IN CYBER FORUM EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Prospective Scenarios

SYSTEMIC CRASH

We are in 2030

IN CYBER FORUM EUROPE

THE STARTING POINT

SOCIAL ACCEPTANCE

The integration of artificial intelligence (AI) into society has become a norm, governed by rigorous European regulations.

TECHNOLOGICAL PROGRESS

Moore's Law remains relevant, generating ever more powerful computing capacities in ever smaller volumes.

USE OF AI IN THE FINANCIAL SECTOR

AI is being put to good use in a number of areas, most notably by financial institutions, which have managed to significantly reduce their costs and increase their profits through its use. Stock and commodities markets are now dominated by institutions that use AI to manage their transactions. These automated systems search continuously (24/7) for up-to-date information, whether positive or negative signals concerning the economic activities of a company, sector or country, in order to assess the potential impact on demand for a commodity and autonomously trigger buying or selling operations before other market players can react.

CYBERSECURITY

Cybersecurity is controlled by a few large non-European companies, and in this sector, a single supplier is often favored. Unfortunately, attack methods against the financial system have developed as rapidly as AI applications. Malware such as FraudGPT and WormGPT is readily available on the dark web and poses a significant threat.

SYSTEMIC CRASH

What if...

IN CYBER FORUM EUROPE

CYBERATTACK

BACKGROUND

Since 2023, we have become accustomed to increasingly sophisticated attacks employing artificial intelligence to analyze the profiles of targeted individuals on social networks and to orchestrate large-scale social engineering attacks, with the aim of stealing funds.

CURRENT SITUATION IN 2030

Several financial institutions have been alerted to a problem affecting their AI-automated trading platform. It is reported that the AI system has undergone unauthorized modifications (via a backdoor), triggering a cascade of sales transactions. Infrastructures dependent on ultra-fast AI and very high-speed connections are particularly vulnerable: if one AI system fails, it is likely that related systems will react in chain. The threat of a crash in the financial markets looms large, unless a ransom is paid within a very short timeframe.

CONCERNING THE ATTACKER

The real problem lies in the uncertainty surrounding the alleged modification of the AI: so far, no abnormal behavior has been detected. Could this claim be a bluff?

SYSTEMIC CRASH

As a result...

POSITIVE BIFURCATION SCENARIO

AI REDUNDANCY

Each institution has two AI systems running in parallel: a primary system and a secondary system, each operating autonomously. In the event of a significant discrepancy between the two systems, or if behavioral alert thresholds are exceeded, human intervention becomes imperative.

EMERGENCY STOP MECHANISM

An emergency stop mechanism is in place, enabling the entire trading system to be suspended if necessary.

FORENSIC ANALYSIS

AI systems are designed to enable post-incident forensic analysis.

STAKEHOLDER COORDINATION

The financial entities' cybersecurity teams, located within a dedicated operations center, work closely with leading cybersecurity experts in the local field, facilitating rapid communication of the latest relevant information and immediate dissemination of alerts to other institutions.

IN CYBER FORUM EUROPE

NEGATIVE BIFURCATION SCENARIO

FLASH CRASH

AI systems, getting out of control, cause an instant collapse of the financial markets - a "flash crash" - before human intervention can take place.

MEDIA REPERCUSSIONS

The crisis is massively covered by the media, drawing comparisons with the 2008 financial crisis.

DOMINO EFFECT

In the worst-case scenario, the situation generates a widespread crisis of confidence, leading to massive capital withdrawals by the public, threatening to precipitate the collapse of the financial system.

SCAPEGOATING

Following the financial collapse, all AI applications are discredited.

DEMOCRACIES IN PERIL

We are in 2030

IN CYBER FORUM EUROPE

STARTING POINT

SOCIAL ACCEPTANCE

The integration of artificial intelligence (AI) into society is proceeding steadily, framed by European regulations that are distinct from those in the USA and China. However, this integration raises concerns about job losses and the associated energy impact.

TECHNOLOGICAL INNOVATION

Automation is gaining significant ground with the rapid advance of the Internet of Things; an increasing number of objects are now equipped with microprocessors that collect valuable data.

AI APPLICATIONS

Given the abundance and diversity of data available, AI is increasingly being used to detect patterns within this data. For example, AI analyses can be used to model areas of drug consumption by analyzing sewage water quality. The use of historical data helps identify the most dangerous intersections or the streets most likely to be burglarized. In addition, traditional media are finding themselves increasingly forced to rely on AI for content production, in the face of steadily declining revenues.

CYBERSECURITY

In Europe, AI training algorithms and datasets must be audited by an independent entity and comply with copyright legislation, as well as other criteria such as the prevention of discrimination.

DEMOCRACIES IN PERIL

What if...

IN CYBER FORUM EUROPE

CYBERATTACK

BACKGROUND

Since the year 2023, extremists from a variety of backgrounds have been exploiting artificial intelligence to destabilize the political landscape. Some practice traditional disinformation, creating deepfake videos and articles that undermine the credibility of opposing political figures, with such sophistication that authenticity appears unmistakable. Other groups use AI to target and disseminate this misleading information to the most receptive individuals.

CURRENT SITUATION IN 2030

It is now possible to synthesize the results of various AIs and data from the Internet of Things (IoT) to deduce the political inclinations of virtually all citizens. What's more, AI facilitates mass personalization of messages sent to maximize outrage. With the gradual decline of professional journalism, it is becoming increasingly difficult to find independent entities capable of rigorous fact-checking.

CONCERNING THE AGGRESSOR

Political extremists continue to exist, and it is suspected that they benefit from the support of certain authoritarian states seeking to undermine democracies.

DEMOCRACIES IN PERIL

As a result...

IN CYBER FORUM EUROPE

POSITIVE BIFURCATION SCENARIO

COLLECTIVE INTELLIGENCE

We benefit from advances in cognitive warfare, implement public and private initiatives to combat disinformation, and step up education on this issue both in schools and among the general public.

TECHNO-LEGAL SUPPORT

The adoption of a European digital identity, guaranteeing ownership of personal data to individuals rather than companies, reduces the possibility of profiling individual behavior. In addition, digital watermarking systems are proving effective in identifying and removing falsified content, such as deepfakes, in collaboration with Internet service providers (ISPs) who take responsibility for online content.

DIFFERENT LEVELS OF GOVERNANCE

For European states vulnerable to disinformation campaigns, the European Union also plays a regulatory and protective role.

NEGATIVE BIFURCATION SCENARIO

EROSION OF CONFIDENCE

In a climate of heightened political and geopolitical polarization, agreement on the perception of reality is compromised. Undeniable facts are called into question, and unfounded rumors are taken at face value. Combating the growing skepticism of citizens towards the system (politics, media, institutions, etc.) and maintaining trust is a major challenge.

EXTREMES IN POWER

In a period of heightened unrest, digital tensions materialize, provoking demonstrations, urban blockades and potential riots. Political movements adhering to an "illiberal democracy" vision are coming to power and using AI to "fight crime", resulting in increased surveillance and repression of dissidents.

AI INFLUENCED AND INFLUENCING

AI is now forced to align itself with government perspectives, influencing the news and recommendations it generates.

FOG OF WAR 2.0

We are in 2030

IN CYBER FORUM EUROPE

STARTING POINT

SOCIAL ACCEPTANCE

There are reservations about the implementation of artificial intelligence in society, mainly due to concerns about job losses and increased surveillance by AI systems. However, the crucial role of AI in the military field is indisputable, in particular the use of drones - whether operating on land, in the air or at sea - whose presence in large numbers is deemed indispensable.

TECHNOLOGICAL INNOVATION

The continuing evolution predicted by Moore's Law ensures a steady increase in the power of the microprocessors integrated into UAVs.

APPLICATION OF AI

The progressive autonomy of UAVs has become essential to overcome interference and respond rapidly to offensives. What's more, these drones are now capable of autonomously carrying out the entire OODA cycle (observe, orientate, decide, act). Human reaction time, however valuable, can be a major disadvantage for these devices.

CYBER PROTECTION

Gone are the days when military projects required a limited number of high-performance machines, made up of parts produced and regulated locally. It is now imperative to have a large number of drones, often commercially available and cost-effective. This means that many components, particularly microprocessors, are designed and manufactured abroad. Any attempt to deviate from this trend runs up against problems of cost (prohibitive) and design (obsolete compared to the commercial sector). Cyber security is generally integrated post-purchase, when the drone is converted and equipped for military service.

FOG OF WAR 2.0

What if...

IN CYBER FORUM EUROPE

CYBERATTACK

BACKGROUND

Since the year 2023, it has become progressively clear that democratic countries are facing a major problem. Their citizens demand that the laws of war be respected, and persist in demanding that the decision to launch an attack be taken by a human being. However, it is becoming increasingly clear that potential enemies have no qualms about deploying autonomous killer drones, and now possess the technological capability to do so.

CURRENT SITUATION IN 2030

Information transmitted by our drones indicates the massive approach of hundreds of enemy drones on the outskirts of the border. The command center has been informed. In the event of an unexpected assault, time is running out, and there are only a few moments left to avoid the destruction of our drones or border units. A decision must be taken immediately: either let the attack proceed without intervention, or initiate a pre-emptive offensive.

CONCERNING THE AGGRESSOR

Geopolitical escalation is reaching a critical level. The hypothesis of an imminent attack is taken seriously. But what if the threat were fictitious? An AI attack simulation designed to simulate a swarm of drones where there are only a few? What if the objective was to incite us to retaliate, offering the adversary the opportunity to present himself as the legitimate defender of his rights? Or, even more worryingly, what if it's simply a software failure?

FOG OF WAR 2.0

As a result...

POSITIVE BIFURCATION SCENARIO

DIPLOMACY

Diplomacy succeeds in building mutual trust to establish preventive rules against immediate and automatic reaction, such as an "AI red line", providing the time needed to defuse tensions.

DETERRENCE

Our deterrence capability is strong enough to deter any hostile attempt. Thanks to an arsenal of drones and independent cyber-defense systems, the likelihood of widespread infection is greatly reduced.

SURVEILLANCE

Continuous monitoring is carried out, including by AIs specialized in the supervision and control of our own drones. In addition, we have a sufficient number of qualified personnel capable of understanding and interpreting the activities of our drones.

IN CYBER FORUM EUROPE

NEGATIVE BIFURCATION SCENARIO

ESCALATION

In the absence of international standards on the use of AI and autonomous military systems, communication with potential adversaries proves difficult. The decision to launch an attack must be taken without delay.

SPIRAL OF WAR

Once we have initiated the offensive, it is certain that the adversary will respond. With its drones programmed to react without human intervention, retaliation is inevitable.

SERIAL BLACKOUT

We are in 2030

IN CYBER FORUM EUROPE

STARTING POINT

SOCIAL ACCEPTANCE

The high energy consumption of artificial intelligence systems has drawn criticism from the public, leading to the development of a new generation of energy-efficient AIs. These systems, often decentralized, are characterized by specific functions and training based on a limited number of parameters.

APPLICATION OF AI

Artificial intelligence has become essential for balancing the power grid, which integrates a growing share of renewable energy production. Given the intermittency of many energy sources, AI is proving particularly effective in adjusting production fluctuations, sometimes in a matter of seconds. Other forms of AI are used for predictive maintenance, enabling equipment to be repaired before it fails.

TECHNOLOGICAL INNOVATION

The rapid expansion of the Internet of Things is reflected in the widespread use of smart meters and smart grids. At the same time, the accelerated transition to decarbonization is leading to increasing electrification of objects, including in the fields of mobility and heating.

CYBER PROTECTION

The market for cybersecurity suppliers is dominated by a small number of very large companies, all located outside Europe. In addition, it's worth noting that the majority of solar panels, mainly manufactured in China, are equipped with data collection and transmission systems. This means that, during periods of strong sunlight, China is able to collect large quantities of data on European energy networks.

SERIAL BLACKOUT

What if...

IN CYBER FORUM EUROPE

CYBERATTACK

BACKGROUND

Since 2023, cyber attacks have not been the main concern; the real issue has been the mismatch between energy supply and demand. During summer periods, water shortages for power plant cooling and consumption peaks linked to air-conditioning systems, which are increasingly in demand with the advance of climate change, prompted the use of AI to optimize power grid management.

CURRENT SITUATION IN 2030

The adversary is attacking the foundation of our infrastructure: the power grid. Exploiting a flaw in software crucial to grid management would trigger random and continuous service interruptions. The consequences would be systemic: in the absence of electricity, the majority of vital infrastructures would come to a standstill, particularly once the reserves of emergency generators were exhausted - no access to banking services, gas pumps or water supplies.

CONCERNING THE AGGRESSOR

It is plausible that the act is the work of a hostile state seeking to express its hostility towards the European Union. However, it is also possible that the flaw was initially introduced by a foreign agency from another country and subsequently discovered by this hostile state. The situation remains uncertain.

SERIAL BLACKOUT

As a result...

POSITIVE BIFURCATION SCENARIO

CO-PILOT AI

Operators monitoring our power grids are assisted by co-pilot AIs, independent of the potentially compromised system, whose function is also to detect anomalies in grid management.

EMBODIED EXPERTISE

Manual control protocols exist in parallel, ready to be activated if the AI needs to be disconnected urgently. What's more, staff are specifically trained to take over if necessary.

DOCTRINE

In the face of a life-threatening threat to critical infrastructure, the doctrine authorizes the use of hack-back, an IT counter-attack designed to neutralize the threat at its source.

IN CYBER FORUM EUROPE

NEGATIVE BIFURCATION SCENARIO

DAILY CHAOS

Attacks are punctual and precise - one day targeting a city's traffic lights, the next all the country's hospitals, then public transport. Uncertainty reigns as to the next target.

FALSE POSITIVES

Lacking adequate tools for the precise identification of anomalies, we are sometimes confronted with unfounded alerts, wasting our limited resources in the hunt for non-threats.

QUESTIONING AI

Prolonged power cuts, induced by AI malfunctions, could lead to widespread skepticism about the reliability of AI in all its applications, especially if the cybernetic origin of the failures cannot be clearly established.

BODY HACKING

We are in 2030

IN CYBER FORUM EUROPE

STARTING POINT

SOCIAL ACCEPTANCE

The adoption of artificial intelligence in everyday life has become a reality, particularly in the medical field where it is now an essential support, reinforced by the introduction of stringent European regulations concerning the use of personal data.

TECHNOLOGICAL INNOVATION

Innovation lies primarily in the interaction between humans and technology. Technology is no longer a tool used occasionally, such as a computer or smartphone, but a companion in constant interaction with us, such as an anthropomorphic friend with a pleasant voice, a watch with multiple functions, or microprocessors implanted in the human body. Edge computing and edge AI enable small systems to perform complex tasks independently of a central computer.

AI APPLICATION

The aggregation of heterogeneous personal data, often collected by wearable devices, enables AI to diagnose illnesses upstream and refine teleconsultation. In addition, anthropomorphic chatbots, which have become integrated into our homes, workplaces and public spaces, are highly appreciated. Included in the healthcare network, they are used, among other things, to remind people to take their medication. For many people, particularly the elderly or isolated, these chatbots are perceived as true companions.

CYBER PROTECTION

Every small, autonomous system needs to be cyber-secure. This is why AIs recommended by other AIs are often used to guarantee this protection.

BODY HACKING

What if...

IN CYBER FORUM EUROPE

CYBERATTACK

BACKGROUND

Since 2023 there have been repeated attempts to steal private patient data, via chatbots compromised by hackers. But the data thus obtained was secured by a cybersecurity AI. Criminals hope that one day they'll be able to decrypt the data using quantum computing, but that's a long way off.

CURRENT SITUATION IN 2030

A pioneering healthcare systems company is about to launch a takeover bid. The company specializes in AI systems that interact with humans via chatbots, and even physically, being installed in heart regulators and chips implanted in more and more people (originally only for people who can no longer communicate with the outside world, now it's become "cool" to be able to manage one's computer this way). But a worried doctor contacts the company. His chatbot had just suggested he take an excessive dose of medicine. Was the chatbot poisoned?

ABOUT THE ATTACKER

In the absence of a ransom demand, one wonders whether this is a technical error - or whether a rival company, from elsewhere in the world, is trying to discredit the company before it has access to large funds with the takeover bid.

BODY HACKING

As a result...

POSITIVE BIFURCATION SCENARIO

ACA

A decentralized AI ("Autonomous Cyber-defense Agent") also detects malfunctioning of the AI system, and warns the company and the user.

A VARIEGATED DEFENSE

Having the option of purchasing a defense system from several different local and foreign companies makes the attacker's task more difficult, since he has to attack several different systems.

IN CYBER FORUM EUROPE

NEGATIVE FORK SCENARIO

CASUALTIES

If the attack is successful, there may be casualties. Chatbots will give bad advice, and some may die of over-medication. Others will have heart problems, or will no longer be able to communicate via the implanted microprocessors.

ECONOMIC DAMAGE

the company's reputation will be ruined, as will its hopes of a takeover bid.

PUBLIC DISTRUST

The AI-based healthcare system will be called into question by the public.

The Pivot Points

↘ AVAILABLE EXPERTISE

— Experts in computer science, coding and the use of IIA

— Experts who can perform a task without AI if necessary

↘ GOVERNANCE

— Regulatory framework

— Cyberdiplomacy

— Competition law

— Trust providers (certification, etc.)

— Digital identity and privacy protection

↘ AI FOR CYBER DEFENSE

IN CYBER FORUM EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Acknowledgements

↘ THE SCENARIOS WERE DEVELOPED USING INFORMATION FROM A NUMBER OF SOURCES, INCLUDING:

— Interviews with Henri d'Agrain, Jacob Galbreath, Yann Bonnet, Piret Pernik, Siraj Shaikh, Thierry Berthier, Yann Bonnet and Urmas Ruuto

— A workshop at IHEDN