Monday, January 22, 2024

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.

Paracelsus believed that poison is in everything, and no thing is without poison. The dosage makes it either a poison or a remedy.

Well, poison is in everything, even in Artificial Intelligence (AI) systems. According to the US National Institute of Standards and Technology, adversaries can deliberately confuse or even poison AI systems to make them malfunction — and there's no foolproof defense that their developers can employ.

Poisoning attacks occur in the training phase by introducing corrupted data. An example would be slipping numerous instances of inappropriate language into conversation records, so that a chatbot interprets these instances as common enough parlance to use in its own customer interactions.

Evasion attacks, which occur after an AI system is deployed, attempt to alter an input to change how the system responds to it. Examples would include adding markings to stop signs to make an autonomous vehicle misinterpret them as speed limit signs or creating confusing lane markings to make the vehicle veer off the road.

Privacy attacks, which occur during deployment, are attempts to learn sensitive information about the AI or the data it was trained on in order to misuse it. An

adversary can ask a chatbot numerous legitimate questions, and then use the answers to reverse engineer the model so as to find its weak spots — or guess at its sources. Adding undesired examples to those online sources could make the AI behave inappropriately, and making the AI unlearn those specific undesired examples after the fact can be difficult.

Abuse attacks involve the insertion of incorrect information into a source, such as a webpage or online document, that an AI then absorbs. Unlike the aforementioned poisoning attacks, abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source to repurpose the AI system's intended use.

Marcus Tullius Cicero has said: "When you have no basis for an argument, abuse the plaintiff."

Read more at number 7 below. Welcome to 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 5)

Speech by President von der Leyen in memoriam of Jacques Delors

Number 2 (Page 8)

Annual Report

Office of the Comptroller of the Currency

Number 3 (Page 10)

Statement on the Approval of Spot Bitcoin Exchange-Traded Products

Gary Gensler, Chair of the U.S. Securities and Exchange Commission

Number 4 (Page 13)

Draft Implementing Technical Standards specifying certain tasks of collection bodies and certain functionalities of the European single access point under Regulation (EU) 2023/2859

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Number 5 (Page 15)

Testing the cognitive limits of large language models

Fernando Perez-Cruz and Hyun Song Shin

BIS

Number 6 (Page 17)

Pioneering a New National Security

GCHQ

Number 7 (Page 19)

NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

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

Number 8 (Page 22)

Operationalising the Framework for Evaluating Capability against Information Influence Operations

A Case Study of the Psychological Defence Agency's Courses

Number 9 (Page 25)

ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Number 10 (Page 26)

FBI, Human Trafficking Prevention Month

Number 1

Speech by President von der Leyen in memoriam of Jacques Delors

Your Majesties,

Prime Minister, dear Alexander,

President of the European Council,

President of the Senate,

Dear colleagues,

Ladies and Gentlemen,

Tonight, we celebrate the beginning of a new year and the beginning of the Belgian Presidency. But as we celebrate Europe together tonight, I want to pay tribute to a great European to whom we bid farewell this morning: the late Commission President Jacques Delors.

It was right here, in the Palais des Beaux-Arts, that he decided to give his legacy speech, at the very end of his Presidency of the European Commission. It was 30 years ago.

A dark winter night, just like tonight, in the presence of the future King Philippe. And the Bozar tributed him with a never-ending standing ovation. He loved Brussels, and Brussels loved him back.

We all owe so much to Jacques Delors. He turned an economic community into a Union of people and nations. There is a quote by Delors that has accompanied me since the very first day of my mandate. Il a dit : « C'est le moment de donner une âme à l'Europe. »

He said it at the beginning of the 1990s. The fall of the Iron Curtain had created great geopolitical turmoil, but also great hopes that all of Europe could finally unite in peace and democracy. Jacques Delors was the first to understand that – 'we should not only enlarge the Community.

We should unify Europe.' And for this, Europe had to rediscover its soul. We had to go back to our roots, to the founding values of our Union, so that we could craft a way forward.

Ladies and Gentlemen,

Many have and will in the next weeks and days speak of Delors remarkable, very often historic achievements. They will no doubt praise – and rightly so – the countless landmark policies he fathered. From the euro to the Single Market; from Schengen to Erasmus.

They will no doubt applaud – and rightly so – his decisive leadership in making our Union ever fairer, stronger and more integrated. They will no doubt celebrate – and rightly so – the founding architect of the modern European Union. And I will join them – as much and as many times as I can – in both honouring his extraordinary legacy and expressing our deepest gratitude.

But tonight, I also want to look ahead. Tonight, I want not only to speak about all that Jacques Delors has done for us but on how we can take inspiration from him.

Jacques Delors presided the Commission in a period marked by tremendous geopolitical challenges: a horrific war on our continent, a structural reshuffle of the international world order and the profound European aspirations of millions at our borders.

As we face today many of the same challenges, let us take inspiration from what he believed in. Jacques Delors believed in peace.

He knew that an occupation could never result in a just and lasting peace. He had inherited from his father – a gravely and permanently wounded WWI veteran – the unshakable conviction that mutual respect and constructive dialogue must prevail between nations.

Jacques Delors believed in solidarity. He understood – before anyone else – the absolute necessity of enlarging our Union to the East in the immediate aftermath of the fall of the Berlin wall.

He understood – before anyone else – the absolute necessity of ensuring cohesion, equity and just wealth distribution among European peoples. And Jacques Delors believed in Europe.

He trusted our democratic values and traditions. He trusted our way of life, our attachment to fairness and our commitment to freedom to be a unique source of positive influence in the world. And he trusted that we are never as powerful as when we act all together as Europeans, united behind a common purpose.

Ladies and Gentlemen,

The challenges that Delors faced were unique and yet not so distant from those we face today.

In this Belgian Presidency, we will also have to focus on restoring our economic competitiveness, reforming our Union and unifying our continent. So once again, we should take inspiration from Jacques Delors. Whatever the difficulties we face,

however severe they might appear, we should always remember his advice to future generations: « La Grande Europe a son avenir devant elle. N'ayez pas peur, nous y arriverons. »

Ladies and Gentlemen,

At the start of this Belgian Presidency, let us all be inspired by his energy and his faith in Europe. And let me wish you all a great evening here at Bozar.
Thank you and long live Europe.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/speech_24_42

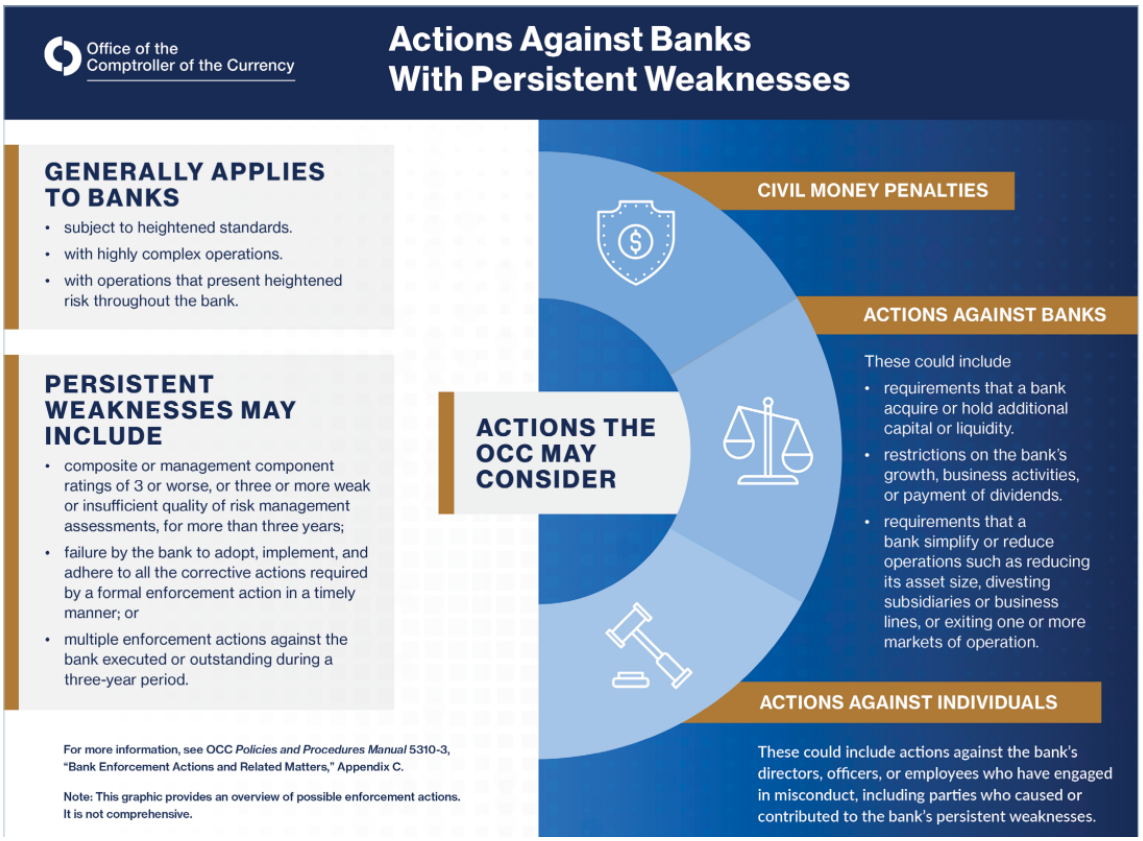
Number 2

Annual Report

Office of the Comptroller of the Currency

The OCC Annual Report provides Congress with an overview of the condition of the federal banking system. The annual report discusses the OCC's strategic priorities and details agency regulatory and policy initiatives. Additionally, the report discusses the agency's financial management and condition, including its audited financial statements.

To read more:
https://www.ots.treas.gov/publications-and-resources/publications/annual-report/files/2023-annual-report.html


Office of the Comptroller of the Currency
Actions Against Banks With Persistent Weaknesses
GENERALLY APPLIES TO BANKS
subject to heightened standards.
with highly complex operations.
with operations that present heightened risk throughout the bank.
PERSISTENT WEAKNESSES MAY INCLUDE
composite or management component ratings of 3 or worse, or three or more weak or insufficient quality of risk management assessments, for more than three years;
failure by the bank to adopt, implement, and adhere to all the corrective actions required by a formal enforcement action in a timely manner; or
multiple enforcement actions against the bank executed or outstanding during a three-year period.
For more information, see OCC Policies and Procedures Manual 5310-3, "Bank Enforcement Actions and Related Matters," Appendix C.
Note: This graphic provides an overview of possible enforcement actions. It is not comprehensive.
ACTIONS THE OCC MAY CONSIDER
CIVIL MONEY PENALTIES
ACTIONS AGAINST BANKS
These could include
requirements that a bank acquire or hold additional capital or liquidity.
restrictions on the bank's growth, business activities, or payment of dividends.
requirements that a bank simplify or reduce operations such as reducing its asset size, divesting subsidiaries or business lines, or exiting one or more markets of operation.
ACTIONS AGAINST INDIVIDUALS
These could include actions against the bank's directors, officers, or employees who have engaged in misconduct, including parties who caused or contributed to the bank's persistent weaknesses.

Number 3

Statement on the Approval of Spot Bitcoin Exchange-Traded Products

Gary Gensler, Chair of the U.S. Securities and Exchange Commission

Today, the Commission approved the listing and trading of a number of spot bitcoin exchange-traded product (ETP) shares.

I have often said that the Commission acts within the law and how the courts interpret the law. Beginning under Chair Jay Clayton in 2018 and through March 2023, the Commission disapproved more than 20 exchange rule filings for spot bitcoin ETPs. One of those filings, made by Grayscale, contemplated the conversion of the Grayscale Bitcoin Trust into an ETP.

We are now faced with a new set of filings similar to those we have disapproved in the past. Circumstances, however, have changed. The U.S. Court of Appeals for the District of Columbia held that the Commission failed to adequately explain its reasoning in disapproving the listing and trading of Grayscale's proposed ETP (the Grayscale Order).

The court therefore vacated the Grayscale Order and remanded the matter to the Commission. Based on these circumstances and those discussed more fully in the approval order, I feel the most sustainable path forward is to approve the listing and trading of these spot bitcoin ETP shares.

The Commission evaluates any rule filing by a national securities exchange based upon whether it is consistent with the Exchange Act and regulations thereunder, including whether it is designed to protect investors and the public interest.

The Commission is merit neutral and does not take a view on particular companies, investments, or the assets underlying an ETP.

If the issuer of a security and the listing exchange comply with the Securities Act, the Exchange Act, and the Commission's rules, that issuer must be provided the same access to our regulated markets as anyone else.

Importantly, today's Commission action is cabined to ETPs holding one non-security commodity, bitcoin.

It should in no way signal the Commission's willingness to approve listing standards for crypto asset securities. Nor does the approval signal anything about the Commission's views as to the status of other crypto assets under the federal securities laws or about the current state of non-compliance of certain crypto asset market participants with the federal securities laws.

As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and thus subject to the federal securities laws.

Investors today can already buy and sell or otherwise gain exposure to bitcoin at a number of brokerage houses, through mutual funds, on national securities exchanges, through peer-to peer payment apps, on non-compliant crypto trading platforms, and, of course, through the Grayscale Bitcoin Trust. Today's action will include certain protections for investors:

First, sponsors of bitcoin ETPs will be required to provide full, fair, and truthful disclosure about the products. Investors in any bitcoin ETP that is listed and traded will benefit from the disclosure included in public registration statements and required periodic filings.

While these disclosures are required, it is important to note that today's action does not endorse the disclosed ETP arrangements, such as custody arrangements.

Second, these products will be listed and traded on registered national securities exchanges. Such regulated exchanges are required to have rules designed to prevent fraud and manipulation, and we will monitor them closely to ensure that they are enforcing those rules.

Furthermore, the Commission will fully investigate any fraud or manipulation in the securities markets, including schemes that use social media platforms.

Such regulated exchanges also have rules designed to address certain conflicts of interest as well as to protect investors and the public interest.

Further, existing rules and standards of conduct will apply to the purchase and sale of the approved ETPs. This includes, for example, Regulation Best Interest when broker-dealers recommend ETPs to retail investors, as well as a fiduciary duty under the Investment Advisers Act for investment advisers.

Today's action does not approve or endorse crypto trading platforms or intermediaries, which, for the most part, are non-compliant with the federal securities laws and often have conflicts of interest.

Third, Commission staff is separately completing the review of registration statements for 10 spot bitcoin ETPs simultaneously, which will help create a level playing field for issuers and promote fairness and competition, benefiting investors and the broader market.

Since 2004, this agency has had experience overseeing spot non-security commodity ETPs, such as those holding certain precious metals. That experience will be valuable in our oversight of spot bitcoin ETP trading.

Though we're merit neutral, I'd note that the underlying assets in the metals ETPs have consumer and industrial uses, while in contrast bitcoin is primarily a

speculative, volatile asset that's also used for illicit activity including ransomware, money laundering, sanction evasion, and terrorist financing.

While we approved the listing and trading of certain spot bitcoin ETP shares today, we did not approve or endorse bitcoin. Investors should remain cautious about the myriad risks associated with bitcoin and products whose value is tied to crypto.

To read more:
https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023

Number 4

Draft Implementing Technical Standards specifying certain tasks of collection bodies and certain functionalities of the European single access point under Regulation (EU) 2023/2859

Regulation (EU) 2023/2859 of the European Parliament and of the Council of 13 December 2023 (hereafter, the ESAP Regulation) mandates ESMA to establish and operate a single access point ("ESAP") by 10 July 2027.

The aim of ESAP is to facilitate access to information already disclosed by companies on the basis of sectoral Directive/Regulation and as such ESAP does not create any additional disclosure obligation.

Reasons for publication

1. Regulation establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability (hereafter, ESAP) tasks the Joint Committee of the European Supervisory Authorities (hereafter, the JC) to develop draft implementing technical standards (ITSs) specifying certain tasks of collection bodies (Article 5) and certain functionalities of ESAP (Article 7).

2. The purpose of this consultation is to provide interested parties with the opportunity to provide their views on the proposed draft ITSs to be submitted to the European Commission.

Respondents to this consultation are encouraged to provide the relevant background information, and qualitative and quantitative data on costs and benefits, as well as concrete redrafting proposals, to support their arguments where alternative ways forward are called for.

If respondents envisage any technical difficulties in implementing the proposed requirements, they are encouraged to provide details regarding the specific technical and operational challenges and specify the costs involved, which are important for the cost-benefit analysis.

Contents

3. Section 4 presents the background to our proposal and questions for consideration. Section 5 includes our proposed draft ITSs. Section 6 includes list of all questions formulated in this consultation.

Next steps

4. The consultation period will run from 8 January 2024 to 8 March 2024.

5. The ESAs will consider the feedback received to this consultation in Q2 and Q3 2024 and should publish a Final Report and the submission of the draft ITS to the European Commission by 10 September 2024.

To read more:
https://www.eba.europa.eu/sites/default/files/2024-01/cb6da797-4254-459e-8037-f74bf7d070f2/ESMA65-11097%20CP%20on%20ITS%20on%20ESAP%20tasks%20of%20collection%20bodies%20and%20ESAP%20functionalities.pdf

Number 5

Testing the cognitive limits of large language models

Fernando Perez-Cruz and Hyun Song Shin

BIS

Key takeaways

1. When posed with a logical puzzle that demands reasoning about the knowledge of others and about counterfactuals, large language models (LLMs) display a distinctive and revealing pattern of failure.

2. The LLM performs flawlessly when presented with the original wording of the puzzle available on the internet but performs poorly when incidental details are changed, suggestive of a lack of true understanding of the underlying logic.

3. Our findings do not detract from the considerable progress in central bank applications of machine learning to data management, macro analysis and regulation/supervision. They do, however, suggest that caution should be exercised in deploying LLMs in contexts that demand rigorous reasoning in economic analysis.

The dazzling virtuosity of large language models (LLMs) has stirred the public imagination.

Generative pretrained transformer (GPT) and similar LLMs have demonstrated an impressive array of capabilities, ranging from generating computer code and images to solving complex mathematical problems.

However, even as users are dazzled by the virtuosity of large language models, a question that often crops up is whether they "know" or "understand" what they are saying, or – as argued by Bender and Koller (2020) – they are merely parroting text that they encountered on the internet during their extensive training routine.

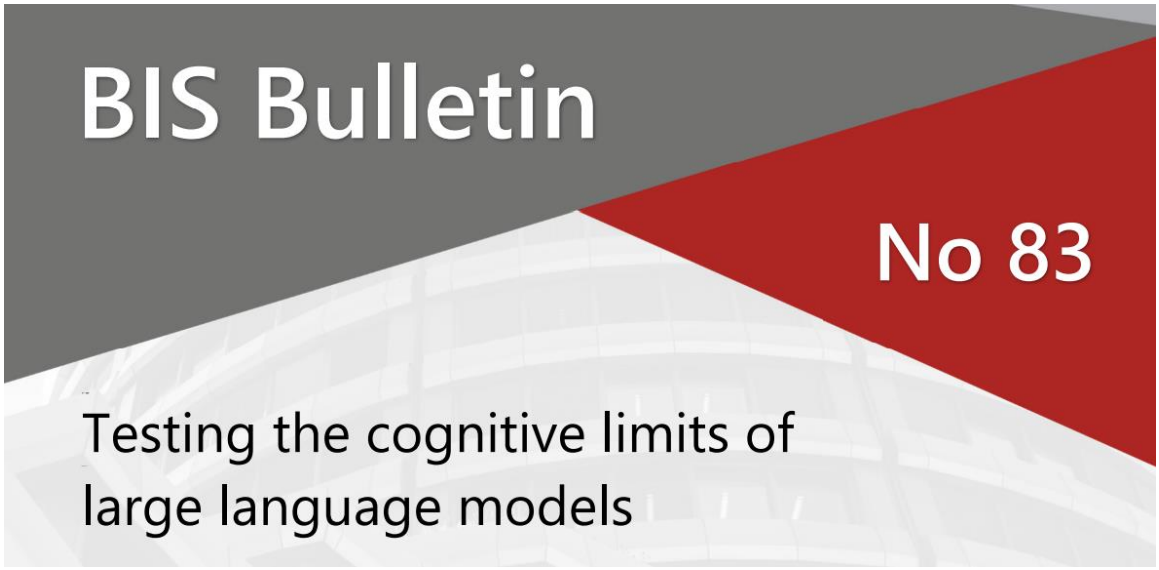
These questions are not only important in terms of the philosophy of knowledge but are likely to be crucial in assessing the eventual economic impact of LLMs.

Devising a test for self-awareness is not easy, but some questions can only be answered through the mastery of reasoning needed for situational awareness. In this spirit, we quizzed GPT-4 (Achiam et al (2023)) with the so-called Cheryl's birthday puzzle.

This is a well-known logic puzzle which went viral in 2015 and has its own Wikipedia page.

Given the extensive online discussion, the latest LLMs will have encountered the puzzle and its solution as part of their extensive corpus of training text.

The solution to the puzzle necessitates reasoning about knowledge (both about one's own knowledge and that of others), as well as sophistication in counterfactual reasoning of the form: "p is false, but if it were true, then q would also be true."



To read more: https://www.bis.org/publ/bisbull83.pdf

https://www.bis.org/publ/bisbull83_annex.pdf

Number 6

Pioneering a New National Security

GCHQ

Britain today is a digital nation, leading and shaping events across a world inextricably linked through cyberspace. Now and into the future, the value of our economy, our way of life, and our global influence will be built on our advanced digital infrastructure, capabilities and knowledge.

Artificial Intelligence – a form of software that can learn to solve problems at a scale and speed impossible for humans – is increasingly essential to the way we live. It is already transforming sectors as diverse as healthcare, telecommunications, and manufacturing.

AI software informs our satnavs, guides our internet searches, and protects us every time we make an electronic purchase, or open an app on our smartphone. In the century since it was founded, GCHQ has been at the forefront of innovation in national security.

Generations of brilliant analysts, with their diverse mix of minds, have used their technical ingenuity, cutting-edge technology and wide-ranging partnerships to identify, analyse and disrupt threats to our nation.

Today, as technological change continues to accelerate, we are pioneering new approaches to understanding the complex and interconnected world around us. We have long championed the responsible use of data science and believe that AI will be at the heart of our organisation's future.

Thinking about AI encourages us to think about ourselves, and what it means to be human: our preferred way of life, our guiding values and our common beliefs.

The field of AI ethics has emerged over the last decade to help organisations turn these ethical principles into practical guidance for software developers – helping to embed our core values within our computers and software.

We won't pretend that there are not challenges ahead of us. In using AI we will strive to minimise and where possible eliminate biases, whether around gender, race, class or religion. We know that individuals pioneering this technology are shaped by their own personal experiences and backgrounds.

Acknowledging this is only the first step – we must go further and draw on a diverse mix of minds to develop, apply and govern our use of AI. Left unmanaged, our use of AI incorporates and reflects the beliefs and assumptions of its creators – AI systems are no better or no worse than the human beings that create them.

Our society is learning and growing: the Alan Turing Institute and similar bodies are helping to show us how we might build and use AI in a more ethical,

responsible manner. GCHQ is committed to creating and using AI in a way that supports fairness, empowerment, transparency and accountability – and to protecting the nation from AI-enabled security threats pursued by our adversaries.

We believe that, by working together with our partners across Britain and beyond, we can deliver this vision.

This paper describes the digital Britain of today, and our values-led approach for the spaces where people, information and technology meet. It lays out GCHQ's AI and Data Ethics Framework, and how we intend to use AI in our operations. It forms part of our commitment to inclusion, debate and openness.

To read more: https://www.gchq.gov.uk/files/GCHQAIPaper.pdf

Number 7

NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

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

1. AI systems can malfunction when exposed to untrustworthy data, and attackers are exploiting this issue.

2. New guidance documents the types of these attacks, along with mitigation approaches.

3. No foolproof method exists as yet for protecting AI from misdirection, and AI developers and users should be wary of any who claim otherwise.

Adversaries can deliberately confuse or even "poison" artificial intelligence (AI) systems to make them malfunction — and there's no foolproof defense that their developers can employ. Computer scientists from the National Institute of Standards and Technology (NIST) and their collaborators identify these and other vulnerabilities of AI and machine learning (ML) in a new publication.

Their work, titled Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (NIST.AI.100-2), is part of NIST's broader effort to support the development of trustworthy AI, and it can help put NIST's AI Risk Management Framework into practice. The publication, a collaboration among government, academia and industry, is intended to help AI developers and users get a handle on the types of attacks they might expect along with approaches to mitigate them — with the understanding that there is no silver bullet.

"We are providing an overview of attack techniques and methodologies that consider all types of AI systems," said NIST computer scientist Apostol Vassilev, one of the publication's authors. "We also describe current mitigation strategies reported in the literature, but these available defenses currently lack robust assurances that they fully mitigate the risks. We are encouraging the community to come up with better defenses."

AI systems have permeated modern society, working in capacities ranging from driving vehicles to helping doctors diagnose illnesses to interacting with customers as online chatbots. To learn to perform these tasks, they are trained on vast quantities of data: An autonomous vehicle might be shown images of highways and streets with road signs, for example, while a chatbot based on a large language model (LLM) might be exposed to records of online conversations. This data helps the AI predict how to respond in a given situation.

One major issue is that the data itself may not be trustworthy. Its sources may be websites and interactions with the public. There are many opportunities for bad actors to corrupt this data — both during an AI system's training period and afterward, while the AI continues to refine its behaviors by interacting with the physical world. This can cause the AI to perform in an undesirable manner.

Chatbots, for example, might learn to respond with abusive or racist language when their guardrails get circumvented by carefully crafted malicious prompts.

"For the most part, software developers need more people to use their product so it can get better with exposure," Vassilev said. "But there is no guarantee the exposure will be good. A chatbot can spew out bad or toxic information when prompted with carefully designed language."

In part because the datasets used to train an AI are far too large for people to successfully monitor and filter, there is no foolproof way as yet to protect AI from misdirection. To assist the developer community, the new report offers an overview of the sorts of attacks its AI products might suffer and corresponding approaches to reduce the damage.

The report considers the four major types of attacks: evasion, poisoning, privacy and abuse attacks. It also classifies them according to multiple criteria such as the attacker's goals and objectives, capabilities, and knowledge.

Evasion attacks, which occur after an AI system is deployed, attempt to alter an input to change how the system responds to it. Examples would include adding markings to stop signs to make an autonomous vehicle misinterpret them as speed limit signs or creating confusing lane markings to make the vehicle veer off the road.

Poisoning attacks occur in the training phase by introducing corrupted data. An example would be slipping numerous instances of inappropriate language into conversation records, so that a chatbot interprets these instances as common enough parlance to use in its own customer interactions.

Privacy attacks, which occur during deployment, are attempts to learn sensitive information about the AI or the data it was trained on in order to misuse it. An adversary can ask a chatbot numerous legitimate questions, and then use the answers to reverse engineer the model so as to find its weak spots — or guess at its sources. Adding undesired examples to those online sources could make the AI behave inappropriately, and making the AI unlearn those specific undesired examples after the fact can be difficult.

Abuse attacks involve the insertion of incorrect information into a source, such as a webpage or online document, that an AI then absorbs. Unlike the aforementioned poisoning attacks, abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source to repurpose the AI system's intended use.

"Most of these attacks are fairly easy to mount and require minimum knowledge of the AI system and limited adversarial capabilities," said co-author Alina Oprea, a professor at Northeastern University. "Poisoning attacks, for example, can be mounted by controlling a few dozen training samples, which would be a very small percentage of the entire training set."

The authors — who also included Robust Intelligence Inc. researchers Alie Fordyce and Hyrum Anderson — break down each of these classes of attacks into subcategories and add approaches for mitigating them, though the publication acknowledges that the defenses AI experts have devised for adversarial attacks thus far are incomplete at best. Awareness of these limitations is important for developers and organizations looking to deploy and use AI technology, Vassilev said.

“Despite the significant progress AI and machine learning have made, these technologies are vulnerable to attacks that can cause spectacular failures with dire consequences,” he said. “There are theoretical problems with securing AI algorithms that simply haven’t been solved yet. If anyone says differently, they are selling snake oil.”

To read more:
https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

Number 8

Operationalising the Framework for Evaluating Capability against Information Influence Operations

A Case Study of the Psychological Defence Agency's Courses

Evaluation is a crucial step in decision-making and strategic planning in most contemporary organisations. This should also be the case for the development of capability in countering information influence operations (IIO).

Different actors, ranging from governments to the private sector, have varying approaches to address these issues, as well as different evaluation norms and standards. However, evaluation of capabilities for countering IIO is a relatively new concept.

IIO capabilities, in a civilian context, include several functions and activities that need to be performed in a coordinated manner, by multiple actors and units, and over different timeframes.

It is therefore not always easy to know what kind of strategy and method should be used for assessment; often it differs depending on what is being assessed, the purpose of the assessment, and for whom it is made.

Still, without evaluating these capabilities an organisation might not use its resources efficiently or might not be working towards the required capability level.

Evaluation is therefore an important and necessary part of quality assurance, and a means for improving the work of the community as a whole.

An initial step was taken in 2022 to establish a common framework for evaluating capability in countering different threats in the information environment through the paper A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence and Foreign Interference written by James Pamment and published by the NATO Strategic Communications Centre of Excellence.

For this follow-up report, we focus on education and training to represent a starting point for applying the framework. Education and training are crucial components in developing a prepared and capable organisation.

The benefits of improving education and training capabilities are scalable across society. These benefits often reach beyond the specific area of focus, as individuals

gain valuable skills and knowledge that can be applied in other areas of their personal and professional lives.

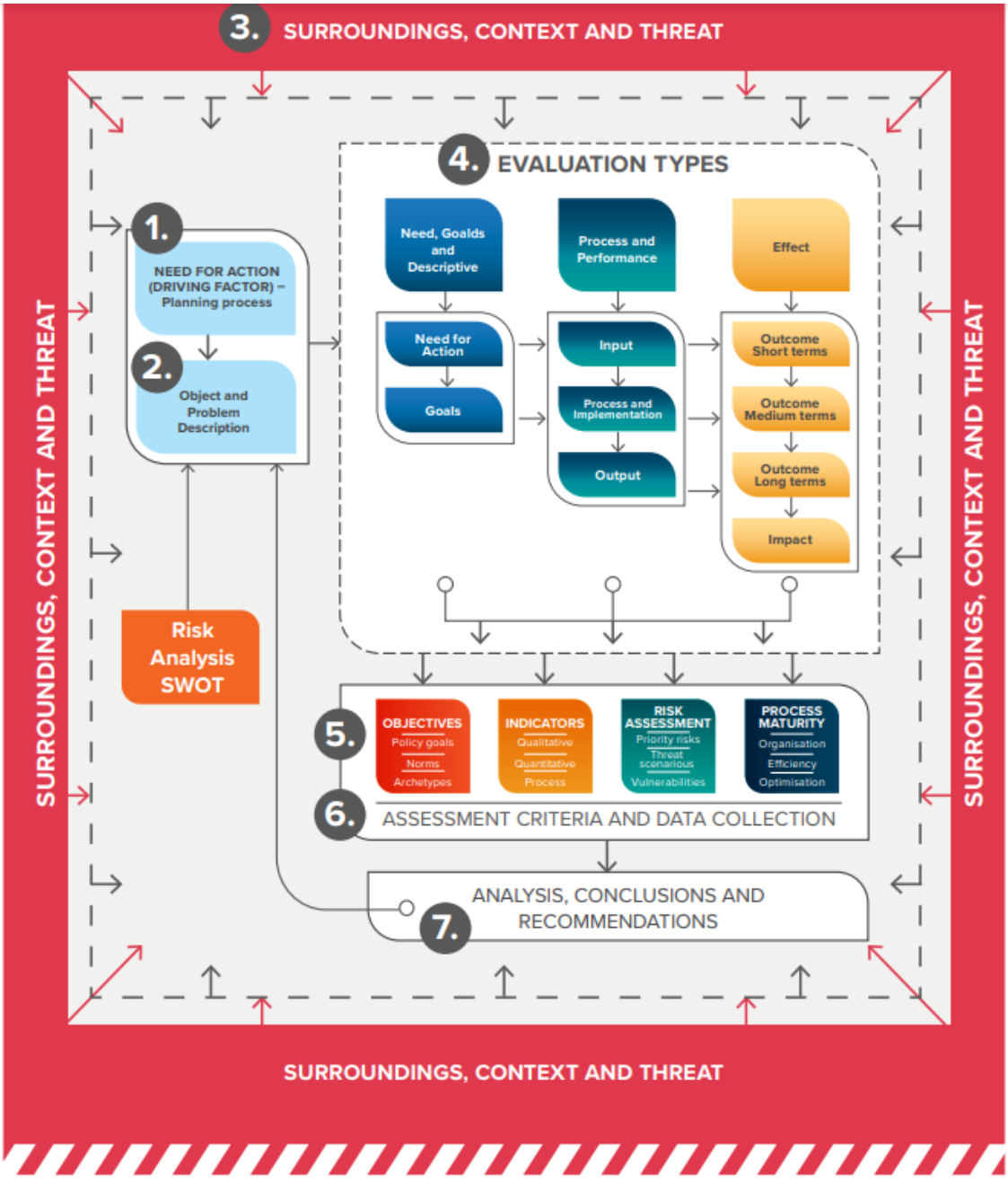


FIGURE 2. An example of an evaluation map that described the basis of evaluation methodology.

Improving education and training in one area of a community or part of the public can have a ripple effect on the entire society, making it a vital component to address.

This report presents an evaluation of the education and course structure of the Swedish Psychological Defence Agency (Myndigheten för psykologiskt försvar, MPF), in effect applying the framework to a concrete example.

The MPF was founded with the main objective of coordinating and developing the advancement of Sweden's psychological defence in partnership with public institutions and other stakeholders in society.

The aim of the report is to offer advice on how to deploy the evaluation methodology using the previous framework and also some best practice guidance on how to use the framework toolset in the evaluation process.

To read more:
https://stratcomcoe.org/publications/operationalising-the-framework-for-evaluating-capability-against-information-influence-operations-a-case-study-of-the-psychological-defence-agencys-courses/295

Number 9

ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA has observed widespread and active exploitation of vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure solutions, hereafter referred to as "affected products."

Successful exploitation of the vulnerabilities in these affected products allows a malicious threat actor to move laterally, perform data exfiltration, and establish persistent system access, resulting in full compromise of target information systems.

CISA has determined these conditions pose an unacceptable risk to Federal Civilian Executive Branch (FCEB) agencies and require emergency action.

This determination is based on widespread exploitation of vulnerabilities by multiple threat actors, the prevalence of the affected products in the federal enterprise, the high potential for a compromise of agency information systems, the impact of a successful compromise, and the complexity of the proposed mitigations.

To read more:
https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities

Number 10

FBI, Human Trafficking Prevention Month

Human trafficking is the illegal exploitation of a person. Anyone can be a victim of human trafficking, and it can occur in any U.S. community—cities, suburbs, and even rural areas. The FBI works human trafficking cases under its Crimes Against Children and Human Trafficking program. We take a trauma informed, victim-centered approach in investigating these cases.

In the United States, both U.S. residents and foreign nationals are being bought and sold like modern-day slaves. Traffickers use violence, manipulation, or false promises of well-paying jobs or romantic relationships to exploit victims. Victims are forced to work as prostitutes or to take jobs as migrant, domestic, restaurant, or factory workers with little or no pay. Human trafficking is a heinous crime that exploits the most vulnerable in society.

Under the human trafficking program, the FBI investigates:

1. Sex trafficking: When individuals are compelled by force, fraud, or coercion to engage in commercial sex acts. Sex trafficking of a minor occurs when the victim is under the age of 18. For cases involving minors, it is not necessary to prove force, fraud, or coercion.

2. Labor trafficking: When individuals are compelled by force, threats, or fraud to perform labor or service.

3. Domestic servitude: When individuals within a household appear to be nannies, housekeepers, or other types of domestic workers, but they are being controlled and exploited.

Human Trafficking Task Forces

The most effective way to investigate human trafficking is through a collaborative, multi-agency approach with our federal, state, local, and tribal partners.

1. FBI Child Exploitation and Human Trafficking Task Forces operate within nearly every FBI field office. The ultimate goal of these task forces is to recover victims and investigate traffickers at the state and federal level.

2. The Anti-Trafficking Coordination Team Initiative builds human trafficking enforcement efforts and enhances access to specialized human trafficking subject matter experts, leads, and intelligence. Each team

develops and implements a strategic action plan, which leads to high-impact federal investigations and prosecutions.

The initiative is a collaborative effort among the FBI, the Department of Justice, Department of Homeland Security, and Department of Labor. Twelve FBI field offices participate in the initiative, including Atlanta, Boston, Cleveland, El Paso, Kansas City, Los Angeles, Memphis, Miami, Minneapolis, Newark, Portland, and Sacramento.

3. The Enhanced Collaborative Model Human Trafficking Program is a multi-agency task force initiative funded through the Department of Justice's Office for Victims of Crime and Bureau of Justice Assistance.

   This program supports the development and enhancement of multi-disciplinary human trafficking task forces that implement collaborative approaches to combat all forms of human trafficking.

   These multi-disciplinary task forces include members from the U.S. Attorney's Office, local prosecutor's office, federal law enforcement, state/local law enforcement, and a community service provider, with the goal of proactively identifying and recovering victims of human trafficking.

To read more: https://www.fbi.gov/investigate/violent-crime/human-trafficking

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.

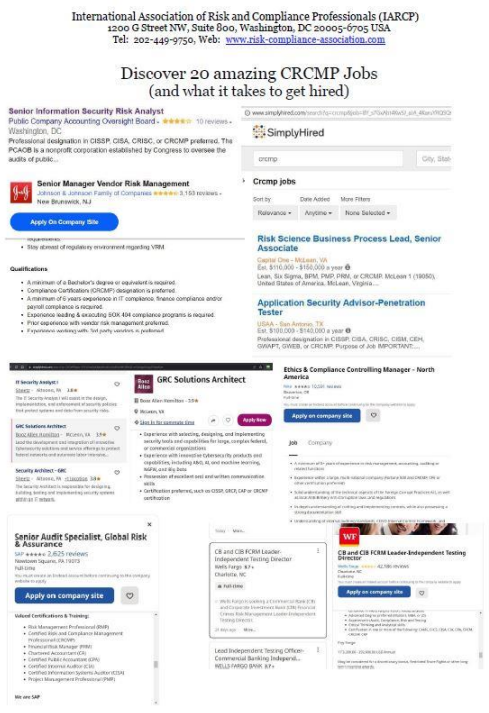
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

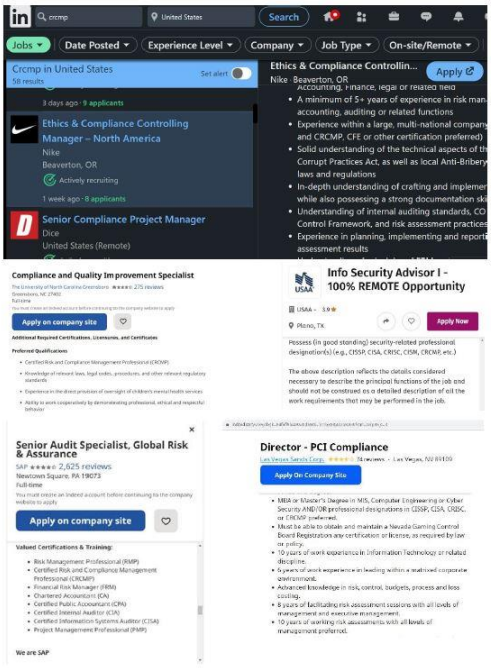
Our training and certification programs:

1. 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

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 57 countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

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





2. 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

3. 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

4. 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

5. 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

The International Association of Risk and Compliance Professionals (IARCP) is a business unit of Compliance LLC, incorporated in Wilmington NC and offices in Washington DC, a provider of risk and compliance training and executive coaching in 57 countries. To learn more: https://www.risk-compliance-association.com/Privacy.htm

You may contact:

Lyn Spooner
Email: lyn@risk-compliance-association.com

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