International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, November 7, 2022

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

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

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

THE COUNCIL OF THE EUROPEAN UNION,

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

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

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

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

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

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

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

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

In the SECURE pillar, we read:

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

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

- Create an EU Hybrid Toolbox that brings together different instruments

to detect and respond to a broad range of hybrid threats. In this context, we will develop a dedicated toolbox to address foreign information manipulation and interference;

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

After these developments, during the summer, we had to amend our *Certified Information Systems Risk and Compliance Professional (CISRCP)* program. IT, risk and compliance professionals live in a different world, with new challenges and opportunities.

Read more at number 1 below. Welcome in the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 6)

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

European Council
Council of the European Union

Number 2 (Page 16)

The U.S. Dollar and Central Bank Digital Currencies

Governor Christopher J. Waller, Board of Governors of the Federal Reserve System, at "Digital Currencies and National Security Tradeoffs," a symposium presented by the Harvard National Security Journal, Cambridge, Massachusetts.

Number 3 (Page 19)

International Regulation of Crypto-asset Activities - Questions for consultation

FSB FINANCIAL STABILITY BOARD

Number 4 (Page 22)

Results of the Bank of England 2021-22 central counterparty supervisory stress-test published

Bank of England

Number 5 (Page 25)

Public Consultation on Issues Paper on Insurance Sector Operational Resilience

Comments due by 6 January 2023

IAIS International Association of Insurance Supervisors

Number 6 (Page 27)

Meeting Investor Demand for High Quality ESG Data

SEC Commissioner Jaime Lizárraga. the Future of ESG Data 2022, London, United Kingdom

Number 7 (Page 29)

Progress Report on Climate-Related Disclosures

FSB FINANCIAL STABILITY BOARD

Number 8 (Page 32)

Remarks by FDIC Acting Chairman Martin J. Gruenberg on the American Bankers Association Annual Convention "The Financial Risks of Climate Change"

Number 9 (Page 36)

31 arrested for stealing cars by hacking keyless tech

EUROPOL

Number 10 (Page 38)

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

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

Number 1

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

THE COUNCIL OF THE EUROPEAN UNION,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

STRESSES the need, in line with the Strategic Compass, to further invest in our mutual assistance under Article 42(7) of the Treaty on European Union

as well as solidarity under Article 222 of the Treaty on the Functioning of the European Union, in particular through frequent exercises, to prevent, prepare against, and counter such actions.

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

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

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

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

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

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

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

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

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

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

STRESSES the need for relevant Council bodies, the High Representative and the Commission to encourage cooperation and synergies in the implementation of measures and actions decided on under this Framework, in particular through the Hybrid Toolbox and FIMI Toolbox, as well as within the EU Cyber Diplomacy Toolbox when and where appropriate.

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

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

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

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

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

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

CALLS on the Member States, the Commission and the High Representative to give full effect to the development of the Framework, putting in place implementing guidelines and testing its procedures through existing and new exercises, including exercises involving the activation of Article 222 TFEU and/or Article 42(7) TEU. The Council will TAKE STOCK of the implementation of these conclusions before the end of 2023 and, if necessary, will review the Framework in order to address the evolving threat landscape.

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

Number 2

The U.S. Dollar and Central Bank Digital Currencies

Governor Christopher J. Waller, Board of Governors of the Federal Reserve System, at "Digital Currencies and National Security Tradeoffs," a symposium presented by the Harvard National Security Journal, Cambridge, Massachusetts.

Thank you, Professor Jackson, and thank you to the Harvard National Security Journal for the invitation to speak at this symposium.

As the payment system continues to evolve rapidly and the volume of digital assets continues to grow, it is critical to ensure that we keep both the benefits and risks of digital assets in the policy conversation, including the implications for America's role in the global economy and its place in the world.

My speech today focuses on exactly this issue and on an aspect of the digital asset world that is now the center of domestic and international attention—central bank digital currencies (CBDCs) and how they relate to the substantial international role of the U.S. dollar.

In January 2022, the Federal Reserve Board published a discussion paper on CBDCs to foster a broad and transparent public dialogue, including the potential benefits and risks of a U.S. CBDC.

To date, no decisions have been made by the Board on whether to move forward with a CBDC. But my views are well known.

As I have said before, I am highly skeptical of whether there is a compelling need for the Fed to create a digital currency.

I am not a national security expert. But one area where economics, CBDCs, and national security dovetail is the role of the dollar.

Advocates for creating a U.S. CBDC often assert how it is important to the long-term status of the dollar, particularly if other major jurisdictions adopt a CBDC. I disagree. As I will discuss, the underlying reasons for why the dollar is the dominant currency have little to do with technology, and I

believe the introduction of a CBDC would not affect those underlying reasons.

I offer this view, again, in the spirit of dialogue, knowing how important these issues are, and I am very happy to engage in vigorous debate regarding my view. I remain open to the arguments advanced by others in this space.

The Role of the U.S. Dollar

After World War II and the creation of the Bretton Woods system, the U.S. dollar served as the central currency for the international monetary system.

Other countries agreed to keep the exchange value of their currencies fixed to the dollar, and eventually, countries came to settle international balances in dollars. That role has continued long after the Bretton Woods system dissolved.

By any measure, the dollar is the dominant global currency—for funding markets, foreign exchange transactions, and invoicing. It also is the world's predominant reserve currency.

In terms of the dollar's reserve currency status, 60 percent of disclosed official foreign reserves are held in dollars, far surpassing the shares of other currencies, with the majority of these dollar reserves held in safe and liquid U.S. Treasury securities.

Even in a world of largely floating exchange rates, many countries either implicitly or explicitly anchor their currencies to the dollar; together, these countries account for about half of world gross domestic product.

The dollar is by far the dominant currency for international trade. Apart from intra-European trade, dollar invoicing is used in more than three-fourths of global trade, including 96 percent of trade in the Americas.

Approximately 60 percent of international and foreign currency liabilities—international banking loans and deposits as well as international debt securities—are denominated in dollars.

And the dollar remains the single most widely used currency in foreign exchange transactions. Why does this matter to the United States?

As indicated in the Board's CBDC discussion paper, the dollar's international role lowers transaction and borrowing costs for U.S. households, businesses, and government.

It widens the pool of creditors and investors for U.S. investments. It may insulate the U.S. economy from shocks from abroad.

It also allows the United States to influence standards for the global monetary system.

The dollar's role doesn't only benefit the United States. The dollar serves as a safe, stable, and dependable form of money around the world. It serves as a reliable common denominator for global trade and a dependable settlement instrument for cross-border payments.

In the process, it reduces the cost of transferring capital and smooths the world of global payments, including for households and businesses outside of America.

For example, consider the dollar's role in foreign exchange markets. To make a foreign exchange transaction between two lightly traded currencies, it is often less expensive to trade the first currency with the dollar, and then to trade the dollar with the second currency, rather than to trade the two currencies directly.

The factors driving the dollar's role as a reserve currency are well researched and well demonstrated, including the depth and liquidity of U.S. financial markets, the size and openness of the U.S. economy, and international trust in U.S. institutions and the rule of law.

We must keep these factors in mind in any debate regarding the long-term importance of the dollar.

To read more:
https://www.federalreserve.gov/newsevents/speech/waller20221014a.htm

Number 3

International Regulation of Crypto-asset Activities - Questions for consultation

FSB FINANCIAL STABILITY BOARD

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

General

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

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

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

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

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

Crypto-assets and markets (CA Recommendations)

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

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

FSB FINANCIAL STABILITY BOARD

International Regulation of Crypto-asset Activities

A proposed framework – questions for consultation

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

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

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

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

Global stablecoins (GSC Recommendations)

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

FSB FINANCIAL STABILITY BOARD

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

Consultative report

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

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

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

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

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

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

Number 4

Results of the Bank of England 2021-22 central counterparty supervisory stress-test published

Bank of England

The Bank of England has published the results of its first public supervisory stress-test of UK central counterparties (CCPs).

The exercise took place over 2021-22 with the clearing services of all UK CCPs, ICE Clear Europe Limited, LCH Limited, and LME Clear Limited, in scope.

The exercise assessed the credit and liquidity resilience of these CCPs under a severe market stress scenario and the simultaneous default of selected clearing member groups.

It was exploratory in nature, aiming to identify potential vulnerabilities or gaps in resilience, rather than testing CCPs against a pass-fail threshold.

The severe market stress scenario consisted of shocks to the prices of a wide range of products cleared by the UK CCPs, and was designed to be at the limits of historical observations.

The findings showed that the UK CCPs were resilient to this market stress scenario and the simultaneous default of the two clearing member groups who, in defaulting, create the largest losses or most negative liquidity balances. While results vary across CCPs, no CCP experienced full depletion of prefunded financial resources or a negative liquidity balance.

The exercise also included a reverse stress test where CCPs are subjected to combinations of increasingly severe assumptions to identify what might fully deplete their prefunded and non-prefunded resources.

The findings will now be used in conjunction with feedback to the Bank's Discussion Paper on CCP supervisory stress-testing to help further develop and refine the Bank's CCP supervisory stress-testing regime. The Bank intends to publish a final framework document for CCP supervisory stress-testing in the course of 2023.

Sir Jon Cunliffe, Deputy Governor for Financial Stability, said:

"The conclusion of the Bank's first public CCP stress-test marks a major milestone in the development in the supervision and regulation of CCPs.

While the stress test was exploratory, with no pass-fail assessments, the results are evidence of the overall resilience of the UK CCPs.

We will engage these CCPs on our findings, which will help the Bank target its supervision and inform CCPs' approach to risk management. This stress test supports our commitment, in line with the UK's status as a global financial centre, to regulating CCPs with due transparency and in line with international best practice."

Executive summary

In October 2021, the Bank announced the launch of the 2021–22 Supervisory Stress Test (SST) of UK Central Counterparties (CCPs) (the 2021–22 CCP SST).

This exercise is the Bank's first public CCP SST, and follows the Bank's (non-public) pilot CCP SST exercise in 2019, the publication of the Bank's Discussion Paper on Supervisory Stress Testing of Central Counterparties, and the Bank's participation in the European Securities and Markets Authority's (ESMA) EU-wide CCP Stress-Test exercises.

Purpose and design

This exercise is exploratory in nature. It aims to identify potential vulnerabilities and gaps in CCP resilience, rather than testing CCPs against particular pass-fail thresholds. The findings will be used to support and inform the Bank's supervisory and regulatory activities.

The lessons from running this exercise will also be used to support the continued development of the Bank's framework for CCP supervisory stress testing, in conjunction with the feedback received on the Bank's Discussion Paper on Supervisory Stress Testing of Central Counterparties.

The 2021–22 CCP SST exercise was launched in October 2021. It explores the individual and system-wide credit and liquidity resilience of the three UK CCPs (ICE Clear Europe Limited (ICEU), LCH Limited (LCH), and LME Clear Limited (LMEC)) and each of their Clearing Services.

In particular, the impact on CCPs' financial and liquidity resources is examined under a combined baseline severe financial market stress scenario (the 'Baseline Market Stress Scenario') plus the simultaneous default of selected Clearing Member groups (including in their capacity as service providers). The selected Clearing Member default scenarios include, but are not limited to, the default of the Cover-2 population at each CCP Clearing Service.

The exercise also explores the impacts of this Baseline Market Stress Scenario and the default of certain groups of Clearing Members on the non-defaulting Clearing Member and client populations at the UK CCPs.

The Baseline Market Stress Scenario consists of shocks to the prices of a wide range of products cleared by the UK CCPs. It is calibrated to be broadly equivalent in overall severity to the worst historical market stress scenario for each UK CCP Clearing Service (as at the time of the launch of this exercise in October 2021).

This scenario does not – and cannot – cover all possible sizes and combinations of market price shocks to which CCPs could be exposed. For example, the scenario is not focused on large hypothetical shocks that go far beyond historical limits in specifically selected asset classes or products.

In addition, sensitivity analysis and reverse stress-testing techniques are used to test CCP resilience against increasingly conservative assumptions. Reverse stress testing is used to evaluate CCPs' resilience to increasingly challenging combinations of assumptions that are intentionally well beyond historical precedence and regulatory requirements, and in combination are extremely severe.

This includes an examination of CCP resilience against additional market stress scenarios that overall are more severe than those historically observed and contain individual market shocks greater than historically observed for a variety of products.

To read more:
https://www.bankofengland.co.uk/news/2022/october/results-of-the-boe-2021-22-central-counterparty-supervisory-stress-test-published

https://www.bankofengland.co.uk/stress-testing/2022/ccp-supervisory-stress-test-results-2021-22

Number 5

Public Consultation on Issues Paper on Insurance Sector Operational Resilience

Comments due by 6 January 2023

Operational resilience has become an increasingly important area of focus, particularly in light of rapidly evolving technology and innovation, changes to where and how people are working, and an increasing cyber threat landscape.

While the concept of operational resilience may not be new to insurers, there is a recognition of the importance to adapt supervisory regimes to account for the growing resilience of insurers on digital systems, the adoption and implementation of new technologies, and the potential for insurance firms to rely on third party providers to assist in implementation and support.

In response to these emerging trends, the IAIS' Operational Resilience Task Force (ORTF) has now published for consultation its Issues Paper on Insurance Sector Operational Resilience.

The paper identifies issues impacting operational resilience in the insurance sector and provides examples of how supervisors are approaching these developments, with consideration of lessons learnt during the Covid-19 pandemic.

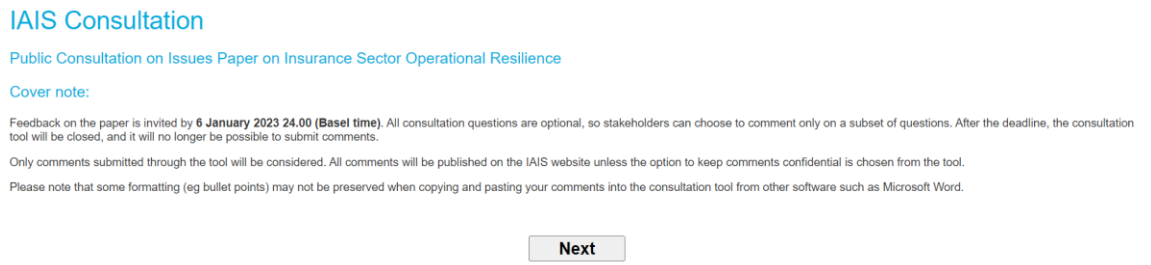
Recognising that operational resilience is a broad and evolving area, the paper addresses three specific operational resilience sub-topics concerning areas the ORTF considers as matters of significant and increasing operational risk and, therefore, of immediate interest to supervisors:

- Cyber resilience
- Third-party outsourcing
- Business Continuity Management

Feedback on the paper is invited by 6 January 2023, 24.00 (Basel time). All consultation questions are optional, so stakeholders may comment only on a subset of questions. After this deadline, the consultation tool will be closed, and it will no longer be possible to submit comments.

How to provide feedback:

The consultation is now open. Please use the consultation tool available at: https://web.iaisweb.org/iaisconsultations/consultationintro/BCD33DEBBE325CDB83FEDF02B625C2F4/9A60EB984525E31997CA0A66318146998E0374F3474C47DDBFFE908E76549BEDF5BFA17006163F2EF21341D10D9BAB93


IAIS Consultation

Public Consultation on Issues Paper on Insurance Sector Operational Resilience

Cover note:

Feedback on the paper is invited by **6 January 2023 24.00 (Basel time)**. All consultation questions are optional, so stakeholders can choose to comment only on a subset of questions. After the deadline, the consultation tool will be closed, and it will no longer be possible to submit comments.

Only comments submitted through the tool will be considered. All comments will be published on the IAIS website unless the option to keep comments confidential is chosen from the tool.

Please note that some formatting (eg bullet points) may not be preserved when copying and pasting your comments into the consultation tool from other software such as Microsoft Word.

Next

Instructions for use are available when you access the tool. Only comments submitted through the tool will be considered. All comments will be published on the IAIS website unless the option in the tool to keep comments confidential is chosen.

Please note that some formatting (eg bullet points) may not be preserved when copying and pasting your comments into the consultation tool from other software such as Microsoft Word.

To read more:
https://www.iaisweb.org/uploads/2022/10/Issues-Paper-on-Insurance-Sector-Operational-Resilience.pdf

https://www.iaisweb.org/2022/10/public-consultation-on-issues-paper-on-insurance-sector-operational-resilience/

Number 6

Meeting Investor Demand for High Quality ESG Data

SEC Commissioner Jaime Lizárraga. the Future of ESG Data 2022, London, United Kingdom

Thank you, Peter, for that kind introduction. It is a pleasure to be here with you today. I look forward to learning from today's discussion, and appreciate the opportunity to participate in this important exchange of ideas and perspectives.

It's an exciting time for ESG. You are working in a dynamic, fast-growing sector of our capital markets that is grabbing headlines and continuing to generate enormous interest among investors and the general public.

You're directly involved with some of the most consequential scientific challenges of our time – from climate change, to artificial intelligence, to big data analytics.

As active participants in this space, your contributions and innovative ideas can enrich the conversation.

I'd like to share with you a snapshot of what's happening in the U.S. ESG has become a lively topic that has moved beyond strictly financial circles. Several states are making headlines for their push against ESG investing, while other states are proactive in their ESG investments.

Against this backdrop, the SEC issued three rule proposals that would each help facilitate comparable ESG disclosures and focus on ensuring statements made to investors are not false or misleading:

- Enhanced climate risk disclosures by issuers.
- Enhanced ESG disclosures by registered funds and investment advisers.
- Modernized rules governing ESG-related fund names.

The common thread that binds these proposals and that guides my work as Commissioner is ensuring investors receive the information they need to make the most informed investment decisions.

We are in the process of reviewing thousands of comments submitted. None of us yet know what the final versions of these rules will look like. We continue to meet with stakeholders and to receive robust public feedback that informs our economic analysis.

To me, the SEC's disclosure framework is most effective when investors benefit from objective, quantitative metrics that provide the highest degree of comparability. I believe the proposed rules are a significant step forward in getting investors this information. I look forward to working to ensure that the final rules are as robust as possible.

The SEC proposed these rules prior to my swearing in. Had I been a Commissioner at the time, I would have voted in favor of them.

Which brings me to the first of the SEC's disclosure initiatives, on climate. Last year, for the first time, the U.S. Financial Stability Oversight Council identified climate change as an "emerging and increasing threat to U.S. financial stability."

A recent climate risk assessment from the Office of Management and Budget found that the U.S. government will need to spend an additional $25 billion to $128 billion annually for policies to mitigate climate-related financial risks. And, an analysis by the Network for Greening the Financial System estimated that, under current policy pathways, climate change could reduce U.S. GDP by 3 to 10 percent by the end of this century.

It is thus not surprising that there's been strong investor demand for climate-related disclosures. Investors with $130 trillion in assets under management have requested that companies disclose their climate risks. And 5,000-plus signatories to the UN Principles for Responsible Investment—a group with a core goal of helping investors protect their portfolios from climate-related risks—manage more than $121 trillion as of June 2022.

To read more:
https://www.sec.gov/news/speech/lizarraga-speech-meeting-investor-demand-high-quality-esg-data

Number 7

Progress Report on Climate-Related Disclosures

FSB FINANCIAL STABILITY BOARD

Executive summary

Work to strengthen the comparability, consistency and decision-usefulness of climate-related financial disclosures has moved forward rapidly over the past year.

A milestone has been the publication in March 2022 by the newly established International Sustainability Standards Board (ISSB) under the IFRS Foundation of two Exposure Draft standards, on general sustainability-related and climate-related disclosures, for public consultation with the aim to issue the final standards by early 2023, subject to feedback.

The timely issuance of a final global baseline climate reporting standard, ready for adoption across jurisdictions, is critical to provide decision-useful information to investors and other stakeholders on climate-related risks and opportunities.

Interoperability between the common global baseline and national and regional jurisdictionspecific requirements is essential.

The ISSB standards aim to establish a common global baseline that is interoperable with jurisdictions' frameworks through a building block approach that will drive more comparability and consistency on common climate disclosures across jurisdictions.

This will help avoid harmful fragmentation and unnecessary costs for preparers of disclosures. It can also ensure that disclosures by different firms are made on a common basis, and that users can compare and aggregate exposures across jurisdictions.

Alongside a global baseline reporting standard on climate, there is a growing recognition of the importance of global assurance standards to drive reliability of disclosures.

The International Auditing and Assurance Standards Board (IAASB) is working to develop a new sustainabilityrelated assurance framework and the International Ethics Standards Board for Accountants (IESBA) is

developing sustainability-related ethics and independence standards, in both cases supported by IOSCO.

The FSB's July 2021 Report on Promoting Climate-Related Disclosures had reported that, already, a large majority of FSB jurisdictions had set or planned to set requirements, guidance or expectations for both financial institutions and non-financial corporates.

Since then most FSB jurisdictions have taken additional actions. In particular, several emerging market and developing economies (EMDEs) have taken active steps to incorporate climate-related information in mainstream disclosures.

More broadly, the Task Force on Climate-related Financial Disclosures (TCFD) Recommendations continue to be referenced as the common basis in most FSB jurisdictions, and many jurisdictions have set out specific metrics or guidance that provide additional detail beyond the recommendations.

Steps to improve the reliability of climate-related disclosures by firms are still at an early stage in most jurisdictions.

Looking ahead to the finalisation of ISSB standards, more than half of FSB jurisdictions state that they already have or are putting in place structures and processes to bring the ISSB standards into local requirements, once finalised.

Authorities note a number of challenges to be addressed in the implementation of the ISSB climate standard, such as consistency and comparability of disclosures across jurisdictions and across firms, data availability, proportionality, transition arrangements, and materiality.

This report highlights the findings of the 2022 TCFD Status Report that reports encouraging further progress in companies' disclosure practices across a wide range of types of firms including asset managers and asset owners as well as non-financial companies.

The percentage of companies disclosing information aligned with TCFD Recommendations and the amount of climate-relevant information in such disclosures has increased.

Even with this continued progress, the TCFD remains concerned that not enough companies are disclosing decisionuseful climate-related financial information, which may hinder investors, lenders, and insurance underwriters' efforts to appropriately assess and price climate-related risks.

During the period until the ISSB global baseline standard is agreed and the implementation of that standard across jurisdictions begins to be monitored, there is a continuing need to maintain momentum by monitoring and reporting on progress in firms' climate disclosures.

The FSB therefore requests TCFD to prepare another progress report on firms' disclosures in 2023.

Table of Contents

To read more: https://www.fsb.org/wp-content/uploads/P131022-2.pdf

Number 8

Remarks by FDIC Acting Chairman Martin J. Gruenberg on the American Bankers Association Annual Convention "The Financial Risks of Climate Change"

Thank you very much for giving me the opportunity to speak with you this morning. I particularly want to express my appreciation to Rob Nichols for the invitation.

I would like to share with you some thoughts this morning on a topic that has received considerable attention and is the source of some concern within the banking industry, particularly with smaller institutions – the financial risks associated with climate change, and the impact they may have on the financial system and financial regulation.

Before I begin, there are two points that I want to make clear:

First, the FDIC's core mission is to maintain stability and public confidence in the U.S. financial system. We carry out this mission through responsibilities for deposit insurance, banking supervision, and the orderly resolution of failed banks, including systemically important financial institutions.

Therefore, our role with respect to climate change is centered on the financial risks that climate change may pose to the banking system, and the extent to which those risks impact the FDIC's core mission and responsibilities.

Second, the FDIC is not responsible for climate policy. As such, we will not be involved in determining which firms or sectors financial institutions should do business with. These types of credit allocation decisions are responsibilities of financial institutions.

We want financial institutions to fully consider climate-related financial risks—as they do all other risks—and continue to take a risk-based approach in assessing individual credit and investment decisions.

There are three parts to this speech.

First, a general discussion of the financial risks of climate change.

Second, a section defining with some specificity climate-related financial risk.

And third, a discussion of what the FDIC has been doing in regard to the financial risks of climate change.

Climate Change is a Risk to the Financial System

The financial system has always had severe weather events to contend with and, thus far, the banking industry has handled these events well.

Agricultural banks know well the effects that drought conditions can have on farming communities; banks in the west understand the impacts of wildfires; and coastal banks have long responded to the annual threat of tropical storms and hurricanes.

However, changing climate conditions are bringing with them challenging trends and events, including rising sea levels, increases in the frequency and severity of extreme weather events, and other natural disasters.

These trends challenge the future resiliency of the financial system and, in some circumstances, may pose safety and soundness risks to individual banks.

It is the goal of our work on climate-related financial risk to ensure that the financial system continues to remain resilient despite these rising risks.

Historically, we have viewed financial crises as stemming from developments in the economy or the financial system. In the United States, this was true of the banking crisis of the 1930s, the thrift crisis of the 1980s, and the global financial crisis of 2008.

We have not generally considered sources exogenous to the economic and financial systems as potential causes of financial crises.

However, we have learned from the pandemic that exogenous shocks can have a profound impact on the economy and financial system. In 2020, the Financial Stability Oversight Council (FSOC), made up of the U.S. Treasury and the federal financial regulatory agencies, described COVID-19 as “the biggest external shock to hit the post-war U.S. economy.”

Climate change and the potential responses to limit its effects could also result in exogenous shocks to the banking system.

There is broad consensus among financial regulatory bodies, both domestically and abroad, that the effects of climate change and the transition to reduced reliance on carbon-emitting sources of energy present unique and significant economic and financial risks, and, therefore, an emerging risk to the financial system and the safety and soundness of financial institutions.

The Financial Stability Board (FSB) of the G-20 countries has warned that climate-related risks may also have a profound impact on the stability of the global financial system. In 2020, the FSB stated that "climate-related risks may also affect how the global financial system responds to shocks" and could "amplify credit, liquidity and counterparty risks and challenge financial risk management in ways that are hard to predict."

Last October, the FSOC issued a public report that identified climate change as an emerging threat to the U.S. financial system, stating that "climate change will likely be a source of shocks to the financial system in the years ahead."

Defining Climate-Related Financial Risk

Financial institutions are likely to be affected by both the physical risks and transition risks associated with climate change. Together these are generally referred to as climate-related financial risks.

Physical Risks

Physical risks generally refer to the harm to people and property arising from acute, climate-related events, such as hurricanes, wildfires, floods, and heatwaves, as well as chronic shifts in the climate, including higher average temperatures, changes in precipitation patterns, sea level rise, and ocean acidification.

Transition risks generally refer to stresses to certain financial institutions or sectors arising from the shifts in public investment, consumer and business preference, or technologies associated with a transition toward reduced carbon reliance.

While physical and transition risks are separate and distinct risks faced by the financial system, both may materially increase the risks posed to a financial institution's financial condition.

For example, acute physical risks, such as flooding, hurricanes, wildfires, and droughts, may result in sudden, significant, and recurring damage to properties securing exposures held by financial institutions or may

otherwise disrupt the operations of their business clients. Some of these properties may be properties that financial institutions currently consider to be outside of flood plains or in areas less prone to this type of damage.

Longer-term physical risks, such as rising average temperatures and sea levels may increase the risk to property values and drive migration patterns, which may result in detrimental impacts to household wealth, corporate profitably, local economies and municipalities.

Further, growing physical risk impacts, including their economic costs, may also have an increasing influence on behavior as individuals and businesses prioritize geographic areas less exposed to physical risks.

While current insurance policies may cover some or all of the loss associated with many severe weather events, policies may over time become more expensive or unavailable to cover losses for a particular geographic area or business activity, particularly if faced with increasing severity and frequency of severe weather events.

Additionally, while the U.S. government may provide assistance with the costs associated with many severe weather events, financial institutions should not be wholly dependent on this assistance, whether directly or indirectly.

To read more: https://www.fdic.gov/news/speeches/2022/spoct0322.html

Number 9

31 arrested for stealing cars by hacking keyless tech

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

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

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

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

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

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

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

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

The following authorities took part in the investigation:

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

- Latvia: State Police of Latvia

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

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

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

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

Number 10

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 individual or entity;

- should not be relied on in the 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 regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

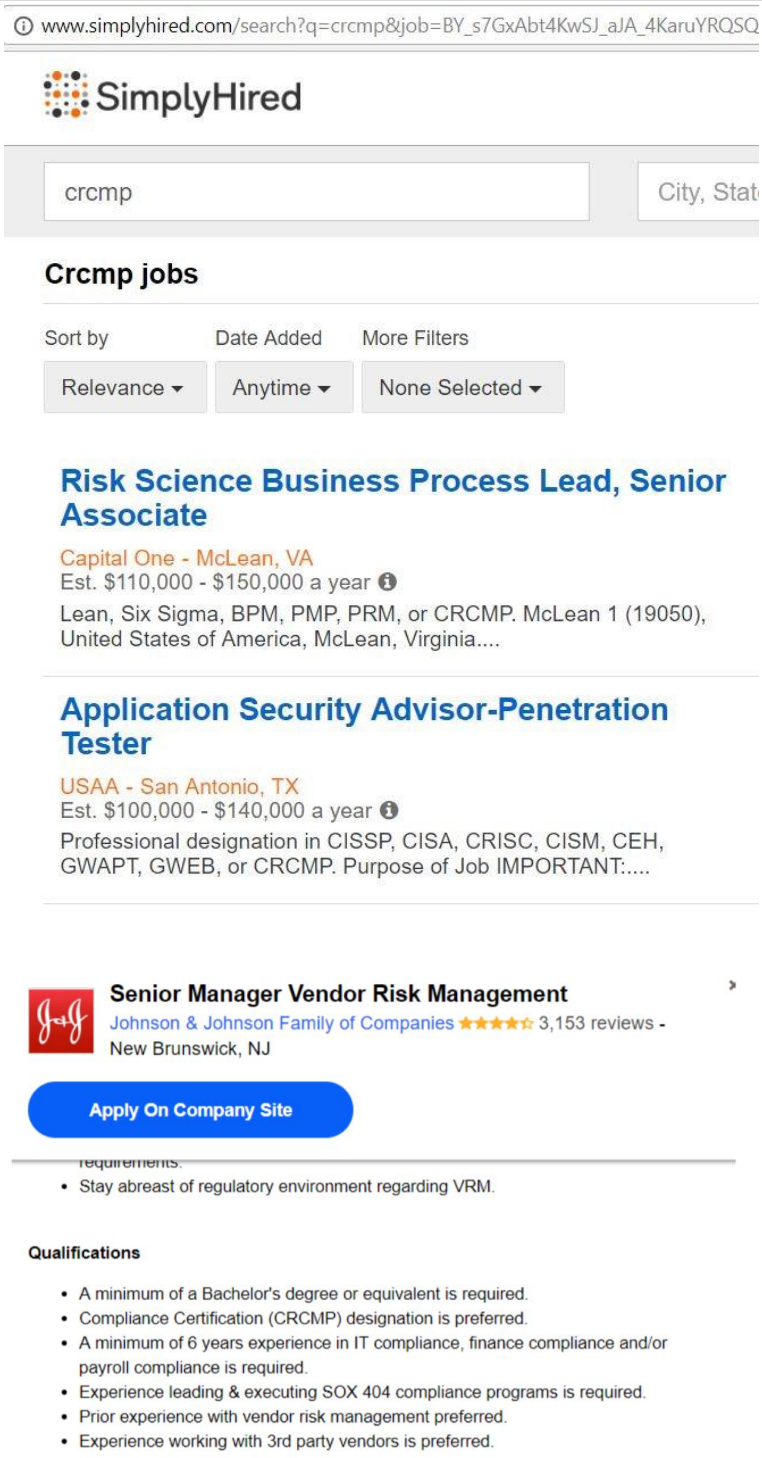
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

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