INCYBER FORUM

EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Programme

IN CYBER FORUM
EUROPE

Ready for AI ?

THEME 2024

Ready for AI ?

Reinventing cybersecurity in the age of AI

INCYBER FORUM

EUROPE

Between dystopian fantasy and techno-bliss, it is hard to determine where artificial intelligence (AI) will lead humanity. One thing is certain: nothing will ever be the same again.

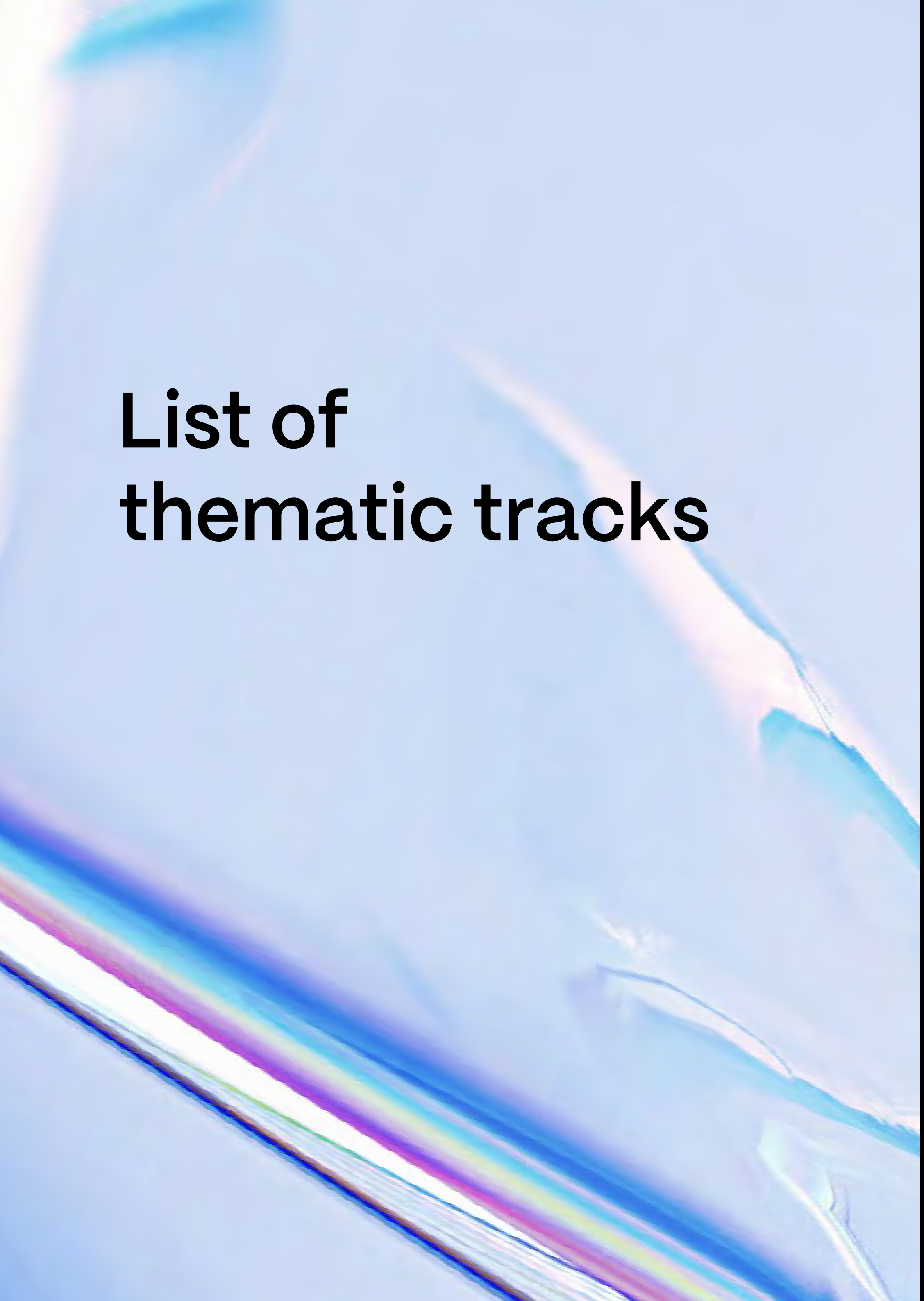
Our professional activities, our personal lives, our ways of thinking, of deciding, of acting, of consuming, of producing, of caring for ourselves, are all going to be permanently disrupted. But tomorrow's world will depend above all on what we collectively decide to do - or not to do - with artificial intelligence, and on the "trust" we manage to build “in” and “through” these technologies.

To be “trusted”, AI must, according to the European Commission, respect 7 principles, including technical robustness and security, respect for privacy and data governance. The widespread use of these technologies will introduce new risks, not only because of the increased attack surface, but also because of their intrinsic vulnerabilities (poisoning attacks, adversarial attacks, etc).

As technological progress is ambivalent by nature, AI is also used by attackers all along the “kill chain” to recognize a target, bypass protection mechanisms, build “deep fakes”, automate an attack and so on.

The first challenge is therefore to secure not only artificial intelligence, but also the data it absorbs and produces. Data and artificial intelligence are inextricably linked. And the figures are staggering: every second, 7 megabytes of data are created for each person, resulting in a global quantity of data that will reach 181 zettabytes in 2025, compared with 2 zettabytes in 2010.

Fortunately, AI is also revolutionizing the “art” of cybersecurity, enabling us to improve our authentication, data security, threat detection, code analysis, orchestration, incident response and other capabilities. A technological leap that should also lead us to radically reinvent our policies, organizations and skills, so that they are “AI - ready”.



List of thematic tracks

→ OPENING SUMMIT

Is Europe ready for AI?

→ PLENARY SESSIONS

Reinventing cybersecurity in the age of AI

Digital revolution and geopolitical upheaval:
is Europe still in the race?

AI in a quest for trust

Cyber Shield: the challenge of solidarity

→ ROUND TABLES

- Fight Against Cybercrime
- Cyber Risk Management
- Data Safety and Digital Transformation
- Security and Stability in Cyberspace
- Digital Sovereignty
- Operational Security

IN CYBER
FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Opening summit

Is Europe ready for AI?

4:00 PM to 7:00 PM on March 26TH

INCYBER FORUM

EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Plenary Sessions

D2

March 27

8:45 to 11:15 AM

Reinventing cybersecurity in the age of AI

Around 50% of organizations say they are already using AI. Yet we are only at the beginning of a revolution that is set to have a lasting impact on humanity. Given its role in securing digital uses and creating trust in a world that is increasingly digitalized, remote, and complex for users, cybersecurity must be at the core of this revolution. How can it reinvent itself to meet these new challenges? How do we keep AI models cyber-secure, given they will increasingly be the target of attackers? How do we defend against attacks as they become increasingly sophisticated and rapid because attackers are using these same technologies? What are the potential impacts and new threats associated with the rise of generative AIs that specialize in generating code? Finally, how can we leverage artificial intelligence to strengthen collective cybersecurity, in particular to reinforce and automate our defenses and turn AI into a formidable shield? Against a backdrop of long-term skills shortages, will these technologies bring about the "democratization" of cybersecurity through automation?

D2

March 27

4:45 to 7:00 PM

Digital revolution and geopolitical upheaval: is Europe still in the race?

The emergence of artificial intelligence will radically change global geopolitics. Given the economic and industrial—not to mention political and military—advantages AI brings, governments are in a frantic race to develop this technology. So much so that Elon Musk tweeted in 2017: “Competition for AI superiority at national level [is the] most likely cause of World War 3”. Where does Europe—currently outpaced by the US and China—stand in this race? Or will these technologies reshuffle the deck, upending the business models that have made GAFAM (Google, Apple, Amazon, and Microsoft) and BATX (Baidu, Alibaba, Tencent, and Xiaomi) so successful? In terms of technology, is the development of “Edge AI”, with execution as close as possible to local data, an opportunity? In the age of AI, what new power levers can we use to support our strategy? How do we tap into the formidable pool of skills available to us? What industrial policy should be developed to support European ambitions? As an inherently stabilizing power, can the European Union turn the concept of trusted AI into a global opportunity?

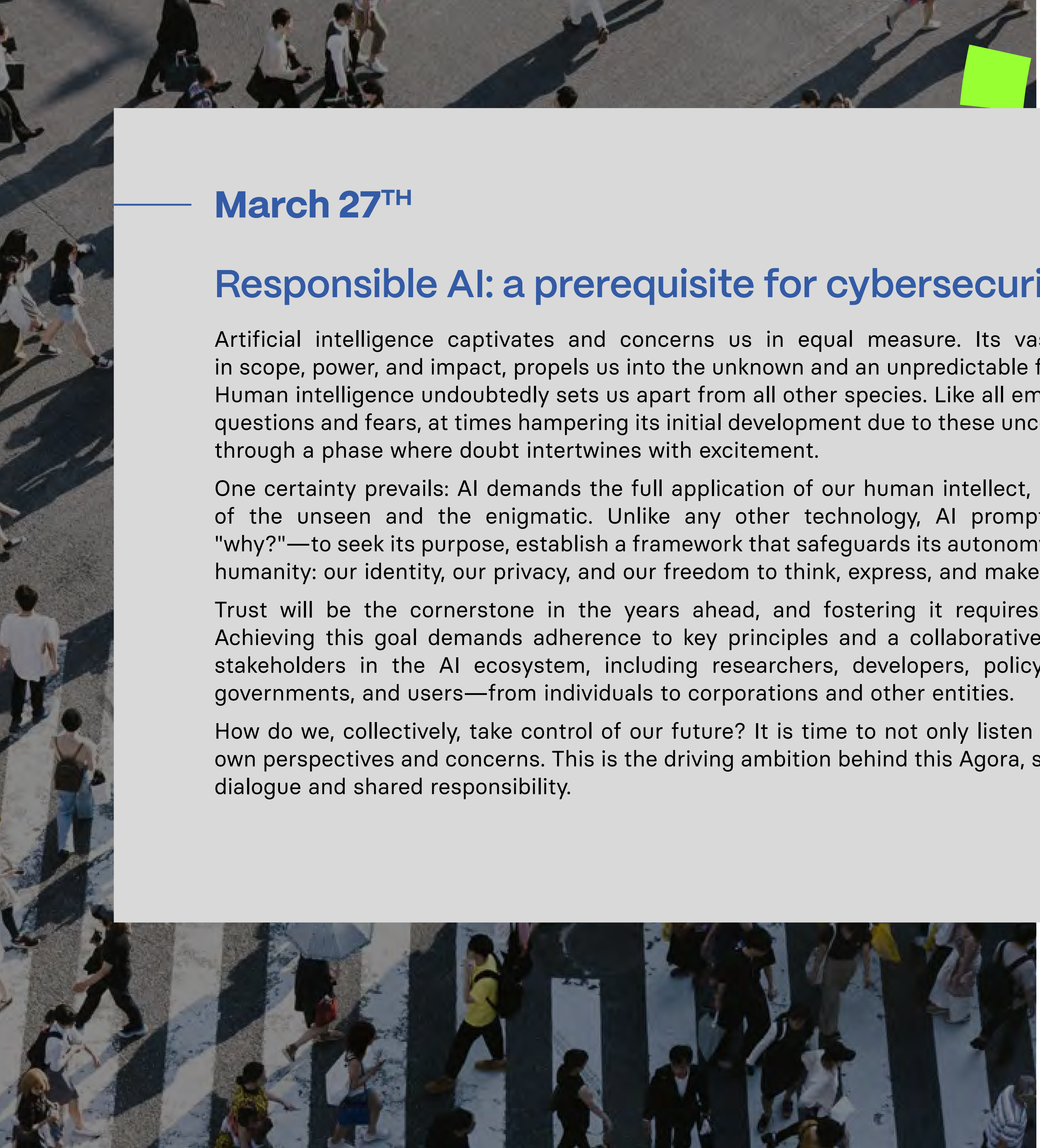
D3

March 28

9:00 to 11:00 AM

AI in a quest for trust

Trust is the key to the adoption and appropriation of technology, especially when it comes to artificial intelligence. Deep learning and neural networks make it impossible for the average person to understand the mechanisms used and the results produced by the machine. We therefore need to “objectify” a “trusted AI” with clear, precise criteria. The AI Act, issued by the European Commission and adopted in June 2023, defines it as legal, ethical, robust, and secure. But are these criteria sufficient? Conversely, do they risk hampering innovation? Can trust in these technologies extend to decision-making using systems that will be autonomous in the future? What are the limits to this trust, particularly in terms of ideological bias and compatibility with our personal and private data? Surely the advent of AI, on its own, will end up eroding trust? Or can AI help to strengthen trust in digital technology through its many uses in cybersecurity? Finally, on a practical level, how can we measure trust in a way that is accessible to the general public? Will we be able to certify it?



March 27TH

Responsible AI: a prerequisite for cybersecurity

Artificial intelligence captivates and concerns us in equal measure. Its vast potential, still largely untapped in scope, power, and impact, propels us into the unknown and an unpredictable future ripe with endless possibilities. Human intelligence undoubtedly sets us apart from all other species. Like all emerging technologies, AI has sparked questions and fears, at times hampering its initial development due to these uncertainties. Currently, AI is navigating through a phase where doubt intertwines with excitement.

One certainty prevails: AI demands the full application of our human intellect, challenging us to penetrate the veil of the unseen and the enigmatic. Unlike any other technology, AI prompts us to explore the fundamental "why?"—to seek its purpose, establish a framework that safeguards its autonomy, all while preserving the core of our humanity: our identity, our privacy, and our freedom to think, express, and make decisions.

Trust will be the cornerstone in the years ahead, and fostering it requires a commitment to responsible AI. Achieving this goal demands adherence to key principles and a collaborative effort. This effort should unite all stakeholders in the AI ecosystem, including researchers, developers, policy makers, academics, civil society, governments, and users—from individuals to corporations and other entities.

How do we, collectively, take control of our future? It is time to not only listen to the experts but also to voice our own perspectives and concerns. This is the driving ambition behind this Agora, signaling a call to action for inclusive dialogue and shared responsibility.

agora
INCYBER FORUM

IN CYBER
FORUM
EUROPE

26–28 MARCH 2024
LILLE GRAND PALAIS

Fight Against Cybercrime

ROUND TABLES

International cooperation: the key to a secure digital future in the fight against cybercrime?

International cooperation between police forces and judicial authorities is gathering pace in the fight against cybercrime. This is reflected in the many international operations already under way. However, discussions at the UN on the Convention on Cybercrime are getting bogged down, revealing a divide in understanding what constitutes a cyber threat. As a result, cyber diplomacy is facing setbacks, not least because of fundamental disagreements over the meaning of "responsible" when it comes to how governments should behave in cyberspace. What recent progress has been made under the Budapest Convention? What were the outcomes of the anti-ransomware conference organized by the US in October 2022? What has Europol achieved in its operations? What are the results and limits of Interpol's global strategy?

How to harness AI in digital investigations?

The digital revolution has radically transformed the investigative landscape, adding a never-before-seen digital dimension and an unparalleled volume of data. AI has a real opportunity to become the investigator's ally in collecting, indexing, and analyzing this data. What changes can investigators expect in this new digital landscape? How can investigators make sure they are "AI ready"? How can decisions made by AI systems be squared with ethical and legal standards? How can we ensure that AI-assisted investigations remain transparent and accountable?

AI-powered scams

Deep fake, deep voice, and vishing: just three of the growing number of new phishing techniques that use AI to create lifelike text, voices, images, and digital characters. The result is virtually undetectable phishing scams. Gartner estimates that, by the end of 2023, 20% of all phishing attacks will use AI tools. How do we protect ourselves from them? What organizational processes do we need to put in place? What solutions are available to combat these attacks?

Capture devices: how do we regulate one of the most intrusive investigative technologies?

Firmly in the realm of fantasy fiction for most people, “spyware” has in fact become the only possible tool available to government agencies when communication encryption masks key elements of their investigations. However, the Pegasus scandal highlighted the extremely negative impact of this type of software when used without safeguards. A specially constituted committee of the European Parliament recently set out to assess the risks of using spyware and subsequently issued a series of recommendations to the European Commission. But what role should member states play in this debate? Should they take up the issue and contribute to the EU initiative—risking a tightening up of the rules governing the use of capture—or should they adopt a more cautious stance, emphasizing the need for “national security”, synonymous with the status quo? Could cross-disciplinary work (vulnerability researchers, telecoms security specialists, systems engineers, etc.) define an effective system that also safeguards privacy?

IN CYBER
FORUM
EUROPE

26–28 MARCH
2024

LILLE GRAND PALAIS

Cyber Risk Management

ROUND TABLES

How do we continuously assess and validate your level of security?

To keep pace with constantly evolving risks and guarantee the highest possible level of security, it is crucial to continuously assess our exposure to threats. Security validation is a set of techniques, processes, and tools that identify how attackers might exploit detected vulnerabilities. With the challenges of multicloud, edge computing, and the software supply chain, the attack surface continues to grow in complexity and scope. This is where Continuous Threat Exposure Management (CTEM) programs come into their own. How do we implement a unified security validation platform that combines elements such as external attack surface management, breach and attack simulation (BAS), and automated penetration testing? How could this integration improve our ability to anticipate and counter threats? What contribution can AI make to continuous assessment?

CISOs: time to tweak your operating model!

Reviewing the CISO's cybersecurity operating model can help us see cyber risk more as a business risk than just a technical problem that needs to be solved. This means adjusting the cybersecurity framework to measure and correlate security activities with business priorities and results. How can cybersecurity be strategically integrated into corporate objectives to better protect assets and reputation? How do we anticipate threats and align cybersecurity efforts with business challenges for better overall risk management?

Wanted: resilient AI for mission-critical systems

AI is often seen as an advantage in terms of overall resilience because we can use it to automate certain tasks. But when it is used to enhance mission-critical systems, they can become weak points. How do we ensure that AI failures will not compromise mission-critical systems? What are the formulas and best practices for creating resilient AIs that can adapt to unforeseen situations and keep running smoothly even in the event of critical incidents? How do we increase the robustness, reliability, and transparency of AI algorithms to meet resilience requirements in strategic areas such as healthcare, security, and critical infrastructure?

From haute couture to ready-to-wear: what kind of cybersecurity is right for SMEs?

"*We need to move from haute couture to ready-to-wear*," said Vincent Strubel, ANSSI's Director General, at the opening of the InCyber Forum 2023. Making cybersecurity more widely accessible, particularly to SMEs, is a crucial issue, especially as these companies are often vulnerable to malicious attacks due to limited resources and a lack of specialized skills. Artificial intelligence can play a key role in meeting this need, providing an affordable solution to bolster security in SMEs by automating certain tasks and bridging the gap in cybersecurity skills. What specific functionalities can it provide to protect SMEs effectively against online threats? What practical solutions can we put in place to combat phishing by securing email systems, for example? Is it possible to create an AI-based "virtual CISO" for SMEs, automating the management of their IT security?

How do we assess and "standardize" AI safety?

AI safety assessment and standardization are crucial issues in a world that is becoming increasingly dependent on AI. How do we effectively assess the risks associated with using AI, such as biases or technical vulnerabilities? What standardized criteria and processes should we put in place to guarantee the safe development and deployment of AI? How should existing standards (e.g. ISO 27001 and ISO 9001) be adapted to keep pace with the growth of AI?

Moving toward a "cybersecurity super oracle" AI: what role will CISOs play in the future?

The advent of artificial intelligence (AI) is radically changing the traditional CISO role. This technological revolution brings with it both unprecedented potential and considerable challenges for security professionals. By leveraging the potential of real-time analysis of massive volumes of data, AI can more effectively predict malicious behavior and vulnerabilities, improving a CISO's ability to respond to security incidents. How is AI transforming the role of CISOs in companies? Will it support them or replace them? Might we see the development of a multimodal "cybersecurity super oracle" LLM in the near future?

How do we manage NIS 2 compliance and maintain it over time?

Expanding the scope of NIS 2 to include more business sectors will help raise the level of cybersecurity in Europe and bring about a significant paradigm shift. While threats are focused on vulnerabilities way down the chain, the digitalization of supply chains is opening up security holes. One of the aims of the NIS 2 directive is therefore to improve cybersecurity among supply chain operators and thereby limit the risk of rebound attacks.

What measures do the organizations affected need to take? What are the consequences of non-compliance with NIS 2 rules? How should supply chain and value chain incidents be managed? How do we ensure long-term compliance?

Preserving the integrity of your supply chains in the era of NIS 2

The NIS 2 DIrective focuses on enhancing the security of supply chain actors, such as digital service providers, to mitigate the risks of compromise. NIS 2 often mandates continuous supervision and mandatory reporting of significant incidents by third parties. How to detect and mitigate risks related to the supply chain? What is the appropriate way to manage the security of these 'third parties,' using solutions such as scoring or auditing? What will be the impact of NIS 2 in this regard? How to ensure regulatory compliance and data protection when they are managed by third parties, whether they are cloud service providers or subcontractors?

INCYBER FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Data Safety and Digital Transformation

ROUND TABLES

Immutable backups: the ultimate solution?

With ransomware attacks on backups on the rise, secure storage is becoming increasingly important. Backups are more than just a second copy of data: you need to be able to restore them quickly when needed, to ensure data efficiency and durability. Three quarters of organizations lose at least some of their backups during attacks. How do we make these backups immutable? How do we protect them against attacks? How do we adapt in the near future to a situation where there is more data than storage capacity? Immutable storage won't be so immutable anymore.

Are EDR, XDR, and MDR miracle solutions for hospitals?

Medical equipment is often vulnerable and practically impossible to update. To keep them running, it is essential to constantly analyze network and endpoint activity, to be able to detect and react instantly. This is why hospitals have invested heavily in EDR and XDR software, along with MDR solutions and services. But questions still persist, such has how XDR technologies complement the services provided by SIEM technologies and the SOC.

When equipment has no built-in security, how do we use AI to monitor IT networks, detect malicious behavior, and prevent potential intrusions? Can it guarantee business continuity? How can collaboration between healthcare facilities, medical equipment manufacturers, and cybersecurity solution providers strengthen the protection of vulnerable equipment?

Responsibility and legality: how do you deal with data leaks?

At a time when data leaks are rife on the web, many companies are turning to Internet-based information leak investigations. The aim of these is to detect data leaks as early as possible. Ultimately, they can be used to warn customers and highlight potential data leaks.
How do we demonstrate that information leak investigations are necessary to achieve the desired objective? How can companies be sure they are operating within a legal framework when using such data? Is anonymization a potential solution? Should we review the law and change our practices?

IN CYBER
FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Security and Stability in Cyberspace

ROUND TABLES

Artificial intelligence: the race for regulation

A global race to set the rules for artificial intelligence (AI) is well under way. Governments and international organizations are trying to strike a tricky balance between technological innovation and the need to regulate this disruptive breakthrough. While the EU is taking a pioneering stance with strict legislation, the US favors empowering private-sector companies through non-binding directives and investment in innovation. The UK, while aspiring to become a global AI regulator, is taking a lighter approach, focusing on broad principles rather than strict controls. China, meanwhile, plans to regulate AI products with mandatory pre-market assessments. How will AI regulation affect business innovation and competitiveness in different geographical areas? How does global competition strike the right balance between innovation and legislative constraints?

Autonomous weapons: what are the regulatory implications?

The armed forces of several countries are already using algorithms to make decisions and plan military strategies, including the use of autonomous drones in counter-terrorism operations. However, these developments raise legal, ethical, and security concerns. To move forward in the debate on the use of AI in military operations, there is a need for further independent discussion that leads to agreement. Although there is no consensus on a universal ban on lethal autonomous weapon systems (LAWS), reaching such an agreement could help set new standards for appropriate actions. This would keep the proliferation of these technologies under control and lead to the gradual introduction of new practices in the military field. Many questions and issues relating to military autonomy currently remain unanswered. The unregulated nature of these technologies gives governments developing them the opportunity to influence combat practices. What initiatives has the UN taken to regulate autonomous systems? What are the prospects for further debate and potential regulation? Could too much regulation hinder technological progress?

After war, what are the conditions for digital peace?

In a complex geopolitical landscape, digital infrastructure is increasingly vulnerable to attack, as Dimitri Medvedev's threat to destroy enemy undersea cables after the destruction of the Nord Stream pipeline demonstrates. These kinds of threats call for careful consideration of the measures needed to protect what some refer to as the "public heart" of the Internet, even though it is not actually public. This also raises the question of the Paris Appeal and its role in protecting digital infrastructure and promoting collaboration between states. Will digital infrastructure be targeted more frequently in the future? What are the solutions for protecting this "public heart"?

INCYBER
FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Digital Sovereignty

ROUND TABLES

How can AI safety be assessed and "standardized"?

The assessment and standardization of AI safety are critical issues in an increasingly AI-dependent world. How can we effectively evaluate the risks associated with AI usage, such as biases or technical vulnerabilities? What standardized criteria and processes should be established to ensure secure development and deployment of AI? How can we ensure that standardization does not hinder innovation? To what extent should existing standards (e.g., 27001, 9001) be adapted to the growing development of AI? Isn't standardization also a matter of sovereignty?

Data spaces: European revenge?

Europe is struggling to compete with the US in the cloud, but it could regain a form of digital sovereignty by developing shared data spaces between its main economic sectors (banking, finance, etc.). How might a legal framework, such as the Data Act, facilitate and secure this resource sharing? Could these shared data spaces be the key to strengthening Europe's position on the global digital stage? How could European companies and governments work together to create these shared data infrastructures and manage them effectively? What challenges, benefits, and limitations would this entail for security, privacy, and digital innovation in Europe?

AI and cybersecurity: how do we develop and "hybridize" skills?

AI has been making inroads into the cybersecurity sector for many years, and research in these two disciplines has resulted in some exciting product convergences. Bringing together these two already scarce and valuable areas of expertise is essential if we are to develop effective machine learning models for cybersecurity. Yet experts, engineers, developers, and architects with these dual sets of skills are in short supply. This shortage is closely linked to the lack of training courses combining the two disciplines and to the resources we allocate to them. How do we develop the skills of cybersecurity professionals in the age of AI? How do we encourage interdisciplinary collaboration between AI and cybersecurity experts to create robust solutions to deal with today's cyber threats?

INCYBER FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Operational Security

ROUND TABLES

Penetration testing at AI speed?

Penetration testing that harnesses the power of artificial intelligence is a major step forward in the cybersecurity sector. These assessments use the advanced capabilities of AI to automate and accelerate the identification of vulnerabilities and intrusion attempts in IT systems. By leveraging techniques such as source code analysis, configuration error detection, and the creation of targeted attacks, AI can quickly pinpoint weak points and simulate realistic attack scenarios. However, it is important to note that AI-based penetration testing is not a solution in itself. It needs to be integrated into a comprehensive cybersecurity strategy and combined with other protective measures, continuous monitoring, and proactive risk management. Furthermore, data confidentiality and ethical considerations must serve as a compass for the responsible use of AI in penetration testing, to avoid compromising security and privacy.

How does the use of AI in penetration testing affect the way attack tactics and defense countermeasures evolve? How might attackers themselves exploit AI to circumvent AI-based defenses?

SOC automation: how far do we go?

The growing trend toward automating Security Operations Centers (SOCs) raises fundamental questions about how far it should go and what role artificial intelligence should play within SOC solutions, including Security Information and Event Management (SIEM) systems, User and Entity Behavior Analytics (UEBA), and Security Orchestration, Automation and Response (SOAR) tools. This technological revolution calls for a radical rethink of the organizational structures and skills required to maintain robust cybersecurity. However, one key question remains: what role should humans play in this automated ecosystem? While AI can speed up threat detection and incident response, is human expertise still irreplaceable for interpreting, anticipating, and making ethical decisions?

AI-based code production and analysis: a revolution?

The long-awaited arrival of artificial intelligence (AI) in code analysis (API testing, unit testing, user interface testing, etc.) and, with its “generative” variants, in code production, is revolutionizing programming and software development. This convergence opens up innovative opportunities for automating and perfecting processes linked to creating, inspecting, and optimizing source code, and to interacting with user interfaces. AI, leveraging techniques such as machine learning and natural language processing, can not only identify potential problems in code, but can also suggest solutions, thereby increasing development efficiency and quality. However, this shift raises questions about how reliable the choices made by AI are, about the balance between human skills and AI capabilities, and about the ethical dilemmas surrounding automation in a field as crucial as programming. Ultimately, the growing adoption of AI is undeniably driving a major transformation in the way we approach software development, creating an opportunity to redefine industry standards and practices.

The challenge of public-private partnerships at local level

Attacks on local authorities are on the rise, with damaging consequences for essential services such as managing public records and distributing social benefits. It is therefore striking to discover that, in 2022, only 29% of local authorities with between 3,500 and 10,000 inhabitants had an Information Systems Security Officer (ISSO).

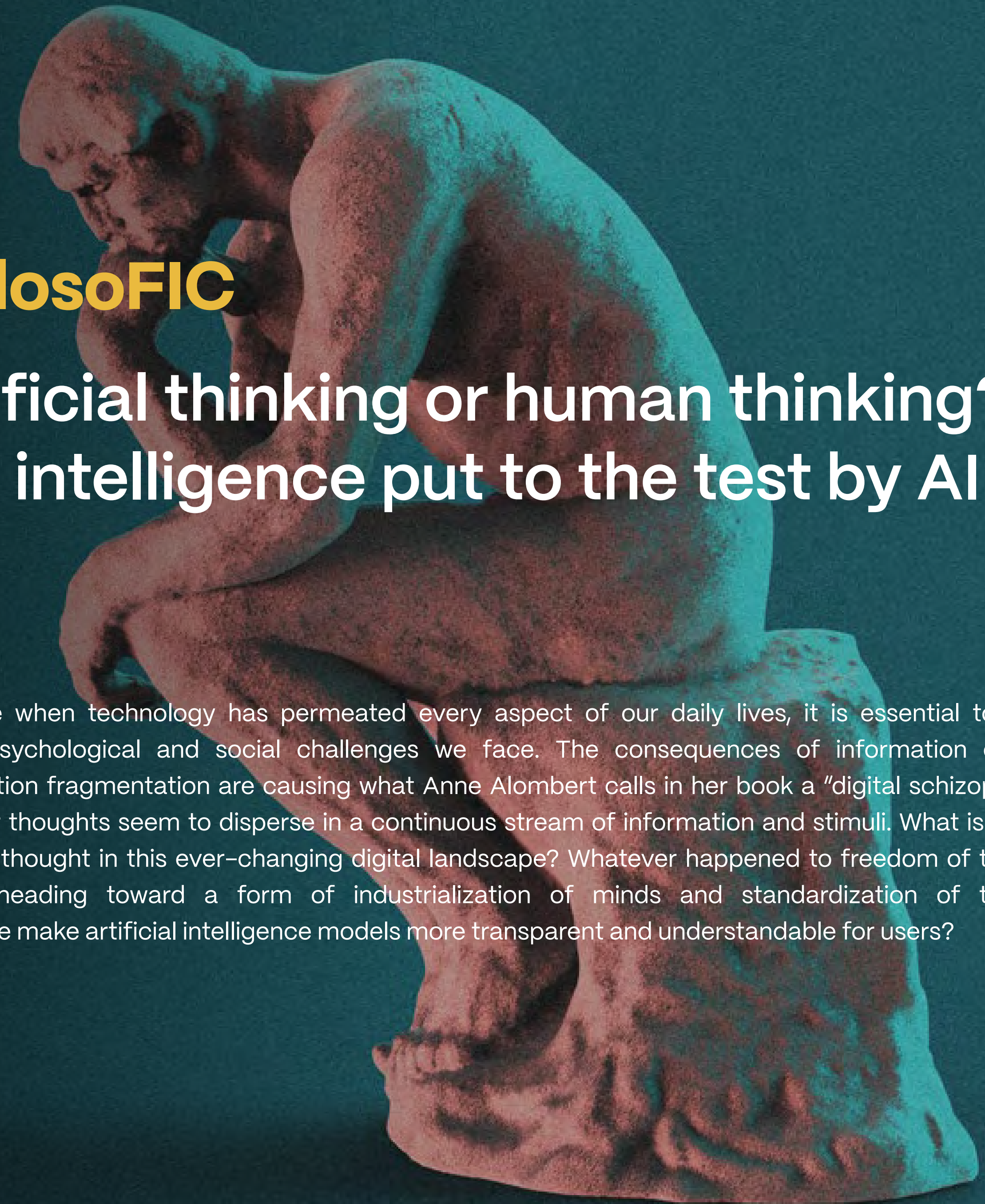
A proactive response to this growing—and primarily local—threat has emerged with the creation of Cyber Campuses and Computer Security Incident Response Teams (CSIRTs) at the regional level. However, the adoption of these regional CSIRTs varies considerably from one region to another. How should collaboration between the national Cybermalveillance service, the regional Cyber Campuses and the various CSIRTs be structured? Is it possible to pool resources to help smaller communities benefit from the expertise and financial resources of larger organizations? How should local authorities adapt to NIS 2 requirements? How can we help them choose the most effective and trustworthy technological solutions and service providers, while bearing in mind their specific constraints?

What technical solutions do we need to secure AI?

AI models are vulnerable to adversarial attacks, spoofing, data poisoning, injection of malicious code, exfiltration, and reverse engineering. A rigorous process for selecting and managing training data is essential to protect AI, prevent bias, and guarantee the quality of the resulting models. At the same time, prioritizing bias preventions requires ongoing monitoring and the implementation of mitigation strategies. The security of AI data, whether through encryption or restricted access management, is crucial to prevent any disclosure of sensitive information. It is also essential to ensure that we protect models against hostile attacks and keep them up to date with the latest security patches. How do we defend against these attacks? How do we fix vulnerabilities and secure these models? What role can “federated learning” play without jeopardizing the confidentiality and protection of collected data? What are the challenges and benefits of regularly updating AI models with security patches?

AI reinvents the foundations of CTI

Cyber threat intelligence (CTI) provides organizations with an in-depth understanding of potential threats by collecting, analyzing, and interpreting information about bad actors. By using CTI to anticipate threats, organizations can take preventive measures and improve their incident response capabilities. AI can automate much of the CTI data analysis process. This frees up experts to focus on the more complex and strategic aspects of security. Human skills are still essential to interpret results correctly and assess real risks. False positives—errors where a non-existent vulnerability is reported—can occur due to the complexity of systems and AI not always fully understanding the context. AI also requires a significant amount of training data to be effective, which can pose challenges in terms of data confidentiality and availability. How do we take a step-by-step approach, starting with identifying useful data? How do we continually train and adapt AI models to keep pace with the changing tactics and techniques used by cybercriminals? How can we guarantee seamless collaboration between cyber threat intelligence and operational security teams?



PhilosoFIC

Artificial thinking or human thinking? Our intelligence put to the test by AI

In an age when technology has permeated every aspect of our daily lives, it is essential to reflect on the psychological and social challenges we face. The consequences of information overload and attention fragmentation are causing what Anne Alombert calls in her book a "digital schizophrenia," where our thoughts seem to disperse in a continuous stream of information and stimuli. What is the true nature of thought in this ever-changing digital landscape? Whatever happened to freedom of thought? Are we heading toward a form of industrialization of minds and standardization of thought? How do we make artificial intelligence models more transparent and understandable for users?

IN CYBER
FORUM
EUROPE

26-28 MARCH 2024

LILLE GRAND PALAIS

Contacts

partnerships

partenariat@forum-incyber.com

programme

programme@forum-incyber.com