CONTENTS

To read more:
https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/032065868 0B8F1D29C9A94895044DA31.cips-report.pdf

Number 22

Council conclusions on a Framework for a coordinated EU response to hybrid campaigns

THE COUNCIL OF THE EUROPEAN UNION,

1. RECALLS the relevant conclusions of the European Council and the Council,

ACKNOWLEDGES that state and non-state actors are increasingly using hybrid tactics, posing a growing threat to the security of the EU, its Member States and its partners.

RECOGNISES that, for some actors applying such tactics, peacetime is a period for covert malign activities, when a conflict can continue or be prepared for in a less open form.

EMPHASISES that state actors and non-state actors also use information manipulation and other tactics to interfere in democratic processes and to mislead and deceive citizens.

NOTES that Russia's armed aggression against Ukraine is showing the readiness to use the highest level of military force, regardless of legal or humanitarian considerations, combined with hybrid tactics, cyberattacks, foreign information manipulation and interference, economic and energy coercion and an aggressive nuclear rhetoric, and

ACKNOWLEDGES the related risks of potential spillover effects in EU neighbourhoods that could harm the interests of the EU.

2. REITERATES that, in the face of the current geopolitical shifts, the strength of our Union lies in unity, solidarity and determination, by enhancing the EU's strategic autonomy and its ability to work with partners to safeguard its values and interests, and by swiftly implementing the Strategic Compass, including to counter hybrid threats and campaigns.

UNDERLINES that a stronger and more capable EU in the field of security and defence will contribute positively to global and transatlantic security and is complementary to NATO, which remains the foundation of collective defence for its members.

REAFFIRMS the EU's intention to intensify support for the rules-based international order, with the United Nations at its core.

3. RECALLS that the Strategic Compass, approved by the Council on 21 March 2022 and endorsed by the European Council on 24 and 25 March 2022, underlines the need to develop in 2022 an EU Hybrid Toolbox that should bring together existing and possible new instruments and provide a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States, comprising for instance preventive, cooperative, stability, restrictive and recovery measures and strengthening solidarity and mutual assistance, as well as the need to develop in 2022 the Foreign Information Manipulation and Interference Toolbox ('FIMI toolbox'), which will strengthen our ability to detect, analyse and respond to the threat, including by imposing costs on perpetrators.

STRESSES that hybrid campaigns will be detected and countered at their early stages using all necessary EU policies and instruments. Thus, for the development of this broad EU Hybrid Toolbox,

INTRODUCES a Framework for a coordinated response to hybrid threats and campaigns affecting the EU, Member States and partners, and

UNDERLINES that this Framework should also be used to address foreign information manipulation and interference in the information domain (FIMI).

4. NOTES that while definitions of hybrid threats and campaigns may vary, they need to remain flexible in order to allow for proper responses to the evolving nature of the threat. For the purpose of this Framework and to allow it to be used effectively,

ACKNOWLEDGES the conceptualisation of 'hybrid threat' and 'hybrid threat campaign' – hereby referred to as 'hybrid campaign' - provided by the Commission and the European Centre of Excellence for Countering Hybrid Threats in 'The Landscape of Hybrid Threats: A Conceptual Model'

UNDERLINES that the Hybrid Risk Survey plays a key role in developing a common understanding and analysis of hybrid threats and campaigns, as well as in identifying vulnerabilities potentially affecting national and pan-European structures and networks, as well as EU partners in neighbourhood regions.

5. EMPHASISES the importance of a strong coordinated response demonstrating EU solidarity in the event of hybrid attacks targeting the EU and its Member States, and

STRESSES that the EU Hybrid Toolbox, as well as this Framework, should contribute to responses to hybrid attacks, as appropriate.

UNDERLINES the relevance of existing EU crisis management mechanisms, including the Council's Integrated Political Crisis Response (IPCR) arrangements, in supporting coordinated action in response to major, complex crises.

6. UNDERLINES that, as the distinction between internal and external threats is becoming increasingly blurred by actors using hybrid tactics, a comprehensive response to hybrid threats and campaigns should mobilise all relevant internal and external EU policies and tools, as set out in the EU Security Union Strategy 2020-2025, and include all relevant civil and military tools and measures.

EMPHASISES the increased need to prevent, detect, mitigate and respond to hybrid threats and activities and that the EU and its Member States should be able to mitigate and terminate the impact of a hybrid campaign at the earliest stage possible and prevent it from developing into a full-fledged crisis, using the full range of the EU's and its Member States' capacities, tools and instruments, in particular those measures that aim to boost the EU's and its Member States' capacity to build resilience, deny perpetrators the benefits of a hybrid campaign and increase the costs for them.

EMPHASISES that hybrid campaigns in third countries can also have an impact on EU security, values and interests and that it is therefore important that the EU and its Member States can respond to requests for assistance from partner countries, if appropriate, using this Framework.

UNDERLINES that clearly signalling the likely consequences of a coordinated EU response to hybrid campaigns influences the behaviour of potential aggressors and could prevent them from achieving their goals, thus reinforcing the security of the EU and its Member States.

STRESSES the importance for the EU and its Member States of developing an adequate posture in this area, based on the work of the relevant Council bodies.

7. UNDERLINES that when one or multiple incidents that could be part of a hybrid campaign have been detected or have been brought to the attention of Member States by the Commission or the High Representative, Member States may request that the relevant Council body examine the issue.

EMPHASISES the need for a fast and efficient decision-making process, on a case-by-case basis, to define and approve coordinated EU responses to hybrid campaigns, including FIMI.

UNDERLINES that in such cases there is a need for the Council to quickly receive proposals prepared jointly by the Commission and the High Representative and, where relevant, make swift decisions on their implementation based on the support that can be given by the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats to Coreper and, when activated, to the IPCR arrangements.

NOTES that the Political and Security Committee (PSC) may deliberate on the measures decided on within this Framework that fall within its mandate.

8. REITERATES that primary responsibility for countering hybrid threats lies with Member States and STRESSES that decisions on a coordinated EU response to hybrid campaigns should be guided by the following main principles:

- serve to protect democratic values, processes and institutions, as well as the integrity and security of the EU, its Member States and their citizens, and its strategic interests, including the security of partners in our neighbourhood and beyond;

- respect international law and protect fundamental rights and freedoms, and support international peace and security;

- provide for the attainment of the objectives of the Union, in particular the Common Foreign and Security Policy (CFSP) objectives, as set out in the Treaty on European Union (TEU), and the objectives set out in Treaty on the Functioning of the European Union (TFEU), as well as the procedures required for their attainment;

- be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of each particular hybrid campaign;

- be based on a shared situational awareness among the Member States and correspond to the needs of the specific situation at hand;

- take into account the broader context of the EU's external relations with the state concerned by the response.

9. INVITES the High Representative – through the Single Intelligence Analysis Capacity (SIAC), in particular the Hybrid Fusion Cell – to continue to provide comprehensive assessments of hybrid threats affecting the EU and its Member States, based primarily on the Member States' contributions, including annual Hybrid Trends Analysis (HTA) reports, and

CALLS on Member States and relevant institutions to enhance their participation and contributions to these reports.

10. ENCOURAGES the EU and its Member States to take further action to develop an efficient monitoring mechanism covering various hybrid domains and the variety of hybrid activities taking place in each of them, using new technologies – including artificial intelligence – and mobilising the necessary networks.

TAKES NOTE in that regard of the proposal by the High Representative to create an appropriate mechanism to systematically collect data on FIMI incidents, facilitated by a dedicated Data Space.

STRESSES the role of CSDP missions and operations in enhancing EU situational awareness by monitoring hybrid threats, in line with their mandate.

11. ENCOURAGES the EU and Member States to collect and decode relevant early signals, exchange information and constantly assess possible links between them in order to characterise a threat quickly;

EMPHASISES that Member States and relevant EU institutions, bodies and agencies should enhance their contributions to building shared situational awareness by sharing relevant information through the SIAC – as a single entry point for strategic intelligence contributions from Member States' civilian and military intelligence and security services, through the Rapid Alerts System, by sharing relevant situational updates and by providing their national assessments as part of awareness-raising activities within the relevant Council working party;

STRESSES that the SIAC, in particular the Hybrid Fusion Cell, will play a central role contributing to the decision-making process by providing strategic foresight and comprehensive situational awareness, notably to identify the origin and features of the hybrid campaign, provided they have the appropriate resources; and

NOTES that this work can be complemented by other relevant EU institutions, bodies and agencies, as well as CSDP missions and operations, as appropriate and at the request of the Council.

12. REITERATES the need to enhance the EU's overall level of resilience to hybrid threats and campaigns, based on a whole-of-society and whole-of-government approach, through the adoption of the Directive on measures to achieve a high common level of cybersecurity across the Union (NIS 2 Directive) and the Directive on the resilience of critical entities (CER Directive), and in the light of the proposed Regulation on the transparency

and targeting of political advertising, the Digital Services Act (DSA), the proposed Anti-Coercion Instrument (ACI), the revised Code of Practice on Disinformation, and the implementation of the EU foreign investment screening mechanism, and

INVITES Member States, with the support of the Commission, to make the best use of the joint operational mechanism on electoral resilience.

ENCOURAGES the Commission to make use of new instruments, including the Observatory of Critical Technologies, to identify dependencies and vulnerabilities that could be used in the framework of hybrid campaigns.

INVITES the Commission and the High Representative to identify by the end of 2022, as part of the development of the EU Hybrid Toolbox, operational proposals to bolster societal and economic resilience to hybrid threats, based, where appropriate, on the EU's sectoral hybrid resilience baselines, the Hybrid Risk Survey and the EU Flagship report on resilience.

13. STRESSES that priority should be given to measures aiming to mitigate and terminate the impact of a detected campaign, as well as to prevent its further expansion and escalation, discourage its perpetrator from conducting further action and facilitate the quick recovery of the targeted Member State or EU institution, body or agency. In doing so,

ENCOURAGES the Commission and the High Representative to mobilise all the EU's tools and instruments drawing from external and internal policies, in accordance with their respective rules and governance.

14. EMPHASISES that when the perpetrator of a hybrid campaign can be identified with a high degree of certainty, asymmetric and proportionate measures in line with international law may be taken – including forms of diplomatic, political, military, economic or strategic communication – to prevent or respond to a hybrid campaign, including in the event of malicious activities that are not classified as internationally unlawful acts but are considered unfriendly acts;

AFFIRMS that measures within foreign, security and defence policy, including, if necessary, restrictive measures, are suitable for this Framework and should strengthen prevention, encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term;

INVITES the Commission and the High Representative to develop options for well-defined measures that could be taken against FIMI actors when this is necessary to protect EU public order and security; and

RECALLS that Member States may propose coordinated attribution of hybrid activities, recognising that attribution is a sovereign national prerogative.

15. NOTES that the measures falling within the foreign, security and defence policies can be inter alia preventive measures, including capacity and confidence building measures, exercises and training, including through CSDP missions and operations; cooperative measures, including dialogue, cooperation, coordination, sharing of best practices and training with partner countries and organisations; stability building measures, including public diplomacy and diplomatic engagement with the involved state actor, when and where appropriate in coordination with relevant international organisations and with like-minded partners and countries; restrictive measures (sanctions), including against those responsible for the campaign, according to the relevant provisions of the Treaties; measures to support Member States, upon their request, that choose to exercise their inherent right of individual or collective self-defence as recognised in Article 51 of the Charter of the United Nations and in accordance with international law.

NOTES that those measures include obligations stemming from the Treaty on European Union, such as support in response to the invocation of Article 42(7) of the Treaty on European Union, which stipulates that, if a Member State is a victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organization, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.

16. UNDERLINES that the use of military force can be an integral component of some state actors' hybrid tactics and

NOTES their readiness to use hybrid tactics combined with or in preparation for or as a substitute for armed aggression.

STRESSES the need, in line with the Strategic Compass, to further invest in our mutual assistance under Article 42(7) of the Treaty on European Union as well as solidarity under Article 222 of the Treaty on the Functioning of the European Union, in particular through frequent exercises, to prevent, prepare against, and counter such actions.

17. UNDERLINES that attribution is defined as the practice of assigning responsibility for a malicious hybrid activity to a specific actor;

ACKNOWLEDGES that attribution may contribute to building greater resilience, by preparing and educating the public about the threat, and may also help build support for possible further measures;

RECALLS that attribution to a state or a non-state actor remains a sovereign political decision based on all-source intelligence and taken on a case-by-case basis;

STRESSES that Member States may employ different methods and procedures to attribute malicious hybrid activities, and

UNDERLINES that the SIAC plays a key role in supporting Member States in this regard.

18. NOTES that hybrid campaigns are often designed in such a way as to create ambiguity around their origins and to hinder decision-making processes. In that regard,

STRESSES that not all measures forming part of a coordinated EU response to hybrid campaigns require responsibility to be assigned to a state or a non-state actor and that measures within the Framework can be tailored to the degree of certainty that can be established in any particular case;

UNDERLINES that when coordinated attribution is not possible or public attribution is not in the best interest of the EU and its Member States, well-calibrated asymmetric actions responding to a hybrid campaign against the EU, its Member States or partners, according to this Framework and in accordance with international law, could also be envisaged on a case-by-case basis, upon due approval.

19. ACKNOWLEDGES that malicious cyber activities are often a key element of hybrid campaigns and the continued development of the EU cyber posture is an important step towards preventing, discouraging, deterring and responding to malicious cyber activities, including malicious cyber activities that form part of a hybrid campaign.

UNDERLINES that the EU Cyber Diplomacy Toolbox counters cyber security threats and could contribute to the EU response to a hybrid campaign, in line with to its own rules and procedures;

STRESSES the need for relevant Council bodies, the High Representative and the Commission to encourage cooperation and synergies in the

implementation of measures and actions decided on under this Framework, in particular through the Hybrid Toolbox and FIMI Toolbox, as well as within the EU Cyber Diplomacy Toolbox when and where appropriate.

20. EMPHASISES the need for cooperation and coordinated responses, where appropriate, with like-minded partners when implementing this Framework.

STRESSES the importance of further cooperating with relevant international organisations, such as NATO, and like-minded partners and countries, including in the UN and the G7, as well as with civil society and private sector in countering hybrid threats and in view of defining a leading role for the EU in international norm development for countering hybrid threats, including FIMI.

EMPHASIZES in particular the need to develop synergies and explore further avenues for counter-hybrid cooperation with NATO, inter alia by building on the Parallel and Coordinated Exercises organised by the EU and NATO to prepare for tackling complex hybrid attacks, taking into account the shifting geopolitical and technological trends currently underway, in full respect of the principles of transparency, reciprocity and inclusiveness, as well as the decision-making autonomy and procedures of both organisations.

21. STRESSES the need to further develop in 2022 both the EU Hybrid Toolbox and the FIMI Toolbox, in line with the guidance given by the Strategic Compass.

INVITES the High Representative and the Commission to continue to identify measures to be implemented within this Framework based on a regular update of the existing mapping and, before the end of 2022, to submit proposals on the creation of EU Hybrid Rapid Response Teams, in order for these to be approved by the Council.

INVITES the Commission and the High Representative to conclude the review of the EU operational protocol for countering hybrid threats ('EU Playbook') and present its revised version by the end of 2022.

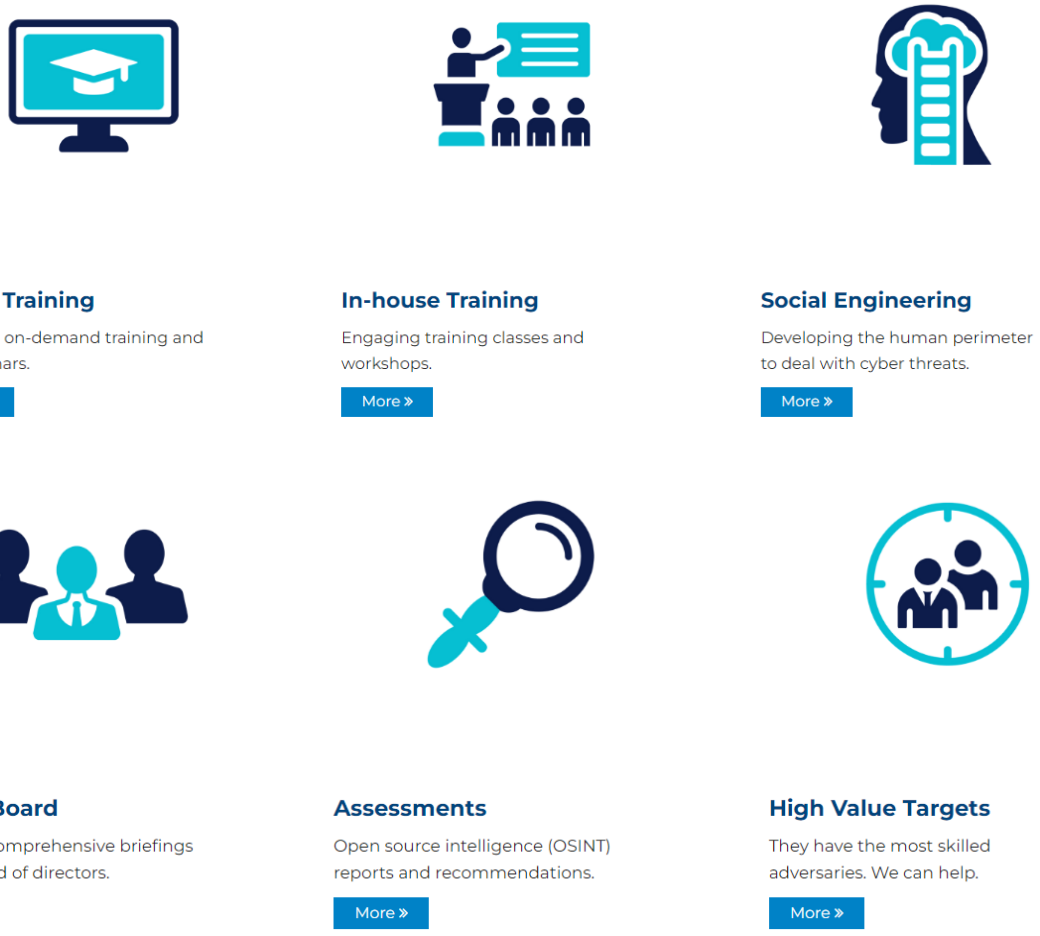
CALLS on the Member States, the Commission and the High Representative to give full effect to the development of the Framework, putting in place implementing guidelines and testing its procedures through existing and new exercises, including exercises involving the activation of Article 222 TFEU and/or Article 42(7) TEU. The Council will TAKE STOCK of the implementation of these conclusions before the end of

2023 and, if necessary, will review the Framework in order to address the evolving threat landscape.

You may visit: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

Cyber Risk GmbH

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



Cyber security training

Overview

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

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

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

Duration

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

Our Education Method

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

Our Instructors

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

Our training programs include:

1. *Information Security Awareness Training*. You may visit: https://www.cyber-risk-gmbh.com/1_Information_Security_Awareness_Training.html

2. *Social Engineering, Awareness and Defense*. You may visit: https://www.cyber-risk-gmbh.com/2_Social_Engineering_Awareness_Defence.html

3. *Practical Social Engineering. Defense and Protection of Sensitive Information*. You may visit: https://www.cyber-risk-gmbh.com/3_Practical_Social_Engineering.html

4. *Insider Threats Awareness Training*. You may visit: https://www.cyber-risk-gmbh.com/4_Insider_Threats_Awareness_Training.html

5. *The target is the bank. From hacking to cybercrime to cyberespionage*. You may visit:
https://www.cyber-risk-gmbh.com/5_The_Target_Is_The_Bank.html

6. *Cybersecurity training for managers and employees working in the hospitality industry*. You may visit:
https://www.cyber-risk-gmbh.com/6_Cybersecurity_Training_Hospitality_Industry.html

7. *Cybersecurity training for managers and employees working in the commercial and private aviation industry*. You may visit:
https://www.cyber-risk-gmbh.com/7_Cybersecurity_Training_Aviation_Industry.html

8. *Cybersecurity training for managers and employees working in the healthcare industry*. You may visit:
https://www.cyber-risk-gmbh.com/8_Cybersecurity_Training_Healthcare_Industry.html

9. *The General Data Protection Regulation (GDPR) for EU and non-EU based companies*. You may visit:
https://www.cyber-risk-gmbh.com/9_GDPR.html

10. *The General Data Protection Regulation (GDPR) for the Board of Directors and the CEO of EU and non-EU based companies*. You may visit:
https://www.cyber-risk-gmbh.com/10_GDPR_Board.html

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

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

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

7. The 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.