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, October 2, 2023

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 was reading carefully (again) the DORA regulation of the EU (Regulation 2022/2554 on digital operational resilience for the financial sector). After reading a document, I always try to "feel" what is important. Frequency analysis is a good approach for that.

Well, in 80 pages, the term "third-party" is repeated 366 times.

REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

The term “third-party risk” is repeated 32 times.

According to DORA, *‘ICT third-party risk’* means an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.

According to Article 28, financial entities must manage ICT *third-party risk* as an integral component of ICT risk within their ICT risk management framework.

We have some surprises for third parties. According to Article 31, the European Supervisory Authorities (ESAs) - the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA) – shall designate the ICT third-party service providers that are critical for financial entities, and appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible.

You can easily guess that service providers will have a difficult time, as we have an Oversight Framework (Article 32-35), and the exercise of the powers of the Lead Overseer outside the European Union (Article 36).

The Lead Overseer may exercise the powers referred to in DORA on any premises located in a third-country which is owned, or used in any way, for the purposes of providing services to Union financial entities, by a critical ICT third-party service provider, in connection with its business operations, functions or services, including any administrative, business or operational offices, premises, lands, buildings or other properties.

An ICT third-party service provider established in a third country which has been designated as critical in accordance with DORA, must undertake, within 12 months of such designation, “all necessary arrangements to ensure its incorporation within the Union, by means of establishing a subsidiary”.

The term “third country” is repeated 33 times in the regulation.

You can find more about DORA at:
https://www.digital-operational-resilience-act.com

DORA will apply from 17 January 2025.

Welcome to the Top 10 list.

Best regards,

George Lekatis

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)

CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence

Consumers must receive accurate and specific reasons for credit denials

Number 2 (Page 9)

PCAOB Issues Proposal to Strengthen Accountability for Contributing to Firm Violations

Number 3 (Page 12)

BIS Quarterly Review, September 2023
International banking and financial market developments

Number 4 (Page 15)

EIOPA launches survey on access to cyber insurance by SMEs

Number 5 (Page 17)

SEC Approves Revised Privacy Act Rule

Number 6 (Page 19)

Extreme Weather and Climate Change

Number 7 (Page 22)

Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation

Number 8 (Page 24)

Dive into the Deep Sea: A View of the Subsea Cable Ecosystem

Number 9 (Page 29)

The Ethics of Outsourcing Information Conflict

Outlining the Responsibilities of Government Funders to their Civil Society Partners

Number 10 (Page 33)

New Spin-Squeezing Techniques Let Atoms Work Together for Better Quantum Measurements

Number 1

CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence

Consumers must receive accurate and specific reasons for credit denials

Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau (CFPB) issued guidance about certain legal requirements that lenders must adhere to when using artificial intelligence and other complex models.

The guidance describes how lenders must use specific and accurate reasons when taking adverse actions against consumers.

This means that creditors cannot simply use CFPB sample adverse action forms and checklists if they do not reflect the actual reason for the denial of credit or a change of credit conditions.

This requirement is especially important with the growth of advanced algorithms and personal consumer data in credit underwriting.

Explaining the reasons for adverse actions help improve consumers' chances for future credit, and protect consumers from illegal discrimination.

"Technology marketed as artificial intelligence is expanding the data used for lending decisions, and also growing the list of potential reasons for why credit is denied," said CFPB Director Rohit Chopra. "Creditors must be able to specifically explain their reasons for denial. There is no special exemption for artificial intelligence."

In today's marketplace, creditors are increasingly using complex algorithms, marketed as artificial intelligence, and other predictive decision-making technologies in their underwriting models.

Creditors often feed these complex algorithms with large datasets, sometimes including data that may be harvested from consumer surveillance.

As a result, a consumer may be denied credit for reasons they may not consider particularly relevant to their finances.

Despite the potentially expansive list of reasons for adverse credit actions, some creditors may inappropriately rely on a checklist of reasons provided

in CFPB sample forms. However, the Equal Credit Opportunity Act does not allow creditors to simply conduct check-the-box exercises when delivering notices of adverse action if doing so fails to accurately inform consumers why adverse actions were taken.

In fact, the CFPB has confirmed in a circular from last year, that the Equal Credit Opportunity Act requires creditors to explain the specific reasons for taking adverse actions.

CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms

Companies relying on complex algorithms must provide specific and accurate explanations for denying applications

MAY 26, 2022

You may visit:
https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/

This requirement remains even if those companies use complex algorithms and black-box credit models that make it difficult to identify those reasons. Today's guidance expands on last year's circular by explaining that sample adverse action checklists should not be considered exhaustive, nor do they automatically cover a creditor's legal requirements.

Specifically, today's guidance explains that even for adverse decisions made by complex algorithms, creditors must provide accurate and specific reasons. Generally, creditors cannot state the reasons for adverse actions by pointing to a broad bucket.

For instance, if a creditor decides to lower the limit on a consumer's credit line based on behavioral spending data, the explanation would likely need to provide more details about the specific negative behaviors that led to the reduction beyond a general reason like "purchasing history."

Creditors that simply select the closest factors from the checklist of sample reasons are not in compliance with the law if those reasons do not sufficiently reflect the actual reason for the action taken.
Creditors must disclose the specific reasons, even if consumers may be surprised, upset, or angered to learn their credit applications were being graded on data that may not intuitively relate to their finances.

In addition to today's and last year's circulars, the CFPB has issued an advisory opinion that consumer financial protection law requires lenders to provide adverse action notices to borrowers when changes are made to their existing credit.

CFPB Issues Advisory Opinion on Coverage of Fair Lending Laws

Equal Credit Opportunity Act continues to protect borrowers after they have applied for and received credit

MAY 09, 2022

You may visit:
https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-advisory-opinion-on-coverage-of-fair-lending-laws/

The CFPB has made the intersection of fair lending and technology a priority.

For instance, as the demand for digital, algorithmic scoring of prospective tenants has increased among corporate landlords, the CFPB reminded landlords that prospective tenants must receive adverse action notices when denied housing.

The CFPB also has joined with other federal agencies to issue a proposed rule on automated valuation models, and is actively working to ensure that black-box models do not lead to acts of digital redlining in the mortgage market.

To read more:
https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/

Number 2

PCAOB Issues Proposal to Strengthen Accountability for Contributing to Firm Violations

To better protect investors, the proposal would update a nearly 20-year-old rule to allow the PCAOB to hold associated persons accountable when they negligently, directly, and substantially contribute to firms' violations.

The Public Company Accounting Oversight Board (PCAOB) issued for public comment a proposal to amend PCAOB Rule 3502, Responsibility Not to Knowingly or Recklessly Contribute to Violations. The rule, originally enacted in 2005, governs the liability of associated persons who contribute to registered public accounting firms' violations of the laws, rules, and standards that the PCAOB enforces.

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

1666 K Street NW
Washington, DC 20006

Office: 202-207-9100
Fax: 202-862-8430

www.pcaobus.org

PROPOSED AMENDMENTS TO PCAOB RULE 3502 GOVERNING CONTRIBUTORY LIABILITY

PCAOB Release No. 2023-007
September 19, 2023

PCAOB Rulemaking
Docket Matter No. 053

The proposal:
https://assets.pcaobus.org/pcaob-dev/docs/default-source/rulemaking/053/pcaob-release-no.-2023-007-rule-3502-proposal.pdf?sfvrsn=7d49cc51_9

Through the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley" or the "Act"), Congress established the Board in the wake of a series of high-profile corporate collapses that laid bare auditor misconduct and the need for a new type of oversight of the public accounting industry.[1] As part of its comprehensive, multipronged approach to such oversight, Congress authorized the Board to investigate, bring charges against, and sanction (when appropriate) registered public accounting firms and associated persons[2] thereof for violations of the laws, rules, and standards that Congress charged the Board with enforcing.[3] That enforcement authority covers a wide array of auditor conduct, including negligent conduct.

The deadline for public comment on the proposal is November 3, 2023.

"This proposal is simply updating PCAOB rules to match what investors already expect: that auditors act with reasonable care whenever they are performing their duties – and when an auditor's negligence results in firm violations that can put investors at risk, the PCAOB has tools to hold them accountable," said PCAOB Chair Erica Y. Williams.

Rule 3502's purpose is to enable the Board to hold accountable associated persons of PCAOB-registered firms who directly and substantially contribute to violations committed by registered firms.

Today's proposal better protects investors with two key updates:

1. It strengthens accountability for those who put investors at risk by updating the threshold for liability:

Auditors are already required to exercise reasonable care anytime they perform an audit – and failure to do so constitutes "negligence."

The current Rule 3502, however, only allows auditors to be held liable for firms' violations when they "recklessly" contribute to those violations – which represents a greater departure from the standard of care than negligence.

This means even when a firm commits a violation negligently, an associated person who directly and substantially contributed to the firm's violation can be sanctioned only if the PCAOB shows that the associated person acted recklessly.

The proposal, if adopted, would update Rule 3502's liability standard from recklessness to negligence, aligning it with the same standard of reasonable care auditors are already required to exercise anytime they are executing their professional duties.

Similarly, the U.S. Securities and Exchange Commission already has the ability to bring enforcement actions against associated persons when they negligently cause firm violations.

The proposal maintains the requirement under the current version of Rule 3502 that an associated person must have contributed to the firm's violation both "directly and substantially" in order to be held liable.

2. It clarifies the relationship between the contributory actor and the primary violator:

To be held liable under the current Rule 3502, an associated person who contributes to a firm's violation must be an associated person of that particular firm.

Given the increasing complexity of arrangements among firms and the constantly evolving nature of technology, the proposal clarifies that associated persons of any firm can be held liable as long as their conduct at least negligently, and directly and substantially, contributes to any firm's violation, not just violations by a firm with which they are associated.

Throughout the proposal, the Board requests comments on specific aspects of the proposed amendments. Readers are encouraged to answer the Board's questions, to comment on any aspect of the proposal, and to provide reasoning and relevant data supporting their views.

The public can learn more about submitting comments on PCAOB proposals at the Open for Public Comment page. Learn more about the PCAOB's rulemaking agenda on the PCAOB website.

To read more:
https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-issues-proposal-to-strengthen-accountability-for-contributing-to-firm-violations

Number 3

BIS Quarterly Review, September 2023
International banking and financial market developments

BIS

Resilient risk-taking in financial markets

With the end of the hiking phase in sight, investors focused on macroeconomic developments during the review period, while staying attuned to their policy implications.

Government bond yields rose in advanced economies (AEs), with term structures reflecting increasingly diverse economic outlooks.

Despite a spell of derisking in August, risk-taking was generally resilient, including in emerging market economies (EMEs).

Notable differences marked the evolution of government bond yields in China, the euro area and the United States.

While US long-term yields reached highs not seen since before the Great Financial Crisis, such yields barely rose in the euro area.

These dissimilar paths were driven by inflation-adjusted, ie real, yields consistent with a stronger economic outlook in the US than in the euro area.

As short-term rates rose in the euro area on the back of stubborn inflation, the term structure there inverted further.

Bond yields largely declined in China, amid a faltering recovery from Covid restrictions and monetary policy easing.

US Treasuries were at the centre of heightened market volatility in early August. Yield rises accelerated as investors became more convinced that higher rates were here to stay following better than expected US growth numbers.

In addition, several, almost concurrent announcements fueled investor unease and led to a sell-off: an unexpected increase in the issuance of long-dated bonds by the US government; the greater flexibility in the Bank of Japan's yield curve control policy; and a downgrade of the US sovereign credit rating.

The upward pressure on US yields spilled over to other AE government bond markets. Risky assets held up firmly, but also exhibited some divergence across major economies due to the differing outlooks.

Consistent with developments in core bond markets, stock returns were higher in the US than in the euro area and China.

Likewise, sentiment in corporate credit markets seemed to improve in the US but remained relatively subdued in the euro area. US credit spreads narrowed below historical landmarks and issuance gained some traction.

In contrast, bank lending to firms was still sluggish across jurisdictions. Financial market developments in EMEs reflected a new phase of monetary policy across most jurisdictions as well as external factors.

Short yields fell as the monetary policy stance began to turn, with most central banks pausing rate hikes or implementing cuts.

Risk-taking continued, with higher-yielding currencies attracting capital inflows.

In August, EME spreads and exchange rates also appeared sensitive to the temporary bout of de-risking in AE financial markets: the appreciation of Latin American currencies came to a halt, speculative positions in currency futures declined, and the rise of long-term yields accelerated.

In addition, headwinds seemed to emerge from China's slowdown.

International banking and financial market developments

Special features

To read more: https://www.bis.org/publ/qtrpdf/r_qt2309.pdf

Number 4

EIOPA launches survey on access to cyber insurance by SMEs

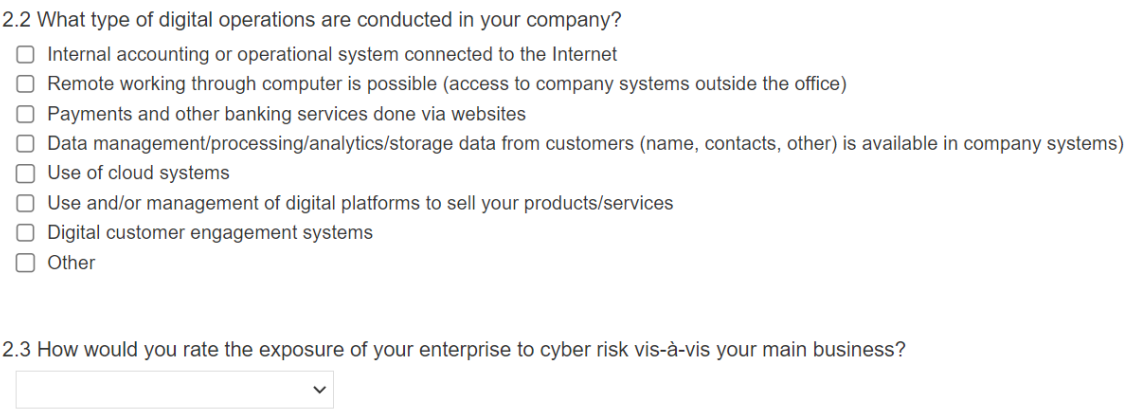
The European Insurance and Occupational Pensions Authority (EIOPA) launched a survey on access to cyber insurance by Small and Medium Enterprises (SMEs) to gain deeper insights into the challenges small businesses face in protecting themselves from cyber risks and to evaluate the level of access to cyber insurance.

Access to (cyber) insurance coverage plays a significant role in mitigating risks stemming from digitalisation by absorbing shocks and managing risks associated with irregular and unpredictable income. Insurance can make SMEs resilient to shocks, also making them more financially sound.

The survey will gather information on the size and type of business of the surveyed enterprises, the level of cyber risk awareness vis-à-vis their business, the availability, affordability, and understanding of cyber insurance products.

It will also shed light on the experience and perceptions of SMEs regarding cyber insurance, including whether they have considered purchasing a policy, the factors that influenced their decision (not) to purchase coverage, and the potential barriers to access.

The survey is available in all 24 official EU languages, and SMEs are invited to take part until 20 March 2024.



The survey:
https://ec.europa.eu/eusurvey/runner/SMESurveyCyberInsurance2023

* 2.4 What are the main cyber risks that your company might face, considering the digital operations (as identified above) it performs?

- ☐ Phishing attempts (Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually performed through email to steal sensitive data or to install malware on the victim's machine)
- ☐ Malware attacks (Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge It is most frequently used to steal personal, financial or business information)
- ☐ Network security breaches (A network security breach is any unauthorized access to a device, network, program, or data. Security breaches happen when network or device security protocols are penetrated or otherwise circumvented)
- ☐ Data breaches (A data breach is a security incident in which malicious insiders or external attackers gain unauthorized access to confidential data or sensitive information such as medical records, financial information or personally identifiable information)
- ☐ Insider data theft, including the leak of clients' personal information (Insider data theft may be due to a malicious employee taking or selling your corporate data or simply making an unintentional mistake)
- ☐ Ransomware (Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid)
- ☐ Attacks through third-party provider (A third-party provider attack is a form of a cyberattack that originates through third party vendors)
- ☐ Denial of Service attacks (A Denial-of-Service attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users)
- ☐ Other

To read more:
https://www.eiopa.europa.eu/eiopa-launches-survey-access-cyber-insurance-smes-2023-09-20_en

Number 5

SEC Approves Revised Privacy Act Rule

The Securities and Exchange Commission approved a rule to revise the Commission's regulations under the Privacy Act, which is the principal law governing the handling of personal information in the federal government.

The rule: https://www.sec.gov/files/rules/final/2023/34-98437.pdf

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: The Securities and Exchange Commission ("Commission" or "SEC") is adopting amendments to the Commission's regulations under the Privacy Act of 1974, as amended ("Privacy Act"). The amendments revise the Commission's regulations under the Privacy Act to clarify, update, and streamline the language of several procedural provisions.

The final rule clarifies, updates, and streamlines the Commission's Privacy Act regulations. In addition, the final rule revises procedural and fee provisions and eliminates unnecessary provisions. The final rule also allows for electronic methods to verify one's identity and submit Privacy Act requests.

"I was pleased to support this adoption because it will update the Commission's rules with respect to this important law," said SEC Chair Gary Gensler. "These amendments will provide more clarity on how the public can access their records maintained by the Commission and request amendments."

The Commission last updated its Privacy Act rules in 2011. The revisions approved today will codify current practices for processing requests made by the public under the Privacy Act. This provides greater clarity regarding the Commission's process for how individuals can access information pertaining to themselves.

Due to the scope of the revisions, the final rule replaces the Commission's current Privacy Act regulations in their entirety.

The final rule is published on SEC.gov and will be published in the Federal Register. The final rule becomes effective 30 days after publication in the Federal Register.

To read more: https://www.sec.gov/news/press-release/2023-189

Number 6

Extreme Weather and Climate Change

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

CISA protects the critical infrastructure from damage caused by extreme weather and promotes resiliency planning and recovery through collaboration and engagement with stakeholders across the country.

Overview

Over the last 50 years, much of the U.S. has seen increases in prolonged periods of excessively high temperatures and an associated expansion of drought. This contributes to larger wildfires burning more acreage per incident, heavier downpours leading to torrential flooding, more intense winter weather events, stronger tropical storms, and a persistent increase in sea level rise across all coasts as baseline temperatures continue to rise.

These shifts from severe weather to more damaging events nation-wide has led to impacts across all 16 critical infrastructure sectors and a growing need to improve resiliency. Extreme weather events have become far more disruptive and destructive than ever recorded and are projected to steadily worsen as global warming progresses.

CISA's Role

It is CISA's mission to ensure critical infrastructure is protected against extreme weather threats and events. Infrastructure built in the 1900s to early 2000s using climate data from the mid-1900s lacks the ability to withstand the changes occurring in both intensity and frequency of extreme weather events and could experience excessive damage or destruction.

CISA analyzes extreme weather and its impacts to critical infrastructure. We discuss potential increases in weather damages with infrastructure owners and operators, conduct exercises centered around damages from major weather events with stakeholders, and develop resiliency focus documents to outline practical guidelines and strategies for implementation.

CISA analyzes and shares current data trends and findings through:

- Weekly summaries on the national-international climate

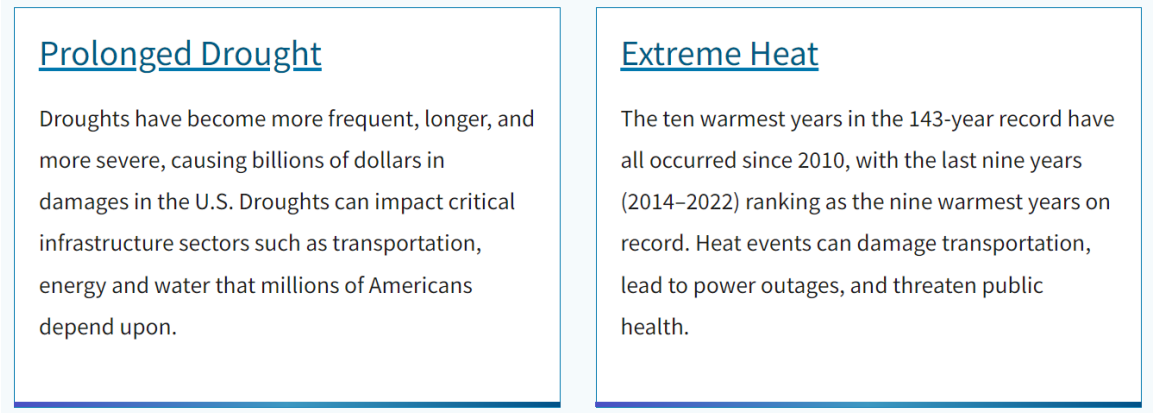
- Presentations about national, regional, state, or infrastructure-related climate shift and the cascading impacts to physical infrastructure, site operations, and community resilience
- Impact analyses of National Critical Functions
- Factsheets to address mitigation options for consideration against climate extremes

Severe Weather vs. Extreme Weather

Severe weather is considered to be an intense variation of a regionally common weather event, such as a heavy rainfall event or damaging winds. Extreme weather identifies the trend of more severe weather events both in frequency and intensity, such as torrential rain (excessive rain periods where over one month of rain can fall during a single storm) or record breaking peak gusts with widespread wind damage.

Extreme weather is the most intense climate element observed during a given period, typically longer lasting or more damaging than the historical 'worst case' events. Infrastructure is built to climatological norms for the 20-40 years prior to development, accounting for typical severe weather events experienced regionally but not planning for withstanding extreme weather events. As climate change continues to amplify extreme weather events, critical infrastructure sites will need to revisit building codes, material limitations, and regional damages during past severe events to address areas at greatest immediate risk.

Extreme Weather Threats



Extreme weather threats are occurrences of unusually severe weather of climate conditions that can cause devastating impacts on communities and agricultural and natural ecosystems. Climate change fuels extreme weather threats.

Wildfires

Over the past 40 years, the average number of acres of forested land consumed by wildfire each year in the United States has increased by 1,000%. Wildfires can disrupt transportation, communications, power and gas services, and water supply.

Extreme Cold

Over the past 40 years, major extreme cold events have caused disasters totaling over $120 billion dollars. Damages from these events were caused by icing, freezing rain, heavy snow, ice storms, freezing spray/fog, and lake effec

Sea Level Rise

Of the 25 most densely populated and rapidly growing U.S. counties, 23 are along a coast facing exposed infrastructure networks, saltwater contamination, immobilization of transportation, grid failures, and prolonged disruption.

Torrential Flooding

Over the past 20 years the US has reported 4x the amount of billion-dollar flood disasters compared to 1980-2000. Large floods can damage assets in nearly all critical infrastructure sectors and can be life threatening.

Tropical Cyclones

Climate amplified tropical cyclones have caused over $1,333 billion in damages since 1980. Winds, hail, and rising waters in a storm path can span numerous states and cause severe damage to critical infrastructure systems.

Severe Storms

Since 1980, severe storms have caused over $383 billion in total damages. As developments in hazardous areas continue and atmospheric instability increases, critical infrastructure sites will see increased damage."

To read more:
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/extreme-weather-and-climate-change

Number 7

Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation

RICHARD BLUMENTHAL
U.S. SENATOR FOR CONNECTICUT

U.S. Senators Richard Blumenthal (D-CT) and Josh Hawley (R-MO), Chair and Ranking Member of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, announced a bipartisan legislative framework to establish guardrails for artificial intelligence.

The framework lays out specific principles for upcoming legislative efforts, including the establishment of an independent oversight body, ensuring legal accountability for harms, defending national security, promoting transparency, and protecting consumers and kids.

The announcement follows multiple hearings in the Subcommittee featuring witness testimony from industry and academic leaders, including OpenAI CEO Sam Altman, Anthropic CEO Dario Amodei, and Microsoft President and Vice Chair Brad Smith who will testify before the Subcommittee on Tuesday.

“This bipartisan framework is a milestone—the first tough, comprehensive legislative blueprint for real, enforceable AI protections. It should put us on a path to addressing the promise and peril AI portends,” said Blumenthal.

“We’ll continue hearings with industry leaders and experts, as well as other conversations and fact finding to build a coalition of support for legislation. License requirements, clear AI identification, accountability, transparency, and strong protections for consumers and kids—such common sense principles are a solid starting point.”

“Congress must act on AI regulation, and these principles should form the backbone,” said Hawley. “Our American families, workers, and national security are on the line. We know what needs to be done—the only question is whether Congress has the willingness to see it through.”

Specifically, the framework would:

Establish a Licensing Regime Administered by an Independent Oversight Body. Companies developing sophisticated general purpose AI models (e.g.,GPT-4) or models used in high risk situations (e.g., facial recognition) should be required to register with an independent oversight body, which would have the authority to audit companies seeking licenses

and cooperating with other enforcers such as state Attorneys General. The entity should also monitor and report on technological developments and economic impacts of AI.

Ensure Legal Accountability for Harms. Congress should require AI companies to be held liable through entity enforcement and private rights of action when their models and systems breach privacy, violate civil rights, or cause other harms such as non-consensual explicit deepfake imagery of real people, production of child sexual abuse material from generative AI, and election interference. Congress should clarify that Section 230 does not apply to AI and ensure enforcers and victims can take companies and perpetrators to court.

Defend National Security and International Competition. Congress should utilize export controls, sanctions, and other legal restrictions to limit the transfer of advanced AI models, hardware, and other equipment to China Russia, other adversary nations, and countries engaged in gross human rights violations.

Promote Transparency. Congress should promote responsibility, due diligence, and consumer redress by requiring transparency from companies. Developers should be required to disclose essential information about training data, limitations, accuracy, and safety of AI models to users and other companies. Users should also have a right to an affirmative notice when they are interacting with an AI model or system, and the new agency should establish a public database to report when significant adverse incidents occur or failures cause harms.

Protect Consumers and Kids. Consumers should have control over how their personal data is used in AI systems and strict limits should be imposed on generating AI involving kids. Companies deploying AI in high-risk or consequential situations should be required to implement safety brakes and give notice when AI is being used to make adverse decisions.

A copy of the bipartisan framework can be found at:
https://www.blumenthal.senate.gov/imo/media/doc/09072023bipartisanaiframework.pdf

To read more:
https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-hawley-announce-bipartisan-framework-on-artificial-intelligence-legislation

Number 8

Dive into the Deep Sea: A View of the Subsea Cable Ecosystem

More than 97% of the world's internet traffic passes through subsea cables at some point. Subsea cables are a vital component of the global internet infrastructure, and it is critical to protect them from cyberattacks, physical attacks and other threats.

What are the challenges?

With the growing reliance on the internet, and the growing amounts of data being transmitted, subsea cable incidents could cause outages and disruptions. The cable landing stations as well as subsea areas, where many cables are close to each other are considered weak points.

The International Cable Protection Committee in its 2022 report concludes that most subsea cable incidents are accidental, due to anchoring and fishing. Some cable incidents are caused by natural phenomena like underwater earthquakes. In rare cases, system failures are responsible for incidents.

Malicious actions such as sabotage attacks and espionage have to be considered also. Particularly, a coordinated sabotage attack on multiple cables at once could cause significant disruptions of internet connectivity. Repairing subsea cables is complex, takes a long time, and requires highly specialised cable repair ships, only few in the world. While eavesdropping on cables on the seabed is considered unlikely, accessing communications data at the cable landing stations or at cable landing points is feasible, and should be considered as a threat.

Global subsea cable ecosystem in a nutshell

- Subsea cables can fall under a wide range of regulatory regimes, laws and authorities. At national level, there may be several authorities involved in their protection, including national telecom authorities, authorities under the NIS Directive, cybersecurity agencies, national coastguard, military, etc.
- There are also international treaties in place to be considered, establishing universal norms and the legal boundaries of the sea,
- On the private sector side, the subsea cable ecosystem consists of undersea cable owners and operators, integrated suppliers, suppliers

without a fleet, owners of installation and repair vessels, and undersea cable maintenance companies.

Key takeaways

- Accidental, unintentional damage through fishing or anchoring has so far been the cause of most subsea cable incidents.
- Natural phenomena such as undersea earthquakes or landslides can have a significant impact, especially in places where there is a high concentration of cables.
- Chokepoints, where many cables are installed close to each other, are single points of failure, where one physical attack could strain the cable repair capacity.
- Physical attacks and cyberattacks should be considered as threats for the subsea cables, the landing points, and the ICT at the landing points.
- There is a lack of information about the resilience, redundancy and capacity of subsea cables and further analysis is needed. The European Commission recently launched a dedicated study for this.
- At a national level, the mandate and supervision over the subsea cables should be clarified, to ensure that the cables and landing points are protected, and that chokepoints are avoided.
- National authorities should exchange good practices about subsea cable protection, involving also authorities for the energy sector, who have experience with protection of subsea power cables, as well as authorities under the Critical Entities Resilience Directive, whose experience with physical protection of critical infrastructure could be insightful.

What are subsea cables?

There are about 400 subsea cables across the world, connecting islands, countries, regions, and continents. Subsea cables use optical fibre technology, transmitting electronic communications data at the speed of light. Subsea cables are about as thick as a garden hose. Subsea cables come on land at landing stations, where they connect to the land-based internet backbone, the underground cables. Landing stations can be at beaches or in ports.

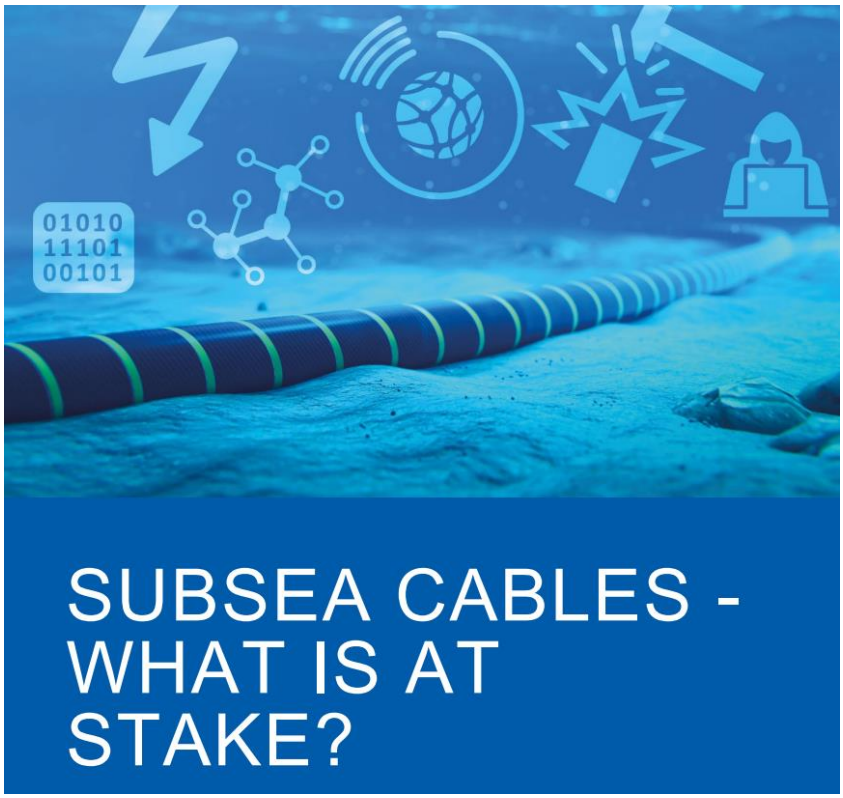
Target audience

ENISA publishes this report to support national authorities in the EU Member States supervising telecom networks and core internet infrastructure, under the European Electronic Communications Code (EECC) and the Directive on measures for a high common level of

cybersecurity across the Union (the NIS1 and the NIS2). Undersea cables are specifically mentioned in the NIS2 directive, and have to be addressed in national cybersecurity strategies.

To read more:
https://www.enisa.europa.eu/news/dive-into-the-deep-sea-a-view-of-the-subsea-cable-ecosystem

SUBSEA CABLES - WHAT IS AT STAKE?



Subsea cables, are some of the most critical components of the global internet infrastructure. Estimates say that more than 97% of the world's internet traffic is transmitted via subsea cables.

Subsea cables are therefore critical for the EU and protecting them from physical and cyber-attacks is strategically important. Modern subsea cables use optical fibre technology to transmit communications data literally at the speed of light.

Close to shore subsea cables are thicker and strengthened with armour, but for most of their length subsea cables have a diameter that is not much greater than that of a garden hose.

Figure 1: Legal boundaries of the ocean *(source: UNCLOS)*

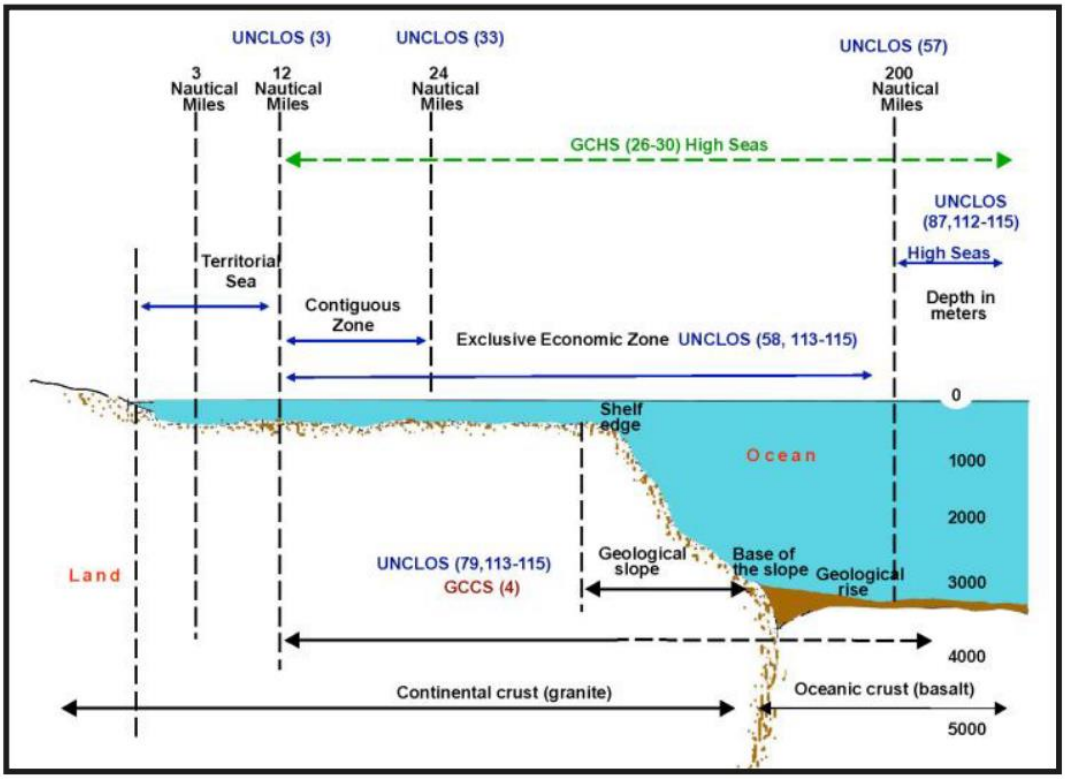
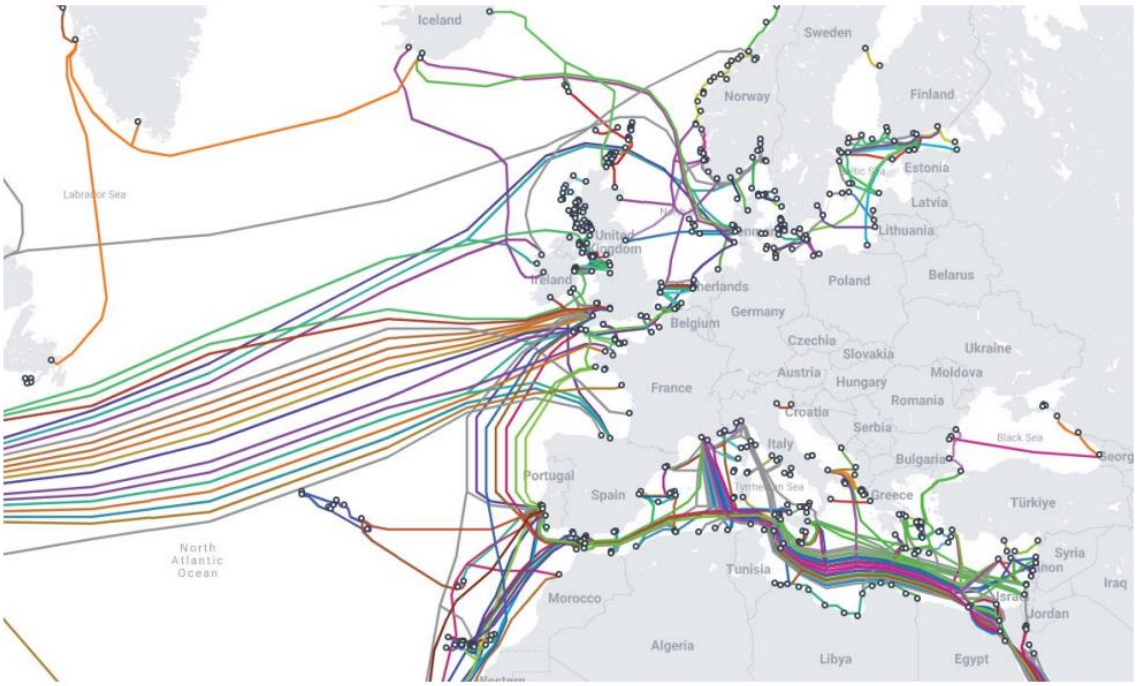


Figure 2: Subsea cable map *(source: SubseaCableMap.org)*



While the number of subsea cables is growing constantly, in 2019 there were more than 378 subsea cables worldwide, spanning more than 1.2 million kilometres.

Subsea cables are covered by national telecom laws, but also by international treaties. In practice, a wide range of different authorities may be involved in the protection of subsea cables, including currently national competent authorities for telecom security, cybersecurity agencies, civil protection, defence, and coast guard.

Although subsea cables can be targets of malicious actions, for instance sabotage attacks, currently, the most common incidents affecting subsea cables have been accidental, unintentional incidents.

Most often the unintentional cable damage is caused by commercial fishing and shipping activities. Sometimes, also natural phenomena can cause cable breaks, for instance underwater earthquakes.

There are about 150-200 accidental, unintentional subsea cable faults every year. The subsea cable landing stations, where the cable surfaces and connects to land-based infrastructure, are located on beaches or in cities, and they can be a weak point.

Cable landing stations can be targeted by attackers, for example, with espionage attacks, deliberate power cuts, sabotage attacks with explosives, or even missile attacks in the case of a military conflict.

Repairing the damage to a subsea cable or to a subsea cable landing station is a complex and difficult, lengthy operation.

Repair is also highly dependent on the availability of specialized and dedicated repair ships, of which there is only a limited number worldwide. In some areas repair may require powerful icebreakers, for instance.

Given the complexity of repair operations and the scarcity of repair capacity, a coordinated attack against multiple subsea cables could have a major impact on global internet connectivity.

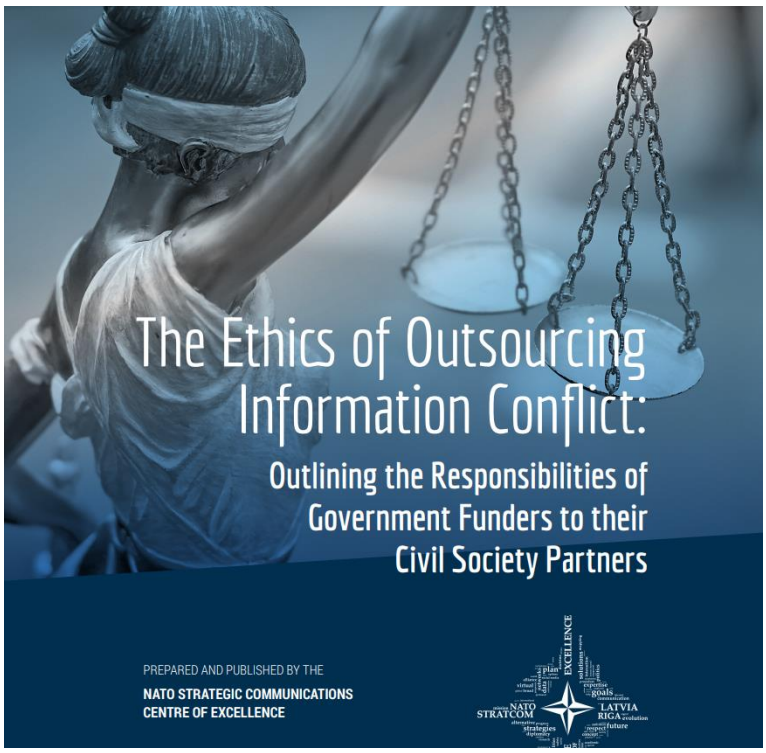
https://www.enisa.europa.eu/publications/undersea-cables

Number 9

The Ethics of Outsourcing Information Conflict

Outlining the Responsibilities of Government Funders to their Civil Society Partners

Non-governmental organisations (NGOs), researchers, journalists, and the private sector are often the main actors actively countering disinformation and influence operations.



While governments maintain some counter-disinformation capabilities, they tend to outsource much of the day-to-day work through, for example, programmatic funding.

It is more cost effective and credible to fund independent, nonpartisan NGOs to debunk disinformation than for a government to get caught up in trying to correct the sensitive issues that disinformation often entails. Indeed, in a recent Washington Post op-ed, former Radio Free Europe / Radio Liberty President Thomas Kent lauds the role of NGOs in countering disinformation and urges governments to keep finding funding for them:

"Volunteer activists fight it out with trolls online, penetrate and disrupt conspiracy chat rooms, campaign for companies to stop advertising on disinformation sites, and post memes ridiculing Russian propaganda."

They do all the things, in other words, that governments can't or won't do at scale. Similarly, journalists play a central role in exposing and countering disinformation, though they are often not directly backed by governments.

Nor are private sector actors such as intelligence firms and social media companies, although the relationship can be close.

Contents

For the purposes of this report, outsourced (operators/agencies) is then best defined as NGOs, researchers, and other actors who receive direct tasking from a government, as opposed to those who participate in countering disinformation for other (personal, commercial, or ideological) motivations.

This report investigates the roles and responsibilities governments assume when they collaborate in areas of information conflict.

In particular, it assesses the risks to civil society and the private sector when they engage in countering hostile foreign influence operations with funding from governments.

What are governments' options and limitations when supporting civilian populations to counter information attacks? To what extent can and should governments outsource these activities? And what are governments'

responsibilities to civil society and the private sector if and when they come under attack by hostile actors?

Conceptually, this report contributes to the field by developing the term information conflict. While disinformation and influence operations are typically the preferred vocabulary for this policy area, both lack a sense of adversarial interaction that characterises the operational realities of countering influence operations.

Information conflict is used to reposition actors engaged in countering disinformation and influence operations as participants in adversarial contestation over questions such as asserting matters of fact and truth, determining the legitimacy of public influence methods, and in the ability to take effective countermeasures.

In practical terms, this report contributes to the field by mapping out a range of adversarial measures that can be taken against non-governmental actors who directly or indirectly support the objectives of governments in information conflict.

This is not a question of connecting influence operations to methods of countering them. It is about the attacks organisations face for participating in information conflict, often designed to remove them from the disinformation-countermeasure dynamic.

It reflects the practical realities of adversarial contestation as it is faced by civil society and the private sector when they take responsibility for engaging adversaries head on.

In addressing several areas of information conflict targeting civilian activities, this report maps out some of the most serious risks and makes recommendations for improving the ways in which civil society is protected.

This includes better understanding of vulnerabilities such as legal and regulatory measures, application of terms of service on tech platforms, hack and leak attacks, political and reputational attacks, and harassment of individuals.

There are at present no international norms or standards governing the responsibilities of governments over the organisations they fund or support in information conflict; this report may be seen as the start of a conversation about what best practice could and should look like.

To read more:

https://stratcomcoe.org/publications/the-ethics-of-outsourcing-information-conflict-outlining-the-responsibilities-of-government-funders-to-their-civil-society-partners/292

Retaliation in information conflict

When conducted by democratic countries, countering disinformation is rarely limited to one actor alone. Invariably, there is some level of collaboration between governments, the private sector, civil society, and research to strengthen the efforts. Often, but not always, a mixture of governments, the private sector, and public interest foundations fund the activities. This gives the impression that information conflict is sometimes outsourced, for example by governments to civil society, or by tech platforms to universities. A key question for this report is, therefore, what level of protection does outsourced information conflict deserve from its funders if and when they are specifically targeted by threat actors with, for example, cyber or intelligence capabilities.

Funding an NGO to participate, or which is participating, in information conflict risks making it appear as a legitimate target to an adversary. If that adversary has state-backed influence, cyber, or intelligence capabilities, the risks are considerable. The purpose of this section is to offer some examples of when participants in information conflict have become targets of adversaries either because of what they were doing, or because of who they were funded by. It raises questions about what levels of protection outsourced information conflict participants should expect from funders, and, more specifically, what the role of government is in protecting democratic societies when motivated and capable adversaries seek to remove civil society actors from the information environment.

Number 10

New Spin-Squeezing Techniques Let Atoms Work Together for Better Quantum Measurements

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Opening new possibilities for quantum sensors, atomic clocks and tests of fundamental physics, JILA researchers have developed new ways of "entangling" or interlinking the properties of large numbers of particles.

In the process they have devised ways to measure large groups of atoms more accurately even in disruptive, noisy environments.

The new techniques are described in a pair of papers published in Nature. JILA is a joint institute of the National Institute of Standards and Technology (NIST) and the University of Colorado Boulder.

"Entanglement is the holy grail of measurement science," said Ana Maria Rey, a theoretical physicist and a JILA and NIST Fellow. "Atoms are the best sensors ever. They're universal. The problem is that they're quantum objects, so they're intrinsically noisy. When you measure them, sometimes they're in one energy state, sometimes they're in another state. When you entangle them, you can manage to cancel the noise."

When atoms are entangled, what happens to one atom affects all the atoms entangled to it. Having dozens — better yet, hundreds — of entangled atoms working together reduces the noise, and the signal from the measurement becomes clearer, more certain.

Entangled atoms also reduce the number of times scientists need to run their measurements, getting results in less time.

One means of entanglement is with a process called spin squeezing. Like all objects that obey the rules of quantum physics, atoms can exist in multiple energy states at once, an ability known as superposition.

Spin squeezing reduces all those possible superposition states in an atom to just a few possibilities. It's like squeezing a balloon.

When you squeeze the balloon, the middle shrinks and the opposite ends become bigger.

When atoms are spin squeezed, the range of possible states they can be in narrows in some directions and expands in others.

But it's harder to entangle atoms that are farther away from each other. Atoms have stronger interactions with atoms that are closest to them; the farther away the atoms, the weaker their interactions.

Think of it like people talking at a crowded party. People closest to each other can have a conversation, but those across the room can barely hear them, and the information gets lost down the line.

Scientists want the whole party of atoms to talk to each other at the same time. Physicists around the world are all looking at different ways to achieve that entanglement.

"A major goal in the community is to produce entangled states to get higher-precision measurements in a shorter amount of time," said Adam Kaufman, a physicist and JILA Fellow.

Kaufman and Rey worked together on proposals to achieve that entanglement, one of which Rey and her collaborators at the University of Innsbruck in Austria demonstrated.

In this experiment, the team lined up 51 calcium ions in a trap and used lasers to induce interactions between them. This is because the laser excites phonons, vibrations sort of like sound waves between the atoms.

Those phonons spread down the line of atoms, linking them together. In prior experiments, these links were engineered to be static, so an ion could only talk to a specific set of ions when illuminated by the lasers.

By adding external magnetic fields, it was possible to make the links dynamic, growing and changing over time. That meant an ion that could talk to only one group of ions at first could talk to a different group, and eventually, it was able to talk to all other ions in the array.

This overcomes that distance problem, Rey says, and the interactions were strong all the way down the line of atoms. Now all the atoms were working together, and they could all talk to each other without losing the message along the way.

Within a short amount of time, the ions became entangled, forming a spin-squeezed state, but with a little more time, they transformed into what's called a cat state.

This state is named for Erwin Schrodinger's famous thought experiment about superposition, in which he proposed that a cat trapped in a box is both alive and dead until the box is opened and its state can be observed.

For atoms, a cat state is a special kind of superposition in which the atoms are in two diametrically opposed states, like up and down, at the same time. Cat states are highly entangled, Rey points out, making them especially great for measurement science.

The next step will be to try this technique with a two-dimensional array of atoms, upping the number of atoms to improve how long they can stay in these entangled states. Additionally, it could potentially let scientists make measurements more precisely and much quicker.

Spin-squeezing entanglement could also benefit optical atomic clocks, which are an important measurement science tool. Kaufman and his group at JILA, along with collaborators in NIST/JILA colleague Jun Ye's group, tested a different method in another study of Nature.

The researchers loaded 140 strontium atoms into an optical lattice, a single plane of light to hold the atoms. They used finely controlled beams of light, called optical tweezers, to place the atoms into little subgroups of 16 to 70 atoms each.

With a high-power ultraviolet laser, they excited the atoms into a superposition of their usual "clock" state and a higher-energy Rydberg state. This technique is called Rydberg dressing.

The clock state atoms are like the quiet people at the crowded party; they don't strongly interact with others. But for atoms in the Rydberg state, the outermost electron is so far from the center of the atom that the atom is effectively very large in size, enabling it to interact more strongly with the other atoms.

Now the whole party is talking. With this spin-squeezing technique, they can create entanglement across the entire array of 70 atoms.

The researchers compared frequency measurements between 70-atom groups and found that this entanglement improved precision below the limit for unentangled particles, known as the standard quantum limit.

Quicker, more precise measurements will allow these clocks to be better sensors to search for dark matter and produce better time and frequency measurements.

To read more:
https://www.nist.gov/news-events/news/2023/09/new-spin-squeezing-techniques-let-atoms-work-together-better-quantum

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,

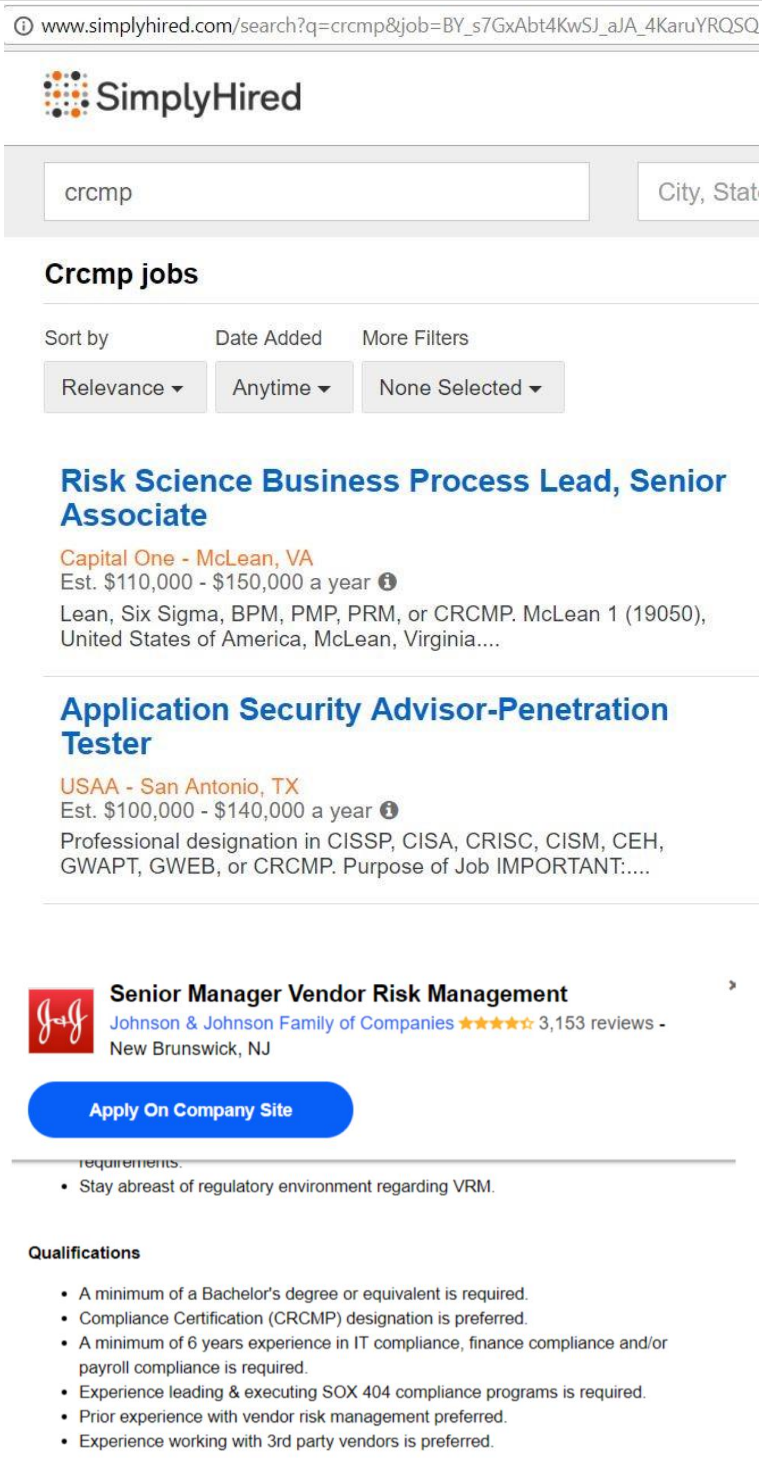
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.