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

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

Dear readers,

Sun Tzu believed that *the supreme art of war is to subdue the enemy without fighting*. He has also said that *there is no instance of a nation benefitting from prolonged warfare*.

The war in Ukraine includes *cyber-attacks* that impact organizations both within and beyond the war region, particularly in the wake of sanctions imposed by the United States, the European Union and their Allies. Every organization—large and small—must be prepared to respond to cyber-attacks.

According to the Cybersecurity and Infrastructure Security Agency (CISA), a leader in the efforts to understand, manage, and reduce risk to the cyber and physical infrastructure, this is what *the Board and the CEO* must do:

- *Empower Chief Information Security Officers (CISO):* In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat

environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term.

- *Lower Reporting Thresholds:* Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal.

  Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI.

  Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.

- *Participate in a Test of Response Plans:* Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.

- *Focus on Continuity:* Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions.

  Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.

- *Plan for the Worst:* Organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

CISA urges *individuals* to practice the following:

- *Implement multi-factor authentication on your accounts*. A password isn't enough to keep you safe online.

By implementing a second layer of identification, like a confirmation text message or email, a code from an authentication app, a fingerprint or Face ID, or best yet, a FIDO key, you're giving your bank, email provider, or any other site you're logging into the confidence that it really is you.

Multi-factor authentication can make you 99% less likely to get hacked. So enable multi-factor authentication on your email, social media, online shopping, financial services accounts. And don't forget your gaming and streaming entertainment services!

- *Update your software*. In fact, turn on automatic updates. Bad actors will exploit flaws in the system.

  Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too.

  Leverage automatic updates for all devices, applications, and operating systems.

- *Think before you click*. More than 90% of successful cyber-attacks start with a phishing email.

  A phishing scheme is when a link or webpage looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information.

  Once they have that information, they can use it on legitimate sites. And they may try to get you to run malicious software, also known as malware.

  If it's a link you don't recognize, trust your instincts, and think before you click.

- *Use strong passwords, and ideally a password manager to generate and store unique passwords.* Our world is increasingly digital and increasingly interconnected.

  So, while we must protect ourselves, it's going to take all of us to really protect the systems we all rely on.

Read more at number 1 and 4 below.

Friedrich Nietzsche believed that the *demand* to be loved is the greatest of all arrogant presumptions. Today we have some great news for another kind of demand.

I have just read the "Semiannual Monetary Policy Report to the Congress" (before the Committee on Financial Services, House of Representatives, Washington, D.C.) from Chair Pro Tempore Jerome H. Powell.

There are some very interesting developments. Labor *demand* has been remarkably strong, labor *supply* has been slow to rebound, wage and employment *gains* were widespread across jobs and industries. We read:

"*Low labor supply*. Labor supply has been slow to rebound even as labor demand has been remarkably strong. The labor force participation rate remains well below estimates of its longer-run trend, principally reflecting a wave of retirements among older individuals and increases in the number of people out of the labor force and engaged in caregiving responsibilities. The ongoing pandemic has also affected labor supply through fear of the virus or the need to quarantine. Moreover, savings buffers accumulated during the pandemic may have enabled some people to remain out of the labor force."

"*Wage and employment growth across jobs and workers*. Wage and employment gains were widespread across jobs and industries last year, with the lowest-wage jobs experiencing the largest gains in both median wages and employment.

Wage growth in the leisure and hospitality industry accelerated sharply, which, together with a lagging employment rebound and high job openings, suggests a lack of available workers in the industry.

Median wages also increased across racial and ethnic groups, leaving differences in wage levels across groups little changed relative to 2019."

"*Broadening of inflation*. Higher PCE price inflation broadened out over the course of 2021, with the share of products experiencing notable price increases moving appreciably higher.

The broadening was evident in both goods and services, though most of last year's very high inflation readings were concentrated in goods, a reflection of the strong demand and supply bottlenecks that have particularly affected these items."

Read more at number 7 below.

I have read again the “Strengthening American Cybersecurity Act of 2022”. There are some very important parts, including new offensive cybersecurity tools.

For example, the new *Joint Ransomware Task Force* will prioritize intelligence-driven operations to disrupt specific ransomware actors, and to disrupt ransomware criminal actors, associated infrastructure, and their finances.

SEC. 206. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) Joint Ransomware Task Force.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, shall establish and chair the *Joint Ransomware Task Force* to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of *after-action reports and other lessons learned* from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks.

The "Strengthening American Cybersecurity Act of 2022" has some interesting definitions:

The term *'ransomware attack'*—

"(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

"(B) does not include any such event where the demand for payment is—

"(i) not genuine; or

"(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

Read more at number 13 below.

Every time I meet a good friend who works as an attorney appearing and practicing before the Securities and Exchange Commission (SEC) in the representation of issuers, I ask him the same question: *Has the SEC fulfilled Congress's mandate under Section 307 of the Sarbanes-Oxley Act (to adopt minimum standards of professional conduct) for attorneys?* His answer is always short: *No*.

For me, Section 307 is the most difficult part of the Sarbanes-Oxley Act. Establishing minimum standards of professional conduct for attorneys

can put the attorneys into conflict between fulfilling section 307's disclosure requirements and protecting the attorney-client relationship.

Corporate lawyers (that represent a corporation and its shareholders) could end up owing conflicting duties to their clients and to the public. Section 307 it is one federal legislative attempt to regulate attorney professional responsibility, which has traditionally been controlled by the States and local bar organizations.

I was waiting for my breakfast when I read that SEC Commissioner Allison Herren Lee gave a presentation with title: *"Send Lawyers, Guns and Money: (Over-) Zealous Representation by Corporate Lawyers"*. I forgot the breakfast and started reading:

"I want to talk about supporting securities lawyers, both in-house and outside counsel, in upholding the best traditions of the profession.

Specifically, by fulfilling a mandate in the Sarbanes-Oxley Act designed to do just that. As we near the twentieth anniversary of its passage, we still have not fulfilled Congress's mandate under Section 307 of Sarbanes-Oxley to adopt minimum standards of professional conduct for attorneys appearing and practicing before the Commission in the representation of issuers.

A key element of Sarbanes-Oxley, passed in the wake of the massive financial failures of the Enron era, was to create structures of accountability for professionals—executives, accountants and auditors, and, under Section 307 of the Act, accountability for lawyers.

In considering Section 307, Congress recognized that executives and accountants did not "work alone," and that lawyers were "virtually always there looking over their shoulders."

Congress was concerned, however, that counsel often acted in the interests of the executives who hired them rather than the company and its shareholders to whom their duty and responsibility is owed.

Unfortunately, in response to this mandate, the SEC adopted only one standard: the so-called "up-the-ladder" rule, requiring lawyers to report certain potential violations up the chain of management inside a corporate client.

We did not adopt a broader set of rules as Congress directed, and quite significantly, even this single standard has not been enforced in the nearly 20 years since it was adopted.

The policies behind this unfulfilled mandate—which are designed to support lawyers in their gatekeeping role—are as relevant and compelling today as they were 20 years ago, if not more so. Indeed, the role of corporate lawyers as gatekeepers in the capital markets—distinct from the litigator's role—has long been acknowledged by a broad and bipartisan group from William O. Douglas, to A.A. Sommer and Stanley Sporkin. It also includes Independent, Republican, and Democratic Chairs of the SEC.

And it wasn't just during the Enron era that we saw lapses in the gatekeeping role. We saw such lapses with stock option backdating and mutual fund market timing cases, and to some extent in the 2008 financial crisis.

More recently, we have seen an entirely new, multi-trillion dollar industry develop around cryptocurrency and digital assets that largely defies existing laws and regulations."

This is new. Section 307 of the Sarbanes-Oxley Act and cryptocurrencies. I didn't expect that. Life is full of surprises.

Read more at number 12 below.

There is a new brochure published by the FDFA and the DDPS (d/fr)

Neutrality is a successful instrument of Swiss foreign and security policy. It has strong support among the Swiss population. Switzerland's neutrality is *self-chosen, permanent, internationally recognised and armed.*

In a new brochure, the FDFA and the DDPS explain what Swiss neutrality entails and how it is implemented.


Neutralität
kurz und knapp
1
Die Neutralität ist ein erfolgreiches Instrument der Schweizer Aussen- und Sicherheitspolitik. Sie geniesst grossen Rückhalt in der Schweizer Bevölkerung.
2
Die Neutralität setzt sich aus dem Neutralitätsrecht und der Neutralitätspolitik zusammen. In der Bundesverfassung ist die Wahrung der Neutralität als Aufgabe von Bundesrat und Parlament definiert (Art. 173 und 185 BV).
3
Das Neutralitätsrecht verpflichtet den neutralen Staat, an keinen internationalen bewaffneten Konflikten teilzunehmen und den kriegführenden Parteien weder Truppen noch sein Territorium zur Verfügung zu stellen. Im Gegenzug müssen die Kriegsparteien die Unverletzlichkeit des Territoriums des neutralen Staates respektieren.
4
Die Neutralitätspolitik umfasst Massnahmen, die ein neutraler Staat trifft, um die Glaubwürdigkeit und Wirksamkeit seines Status als Neutraler in der internationalen Gemeinschaft zu gewährleisten. Nebst den völkerrechtlich festgelegten Rechten und Pflichten orientiert sich die Neutralitätspolitik an den jeweiligen Landesinteressen, an der internationalen Lage sowie an Geschichte und Tradition des Landes.
5
Die Neutralität der Schweiz ist selbstgewählt, dauernd, international anerkannt und bewaffnet. Die Schweiz verfügt über eine eigene Armee, um ihre Unabhängigkeit und ihre territoriale Integrität zu verteidigen und neutralitätswidrige Handlungen kriegführender Staaten auf ihrem Gebiet zu verhindern.
6
Die Neutralität hindert die Schweiz nicht daran, Vorkehrungen zur Abwehr neuer Bedrohungen zu treffen, die sich häufig nur durch grenzüberschreitende Zusammenarbeit bekämpfen lassen. Dabei geht die Schweiz keine Verpflichtungen ein, mit denen sie riskiert, in einen Konflikt hineingezogen zu werden.
7
Gestützt auf ihre lange Tradition der Guten Dienste und der humanitären Hilfe gibt die Schweiz ihrer Neutralität eine friedensbezogene und humanitäre Ausrichtung.
8
Die Schweizer Neutralität beeinträchtigt nicht das Recht zur freien politischen Stellungnahme und zum aktiven Einsatz für die Achtung und Förderung der Schweizer Grundwerte wie Demokratie, Rechtsstaatlichkeit und Menschenrechte.

You may visit:
https://www.eda.admin.ch/dam/eda/de/documents/publications/SchweizerischeAussenpolitik/neutralitaet-schweiz_DE.pdf

---

The Swiss Financial Market Supervisory Authority (FINMA) implements a new countercyclical capital buffer.

The Federal Council decided to reactivate the countercyclical capital buffer at a level of 2.5% on loans secured against residential properties in Switzerland.

The press release:
https://www.admin.ch/gov/en/start/documentation/media-releases/media-releases-federal-council.msg-id-86922.html

The banks will be given until 30 September 2022 to meet the increased capital requirements. FINMA is responsible for overseeing the implementation of the countercyclical capital buffer.

It will therefore review in the course of its ongoing supervision how the Swiss banks integrate the higher capital requirements in particular into their capital planning.

In its statement to the Swiss National Bank (SNB), FINMA recommended that the countercyclical capital buffer be reactivated and that the maximum level of 2.5% be applied.

This was also the SNB's view. The real estate and mortgage markets are showing clear signs of overheating for residential properties. Various factors point towards such properties being overvalued.

For example, real estate prices have risen much more sharply in the last 20 years than consumer prices or GDP. This trend has accentuated even more since the outbreak of the coronavirus pandemic, thereby further increasing the vulnerabilities on the mortgage and real estate markets in the event of a correction.

In addition, analyses carried out by FINMA show that some of the banks and also some of the insurance companies would fall far below the threshold of the capital requirements in force in the event of a severe real estate crisis and would have to be recapitalised as a result.

Jan Blöchliger, Head of the Banks division, says: "The volume of mortgages is continuing to grow. And it is even accelerating – despite the coronavirus pandemic.

The institutions are taking increasingly higher risks in mortgage lending. FINMA sees risks in particular in the residential buy-to-let market. With a volume of over CHF 1,100 billion, the Swiss mortgage market is larger than the balance sheet of a systemically important large bank.

It is therefore de facto "too big to fail". The reactivation of the countercyclical capital buffer at the level of 2.5% will increase the banks' resilience. It is a step in the right direction for greater safety and stability of the financial system."

Countercyclical capital buffer suspended in the context of the coronavirus crisis

The countercyclical capital buffer was deactivated in March 2020 in light of the unfolding coronavirus crisis (see link). This took place as part of the package of measures rolled out by the Federal Council, the National Bank and FINMA.

The aim was to give banks more flexibility in granting credits to companies, thus preventing a possible credit crunch.

You may visit: https://www.finma.ch/en/news/2022/01/20220126-mm-azp/

Welcome to our monthly newsletter.

Best regards,

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

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

Number 1 (Page 16)

SHIELDS UP

Number 2 (Page 20)

Zoning and conduits for railways

Number 3 (Page 24)

The Role of AI in the Battle Against Disinformation

Alfonsas Juršėnas, Kasparas Karlauskas, Eimantas Ledinauskas, Gediminas Maskeliūnas, Julius Ruseckas, Donatas Rondomanskas

Number 4 (Page 27)

SHIELDS UP – Simple steps for individuals

Number 5 (Page 29)

NSA Details Network Infrastructure Best Practices

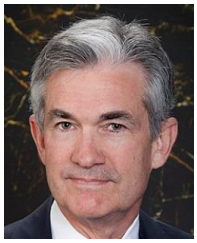
Number 6 (Page 32)

Zero trust becoming the default cyber security posture, but it needs to be done correctly

Number 7 (Page 34)

Semiannual Monetary Policy Report to the Congress

Chair Pro Tempore Jerome H. Powell, before the Committee on Financial Services, U.S. House of Representatives, Washington, D.C.



Number 8 (Page 38)

Europe sets out 6G vision at Mobile Web Congress Barcelona

Commissioner Breton has outlined Europe's plans for technology and infrastructure investment to foster resilience, and pave the way to 6G, addressing the Mobile World Congress.

European Commission

Number 9 (Page 40)

Data Centre Security: Guidance for owners and users

CPNI
Centre for the Protection of National Infrastructure

Number 10 (Page 45)

When 5G meets AI: Next Generation of Communication and Information Sharing

By: Katarina Kertysova

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Number 11 (Page 47)

UK organisations should act amidst heightened tensions

National Cyber Security Centre

Number 12 (Page 50)

Send Lawyers, Guns and Money: (Over-) Zealous Representation by Corporate Lawyers

Commissioner Allison Herren Lee, remarks at PLI's Corporate Governance – A Master Class 2022

Number 13 (Page 55)

S.3600 - Strengthening American Cybersecurity Act of 2022 117th Congress (2021-2022)

CONGRESS.GOV

Number 14 (Page 58)

Aspects of Cooperation between CSIRTs and LE - Handbook 2021

enisa European Network and Information Security Agency

Number 15 (Page 61)

Are Fault-Tolerant Quantum Computers on the Horizon?

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 16 (Page 63)

Incidents Handling and Cybercrime Investigations

enisa European Network and Information Security Agency

Number 17 (Page 66)

2022 Annual Threat Assessment of the U.S. Intelligence Community

Number 1

SHIELDS UP

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

SHIELDS UP

While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia's unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies. Every organization—large and small—must be prepared to respond to disruptive cyber activity.

As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyber-attacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.

Recognizing that many organizations find it challenging to identify resources for urgent security improvements, we've compiled a catalog of free services from government partners, and industry to assist. Recommended actions include:

Reduce the likelihood of a damaging cyber intrusion

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.

- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.

- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.

- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.

- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

Take steps to quickly detect a potential intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.

- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.

- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Ensure that the organization is prepared to respond if an intrusion occurs

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.

- Assure availability of key personnel; identify means to provide surge support for responding to an incident.

- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.

- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization’s network is unavailable or untrusted.

By implementing the steps above, all organizations can make near-term progress toward improving cybersecurity and resilience. In addition, while recent cyber incidents have not been attributed to specific actors, CISA urges cybersecurity/IT personnel at every organization to review Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.

CISA also recommends organizations visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.

For corporate leaders and CEOs

Corporate leaders have an important role to play in ensuring that their organization adopts a heightened security posture. CISA urges all senior leaders, including CEOs, to take the following steps:

- *Empower Chief Information Security Officers (CISO):* In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term.

- *Lower Reporting Thresholds:* Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.

- *Participate in a Test of Response Plans:* Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.

- *Focus on Continuity:* Recognizing finite resources, investments in security and resilience should be focused on those systems supporting

critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.

- *Plan for the Worst:* While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

To read more: https://www.cisa.gov/shields-up

Number 2

Zoning and conduits for railways

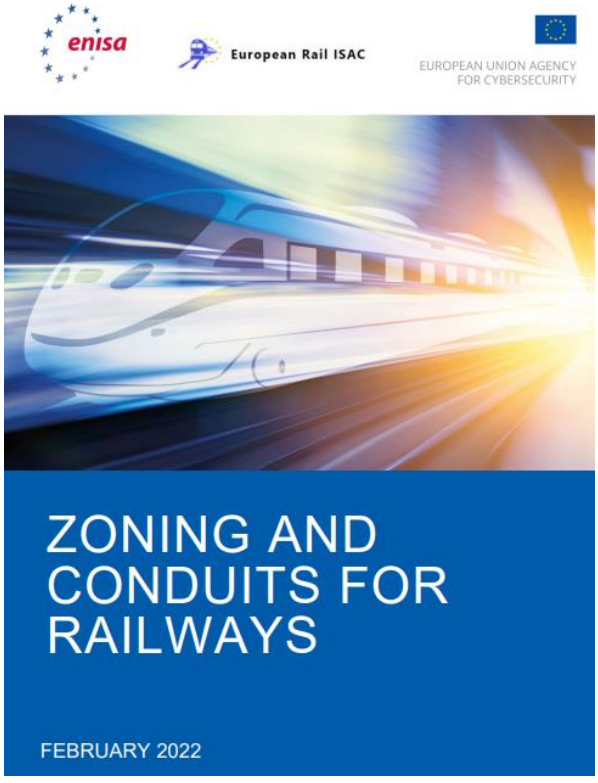
This document gives guidance on building zones and conduits for a railway system. To do so, first the methodology is described. This approach is based on the recently published CENELEC Technical Specification 50701 (CLC/CLC/TS 50701:2021).

The approach is complemented with additional practical information and hints on how to make the implementation of zoning easier for a railway operator.

It gathers the experience of the European Railway Information Sharing and Analysis Center and its members, i.e. European infrastructure managers and railway undertakings.

Each of the steps of the zoning process is explained in detail. The document shows what standards are required in each step and what processes should be performed.

Additionally, the document discusses the documentation that should be created during each step and guidance in the form of a 'cookbook' is given.



During the zoning process, zoning models are developed over three iterations:

1. “Proposal railway zoning model”: it is used in the first steps, ranging from first collecting information and designing initial zones (ZCR 1) up to the stage where zones, conduits, communication lines and security levels (SL) get verified briefly for the first time (ZCR 3). The proposal zone model is generic. It can be aligned with but need not fit the corporate structure.

2. “High-level railway zoning model”: it contains a concrete and defined risk verified architecture (ZCR 4) and is implemented via cybersecurity measures (ZCR 5). The company specific high-level zone model should be orientated to the corporate structure.

3. “Final railway zoning model”: it is a detailed and verified version of the high-level model, reflecting the corporate structure within all zones, conduits and communication lines, the SL ZC and other information (ZCR 6 to ZCR 7).

At the end of this document, the phases after zoning is complete are discussed, i.e. Migration (ZCR 8) and Operation (ZCR 9). Finally, the issue of legacy systems is commented on briefly.

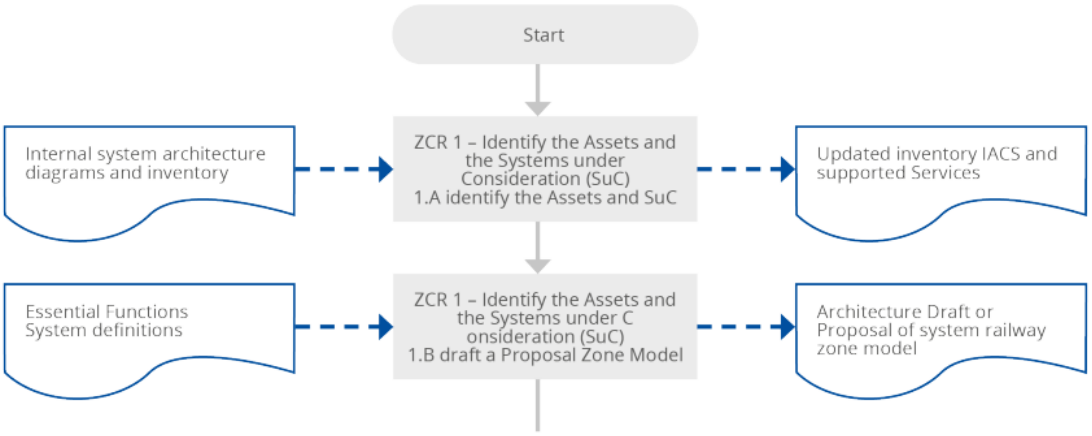
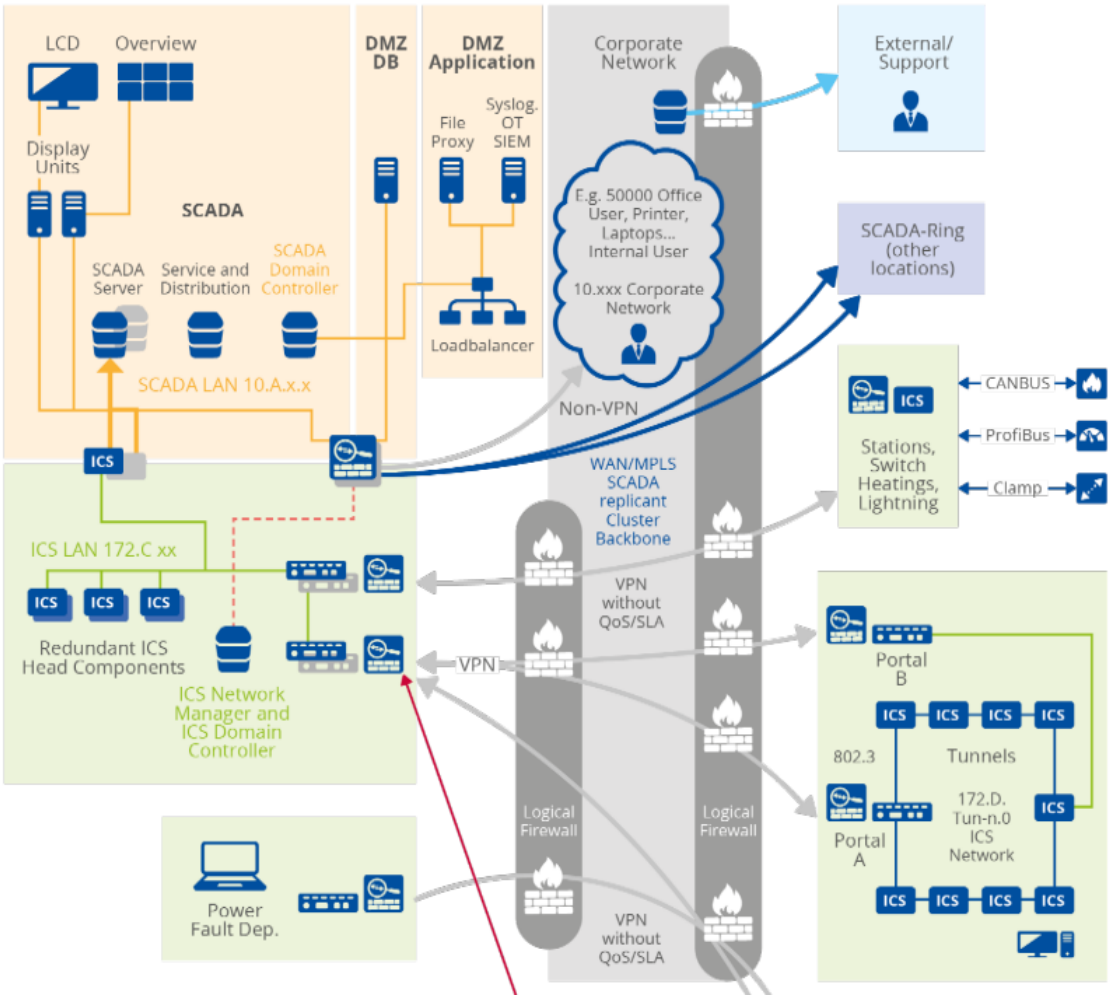


Figure 1 Zoning and conduit methodology



The paper: https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways

Number 3

The Role of AI in the Battle Against Disinformation

Alfonsas Juršėnas, Kasparas Karlauskas, Eimantas Ledinauskas,
Gediminas Maskeliūnas, Julius Ruseckas, Donatas Rondomanskas

Abstract

Detecting and countering disinformation grows increasingly important as social media sites have become a leading news source for most people.

Efficient disinformation campaigns lead to negative real-world consequences on a global scale, both in politics and in society.

Machine learning (ML) methods have demonstrated their potential for at least partial automatisation of disinformation detection and analysis.

In this report, we review current and emerging artificial intelligence (AI) methods that are used or can be used to counter the spread and generation of disinformation, and briefly reflect on ongoing developments in anti-disinformation legislation in the EU.

This overview will shed light on some of the tools that disinformation - countering practitioners could use to make their work easier.

Introduction

Due to the rapid pace of development and adaptation in the field of Artificial Intelligence (AI), the role it plays in disinformation practices is gradually increasing, boosting the work of malicious actors and analysts.

We begin by defining disinformation as false or manipulated information that is created and disseminated in order to deceive, i.e., to mislead public opinion about politics, to divide and polarise society, and to erode trust in public health institutions.

Disinformation practices evolve over time and adopt available technological advancements, including advancements in the field of AI.

Over the last ten years, the field of AI has enjoyed a series of significant and transformative breakthroughs, many of which have been applied to solving science and engineering problems.

In this paper, we use the following broad definition of AI proposed by the European Commission.

The term 'Artificial intelligence system' (AI system) refers to software developed using one or more of the techniques and approaches listed below:

- Machine learning (ML) approaches, including supervised, unsupervised, and reinforcement learning, using a wide variety of methods, including deep neural networks;

- Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning, and expert systems;

- Statistical approaches, Bayesian estimation, search and optimisation methods.

This definition includes both classic AI algorithms8 and the relatively new methods based on deep artificial neural networks that have led to the most current breakthroughs in the field.

AI can automate a wide range of specific tasks and significantly increase analysts' research capabilities. However, due to current limitations, AI can play only a supporting role by helping to process vast amounts of information and detecting what requires further attention.

AI-based tools provide practitioners with previously unavailable capabilities for analysing large amounts of data and exploiting complex patterns in large datasets.

Currently AI methods are most successful in performing rather narrow, well-defined tasks, e.g., classification, regression, etc.

Performing such tasks on large datasets of user activity has made it possible to create recommendation systems that select which information to display to maximise user engagement (e.g., views, shares, likes, comments) and time spent on social media platforms.

The AI algorithms used in recommendation systems have also made social network platforms more vulnerable to disinformation campaigns;11for example, the spread of highly emotional and divisive content is favoured to maximize user engagement.

AI is also used in generating increasingly realistic fake images, audio (voice imitation), video, and text, and can boost the ability of malevolent social bots to imitate human activity more realistically and to generate disinformation content at scale

To read more:
https://stratcomcoe.org/pdfjs/?file=/publications/download/The-Role-of-AI-DIGITAL.pdf?zoom=page-fit

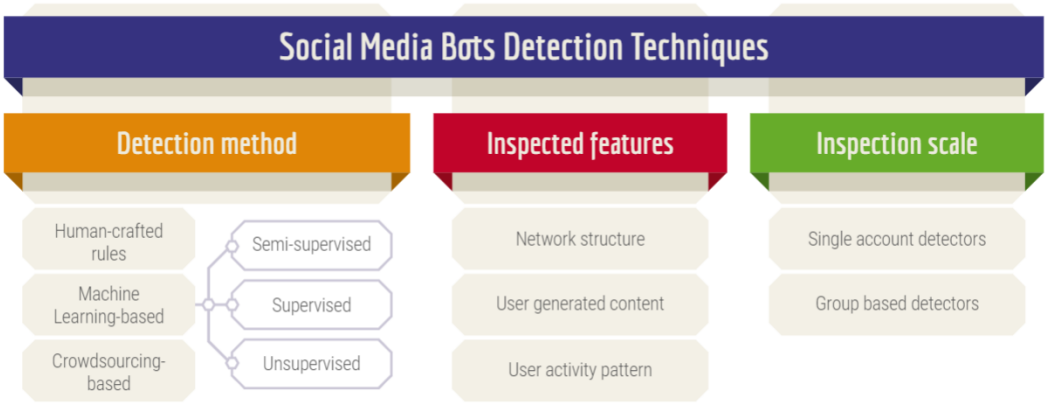


Figure 1. Social media bot detection techniques categorised by method, inspected features, and inspection scale. Partially adopted from Cresci[96] and Orabi et al.[97]

Number 4

SHIELDS UP – Simple steps for individuals

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Every individual can take simple steps to improve their cyber hygiene and protect themselves online.

CISA urges everyone to practice the following:

- Implement multi-factor authentication on your accounts. A password isn't enough to keep you safe online.

  By implementing a second layer of identification, like a confirmation text message or email, a code from an authentication app, a fingerprint or Face ID, or best yet, a FIDO key, you're giving your bank, email provider, or any other site you're logging into the confidence that it really is you.

  Multi-factor authentication can make you 99% less likely to get hacked. So enable multi-factor authentication on your email, social media, online shopping, financial services accounts. And don't forget your gaming and streaming entertainment services!

- Update your software. In fact, turn on automatic updates. Bad actors will exploit flaws in the system.

  Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too. Leverage automatic updates for all devices, applications, and operating systems.

- Think before you click. More than 90% of successful cyber-attacks start with a phishing email.

  A phishing scheme is when a link or webpage looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information.

  Once they have that information, they can use it on legitimate sites. And they may try to get you to run malicious software, also known as malware. If it's a link you don't recognize, trust your instincts, and think before you click.

- Use strong passwords, and ideally a password manager to generate and store unique passwords. Our world is increasingly digital and

increasingly interconnected. So, while we must protect ourselves, it's going to take all of us to really protect the systems we all rely on.

Important CISA Resources:

CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure – you may visit: https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf

Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure

CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats – you may visit: https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf

January 18, 2022

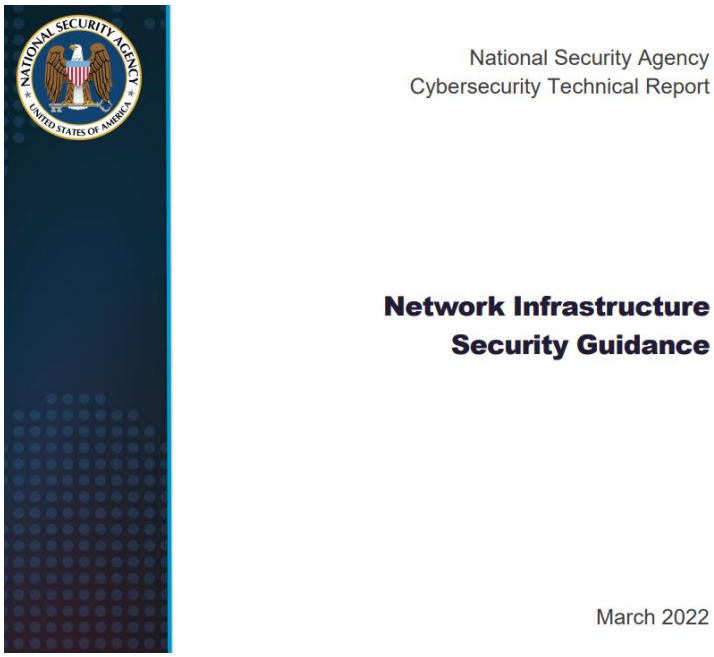
Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

To read more: https://www.cisa.gov/shields-up

Number 5

NSA Details Network Infrastructure Best Practices

The National Security Agency (NSA) released the "Network Infrastructure Security Guidance" Cybersecurity Technical Report. The report captures best practices based on the depth and breadth of experience in supporting customers and responding to threats.



Network environments are dynamic and evolve as new technologies, exploits, and defenses affect them. While compromise occurs and is a risk to all networks, network administrators can greatly reduce the risk of incidents as well as reduce the potential impact in the event of a compromise. This guidance focuses on the design and configurations that protect against common vulnerabilities and weaknesses on existing networks.

Recommendations include perimeter and internal network defenses to improve monitoring and access controls throughout the network.

Existing networks likely have some or most of the recommended configurations and devices noted, so administrators can use the report to help prioritize next steps in continuing to harden their network against cyber threats.

Regarding Zero Trust

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.

The National Security Agency (NSA) fully supports the Zero Trust security model, and much of the guidance in this report can be applied at different boundaries as recommended in Zero Trust guidance.

However, this report is focused on providing guidance to mitigate common vulnerabilities and weaknesses on existing networks.

As system owners introduce new network designs intended to achieve more mature Zero Trust principles, this guidance may need to be modified.

The guidance: https://media.defense.gov/2022/Mar/01/2002947139/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.PDF

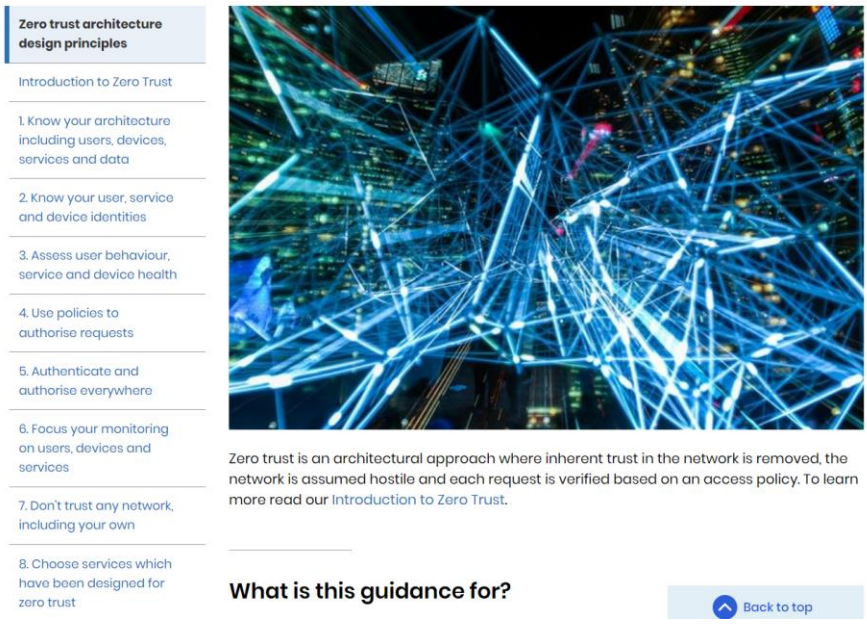
Number 6

Zero trust becoming the default cyber security posture, but it needs to be done correctly

National Cyber Security Centre

During the panel discussion at this year's Cloud and Cyber Security Expo in London, Tim Holman CEO of 2|SEC Consulting, asked the question "Given the sheer scale of attacks in businesses with zero trust, why are businesses getting zero trust wrong?".
You may visit: https://www.cloudsecurityexpo.com/

The answer, unsurprisingly, wasn't a simple one but ultimately came down to companies choosing zero trust out of necessity, often as a result of an attack. If not implemented correctly, it can often mean threats continue to occur.



The NCSC has published guidance for zero trust architecture for organisations and it's a good place to start if you're unsure whether it's the right option for you. The eight principles can help you to implement your own zero trust network architecture in an enterprise environment.

You may visit: https://www.ncsc.gov.uk/collection/zero-trust-architecture

The network is hostile

The network should be treated as compromised and therefore hostile, This means you need to remove trust from the network.

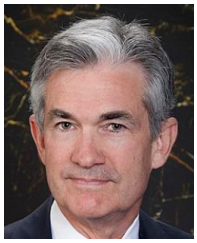
In a zero trust architecture, inherent trust is removed from the network. Just because you're connected to a network, doesn't mean you should be able to access everything on that network. Each request to access data or a service should be authenticated and authorised against an access policy. If a connection does not satisfy the access policy, the connection is dropped.

It is common in breaches to see an attacker gain a foothold on a network and then move laterally. This is possible because everything and everyone already on the network is trusted with access to the rest of the network. In a zero trust architecture, the network is treated as hostile, so every request for data or service access is continually verified against an access policy. This will also improve monitoring and detection of attempts at lateral movement by an attacker, compared to a traditional wall garden, but zero trust won't completely remove the threat.

Number 7

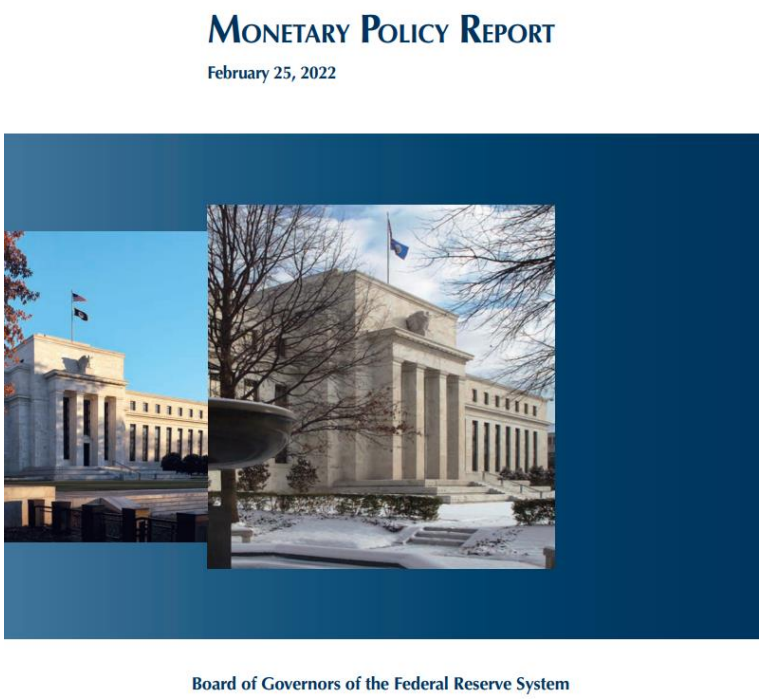
Semiannual Monetary Policy Report to the Congress

Chair Pro Tempore Jerome H. Powell, before the Committee on Financial Services, U.S. House of Representatives, Washington, D.C.



Chair Pro Tempore Powell submitted identical remarks to the Committee on Banking, Housing, and Urban Affairs, U.S. Senate on March 3, 2022.

Chairwoman Waters, Ranking Member McHenry, and other members of the Committee, I am pleased to present the Federal Reserve's semiannual Monetary Policy Report. (https://www.federalreserve.gov/monetarypolicy/files/20220225_mprfullreport.pdf)



Before I begin, let me briefly address Russia's attack on Ukraine. The conflict is causing tremendous hardship for the Ukrainian people. The implications for the U.S. economy are highly uncertain, and we will be monitoring the situation closely.

At the Federal Reserve, we are strongly committed to achieving the monetary policy goals that Congress has given us: maximum employment and price stability.

We pursue these goals based solely on data and objective analysis, and we are committed to doing so in a clear and transparent manner so that the American people and their representatives in Congress understand our policy actions and can hold us accountable. I will review the current economic situation before turning to monetary policy.

Current Economic Situation and Outlook

Economic activity expanded at a robust 5 1/2 percent pace last year, reflecting progress on vaccinations and the reopening of the economy, fiscal and monetary policy support, and the healthy financial positions of households and businesses.

The rapid spread of the Omicron variant led to some slowing in economic activity early this year, but with cases having declined sharply since mid-January, the slowdown seems to have been brief.

The labor market is extremely tight. Payroll employment rose by 6.7 million in 2021, and job gains were robust in January. The unemployment rate declined substantially over the past year and stood at 4.0 percent in January, reaching the median of Federal Open Market Committee (FOMC) participants' estimates of its longer-run normal level.

The improvements in labor market conditions have been widespread, including for workers at the lower end of the wage distribution as well as for African Americans and Hispanics.

Labor demand is very strong, and while labor force participation has ticked up, labor supply remains subdued. As a result, employers are having difficulties filling job openings, an unprecedented number of workers are quitting to take new jobs, and wages are rising at their fastest pace in many years.

Inflation increased sharply last year and is now running well above our longer-run objective of 2 percent. Demand is strong, and bottlenecks and supply constraints are limiting how quickly production can respond.

These supply disruptions have been larger and longer lasting than anticipated, exacerbated by waves of the virus, and price increases are now spreading to a broader range of goods and services.

Monetary Policy

We understand that high inflation imposes significant hardship, especially on those least able to meet the higher costs of essentials like food, housing, and transportation. We know that the best thing we can do to support a strong labor market is to promote a long expansion, and that is only possible in an environment of price stability.

The Committee will continue to monitor incoming economic data and will adjust the stance of monetary policy as appropriate to manage risks that could impede the attainment of its goals.

The Committee's assessments will take into account a wide range of information, including labor market conditions, inflation pressures and inflation expectations, and financial and international developments.

We continue to expect inflation to decline over the course of the year as supply constraints ease and demand moderates because of the waning effects of fiscal support and the removal of monetary policy accommodation. But we are attentive to the risks of potential further upward pressure on inflation expectations and inflation itself from a number of factors.

We will use our policy tools as appropriate to prevent higher inflation from becoming entrenched while promoting a sustainable expansion and a strong labor market.

Our monetary policy has been adapting to the evolving economic environment, and it will continue to do so. We have phased out our net asset purchases. With inflation well above 2 percent and a strong labor market, we expect it will be appropriate to raise the target range for the federal funds rate at our meeting later this month.

The process of removing policy accommodation in current circumstances will involve both increases in the target range of the federal funds rate and reduction in the size of the Federal Reserve's balance sheet. As the FOMC noted in January, the federal funds rate is our primary means of adjusting the stance of monetary policy.

Reducing our balance sheet will commence after the process of raising interest rates has begun, and will proceed in a predictable manner primarily through adjustments to reinvestments.

The near-term effects on the U.S. economy of the invasion of Ukraine, the ongoing war, the sanctions, and of events to come, remain highly uncertain. Making appropriate monetary policy in this environment requires a recognition that the economy evolves in unexpected ways. We

will need to be nimble in responding to incoming data and the evolving outlook.

Maintaining the trust and confidence of the public is essential to our work. Last month, the Federal Reserve finalized a comprehensive set of new ethics rules to substantially strengthen the investment restrictions for senior Federal Reserve officials. These new rules will guard against even the appearance of any conflict of interest. They are tough and best in class in government, here and around the world.

We understand that our actions affect communities, families, and businesses across the country. Everything we do is in service to our public mission. We at the Federal Reserve will do everything we can to achieve our maximum-employment and price-stability goals.

Thank you. I am happy to take your questions.

Number 8

Europe sets out 6G vision at Mobile Web Congress Barcelona

Commissioner Breton has outlined Europe's plans for technology and infrastructure investment to foster resilience, and pave the way to 6G, addressing the Mobile World Congress.

At this year's Mobile World Congress (MWC) Barcelona, Commissioner Breton addressed key representatives of the mobile industry in a video speech summarising Europe's ambitious plans for technology and infrastructure investment to foster resilience and strengthen EU's digital supply chain.

In his video address during the ministerial session on "Digital policies to speed the post-COVID recovery", Commissioner Breton stressed that combining public and private resources with investment-friendly regulatory frameworks is key to allow Europe to build the required level of infrastructure and technology capacities for the data economy.

Following that, at the launch event of the Smart Networks and Services Joint Undertaking (SNS JU) "On the Road to 6G", several of Europe's thought leaders in digital set out the strategy and the tools to enable the sector community to develop technology capacities for 6G systems as a basis for future digital services towards 2030.

6G visions

Speakers from industry highlighted 6G technologies as the next step-change in performance from Gigabit to Terabit capacities as well as to reach sub-millisecond response times.

This should enable new critical applications such as real-time automation or extended reality ("Internet of Senses") sensing, collecting and providing the data for a digital twin of the physical world.

Such new applications and technologies will offer strategic opportunities for European actors to develop new markets and pave the ground for leading technology companies, e.g. in the area of microchips for 6G or next-generation cloud technology.

In addition, 6G will be designed to enhance drastically the energy efficiency of connectivity infrastructures to cope with major traffic growth.

These technologies will form the basis for humancentric services and address Sustainable Development Goals (SDGs) such as greening the economy and supporting digital inclusion.

European and national R&I programmes

To make this happen, ambitious 6G R&I programmes have started both at European level and in several Member States.

In this context, the Smart Networks and Services Joint Undertaking (SNS JU) presented its two strategic pillars: 6G research and innovation and 5G deployment actions funded by European or national funding programmes.

The already committed public-private budget of around €2 billion establishes the necessary financial planning certainty to proceed with an ambitious 6G R&I roadmap.

Speakers from the SNS States Representatives Group emphasised the complementary with national programmes in EU Member States, which are also very ambitious, amounting to several €100 million, partly funded out of Next-Generation EU recovery plans dedicated to 6G R&I.

These programmes cover a wide scope of strategic objectives ranging from fundamental technologies, over testbeds and intellectual property rights and up to specialised digital skills and sustainability solutions.

To read more: https://digital-strategy.ec.europa.eu/en/node/10789/printable/pdf

Number 9

Data Centre Security: Guidance for owners and users

CPNI
Centre for the Protection of National Infrastructure

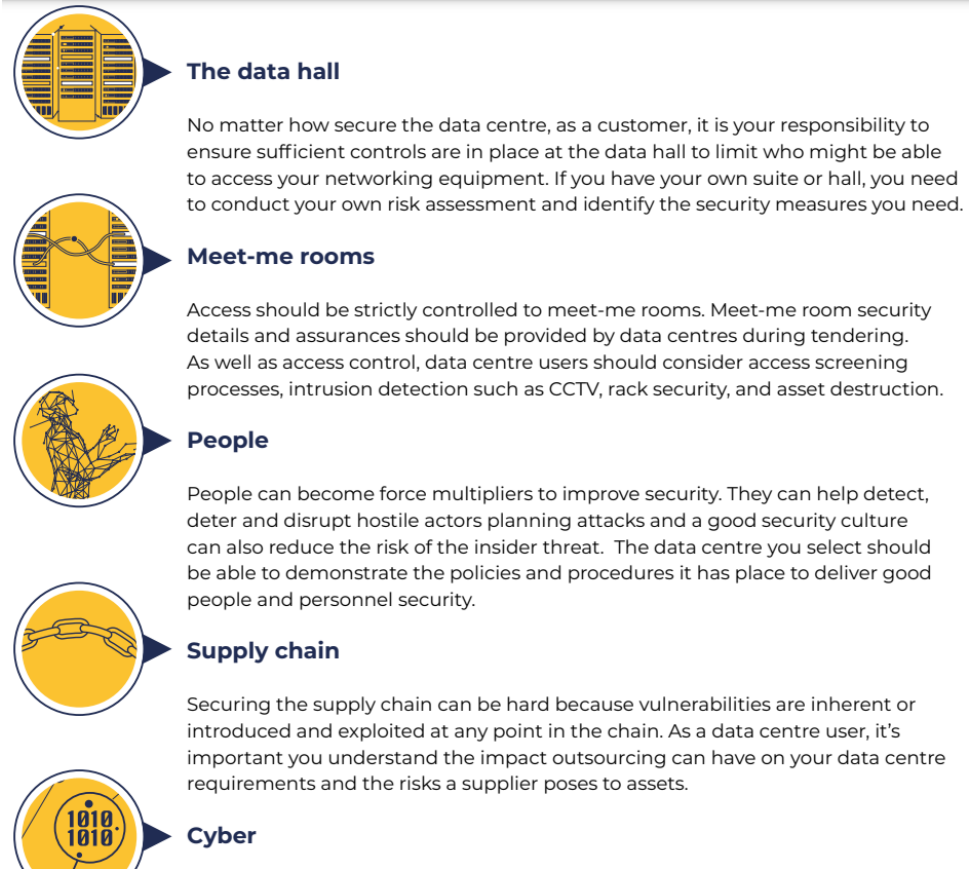
This guidance has been broken up into audiences. To get started on the CPNI and the NCSC data centre guidance, decide whether you are a data centre user or a data centre owner and click on the appropriate button below.

Owners:
https://www.cpni.gov.uk/system/files/documents/a4/8d/cpnidata-centre-owners-considerations.pdf

https://www.cpni.gov.uk/data-centre-security-owners

Users:
https://www.cpni.gov.uk/system/files/documents/4b/34/cpnidata-centre-users-considerations.pdf

https://www.cpni.gov.uk/data-centre-security-users



The data hall

No matter how secure the data centre, as a customer, it is your responsibility to ensure sufficient controls are in place at the data hall to limit who might be able to access your networking equipment. If you have your own suite or hall, you need to conduct your own risk assessment and identify the security measures you need.

Meet-me rooms

Access should be strictly controlled to meet-me rooms. Meet-me room security details and assurances should be provided by data centres during tendering. As well as access control, data centre users should consider access screening processes, intrusion detection such as CCTV, rack security, and asset destruction.

People

People can become force multipliers to improve security. They can help detect, deter and disrupt hostile actors planning attacks and a good security culture can also reduce the risk of the insider threat. The data centre you select should be able to demonstrate the policies and procedures it has place to deliver good people and personnel security.

Supply chain

Securing the supply chain can be hard because vulnerabilities are inherent or introduced and exploited at any point in the chain. As a data centre user, it's important you understand the impact outsourcing can have on your data centre requirements and the risks a supplier poses to assets.

Cyber

Data centres as targets

Data centres and the data they hold are attractive targets. One of the UK's most valuable assets is its data. Together with the data centres that hold and process it, they underpin almost all facets of modern life. This makes data centres an attractive target for threat actors, due to the large and diverse amount of information that supports our national infrastructure and businesses.

The opportunities for attack are diverse. Threat actors will target vulnerabilities in data centres' ownership, geography, physical perimeter, data halls, Meet Me Rooms (MMRs), supply chains, staff, and cyber security in a concerted effort to breach data centres' defences or tamper with sensitive information or disrupt critical services.

The risks of breaches and disruption

The security and resilience of your data and the infrastructure beneath it are therefore critical. High-profile data breaches and disruption to services are frequently reported with each incident, causing operators and data owners potentially huge financial losses in regulatory fines, loss of sensitive IP, downtime, post-incident recovery, security improvements, and perhaps most valuably of all, reputation.

Cyber intrusion methodology evolves constantly, and sophisticated attackers have a strong incentive to defeat the defences you put in place. It should be assumed that at some point your defences will be breached and therefore it is also important to be able respond proactively by detecting attacks and having measures in place to minimise the impact of any cyber security incidents.

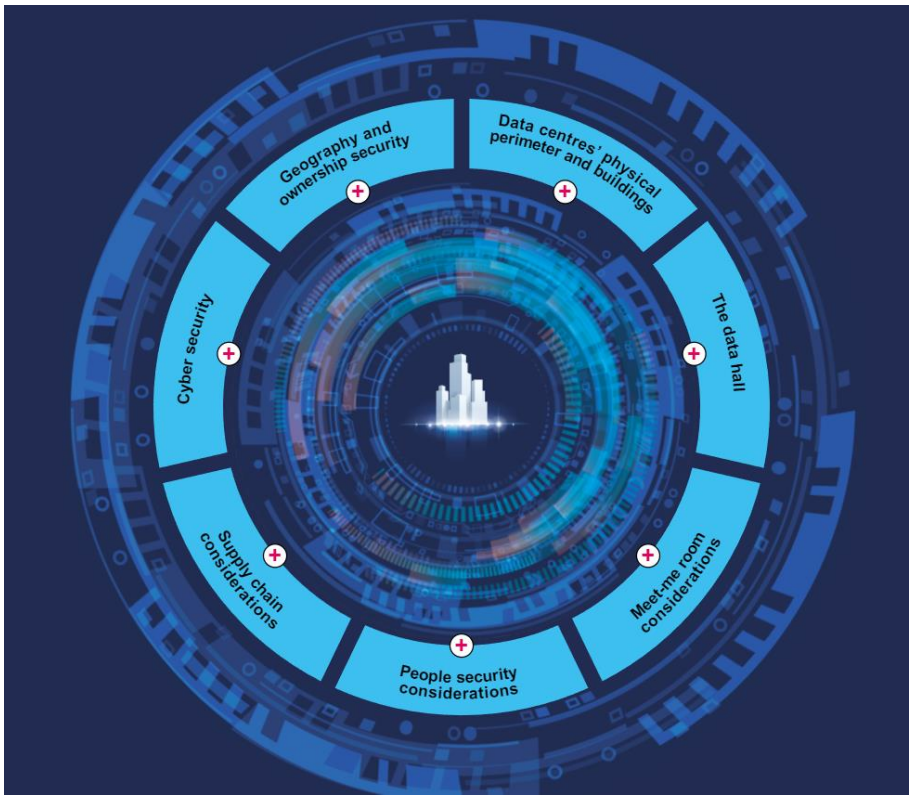
Holistic approach

To combat theses diversified threats, we need to approach data centre security holistically. By bringing together the physical, personnel and cyber security of data centres into a singular single strategy you can better withstand the diversified methods state threat actors, cyber criminals and others may use to attack them.

There is no one-size-fits-all approach to holistic data centre security. Every data centre operator and user will need to consider this guidance based on their own risk assessments. This guidance contains the security considerations you need to be aware of to make sure your data stays protected.

Guidance structure

This guidance is laid out by key areas of risk. Each of these areas should be considered when developing a risk management strategy that encourages a holistic security approach in data centres – moving from where the data centre is located, and who manages and operates it, to protecting against cyber threats. You should use this guidance to inform your own risk management strategy that is unique to your organisation's needs.



Key Types of Data Centre

There are several options for the type of data centre you may choose as a data owner.

They offer different levels of service which can impact the control you have over security arrangements.

It is important to remember that as a data owner, whichever option you choose to go with, the responsibility for managing the risks to your own information remains with you.

You should therefore understand the benefits and disadvantages of each option and use this to inform your risk management strategy.

Enterprise or 'wholly-owned' data centres

These are data centres that an organisation solely owns and operate for their own use. This gives you complete oversight of your security and operational arrangements, which often incurs higher costs.

Co-located data centres

These are centres where your organisation's data system is housed within a shared facility, along with other organisations' data.

This is often more cost effective due to the lack of upfront costs of building and running a data centre.

Whilst allowing flexibility and the ability to scale at speed, you don't have sole access to the data centre and may have fewer, or sometimes no customisable options for its security.

Managed-hosting data centres

The hybrid model – a customised data-hosting package provided by a third-party in a data centre.

The servers you use can be dedicated or shared with other customers.

This option removes the need to hire staff and places responsibility for security on the third party.

Whilst attractive from a convenience point of view, this is balanced with the fact that you have less oversight or control of your security arrangements.

Cloud-hosting data centres

Your data is stored in a network of servers across different data centres, in different locations, which increases your flexibility to scale at speed and may also improve your resilience in the case of an outage due to the distributed nature of your data.

However, you will need to be clear on how your data is stored and managed; for example, where and how your data will be moved, stored, or split while in the cloud.

Cloud service administration systems are often also highly privileged; if they are compromised, they could have a significant impact on your data.

The NCSC provides comprehensive guidance on the use of cloud services and their security.

The below table summarises the degree of control you may have over areas of risk for data centres, depending on the option you choose:

Control of aspects of a data centre	Enterprise	Co-located	Managed hosting	Cloud
Ownership	High	Medium	Medium	No
Location	High	High	Medium	Low
Data hall occupancy	High	No	No	No
Data hall operations	High	Medium	No	No
Building services operation	High	No	No	No
Facilities management	High	No	No	No
Security requirements	High	Medium	Low	Medium
Access to data centre	High	Medium	No	No
Access to your equipment	High	Medium	No	No
Staffing	High	Low	No	No
Supply chain	High	Medium	No	No
Security procedures (physical/personnel)	High	Low	No	No
Cyber security	High	Medium	No	No

To read more: https://www.cpni.gov.uk/data-centre-security

Number 10

When 5G meets AI: Next Generation of Communication and Information Sharing

By: Katarina Kertysova

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

The adoption of fifth generation (5G) wireless technology will touch nearly every aspect of our lives.

While changes brought by 5G will primarily affect sectors that depend on smooth wireless connection – such as transportation, healthcare, or manufacturing – they will also alter the realm of (strategic) communications.

In the coming de-cade, 5G and edge computing will generate new opportunities for how humans interact with each other and experience the world.

Greater connectivity and access to information enabled by 5G also promise to bridge the digital divide, improving democratic participation and citizen mobilization.

At the same time, there will be more opportunities for misuse of this technology.

Events of the last ten years have demonstrated the impact that digital transformation is having on democracy and political life.

Consider the role that social media has played in key political events such as the Arab Spring or how the advent of e-voting and e-political participation changed the outcome of some elections throughout the pandemic.

The emergence and accelerated adoption of new technologies has seen a con-current rise in digital repression and disinformation operations.

While (online) disinformation is not a new phenomenon, rapid advances in information technologies have altered the ways in which information (and disinformation) can be produced and disseminated.

Data capture, speed, and connectivity offered by 5G will equip both state and non-state actors with more effective tools to tighten information control, repress political opponents, and manipulate public opinion online.

In recent years, both 5G and AI have received considerable attention. However, there has been little focus on the complexities presented by AI and 5G operating together in the context of communications and information operations.

This study will cover this gap. Many studies of 5G highlight the technical risks posed by Chinese companies manufacturing 5G equipment.

In contrast, this paper seeks to answer the follow-ing questions:

How are NATO Allies impacted by the 5G/AI revolution?

How will 5G transform the information environment, including the nature of disinformation campaigns?

To do so, this paper first examines the ways in which 5G-enabled applications alter the realm of communications: not only how we communicate, but also how we consume and share information.

It then briefly identifies implications 5G can have for democracy and political life in general.

Next, it outlines broader systemic threats and negative impacts of 5G rollout on political participation.

The paper concludes with a set of recommendations.

To read more:
https://stratcomcoe.org/pdfjs/?file=/publications/download/When-5G-meets-AI-DIGITAL-8d442.pdf?zoom=page-fit

Number II

UK organisations should act amidst heightened tensions

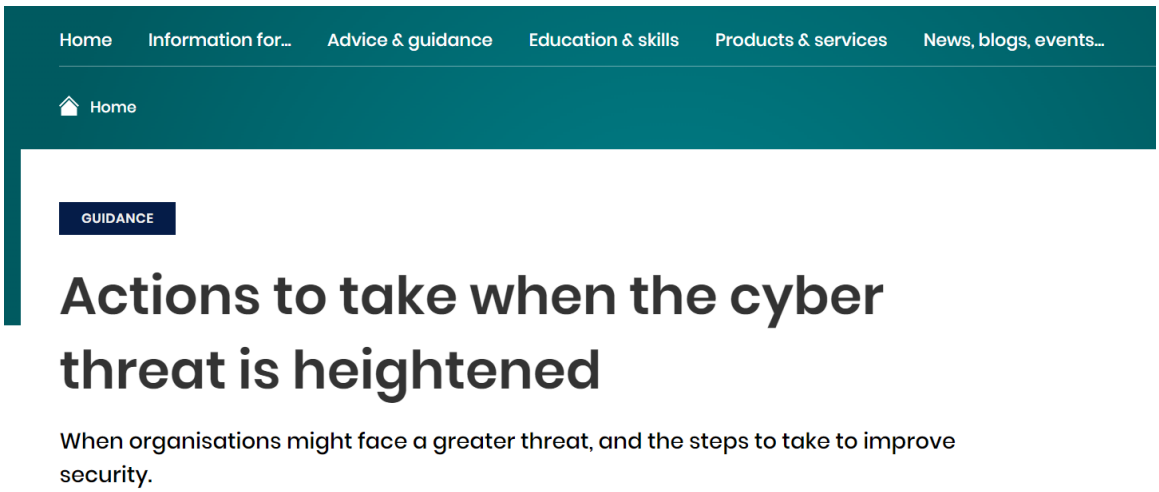
National Cyber Security Centre

Following Russia's further violation of Ukraine's territorial integrity, the NCSC has called on organisations to bolster their online defences.

While the NCSC is unaware of any current threats to UK organisations, it is important that steps are taken to improve cyber resilience in the event of an attack.

Historically, cyber attacks on Ukraine have had wider international consequences and the NCSC's guidance sets out some actions which will help reduce the risk of falling victim to an attack.

The actions to take when the cyber threat is heightened is available to read now on the NCSC website: https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened



Balancing cyber risk and defence

The threat an organisation faces may vary over time. At any point, there is a need to strike a balance between the current threat, the measures needed to defend against it, the implications and cost of those defences and the overall risk this presents to the organisation.

There may be times when the cyber threat to an organisation is greater than usual. Moving to heightened alert can:

- help prioritise necessary cyber security work

- offer a temporary boost to defences

- give organisations the best chance of preventing a cyber attack when it may be more likely, and recovering quickly if it happens

This guidance explains in what circumstances the cyber threat might change, and outlines the steps an organisation can take in response to a heightened cyber threat.

Factors affecting an organisation's cyber risk

An organisation's view of its cyber risk might change if new information emerges that the threat has heightened. This might be because of a temporary uplift in adversary capability, if for example there is a zero-day vulnerability in a widely used service that capable threat actors are actively exploiting. Or it could be more specific to a particular organisation, sector or even country, resulting from hacktivism or geopolitical tensions.

These diverse factors mean that organisations of all sizes must take steps to ensure they can respond to these events. It is rare for an organisation to be able to influence the threat level, so actions usually focus on reducing your vulnerability to attack in the first place and reducing the impact of a successful attack.

Even the most sophisticated and determined attacker will use known vulnerabilities, misconfigurations or credential attacks (such as password spraying, attempting use of breached passwords or authentication token reuse) if they can. Removing their ability to use these techniques can reduce the cyber risk to your organisation.

Actions to take

The most important thing for organisations of all sizes is to make sure that the fundamentals of cyber security are in place to protect their devices, networks and systems.

The actions below are about ensuring that basic cyber hygiene controls are in place and functioning correctly. This is important under all circumstances but critical during periods of heightened cyber threat.

An organisation is unlikely to be able to make widespread system changes quickly in response to a change in threat, but organisations should make every effort to implement these actions as a priority.
To read more: https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

- Check your system patching +
- Verify access controls +
- Ensure defences are working +
- Logging and monitoring +
- Review your backups +
- Incident plan +
- Check your internet footprint +
- Phishing response +
- Third party access +
- NCSC services +
- Brief your wider organisation +

Number 12

Send Lawyers, Guns and Money: (Over-) Zealous Representation by Corporate Lawyers

Commissioner Allison Herren Lee, remarks at PLI's Corporate Governance – A Master Class 2022

Thank you Brian [Breheny] for the introduction and to the Practicing Law Institute for having me today. Before I begin, I want to take a moment to acknowledge the on-going humanitarian disaster in Ukraine.

My thoughts are with the people of Ukraine, who have demonstrated impossible bravery, and with those of you who may have friends or relatives affected by this crisis.

It's a privilege to address my fellow members of the bar. This privilege is very meaningful to me personally in part because of my unexpected path into the legal profession and my deep regard for the ideals of public service that our profession represents.

I do not come from a family of lawyers; in fact my parents did not even attend college. I never laid eyes on an actual lawyer during my childhood.

What I knew about them came from TV shows, which means I assumed their jobs were to cleverly question witnesses at trial until they confessed to the crime for which another had been charged.

Despite (or maybe because of) this misperception, I secretly dreamed of becoming a lawyer and was awed to the point of reverence by the profession.

As I worked my way through college and eventually, in my late thirties, through law school, I began to better understand what lawyers do and what it means to be a member of a "profession"—how the calling stood apart from other businesses principally because advocating for fidelity to the law is, at its core, a form of public service.

Taking this to heart, I launched an initiative in law school that led to the adoption of a requirement for students to complete pro bono work as part of the curriculum.

I have lived the experience of law from the perspectives of an outsider with no idea of what lawyers do, a student, a client, a securities law practitioner, an enforcement lawyer (both civil and criminal), and now as a Commissioner helping to shape regulatory policy.

My belief in the ideals of the profession—ideals that I know you all share—has only grown stronger with time.

I take great pride in being a member of the bar and this is the lens that I bring to the topic I want to address today.

I want to talk about supporting securities lawyers, both in-house and outside counsel, in upholding the best traditions of the profession.

Specifically, by fulfilling a mandate in the Sarbanes-Oxley Act designed to do just that.

As we near the twentieth anniversary of its passage, we still have not fulfilled Congress's mandate under Section 307 of Sarbanes-Oxley to adopt minimum standards of professional conduct for attorneys appearing and practicing before the Commission in the representation of issuers.

A key element of Sarbanes-Oxley, passed in the wake of the massive financial failures of the Enron era, was to create structures of accountability for professionals—executives, accountants and auditors, and, under Section 307 of the Act, accountability for lawyers.

In considering Section 307, Congress recognized that executives and accountants did not "work alone," and that lawyers were "virtually always there looking over their shoulders."

Congress was concerned, however, that counsel often acted in the interests of the executives who hired them rather than the company and its shareholders to whom their duty and responsibility is owed.

Unfortunately, in response to this mandate, the SEC adopted only one standard: the so-called "up-the-ladder" rule, requiring lawyers to report certain potential violations up the chain of management inside a corporate client.

We did not adopt a broader set of rules as Congress directed, and quite significantly, even this single standard has not been enforced in the nearly 20 years since it was adopted.

The policies behind this unfulfilled mandate—which are designed to support lawyers in their gatekeeping role—are as relevant and compelling today as they were 20 years ago, if not more so.

Indeed the role of corporate lawyers as gatekeepers in the capital markets—distinct from the litigator's role—has long been acknowledged by a broad and bipartisan group from William O. Douglas, to A.A. Sommer and Stanley Sporkin.

It also includes Independent, Republican, and Democratic Chairs of the SEC.

And it wasn't just during the Enron era that we saw lapses in the gatekeeping role. We saw such lapses with stock option backdating and mutual fund market timing cases, and to some extent in the 2008 financial crisis.

More recently, we have seen an entirely new, multi-trillion dollar industry develop around cryptocurrency and digital assets that largely defies existing laws and regulations.

The role of lawyers in enabling this approach remains to be fully fleshed out, but the failure to comply with well-known principles of the securities laws has already been costly for many firms.

The bottom line is this: when corporate lawyers give bad advice, the consequences befall not just their clients, but the investing public and capital markets more broadly—especially when it comes to disclosure advice.

But we do not currently have sufficient standards in place upon which to assess this kind of advice.

Standards for professional conduct could help both lawyers and regulators navigate this difficult terrain where bad legal advice can, in the words of a prior Commission, "inflict substantial damage on the Commission's processes, and thus the investing public, and the level of trust and confidence in our capital markets."

It's time to revisit this unfulfilled mandate and consider whether the SEC should adopt (and enforce) a minimum set of standards for lawyers who practice before the Commission to better protect investors and markets.

"Can-do" Corporate Lawyering

The “bad advice” I refer to arises from a type of “can-do” approach to lawyering that is ill-suited to lawyers in a gatekeeping role. It is born from a desire to give management the answer that it wants.

Or, as a Delaware court recently stated, it stems from a “contrived effort to generate the client’s desired result when real-world facts would not support it.”

If you haven’t read this particular Delaware decision (Bandera Master Fund v. Boardwalk Pipeline) from late last year, I commend it to you as a study in the perils of modern corporate law practice.

It involves sophisticated counsel who, as the court put it, engaged in “goal-directed reasoning” to provide an opinion designed to allow the client to exercise a lucrative call right.

However, the court concluded the opinion was based on artifice and sleight of hand. It thus ruled that the opinion was given in bad faith and awarded damages against the client of roughly $700 million.

Unfortunately, this case does not appear to represent an isolated instance of poor judgment by a single lawyer or firm.

Indeed, this same court wrote an expansive opinion in 2020 in which it found another preeminent firm had “committed fraud” by holding back important information during a competitive bidding process.

In yet another recent case, the court laid out chapter and verse how a large law firm took part in a covert plan to “undermine a merger” while concealing their work so as not to “advertis[e] that [the client] was breaching its obligations” to use best efforts to close the deal.

Though these particular cases were not about disclosure under the securities laws, they are nevertheless emblematic of a dynamic—a kind of race to the bottom—that can occur when specialized professionals like securities lawyers compete for clients in high stakes matters and are pressured to provide the answers their clients seek.

As one observer put it: “Can-do lawyering has run amok. Still you don’t want to be the lawyer that just says ‘no.’ You’ll never make it.”

Of course, this type of conduct is far from the norm for securities law practitioners, but it is not as rare as we would like to think. In my 25 years as a securities lawyer, I have observed this kind of conduct on multiple occasions.

It is not easy to strike the right balance between zealous representation in corporate law matters and thoughtful consideration of the potential impact to shareholders, investor protection, and the public interest.

Most lawyers generally err on the side of caution. But examples like those I've noted erode public trust in the highly-skilled, principled attorneys in the financial regulatory space and in our markets more broadly.

To read more: https://www.sec.gov/news/speech/lee-remarks-pli-corporate-governance-030422

Number 13

S.3600 - Strengthening American Cybersecurity Act of 2022
117th Congress (2021-2022)

CONGRESS.GOV

117TH CONGRESS
2D SESSION

S. 3600

AN ACT

To improve the cybersecurity of the Federal Government, and for other purposes.

TITLE II—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

TITLE III—FEDERAL SECURE CLOUD IMPROVEMENT AND JOBS ACT OF 2022

The bill also updates current federal cybersecurity laws to improve coordination between federal agencies, as well as requires all federal civilian agencies to report all substantial cyberattacks to CISA.

In addition, the bill would provide new authorities to CISA and authorize the Federal Risk and Authorization Management Program (FedRAMP) for five years to ensure federal agencies can quickly and securely adopt cloud-based technologies that improve government efficiency and save taxpayer dollars.

An interesting section:

SEC. 114. IMPLEMENTING ZERO TRUST ARCHITECTURE.

(a) Guidance.—Not later than 18 months after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—

(1) shifting away from “trusted networks” to implement security controls based on a presumption of compromise;

(2) implementing principles of least privilege in administering information security programs;

(3) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(4) identifying incidents quickly;

(5) isolating and removing unauthorized entities from agency systems as quickly as practicable, accounting for intelligence or law enforcement purposes;

(6) otherwise increasing the resource costs for entities that cause incidents to be successful; and

(7) a summary of the agency progress reports required under subsection (b).

(b) Agency Progress Reports.—Not later than 270 days after the date of enactment of this Act, the head of each agency shall submit to the Director a progress report on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—

(1) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director, including the adoption of any models or reference architecture;

(2) an identification of activities that have not yet been completed and that would have the most immediate security impact; and

(3) a schedule to implement any planned activities.

The Act:
https://www.hsgac.senate.gov/imo/media/doc/BillText_PetersStrengtheningAmericanCybersecurityAct.pdf

Number 14

Aspects of Cooperation between CSIRTs and LE - Handbook 2021

There are powers, information, equipment, expertise or contacts that are available exclusively to one of the communities – CSIRTs, LE or Judiciary – but, at the same time, these resources could be tremendously useful to others.

In addition, it often happens that these communities deal with the same cases; what should be avoided in these cases is that one community interferes with goals and activities of the other communities.

It is therefore vital for these communities to cooperate as much as possible and make use of available synergies while managing potential interferences.

However, technical, legal, organisational and cultural challenges can hinder this cooperation.

Also, those challenges are managed differently in each country.

Past reports developed by ENISA provide valuable insight into the current state of cooperation and recommendations on how to improve it.

Taking into consideration that cybersecurity incidents do not always amount to cybercrimes (cybersecurity incidents are not necessarily of criminal nature), cooperation between CSIRTs and LE/Judiciary does not take place in all cases.

But cooperation should take place in cases of cyber incidents that are criminal in nature.

In these cases, the role of each community varies, more specifically:

- CSIRT's role is to mitigate the incidents
- LE's role is to conduct the investigations
- the Judiciary's role is to prosecute (prosecutors) and judge (judges)

Also, within the CSIRTs community, there are differences depending on the type of CSIRT (governmental, national, sectoral, etc.).

The same applies to LE and the Judiciary communities (for instance, local, regional, national, federal, or international Law Enforcement Agencies).

When dealing with a cybersecurity incident of criminal nature, each community should consider the outreach to other actors that could be involved, keeping in mind the multiple ways of cooperating and the importance of receiving reciprocal feedback on a case.

Additional stakeholders may be approached in this cooperation process, such as the service operators and service providers, intelligence services, military, and international agencies.

Both formal (e.g. official written requests) and informal procedures (e.g. information shared orally during a phone call) may be followed throughout this cooperation process.

The cooperation channel may be supported through appointed liaison officers.

Figure 5: Graphical representation of scenario 1 – Attack

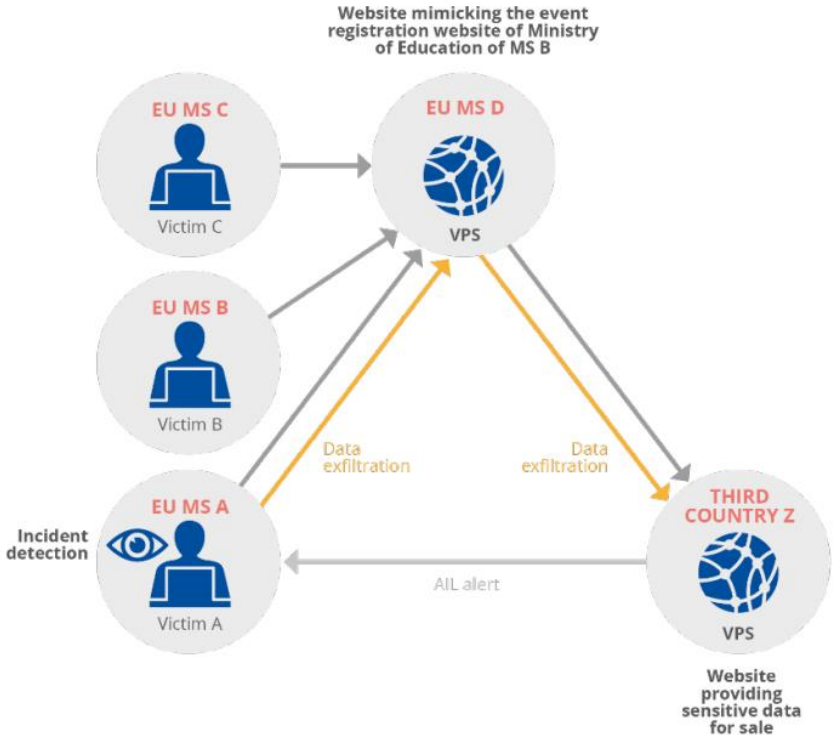


Figure 6: Graphical representation of scenario 1 – Overview of interactions

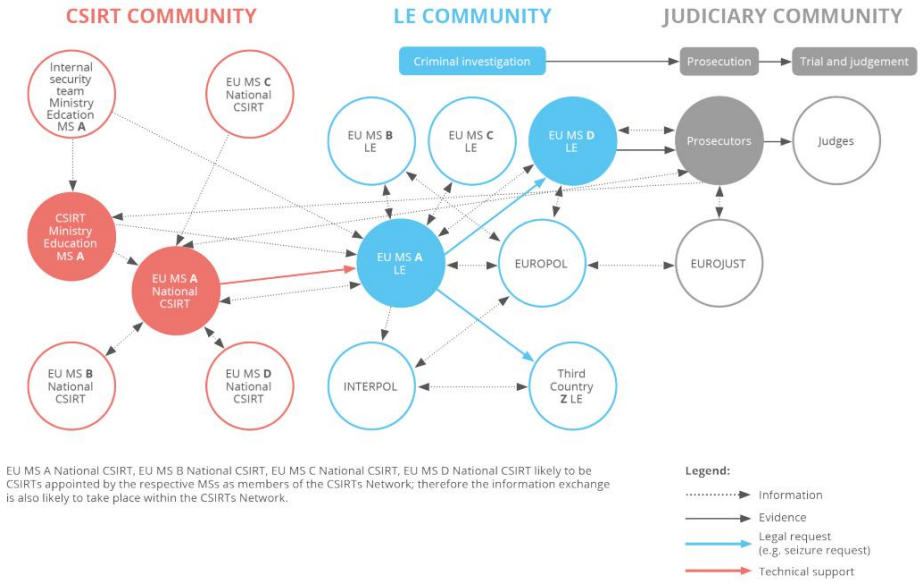
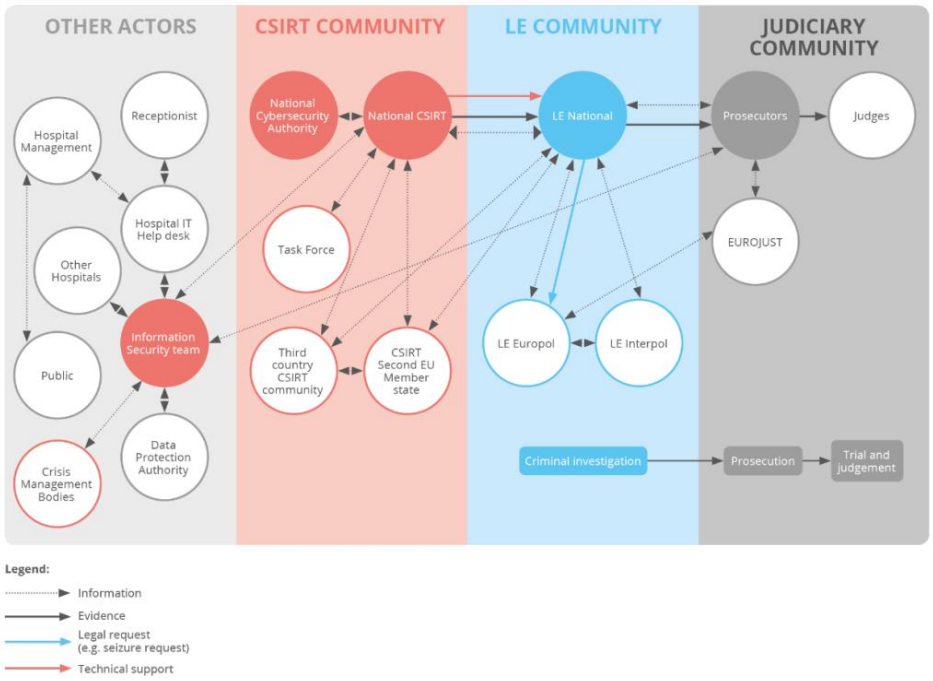


Figure 14: Graphical representation of scenario 2 – Overview of interactions



To read more: https://www.enisa.europa.eu/publications/aspects-of-cooperation-between-csirts-and-le-handbook-2021

Number 15

Are Fault-Tolerant Quantum Computers on the Horizon?

DARPA wants to verify, validate bold claims that a useful quantum computer could be realized soon

It's been hypothesized that quantum computing will one day revolutionize information processing across a range of military and civilian applications – from artificial intelligence, to supply chain optimization, to pharmaceuticals discovery, to cryptography.

Prevailing predictions are that it will be decades before fully fault-tolerant quantum computers capable of solving important problems are available.

As various quantum computing research and development efforts advance globally, however, DARPA wants to rigorously assess any quantum research claims that a useful fault-tolerant quantum computer could be built much sooner.

DARPA announced the Underexplored Systems for Utility-Scale Quantum Computing (US2QC) program. US2QC aims to determine if an underexplored approach to quantum computing is capable of achieving utility-scale operation much faster than conventional predictions.

"DARPA's mission is to create and prevent strategic surprise," said Joe Altepeter, US2QC program manager in DARPA's Defense Sciences Office.

"If there's an underexplored area of quantum computing showing promise for a faster breakthrough than we previously expected, we want to explore it immediately and thoroughly verify and validate the approach's viability."

An existing DARPA program, Quantum Benchmarking, is developing quantitative benchmarks on the software side to thoroughly assess potential applications where quantum computers could provide a meaningful improvement over classical computers for important problems. You may visit: https://www.darpa.mil/program/quantum-benchmarking

US2QC is a complementary hardware effort focused on verifying and validating system, component, and sub-system designs for a proposed fault-tolerant quantum computer.

"If a company or an organization thinks they can make a truly useful, really big, fault-tolerant quantum computer, we want to have a conversation with them," Altepeter said. "We would like them to show us exactly why they're

convinced their machine is going to be revolutionary in the near future, and we want to work collaboratively with them, pay for additional experts to embed with their team, and help advance bold concepts that withstand rigorous testing."

Because innovative approaches to building a quantum computer are extremely varied, US2QC is structured for maximum flexibility and will exclusively use tailorable Other Transaction agreements to fund proposals.

The only common foundation for all proposals is Phase 0, in which proposers will quantitatively describe a complete utility-scale concept, including all components and sub-systems, projected performance capabilities against a variety of metrics, and anticipated technical risks and mitigation strategies.

"There's no one verification and validation program that fits all the different quantum computing approaches out there," Altepeter said. "That means we don't know what follow-on phases will look like or how long they'll be.

Identifying key milestones will be unique for each project depending on how the Phase 0 validation and verification goes. If the proposed concept proves to be sound, Phase 0 could be very short. As teams meet follow-on phase milestones unique to their approach, we'll keep scaling the effort up."

A program solicitation with all details for proposing to US2QC is available here: https://sam.gov/opp/6c8cffdd547b4816bb8b09e4e4448892/view

Number 16

Incidents Handling and Cybercrime Investigations

The European Union Agency for Cybersecurity (ENISA) explores how CSIRTs, law enforcement agencies and the judiciary cooperate and how they can train together to better tackle cyber incidents and respond to cybercrime.

The report facilitates the cooperation between CSIRTs and law enforcement agencies (LEAs) and looks into their interaction with the judiciary (judges and prosecutors). This updated and extended version of the report comes along with an updated version of the training material delivered by ENISA in 2020 in the form of a handbook and a toolset.

ENISA is presenting these newly published report and training material at the Regional Cybercrime Cooperation Exercise and Conference of Law Enforcement/CSIRT Cooperation organised by the Council of Europe and the European Commission taking place from 7-11 March in Athens, Greece. You may visit: https://www.coe.int/en/web/portal/-/council-of-europe-and-european-commission-organise-regional-cyber-training-for-east-and-south-east-european-countries

Why is this cooperation needed?

While CSIRTs mitigate incidents, law enforcement agencies conduct investigations. Although each community has a specific role, they often deal with the same cases. In doing so, the activities of one of them can sometimes overlap and/or could also possibly interfere with the goals and the activities of the others.

In addition, other factors are at play which may have an impact on the cooperation and these include technical, legal, organisational challenges and at times even behavioural differences between the communities.

What is the purpose of the report?

This report addresses the legal and organisational framework, roles and duties of CSIRTs, LEAs and the judiciary. It also analyses their required competences, as well as synergies and potential interferences in their respective activities.

By facilitating the cooperation between the CSIRT and the LE communities and their interaction with the judiciary, this work has the final aim to contribute to a better response to cybercrime.

Key conclusions and next steps

Conclusions from the analysis of sixteen different EU/EEA Member States include:

- the structure and organisation of the different communities vary by country;
- CSIRT-LEA cooperation help decrease the risk of evidence being compromised and of interferences in each other's activities;
- CSIRTs play an important role in informing (potential) victims of cybercrime and in providing them with information on how to report a crime to the Police.

Next steps suggested include:

- the extension of the analysis to additional countries;
- the development of a catalogue of competences in incident handling and cybercrime investigations;
- the organisation of joint training and exercises.

Training material

The training material consists of a handbook designed for the trainer and a toolset for the trainee. The handbook explains the concepts addressed

using scenarios. the toolset includes exercises based on these scenarios. This training material is an updated version of the training material on CSIRT-LE cooperation published last year.

Recommended publication:
https://www.enisa.europa.eu/publications/2021-report-on-csirt-law-enforcement-cooperation

Number 17

2022 Annual Threat Assessment of the U.S. Intelligence Community

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 Intelligence Authorization Act (P.L. 116-260).

This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States during the next year.

The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC. All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future, such as climate change and environmental degradation.

In the coming year, the United States and its allies will face an increasingly complex and interconnected global security environment marked by the growing specter of great power competition and conflict, while collective, transnational threats to all nations and actors compete for our attention and finite resources.

These challenges will play out amidst the continued global disruption resulting from the COVID-19 pandemic, contention over global efforts to deal with a changing climate, increasingly powerful non-state actors, and rapidly evolving technology, all within the context of an evolving world order where the continued diffusion of power is leading actors to reassess their place and capabilities in an increasingly multipolar world.

These challenges will intersect and interact in unpredictable ways, leading to mutually reinforcing effects that could challenge our ability to respond, but also introducing new opportunities to forge collective action with allies and partners against both the renewed threat of nation-state aggression and emerging threats to human security.

The 2022 Annual Threat Assessment highlights some of those connections as it provides the Intelligence Community's (IC's) baseline assessments of the most pressing threats to U.S. national interests, while emphasizing the United States' key adversaries and competitors.

It is not an exhaustive assessment of all global challenges and notably excludes assessments of U.S. adversaries' vulnerabilities.

It accounts for functional concerns, such as weapons of mass destruction and cyber, primarily in the sections on threat actors, such as China and Russia.

Competition and potential conflict between nation-states remains a critical national security threat.

Beijing, Moscow, Tehran, and Pyongyang have demonstrated the capability and intent to advance their interests at the expense of the United States and its allies.

China increasingly is a near-peer competitor, challenging the United States in multiple arenas—especially economically, militarily, and technologically—and is pushing to change global norms and potentially threatening its neighbors.

Russia is pushing back against Washington where it can—locally and globally—employing techniques up to and including the use of force.

In Ukraine, we can see the results of Russia's increased willingness to use military threats and force to impose its will on neighbors.

Iran will remain a regional menace with broader malign influence activities, and North Korea will expand its WMD capabilities while being a disruptive player on the regional and world stages.

Major adversaries and competitors are enhancing and exercising their military, cyber, and other capabilities, raising the risks to U.S. and allied forces, weakening our conventional deterrence, and worsening the longstanding threat from weapons of mass destruction.

As states such as China and Russia increasingly see space as a warfighting domain, multilateral space security discussions have taken on greater importance as a way to reduce the risk of a confrontation that would affect every state's ability to safely operate in space.

The lingering effects of the COVID-19 pandemic will continue to strain governments and societies, fueling humanitarian and economic crises, political unrest, and geopolitical competition as countries, such as China and Russia, seek advantage through such avenues as "vaccine diplomacy."

No country has been completely spared, and even when a vaccine is widely distributed globally, the economic and political aftershocks will be felt for years.

Low-income countries with high debts face particularly challenging recoveries and the potential for cascading crises leading to regional instability, whereas others will turn inward or be distracted by other challenges.

The IC continues to investigate the concerning incidences of Anomalous Health Incidents and the danger they pose to U.S. personnel.

Ecological degradation and a changing climate will continue to fuel disease outbreaks, threaten food and water security, and exacerbate political instability and humanitarian crises.

Great power competition and disputes between wealthy and low-income nations will threaten progress on the collective action that will be needed to meet global goals for reduction of greenhouse gas emissions.

Other transnational challenges will pose an array of direct and indirect threats to the United States.

They will interact in complex and cascading ways with each other and with threats posed by great power competition, increasingly empowered non-state actors, the pandemic, and climate change.

Emerging and disruptive technologies, as well as the proliferation and permeation of technology into all aspects of our lives, pose unique challenges.

The scourge of transnational organized crime, illicit drugs, violent extremism, and endemic corruption in many countries will continue to take their toll on American lives, prosperity, and safety.

Both state and non-state cyber actors threaten our infrastructure and provide avenues for foreign malign influence threats against our democracy.

We will see continuing potential for surges in migration from Afghanistan, Latin America, and other poor countries, which are reeling from conflict and the economic fallout of the COVID-19 pandemic.

Economic and political conditions in Latin America continue to spark waves of migration that destabilize our Southern neighbors and put pressure on our Southern border.

Finally, ISIS, al-Qa'ida, and Iran and its militant allies will take advantage of weak governance to continue to plot terrorist attacks against U.S. persons and interests, including to varying degrees in the United States, and exacerbate instability in regions such as Africa and the Middle East.

Regional instability and conflicts continue to threaten U.S. persons and interests. Some have direct implications for U.S. security.

For example, the Taliban takeover of Afghanistan threatens U.S. interests, including the possibility of terrorist safe havens re-emerging and a humanitarian disaster.

The continued fighting in Syria has a direct bearing on U.S. forces, whereas tensions between nuclear-armed India and Pakistan remain a global concern.

The iterative violence between Israel and Iran, and conflicts in other areas—including Africa, Asia, and the Middle East—have the potential to escalate or spread, fueling humanitarian crises and threatening U.S.

persons, as in the case of Al-Shabaab, which is leveraging continued instability in East Africa and the lack of security capacity of regional states to threaten U.S. interests and American lives.

The 2022 Annual Threat Assessment Report supports the Office of the Director of National Intelligence's transparency commitments and the tradition of providing regular threat updates to the American public and the United States Congress.

The IC is vigilant in monitoring and assessing direct and indirect threats to U.S. and allied interests. As part of this ongoing effort, the IC's National Intelligence Officers work closely with analysts from across the IC to examine the spectrum of threats and highlight the most likely and impactful near-term risks in the context of the longer-term, overarching threat environment.

The report:
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

Cyber Crime

Transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide. These criminals are driven by the promise of large profits, reliable safe havens from which to operate, and a decreasing technical barrier to entry for new actors.

- Many major transnational cybercrime groups have diversified business models that engage in direct wire-transfer fraud from victims, or use other forms of extortion alongside or in place of ransomware. In 2020, business-e-mail compromise, identity theft, spoofing, and other extortion schemes ranked among the top five most costly cybercriminal schemes.

U.S. Government entities, businesses, and other organizations face a diverse range of ransomware threats. Attackers are innovating their targeting strategies to focus on victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions, driving ransomware payouts up.

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.

Our websites include:

- https://www.cyber-risk-gmbh.com
- https://www.social-engineering-training.ch
- https://www.disinformation.ch
- https://www.cyber-espionage.ch
- https://www.hotel-cybersecurity.ch
- https://www.healthcare-cybersecurity.ch
- https://www.railway-cybersecurity.com
- https://www.transport-cybersecurity.com
- https://www.transport-cybersecurity-toolkit.com
- https://www.airline-cybersecurity.ch
- https://www.maritime-cybersecurity.com
- https://www.european-cyber-resilience-act.com
- https://www.european-cyber-defence-policy.com
- https://www.european-chips-act.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