Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, March 2022

Dear members and friends,

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.

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

SHIELDS UP

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

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

SHIELDS UP – Simple steps for individuals

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

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

U.S. Government Accountability Office

Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks

The internet is a vast system of interconnected networks used by billions of people. Its architecture—the backbone of the internet—is owned and governed by organizations around the world. No one organization is responsible for its policy, operation, or security.

Generally, internet architecture is considered resilient, in part because of its decentralized nature. But reports we reviewed and subject matter experts have identified risks to key internet operations.

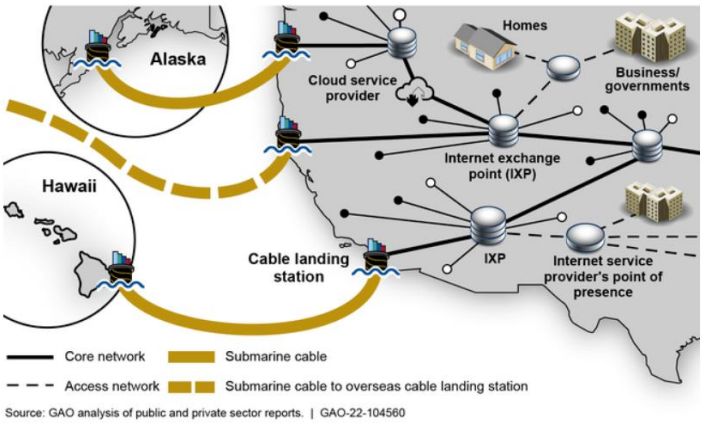
Many federal agencies are involved in addressing these risks, taking actions such as disseminating threat information and participating in global internet governance groups.

What GAO Found

The communications sector operates the multiple, independent networks that form the basis for the internet.

To support the exchange of network traffic, service providers manage and control core infrastructure elements with numerous components, including internet exchange points and submarine cable landing stations that connect to both domestic and international networks (see graphic).

How U.S. Internet Core Networks Connect to Service Providers



Source: GAO analysis of public and private sector reports. | GAO-22-104560

Multiple U.S. service providers operate distinct core networks that traverse the nation and interconnect with each other at several points.

While experts consider the internet architecture to be resilient, it nevertheless faces a variety of cyber and physical risks that can impact its components; such risks can be intentional or unintentional (see table).

Risks to Internet Architecture

Cyber intentional •Denial-of-service attacks •Border gateway protocol (BGP) abuse •Domain name system (DNS) abuse •Supply chain exploitation •Malicious insider(s)	**Cyber unintentional** •BGP failures •DNS failures •Hardware failures •Software failures •Operator error
Physical intentional •Intentional damage to fiber-optic cabling •Attack on an internet architecture facility or related infrastructure	**Physical unintentional** •Accidental damage to fiber-optic cabling •Severe natural event

Source: GAO analysis of federal and nonfederal reports. | GAO-22-104560

In particular, cyber-related risks can impact two sets of protocols needed to ensure the uniqueness of names used in internet-based services and for facilitating the routing of data packets.

Specifically, the domain name system translates names, such as www.gao.gov, to numerical addresses used by computers and other devices to route data.

Additionally, the border gateway protocol is used to exchange network availability and routing information about individual networks (i.e., destinations).

Both of these protocols are threatened by intentional abuse by malicious actors, as well as by unintentional failure.

In addition, the internet architecture can be impacted by physical risks, such as cutting or removing fiber-optic cabling.

Risks, if realized, may result in incidents that disrupt the proper functioning of the internet, including outages, degradation of performance, and interception of traffic.

Panelists serving on two panels convened by GAO also stated that the risk of intentional incidents affecting the internet architecture depends on the capabilities and motives of malicious actors.

GAO and others have reported on the threats posed by criminal groups and nation states, among others, which could potentially use their capabilities to impact components of the internet architecture.

For example, a 2017 Department of Homeland Security information technology-related risk assessment identified organized crime and nation states as threats to operations providing domain name routing services.

As the U.S. government reduced its role regarding internet architecture components, including decommissioning early networks it had developed and relinquishing its oversight role of internet technical functions, those responsibilities passed to the global multistakeholder community.

No one organization is responsible for the entirety of internet policy, operations, and security. However, the federal government fulfills a number of different roles that directly address risks to the internet architecture (see table).

Federal Roles in Infrastructure Architecture Security

Guiding Critical Infrastructure Protection and Performing Private Sector Engagement
Engaging in International Cyber Diplomacy
Supporting Cyber Research and Development
Coordinating Cyber Incident Response
Investigating and Prosecuting Cyber Criminal Activity
Developing Security Standards
Regulating Portions of the U.S. Communication Network
Addressing Supply Chain Concerns Related to Data Routing Hardware and Services
Operating Domain Name System Root Zone Servers
Issuing Licenses to Land and Operate Submarine Cables

Source: GAO analysis of federal law and policy, agency documentation, and prior GAO reports. | GAO-22-104560

To fulfill these roles, agencies have taken actions.
For example, DHS worked with members of the communications and information technology critical infrastructure sectors to, among other things, complete risk assessments on the sectors' ability to provide internet functions.

In addition, the Federal Communications Commission impacts the security of the internet architecture through licensing submarine cables and landing stations, and administering a program to remove and replace equipment determined to pose an unacceptable risk to national security.

Why GAO Did This Study

The internet is a global system of interconnected networks used by billions of people across the world to perform personal, educational, commercial, and governmental tasks.

The U.S. government over time has relinquished its oversight role of the internet. A global, multistakeholder community made up of many organizations shapes internet policy, operations, and security. But the ongoing and increasing reliance on the internet underscores the need to understand the risks to its underlying architecture.

The House Committee on Armed Services Report accompanying the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 included a provision for GAO to examine internet architecture security.

This report (1) identifies security risks related to the internet architecture and (2) determines the extent to which U.S. federal agencies have taken actions to address security risks to the internet architecture.

GAO collected and analyzed publicly available reports from federal and nonfederal organizations to identify risks to internet architecture components (internet exchange points, submarine cabling, the domain name system, and border gateway protocol, among others).

GAO also reviewed federal law and policy and its prior work to identify federal internet architecture security roles and responsible agencies. Based on the agencies' roles, GAO collected and analyzed relevant documents and conducted interviews with officials from the responsible agencies.

In addition, GAO convened two panels with subject matter experts. The panelists have experience in various aspects of the internet architecture, such as owning and operating elements of the infrastructure, participating in and contributing to standards setting organizations, and studying and participating in various multistakeholder governance entities.

During the panel sessions, GAO presented previously identified cyber and physical risks and requested that the experts identify additional risks or concerns that were not identified. GAO and the experts also discussed federal government involvement in addressing the risks.

To read more: https://www.gao.gov/assets/gao-22-104560.pdf

United States Government Accountability Office

Report to the Committee on Armed Services, House of Representatives

March 2022

CYBERSECURITY

Internet Architecture Is Considered Resilient, but Federal Agencies Continue to Address Risks

Navigating change in the global financial system - the role of the Financial Stability Board

Klaas Knot, President of the Netherlands Bank, at the G20 meeting of Finance Ministers and Central Bank Governors, Jakarta.

Good afternoon. It is great to meet you all here in person, as a hopeful step toward normality. First of all I want to thank Governor Perry Warjiyo for inviting me to speak here today. And I want to thank the Indonesian G20 Presidency for their hospitality and their organization of such a smooth event in the face of a still challenging Covid environment.

I feel honored to speak before you as the new Chair of the Financial Stability Board. And I am grateful to my predecessor, Randal K. Quarles, for his leadership in a challenging period. Randy came in when the reform agenda that followed the 2008 crisis was nearing completion.

We had just started to look ahead. Then the pandemic hit. He did a fantastic job as FSB Chair in turning the FSB's focus to the crisis at hand, without losing sight of the need to continue to make progress on longer-term priorities.

Along the way, he further strengthened the FSB in its role as the primary coordinating mechanism on financial stability matters. I will continue the work that Randy had already started. Here I realize I have big shoes to fill. Luckily, they are already pointed in the right direction.

The past three years have seen a fundamental shift in the work of the FSB, from completing the post-2008 reforms to tackling new challenges for financial stability.

Here I think of the crisis management and ongoing coordination during the pandemic, efforts to tackle vulnerabilities in non-bank financial intermediation, work to ensure that digital innovation is safe, and addressing the risks that climate change may create for financial stability.

The FSB has coped with this shift effectively, not least thanks to the continued support of its members and the G20. Yet we may have seen only the beginning of the changes that the pandemic, digitalization and climate change are bringing to the financial system, and our economies more widely.

Today, I would like to discuss with you my view of the role that the FSB should play to ensure that the financial system can navigate these changes safely, while providing the financing that the real economy needs.

The FSB is the centre piece of a multilateral approach to financial stability that until now has proven very effective. This was best demonstrated by the G20 reforms following the great financial crisis.

These reforms have served the financial system well during the Covid pandemic. Greater resilience of major banks at the core of the financial system has allowed the system to absorb, rather than amplify, the economic shock. Without the G20 reforms, governments would now have to deal with a crippled banking sector in full deleveraging mode, on top of an economy hit by Covid restrictions. We would have had a crisis within a crisis.

In my view, this success is in large part thanks to the G20's commitment to dealing with global challenges together, and to the FSB's broad membership, its agility and its engagement with other stakeholders. We will need to fully use these strengths, to which I will return later on, if we want to tackle the new financial stability challenges successfully.

So let me now discuss the nature of these challenges and what it means for the work of the FSB in the coming years.

A big challenge for policy makers worldwide at this moment is navigating their economies out of the Covid pandemic.

Two years after its onset, the economic fall-out of the pandemic appears to be subsiding, and the extraordinary fiscal and monetary support measures that kept economies afloat are being gradually unwound. But as the economic recovery is proceeding at an uneven pace across regions, this unwinding process is increasingly likely to be asynchronous. This creates the potential for cross-border spill-overs.

Moreover, since the onset of the pandemic, both public and private sector debt have increased, while asset prices have grown amid a search for yield. This has made the global financial system more vulnerable to a disorderly tightening of financial conditions - a concern that has been accentuated lately by the return of high inflation.

The FSB is monitoring and analysing developments closely and stands ready to facilitate global coordination of financial policies, where necessary, to minimize the risk of a disorderly exit.

This is being underpinned by the FSB's new financial stability surveillance framework. The framework enables us to identify global financial

vulnerabilities in a systematic manner. It draws on the collective expertise of the FSB's broad membership. It places particular emphasis on incorporating multiple perspectives in the identification and assessment of both current and emerging vulnerabilities.

At the same time as navigating our economies out of Covid, we need to strengthen resilience in the non-bank financial intermediation, or NBFI, sector.

The financial reform agenda after 2008 focused heavily on banks. Greater resilience of major banks at the core of the financial system has allowed the system to absorb, rather than amplify, the economic shock from the pandemic. But as a side-effect, risks in the financial system moved from the banking sector to the non-bank financial sector. This is what I have previously referred to as the 'waterbed effect'. Pressing down on one end of the financial system causes risks to pop up elsewhere. And, indeed, since 2008 NBFI has grown much faster than bank intermediation. It now accounts for about half of all financial assets worldwide.

So, we now have some catching up to do when it comes to reducing systemic risk in non-bank financial markets. This is a top priority for the FSB, as reflected in our ambitious NBFI work programme.

The pandemic has brought into even sharper focus the central role of digital innovation. Digital innovation offers important opportunities for more efficient and inclusive finance. Let's take the FSB's work to enhance cross-border payments. The use of new technology is an important element here. The aim of this initiative is to bring about cheaper, faster and more transparent and inclusive cross-border payment services for the benefit of citizens and businesses worldwide.

Over the past year, in cooperation with CPMI, we have done the foundational work under the G20 Roadmap for Enhancing Cross-Border Payments and we have established quantitative targets. Which means we can now go to the next stage: developing specific proposals for material improvements to existing systems and arrangements, as well as the development of new systems.

But digital innovation also creates risks. The issues raised by digital innovation in finance are in a number of respects similar to those of traditional NBFI: we need to assess the implications of changes in intermediation structures for financial stability. The key difference is that important innovation is happening outside the traditional financial system, often supplied by non-financial entities such as BigTechs, traded on unregulated platforms and transferred on ordinary computer networks globally.

Crypto-asset markets are a case in point. The FSB has been monitoring crypto-asset developments since 2018. Our most recent risk assessment shows that markets for crypto-assets are fast evolving and could reach a point where they represent a threat to global financial stability. I must say I have my concerns about this development.

Let's take for example all the misnomers that are doing the rounds. Unbacked crypto assets suggest all others are backed, which they are not. Most stablecoins are neither stable nor coins. Decentralized finance is often quite centralized. This leads to misconceptions about crypto-assets, which contribute to their fast growth.

The FSB is stepping up to the plate to deliver an effective regulatory approach to crypto-assets. We have issued a set of high-level recommendations for the regulation, supervision and oversight of so-called "global stablecoins". Also we are continuing to work with the standard-setting bodies to review their implementation and whether any changes are needed.

Parallel to this, the FSB has started to examine, together with the relevant standard-setting bodies, regulatory and supervisory issues and approaches to address risks stemming from the so-called "unbacked" crypto-assets. And we will analyse the financial stability implications of Decentralized Finance, in order to understand the need for policy action in that area.

Another feature of digital innovation is the ever-greater use by financial institutions of outsourcing to third-party service providers. While outsourcing may have provided additional resilience during the pandemic, it has also reinforced the importance of effective policies for the oversight of financial institutions' reliance on critical service providers.

To this can be added the greater exposure to cyber risk. Greater interconnections in the financial system increase the surface for cyberattacks, which have escalated during the Covid pandemic. Enhancing operational and cyber resilience will therefore remain important items on the FSB agenda.

Next to digitalization, we face the ever-growing threat of climate change. While emanating outside the financial sector, climate change may severely affect financial stability. The financial risks of climate change reflect its particular nature: it is global in its causes and its implications, and it is pervasive, affecting all kinds of financial assets and contracts.

For safeguarding financial stability and ensuring the financing needed for the transition to net zero, it is key that climate related financial risk is adequately priced in financial contracts. This is crucial because financial

contracts price the future, and that future is about to undergo fundamental change.

The FSB's roadmap for addressing climate-related financial risks, which is being taken forward in close conjunction with the NGFS and many other international bodies, aims to ensure that climate risks are properly reflected in all financial decisions. It covers disclosures, data, vulnerability analysis, and regulatory and supervisory approaches. This is important because, as we all know, what gets measured, gets managed.

Despite the progress made, the challenges are formidable. They range from identifying and collecting the information needed to measure and assess climate-related risks, to designing robust supervisory tools, such as climate stress tests and scenario analysis. Because there are no international standards in place yet, not least relating to disclosures, we have an enormous opportunity to get this right from the start. We should not miss it.

The changes I discussed – the move to a post-covid world, ensuring safe digital innovation, and transitioning to net-zero emissions – are global in nature, including their impact on the financial system. In order to promote global financial resilience and the smooth provision of finance to the real economy in the face of these changes, we need to continue our successful global cooperation. The FSB is uniquely placed to facilitate this, because of its three key strengths.

First of all its broad, diverse and multi-disciplinary membership. The FSB brings together in a collegial spirit of mutual trust senior officials from 71 authorities in 25 jurisdictions, and 10 multilateral institutions, covering multiple mandates across different sectors. This broad membership enables the FSB to take a truly holistic – cross-sectoral and international – perspective on financial stability issues.

Such a perspective is key to understanding and tackling risks from digital innovation and climate change, which affect all parts of the financial system, as well as understanding system-wide risk in complex financial ecosystems like NBFI. It is also key to avoid regulatory arbitrage and fragmentation. And its broad membership, including the sectoral standard setters, puts the FSB in a position to coordinate effectively.

The second strength is the FSB's agility in addressing near-term threats as well as structural changes in the financial system, while keeping sufficient headroom to be able to respond to new emerging vulnerabilities that are detected. This agility was demonstrated at the start of the pandemic, when FSB members exchanged information on market developments and policy actions on a daily basis and reprioritized their work and resources to focus on the pandemic.

The third strength is the FSB's engagement, as part of the policy-making process, with a broad range of stakeholders both inside and, importantly, outside the financial sector. The FSB reaches beyond its membership to include over 70 further jurisdictions through its Regional Consultative Groups.

This engagement is underpinned by its commitment to transparency as well as its accountability to its various stakeholders, including the G20. This outreach will be even more important in the areas of digital innovation and climate change, where relevant expertise and responsibilities may not rest with financial authorities.

I will build upon and further develop these strength during my tenure. I aim to ensure that the FSB remains a member-led and inclusive organization.

Because this has proven key for continued support to a multilateral approach. An approach that has proven to work.

And I would like to thank you, G20 colleagues, for entrusting me the task of chairing this organization. I look forward to working with you and with my fellow FSB members to ensure that the FSB plays its part in supporting the G20 objective of strong, sustainable, balanced and inclusive growth.

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

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

The pressing need to reform the European crisis management framework

Fernando Restoy, Chair, Financial Stability Institute, "Synergizing Multifaceted Regional and Global Perspectives" conference of Japan's Deposit Insurance Corporation, DICJ-IADI Round Table.

Thank you very much to the Japanese Deposit Insurance Corporation (DIC) and the International Association of Deposit Insurers (IADI) for the invitation to participate in this event.

At the FSI we really value our ongoing fruitful cooperation with the deposit insurance community.

This event gives me also the opportunity to share some views on the European crisis management framework with a very distinguished audience.

Introduction

The debate on how to improve the rules and procedures for dealing with bank failures in the European banking union already started a few years ago but gained momentum in 2017 when two significant banks – both of which were under the remit of the Single Supervisory Mechanism (SSM) and the Single Resolution Board (SRB) – failed.

Those episodes illustrated how difficult it can be for the existing rules to facilitate the orderly market exit of different types of institutions whose failure could create systemic distress.

It is somewhat paradoxical that those difficulties have become so evident in the EU, as this is probably the jurisdiction that has most deeply modernised its crisis management framework by adopting the new international standards on bank resolution (the FSB Key Attributes) in a timely, comprehensive and rigorous fashion.

As you all know, the FSB Key Attributes were one of the main regulatory reforms undertaken by the international community in the aftermath of the Great Financial Crisis (GFC) in order to reduce the probability and economic impact of financial crises. They aimed to put in place a bank resolution mechanism that would help maintain the critical functions of

failing systemic institutions without recurring to a massive deployment of public resources.

The EU had a clear motivation for embracing the new resolution framework based on its own experience during the GFC. Europe was the region where the GFC hit the banking sector most intensely and required voluminous public aid. Indeed, the net costs for European governments of supporting financial institutions between 2008 and 2014 exceeded €200 billion.

That of course put significant pressure on the public finances of most affected member states and triggered the adoption of procyclical fiscal austerity programmes that exacerbated the economic contraction that followed the outbreak of the crisis.

Even more importantly, that connection between banks' vulnerabilities and the need for public support initiated a destabilising spiral between financial and sovereign risk that gave rise to redenomination risks, thereby threatening the very continuation of the European monetary union.

Against that framework, in Europe developing crisis management tools that could minimise the dependence on public funds to safeguard financial stability, in line with the FSBs' Key Attributes, was deemed essential to preserve both the social cohesion within member countries and the robustness of the European integration project.

The features of the current framework

In response, as early as 2014 European authorities created a single resolution mechanism (SRM) as part of the banking union project. The SRM establishes rules, tools and procedures for managing the failure of those banks in the banking union that are considered systemic, ie those that meet public interest criteria, to use the legal jargon.

Those rules include an effective prohibition of government bailouts and a predominant reliance on creditors' bail-in to maintain the critical functions of failing institutions. Moreover, the new framework envisages the centralisation of resolution decisions in a European agency (the SRB) and the creation of a progressively mutualised fund (the Single Resolution Fund (SRF)) contributed by the industry.

That fund can be used to support resolution actions, although only after a large amount of creditors' claims have been bailed-in. Consistently with those minimum bail-in conditions, banks are generally required to issue large volumes of financial instruments that could become loss-absorbing at the point of non-viability (the minimum requirement for own funds and eligible liabilities, MREL).

The rules that govern the SRM constitute a highly stringent transposition of the FSB Key Attributes. Arguably, no other jurisdiction has imposed more explicit and severe constraints on the use of external funds (whether public or private) to support resolution.

Moreover, outside the EU it is uncommon for authorities to generally require banks (and not only globally systemic ones) to meet MREL-type obligations. Again, the severity of those restrictions is largely a political response to the recent experience and the specific institutional constraints posed by the multinational character of the European banking union.

The issues

While the design of the EU resolution framework is internally consistent, it fails to provide a robust blueprint for managing the failure of a large part of the institutions in the banking union.

It is important to note in that respect that the common resolution framework coexists with a constellation of domestic insolvency regimes, embedded in national legislation, which have not changed much in the recent past.

National regimes – often consisting of the application of court-based general insolvency procedures – are still applied when failing institutions do not meet the public interest criteria required for resolution.

Interestingly, the availability of public support under insolvency (in the form of liquidation aid) is, in general, substantially less restricted than under resolution.

As bail-in becomes a key component of envisaged resolution actions, the current framework is not particularly effective for dealing with the failure of banks whose liabilities cannot be used – without a major disruption – for loss absorption or recapitalisation.

This is the case of medium-sized banks which are largely funded with deposits. Those institutions are typically too large to be subject to standard liquidation procedures under insolvency, but also too small and unsophisticated to issue large amounts of bail-in-able debt (such as subordinated bonds) which are required for resolution.

In the absence of those instruments on these banks' balance sheets, authorities would not be able to recapitalise the institutions by making use of internal funds or by gaining access to the resolution funds as the minimum bail-in conditions for the latter would not be met. This is what we now generally call the "middle class" issue.

Authorities have addressed the challenges posed by the failure of mid-sized banks precisely by resorting to national insolvency regimes and taking advantage of their flexibility to use public funds to ensure a smooth market exit.

That has required delicate decisions regarding assessment of the systemic impact of banks' failures. In particular, those failures needed to fail the public interest test for resolution in order to be subject to national insolvency. But, at the same time, they had to be assessed as generating an adverse impact on the economic or financial system to justify the deployment of taxpayer funds.

That approach is suboptimal. It implies, somewhat ironically, that in order to activate the support required to avoid systemic stress, authorities have to avoid applying the framework designed precisely to deal with crises of systemic banks (resolution) and employ the regime envisaged for less significant institutions (insolvency).

Moreover, the extensive use of national insolvency regimes – funded fully with domestic resources – entails a departure from the principles that motivated the creation of the banking union, namely the urgent need to break the destabilising link between domestic financial risks and the sovereign. In fact, it would imply the renationalisation of bank failure management and, therefore, the renationalisation of banks' risks.

Some remedies

In order to fix the deficiencies of the current crisis management framework in the banking union, we first need more harmonisation of domestic insolvency regimes.

While a fully fledged common insolvency framework seems politically unfeasible at this stage, there should be scope to further harmonise those features of the domestic arrangements that have more potential to create frictions with the common resolution regime.

Importantly, when facing the failure of mid-sized banks, there is a need to avoid the perverse dilemma of having to choose between open bank bail-in under resolution and piecemeal liquidation under insolvency, as both options are potentially destabilising. Moreover, recourse to public support under insolvency cannot be assumed as a suitable fix for that dilemma.

A potentially useful formula for addressing the above challenges is to facilitate sale-of-business (SoB) (or purchase and assumption) transactions to engineer the orderly exit of failing banks.

Those strategies – in which deposits and other sensitive liabilities of failing banks are transferred to stronger institutions – have been successfully employed in other jurisdictions, like the US, for many years, but cannot be easily employed at present in the European context.

Logically, the success of SoB strategies requires the existence a suitable buyer. This depends very much on the value of transferable assets of the failing bank and the availability of external funding to compensate buyers for taking over failing banks' deposits if, as is often the case, the available assets do not suffice.

The amount of assets that can be transferred can be increased by requiring mid-sized banks to hold, as a counterpart, liabilities that could be written down or converted into capital as the banks fail. A reasonably calibrated MREL could therefore help make the transfer strategies more feasible6.

Yet, given the limited scope for mid-sized banks to issue and remunerate bail-in-able liabilities on a permanent basis, some external funds should be available to compensate buyers.

In several jurisdictions, that external funding can be provided by the deposit guarantee scheme (DGS). However, DGS funding is typically subject to a financial cap: it is available only if the expected cost of the intervention is not greater than that of paying out deposits under liquidation.

In the case of the EU, DGS support for SoB transactions is severely limited (if not made irrelevant) by legal provisions that stipulate that DGS claims are more senior than uncovered deposits in the creditors' hierarchy.

That "super-preference" of DGS claims protects them from assuming losses in liquidation. The result is that the financial cap makes European DGS unable to support SoB transactions, even if those would help avoid a potentially disruptive and value-destructing piecemeal liquidation.

Similarly, in the current framework the SRF is also not, at present, a suitable source of funding to generally support SoB transactions for mid-sized banks. The SRF is available only for failing institutions meeting the public interest condition required for resolution and only after a substantial creditors' bail-in has been executed. As discussed before, mid-sized banks will often find it very difficult to meet those conditions.

Therefore, the feasibility of SoB transactions requires significant changes to the current setup to facilitate sufficient coverage of their funding needs.

One possibility is to relax the financial cap for the deployment of DGS funds to support transfer transactions which is currently linked to the costs

associated with payout deposits in liquidation. However, any action in that regard should preserve the DGS' ability to deliver on its main objective, ie to protect covered deposits.

A related discussion is whether the current super-priority of DGS claims in Europe is warranted on public policy grounds. It could be argued that there is no obvious policy rationale for DGS claims to become senior in relation to uncovered deposits.

Indeed, the super-preference of DGS claims implies that individuals holding deposits above the maximum amount covered by the DGS are less protected in insolvency than the indirect positions held by DGS-affiliated banks vis-à-vis the failing institution.

The logic of that privilege is not straightforward. Moreover, following the example of other jurisdictions like the US and replacing the super-preference of DGS claims with a general deposit preference rule could help to mitigate risks of bank runs, thereby protecting financial stability. Naturally, that alternative preference rule would automatically relax the currently tight constraint on the use of DGS funds to support SoB transactions, without unduly compromising the DGS' main objectives.

Another alternative source of funds could be the SRF. As I discussed earlier, that would entail alleviating the currently stringent minimum bail-in conditions for the use of those resources.

Indeed, there seems to be a clear case for considering that conditions for the SRF to facilitate an orderly market exit of failing banks, for example through an SoB transaction, should not be as restrictive as the ones imposed to ensure that the failing bank could keep operating and performing critical functions.

It could therefore be envisaged lower minimum bail-in conditions for (typically medium-sized) banks following an SoB resolution strategy.

Notice that while funding from the SRF would only be available for banks subject to resolution, DGS funding could support all bank failures regardless of whether the public interest test is passed or not.

It is therefore probably the case that we need to make both DGS and SRF funding more easily available for conducting an SoB transaction for all types of institutions.

We should keep in mind, however, that while the SRF would eventually be fully mutualised, DGS remain, at present, national.

That means that more intensive use of DGS funds, as proposed, to manage banking crises in the banking union may further contribute to a renationalisation of banks' risks.

Moreover, for banks subject to the common resolution framework, reliance on national DGS would also create inconsistencies between the centralised decision-making process and decentralised funding mechanisms.

That is why the proposed formulas to enhance the feasibility of SoB strategies as a key objective to improve the functioning of the European crisis management framework further strengthen the case for completing the banking union with the creation of a European deposit insurance scheme.

Furthermore, since support from a European DGS would be available under both resolution and insolvency, there is clear logic in entrusting the SRB with managing that fund and deciding on how best employ it to facilitate an orderly exit of all types of banks, and not only those which are currently under its remit.

Concluding remarks

To conclude, as I argued before, any successful attempt to strengthen the current crisis management framework in the banking union needs to facilitate appropriate funding sources that could be deployed to support an orderly market exit for most institutions at the point of non-viability.

What I mean by an appropriate funding mechanism should be fully consistent with the banking union's objectives and, in particular, with the denationalisation of banks' risks.

But it should also be compatible with different banks' business models. I have discussed in my presentation some formulas which could be considered to meet that politically complex, but also pressing, objective. Those formulas -which we have been supporting for long- fit some of the options included in the recent public consultation recently issued by the European Commission.

I hope that, as a follow-up to that consultation, authorities will soon move swiftly, if not to deliver a comprehensive blueprint soon, at least to put forward a clear and effective roadmap for continuous progress towards the desired objective.

Many thanks for your attention.

Zoning and conduits for railways

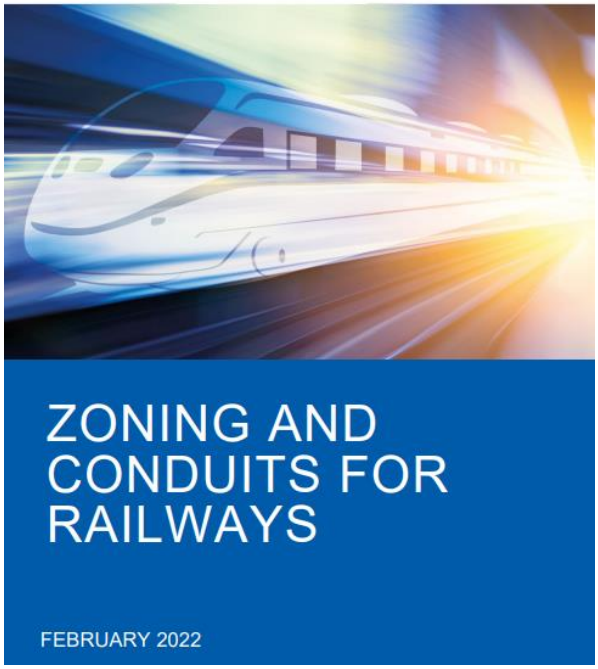
This document gives guidance on building zones and conduits for a railway system. To do so, first the methodology is described. This approach is based on the recently published CENELEC Technical Specification 50701 (CLC/CLC/TS 50701:2021).

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.

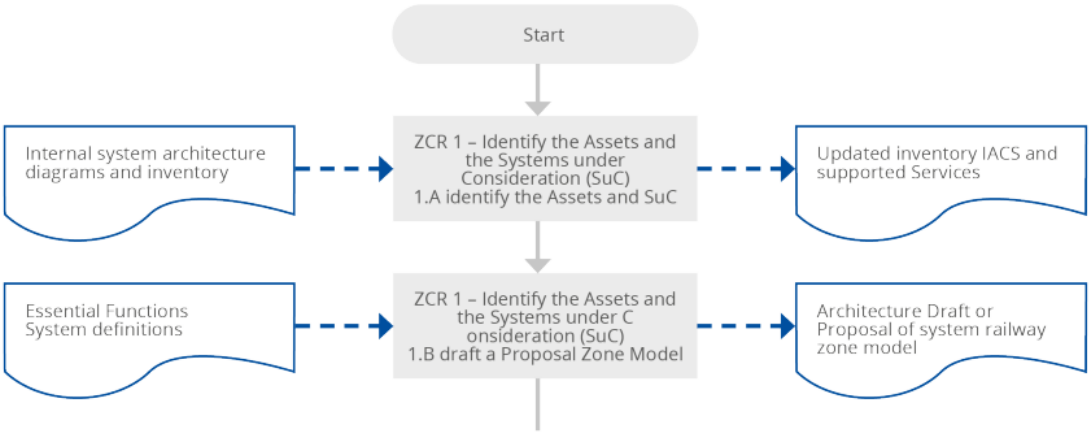
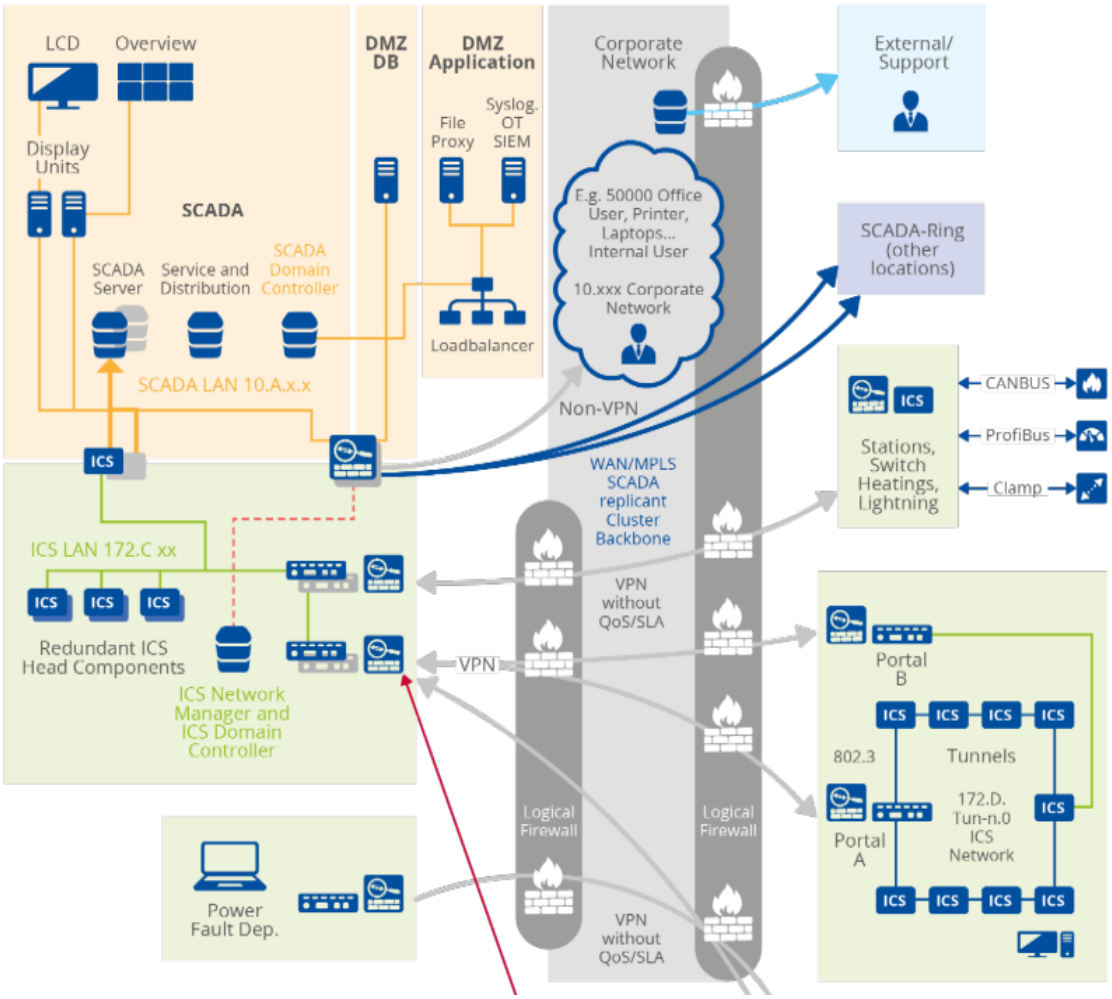


Figure 1 Zoning and conduit methodology



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

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

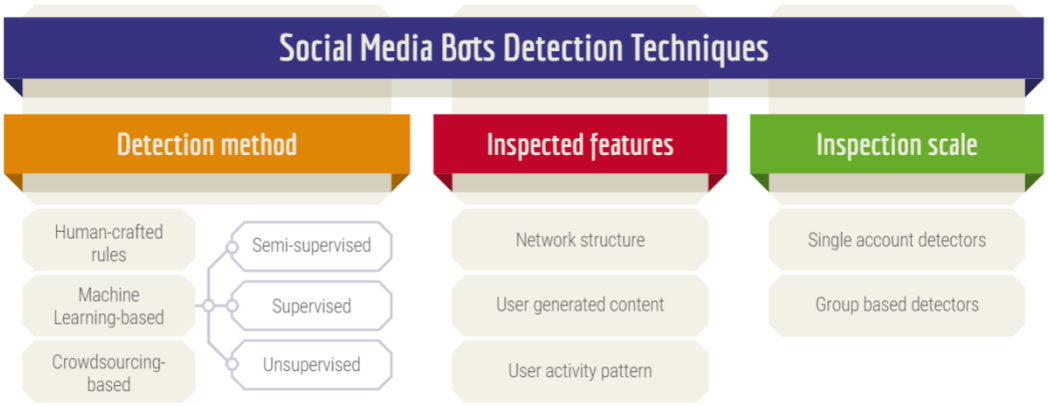
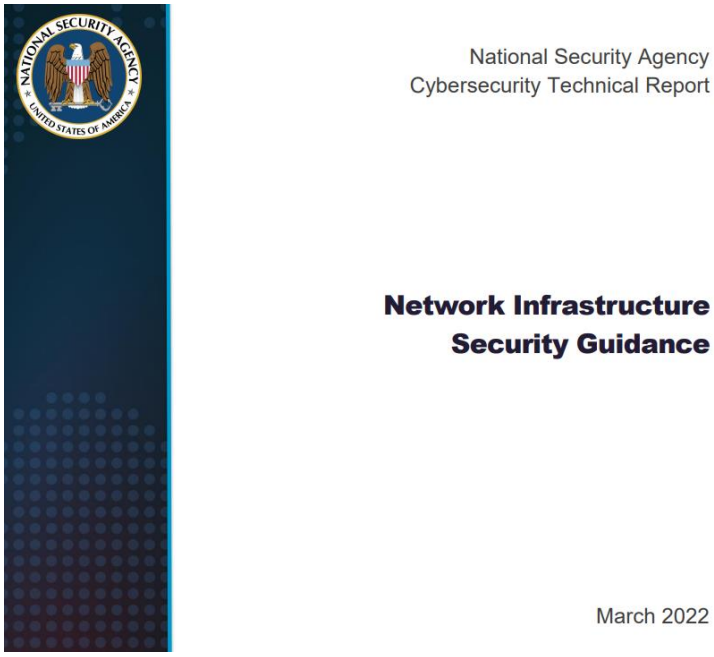


Figure 1. Social media bot detection techniques categorised by method, inspected features, and inspection scale. Partially adopted from Cresci[96] and Orabi et al.[97]

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

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

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

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 an interpretative document;

- 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.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: https://www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: https://www.sarbanes-oxley-association.com/Reading_Room.htm

3. Training and Certification - You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.