CAMPUS CYBER

CYBER HORIZON 2030

OUTLOOKS AND CHALLENGES

FOREWORD

The Cyber Campus is a flagship that charts its course following agile and mobilizing trajectories. This prospective exercise maps the possible or probable path for cybersecurity in a near future. The cybersecurity ecosystem has been mobilizing its diversity of actors for a few months now in order to produce this first Common.

Even thought, the conclusion of this synthesis doesn't constitute a precise strategy, it underlines the numerous challenges to come and the topics on which we must work together at the Campus Cyber. While the issues ahead may feel daunting, this first achievement demonstrates our capacity to collaborate and feredetate the cyber ecosystem. I truly hope that this first Cyber Common will pique your interest and motivate future productions.

Michel Van Den Berghe,
CEO of Campus Cyber

A WORD FROM THE COORDINATORS

We were privileged to collaborate with the teams at both AXA and Wavestone. The findings have been detailed in this summary, which we hope will aid the societal responsibility of mitigating cyber risk.

The level of expertise and knowledge exchanged throughout the duration of these events made it a highly rewarding experience. The cyber ecosystem is thriving, and we are thankful for all contributors that have taken part.

Any work carried out in this sector undoubtedly comes with dangers, given the nature of the choices made. But events like this are exciting and despite the risks. We hope the scenarios discussed and the challenges identified will be instrumental in adapting to a fluctuating future where technology is concerned.

In any event, we hope you will find the report insightful on the challenges ahead!

Arnaud TANGUY, Gérôme BILLOIS

Arnaud TANGUY,
CSO,
Groupe AXA

Gérôme BILLOIS,
Partner cybersecurity,
Wavestone

SUMMARY

ANTICIPATE THE FUTURE: A PERILOUS EXERICE BUT A NECESSARY ONE

The first prospective exercise at the cyber campus mobilised a wide variety of profiles to conjure up a vision of a near future, namely the next 5 to 10 years, where cyber security issues will have escalated. Help in creating this scenario was provided by the Ministry of Defence and Paris Siences & Lettre University.

The objective: To forecast a series of near future scenarios and identify the key characteristics and challenges of the respective scenarios by extrapolating from current trends. This exercise was to be perilous by design and required challenging decisions to be made regarding the key features of the scenarios.

Scores of priorities and hundreds of actions were collated, highlighting the synergies between the attendees of the cyber campus. The first insight was that today's priorities will be those of tomorrow: the foundations of cybersecurity will not necessarily be challenged in the coming years. Conversely, the concrete nature of these responses do present some concerns when considering the vast range of possible futures and the complexities of the changes required to deal with the problems we identified.

We decided to only focus on challenges that felt the most complex to solve, and required cooperation between multiple actors, a principle which is at the heart of the cyber campus.

These choices were made through collaborative workshops composed of more than 60 contributors from public and private entities.

This insights paper doesn't aim to exhaustively describe the entirety of exchanges that took place and neither does it attempt to be a definitive vision of future events.

It presents a purposely short blend, of the conceivable futures as well as the priorities and challenges associated with them. The exercise is designed to continue and improve over time.

Nevertheless, we hope it will eventually set an example for subsequent cyber camps.

We would like to thank the 51 contributing entities which accepted the call to participate in the various workshops despite the sanitary challenges and the almost entirely digital format of the exchanges.

The organisation of the workshop and the production of this report would not have been possible without the commitment of all members, in particular AXA and Wavestone, the coordinators of this dedicated collective.

METHODOLOGY

↗ **The Anticipation Working Group relied on an open and inclusive methodology, bringing together the members of the Cyber Campus. For the first time, it allowed the ecosystem to collaborate to produce a common and far-reaching analysis.**

Over a period of two months, the methodology associated interviews, workshops and analysis aimed at collecting contextual elements and spark debates.

The first phase consisted of sketching the possible evolutions of the world beyond cybersecurity. It relied on a set of interviews, allowing the working group to identify the initial trends in several fields (including social, geopolitical, economical, environmental) and from them the effects on the digital and cyber industries.

The second phase was dependent on the initial exchanges in the first phase. The coordinators opened three workshops, inviting members to explore the possible futures in cyber security, the opportunities each future offers the attackers as well as any potential solutions in defence.

Finally, a cross – analysis workshop allowed the respective propositions presented to be summarized and then prioritised in an effort to establish the themes presented in this report.

An editorial committee was established to review the production of the final document.

CHAPTER 01

FOUR CONCEIVABLE FUTURES

WHAT WILL 2030 LOOK LIKE?

In order to anticipate cyber threats in 10 years, it is necessary to first project ourselves into the future. During the workshops, and based on the experts' interviews, the participants attempted to propose possible futures for 2030. An analysis of the resulting proposals revealed the following four main trends.

→ **Ultra connectivity:** Due to the increase in both volume and rate of information exchange.

→ **Ultra-fragmentation:** Stemming from the aggravation of local governments due to geopolitical distrust and fear about dependencies on digital ecosystems.

→ **Ultra-green:** Resulting from the strengthening of environmentalist and digital sobriety ideologies in face of climate change.

→ **Ultra-regulated:** Owing to regulation of digital ecosystems for the purpose of restoring trust in digital economy.

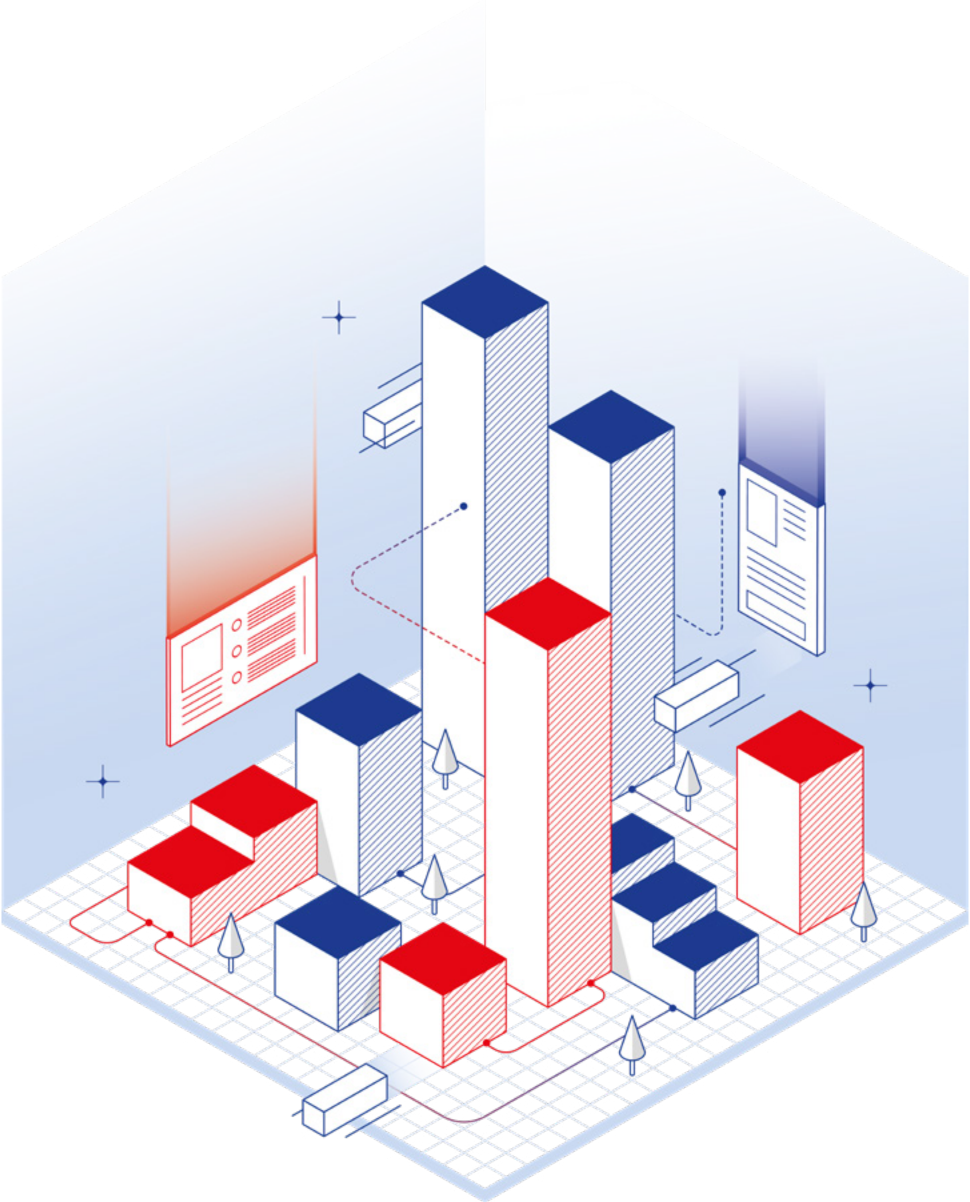
Each of these trends pushed to their extremes presents a possible future scenario. The aim was then to provide a map to allow readers to appreciate each of the trends impact on individuals, organisations and society as a whole.

SCENARIO 1

AN ULTRA CONNECTED SOCIETY

↗ **In 2025, major digital players worldwide have been driven by consumers and states to collaborate and agree on interoperability standards. This event greatly accelerated the development of digital technologies by making their daily use simpler and more fluid by 2030.**

In the meantime, digital worlds have continued their strong growth and parallel economies have been created. A large part of the population fluctuates between real and virtual life in one or more digital universes or metaverses.



FACTS

Economic and political spheres are transformed to adapt to this new societal paradigm. The supply chain is more automated, especially thanks to delivery robots and to automated payments technologies.

In many cases, citizens do not trust data protection mechanisms. They create fake digital profiles or declare false personal information. It becomes increasingly difficult reliable date. Digital currencies and purchases of digital goods are becoming more common (in particular NFT technologies).

Cities, transportation, public spaces and homes are equipped with sensors to facilitate new services (e.g. smart cities, smart home, smart mobility, smart health, smart education).Digital technologies enable a growth in business productivity (e.g. automation, anticipation of employee departures thanks to artificial intelligence).

Civic practices (e.g. administrative procedures and votes) are evolving towards greater inclusiveness and simplicity thanks to technological progress and interconnectivity.

CONSEQUENCES

The borders disappears between personal, professional, digital and real lives are manifesting more and more everyday.

Digital identities make it easier to track citizens actions, over property (e.g. smart home, smart city, smart building) and digital use. It would be apt to say the principle of online anonymity is crumbling, and the commercial uses of personal data collected is exploding. Citizen distrust and hence the use of circumvention strategies are rapidly increasing.

The two main players that monopolise the technology industry (China and US) and its economy (materials and manufacture) have consequently given rise to interdependencies that could lead to geopolitical tensions.

OPPORTUNITIES FOR CYBERATTACKERS

↗ The ultra connectivity of people and systems provides cyber attackers with a wide range of targets and unprecedented access (e.g. theft of sensitive information, control of household or professional objects, supply chain hijacking).

They benefit from the speed and homogeneity of modern technologies to quickly and widely extend the scope of their attacks.

The rise of plateformisation (use of digital platforms or social networks for the dissemination of content and services) supports the economic development of criminal networks that use these platforms to sell their services and organise themselves.

To maximize the impact of attacks, cybercriminal organisations are internationalising their activities (more « clients » and targets, search for the « highest bidder »). They are diversifying and industrialising their recruitment methods to reach the best talent.

ATTACKS ARE INCREASINGLY MORE SUBSTANTIAL:

- ↗ Booby-trapping consumer apps with an aim to shut down services or siphon user data.

- ↗ Extensive use of digital systems for criminal purposes (e.g. botnets to launch attacks).

- ↗ Creation of fake fees and low-cost digital services to trick victims (e.g. fake protection services, fake premium access to free services).

- ↗ Large scale entrapment of physical supply chains (e.g. disruption of factories, stores).

- ↗ Instantaneous spread of malware (e.g. NotPetya type), which are instrumental in attacks on essential services.

- ↗ Dissemination of fake news in all sectors (for example in finance by stock price manipulations, which is all the more effective due to the high levels of automation involved in current stock market activities).

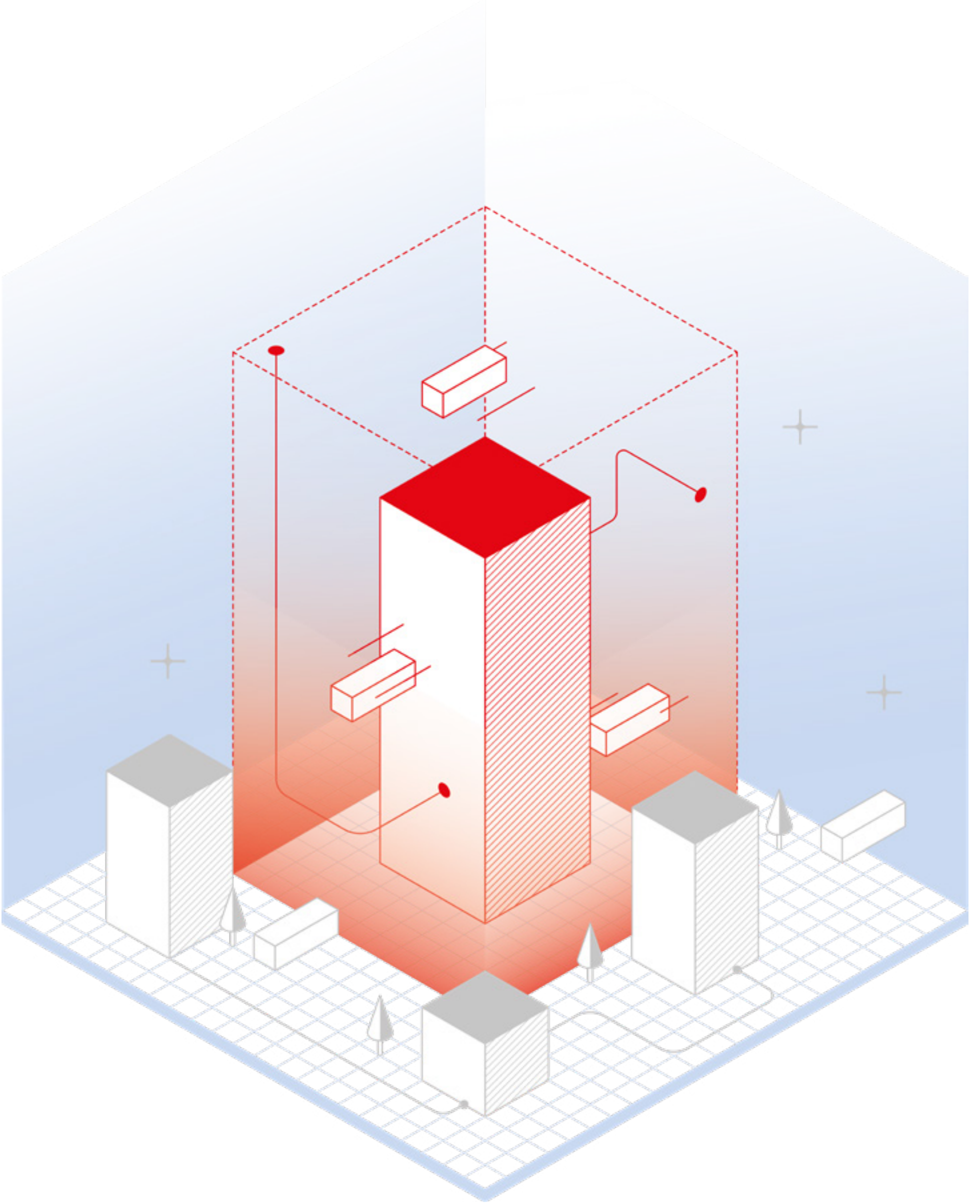
SCENARIO 2

AN ULTRA FRAGMENTED SOCIETY

↗ **In 2025, the revelation of outrageous practices - including hacking, theft, and cross-referencing of data carried out by governments with the support of private companies – has led to the death of digital trust: it's a datastrophe. People are revolting and demonstrating for greater control over the use of digital technologies.**

In response, states are reacting by creating digital borders, closing them immediately, and nationalising strategic supply chains. The period is marked by the partitioning of the Internet and a strong technological isolation.

Priority is given to state-owned solutions (processors, cloud, crypto assets, etc.) to ensure national defense.



FACTS

The reaffirmation of geographic authorities brings back direct conflicts and exacerbates the practices of espionage between states. Cyber and digital technologies are becoming high ticket investment items.

The geopolitical scene is marked by new divisions and alliances between independent nations: bilateralism dominates over international initiatives, institutions are losing in control and in scope (e.g. UN, NATO, EU, WTO, etc.). In this scenario, the European Union is fragmenting.

CONSEQUENCES

Digital identities are largely imposed and regulated as they allow states to track and trace people, objects and services they use. Being watched, individuals can no longer exchange information freely and anonymously.

The closure of digital borders allows more filtering and leads to an increase in the number of territorial platforms and websites (e.g. the use of non-national social networks is prohibited).

International companies are experiencing a major upheaval in the management of their operations and are forced to de-globalise by partitioning their information systems (e.g. network flows, data location), their resources, and their expertise in each sovereign zone. Expansion to new zones is extremely difficult and restricted.

Firms that are experts in intrusion testing, cyber R&D, and vulnerability research are nationalised, and their activities recategorised at the same level of confidentiality as those of counterintelligence.

Some territories introduce legislation relating to digital independence. New penal sanctions are introduced in the event of the use of any encryption or anonymisation software. These rules are reinforced by the state's enhanced powers of digital surveillance.

Various territories are waging a war over the training, acquisition and retention of talent and digital technologies.

OPPORTUNITIES FOR CYBERATTACKERS

The growth in the number of regional platforms gives leads to a surge in groups of attackers specialising in certain targets.

Newspapers regularly report on ongoing cyber wars and cyber clashes. Critical infrastructures are understandably the most targeted.

Maintaining an international market of vulnerabilities promotes the economic growth of cybercriminal organisations. They have the expertise and the resources necessary to exploit these vulnerabilities extremely quickly and efficiently.

The regional partitioning of ecosystems simplifies target detection for attackers but reduces the risk of collateral damage among third-party allies.

The mutualistic relationships between states and cyber criminals allows groups to be equipped with better offensive capabilities, while benefiting from impunity and protection in their own sovereign space.

ATTACKS ARE MORE MALICIOUS, DESTRUCTIVE AND DESTABILISING:

- ↗ Attacks mixing informational, cognitive and cyber aspects.

- ↗ Increased attacks on supply chains (e.g. entrapment of software, entrapment of components), particularly those outside the hacker's digital borders.

- ↗ Reinforcement of complex attacks with rebound (e.g. spy attack followed by a ransomware attack aimed at erasing the traces of the previous « attack and at disorganizing the target to cripple any retaliatory actions »).

- ↗ Attacks on national critical services with the aim of destabilisation. Digital “terror attacks” are emerging.

- ↗ Increase in state-led ransomware attacks for financial gain and destabilisation.

- ↗ Strengthening of cyber espionage: growth in numbers of subcontractors who sell high-end espionage services to states for geopolitical purposes.

- ↗ Reinforcement of retaliatory hacking attacks, military defence capabilities, and “false flag” attacks.

- ↗ Physical destruction of certain submarine cables or satellites and attacks on critical supply chains.

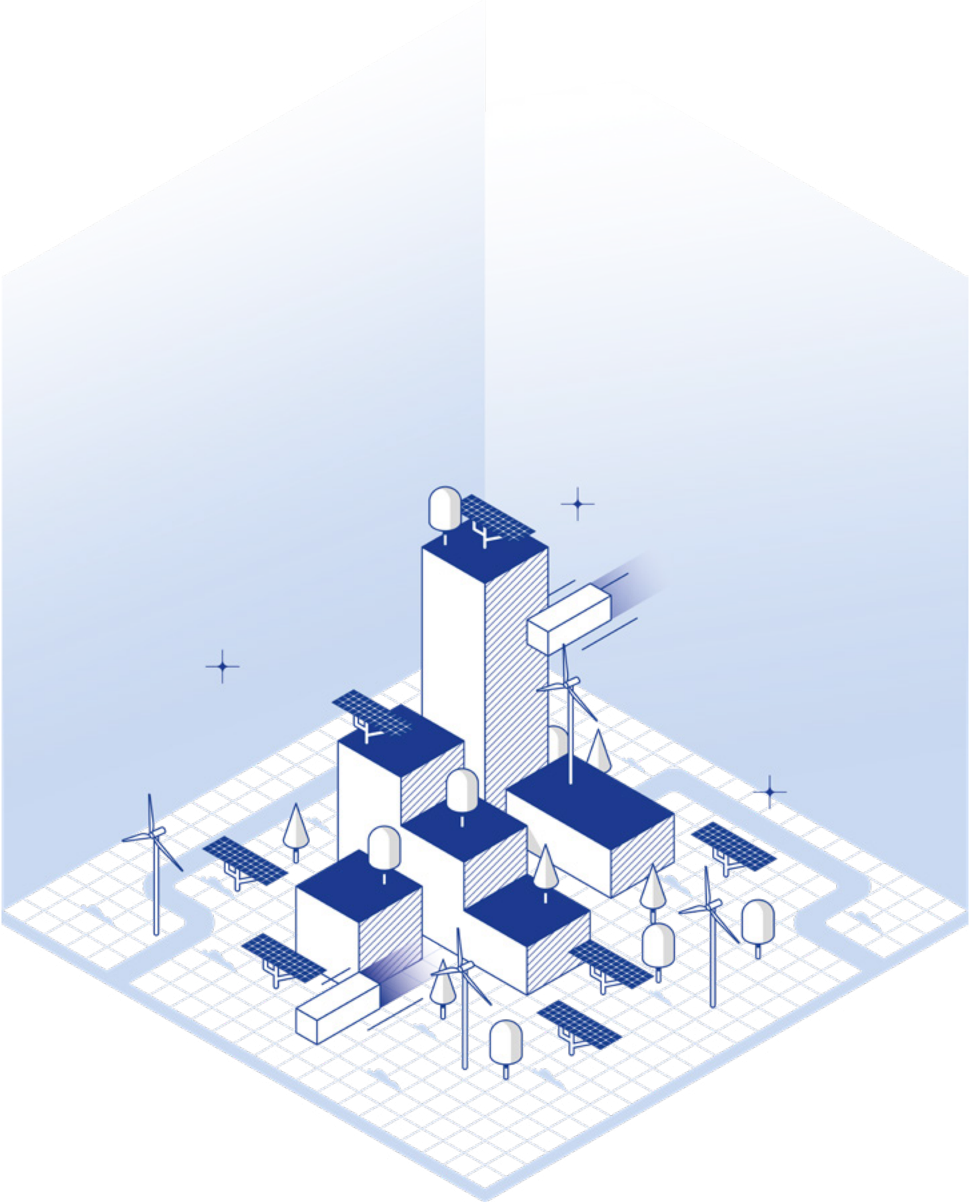
SCENARIO 3

AN ULTRA-GREEN SOCIETY

↗ **In 2025, the world is experiencing more and more natural disasters and global health threats, resulting in unprecedented waves of migration.**

The general public puts pressure on governmental institutions and large organisations to prioritise their responses to environmental issues.

Digital is at the heart of the discussions: its advances are denounced because of the consequences they can have on the environment.



FACTS

Access to digital services are conditional on the level of energy producing resources available, aggravating social and diplomatic tensions between countries.

The countries that are the least committed to the ecological reform are attacked by cyber-green groups. The same goes for organisations that are considered as polluting and wasteful of energy. Hacking campaigns even target users of crypto-currencies or online games.

The exacerbation of ideologies gives rise to digital and physical confrontations between those in favor and those opposed to the environmental policies put in place.

A new social category, the «unconnected» is emerging: they refuse digital practices lower their carbon footprint, and protect their privacy.

CONSEQUENCES

Citizens are campaigning for energy savings, including in the digital sector. Some services are forced to shut down or undergo in-depth opération model transformations. Organisations incur significant losses, incentivising them to expedite their transformations.

Innovators attempting to make technological advances must prioritise reducing their impact on climate change, which is becoming a comparative factor between competing technological breakthroughs.

Individual pollution quotas, including those targeting technology (e.g. number of emails, amount of data stored) are set up, with personal monitoring of consumption by the authorities.

OPPORTUNITIES FOR CYBERATTACKERS

Cyberattackers take advantage of the conflict between groups of opposing ideologies by monetising their services to carry out sometimes violent and very destabilising cyberattacks.

These hacktivists target systems that consume too much energy (digital currency & crypto assets, data centres, etc.) and destroy them while promoting messages for the arrival of digital sobriety. Extreme ideologies, widely shared, nurture like minded individuals on a global scale.

At the same time, the ranks are growing thanks to the exploitation of mechanisms put in place for a more sober digital environment (e.g. thefts, manipulations, scams and/or resale of quota, etc.).

ATTACKS ARE MORE VISIBLE, SHOCKING AND DESTRUCTIVE:

- Attacks on the reputation of public and private individuals.

- Destruction of energy-intensive digital systems.

- Environmental ideologies are commandeered for the benefit of cyberattacks (e.g. ransomware, extortion, etc.).

- Strengthening of hacktivism (digital activism).

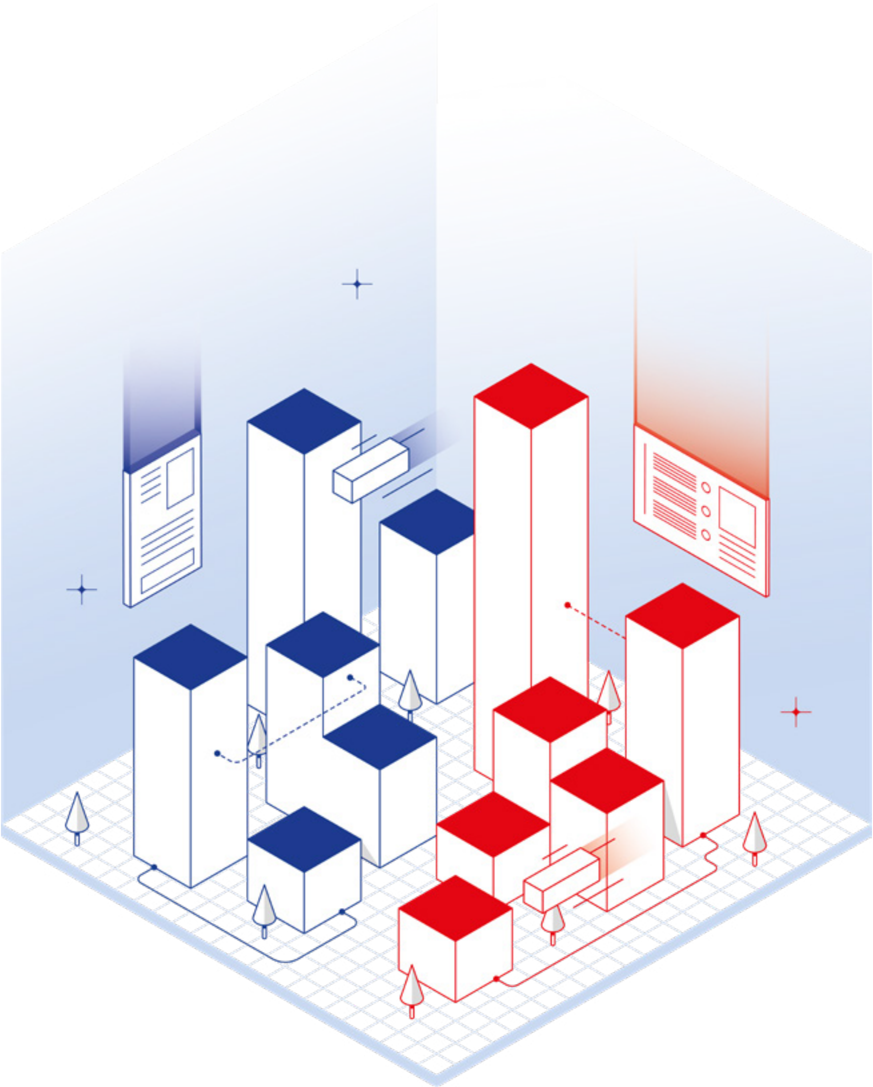
- Attacks against non-local supply chains.

SCENARIO 4

AN ULTRA-REGULATED SOCIETY

↗ **In 2025, attacks and scandals involving the use of personal data continue to multiply and erode trust in digital technology.**

The general public is demanding more transparency, control and autonomy over the management of their data. Governments are mobilising to preserve the economic growth that stemmed from digital transformation.



FACTS

Regulations are increasing, both in their scope and their sanctions. The various authorities are strengthening their control capabilities.

Two philosophies clash: those in favour of the monetisation of user-controlled data and those who see data as a «common good» to be protected. Each major power zone puts in place its own regulations giving more or less control and obligations to users and providers of digital services.

In areas where data is released on a personal scale, individuals have the ability to control and assign value to their “digital traces” (e.g. IP address or digital avatar in the metaverse). Some find it difficult to appropriately manage their sensitive data and to maintain control over their information.

In other areas, the “common good” model protects individuals against the insidious collection of personal data by private actors. Although it is viewed as slowing the development of the digital economy, this model is largely backed by the wider population.

CONSEQUENCES

The proliferation of bodies and state agencies in every country to regulate digital activities leads to a lack of clarity regarding the rules to be respected, the areas of influence and responsibilities of each. Regulations remain subject to interpretation, especially in Europe where new directives are created but implemented in varied methods.

The economic model of major digital players is being undermined in several geographical areas. Some services are closing, others are switching to paid models. New logics of data valorisation are emerging and are subject to many ethical and technological debates.

Only large international groups still manage to comply with numerous regulations, though most still to tailor their compliance processes to all regions and suffer fines or service closures.

Technological solutions for data control and traceability are being deployed on a massive scale. But faced with the lack of confidence regarding the respect of privacy (e.g. centralisation of data, knowledge of the location of data), some players favour the «physical and social“ benefits in user tracking

At the same time, the dark web, blockchain and decentralised metaverses offer an escape from this ultra-regulated society, but without other guarantees than trust in those who make them work.

OPPORTUNITIES FOR CYBERATTACKERS

Cyberattackers take advantage of the multiplicity of regulations to engage in cyber blackmail. They threaten to report their victims to regulators for non-compliance, or offer fake regularisation services.

These extortionate practices are extremely effective: the number of victims and profits from cyberattacks are soaring, encouraging the economic development of criminal networks.

Human and financial investments relating to security are neglected in favour of those solely aimed towards regulatory compliance with new requirements following sometimes ideological positions and not accounting for the actual risks. Global security is all the more destabilised: attackers take advantage of this context to multiply the areas of impact with complete impunity and companies find it difficult to extricate themselves from this vicious cycle.

ATTACKS ARE EASIER, MORE TARGETED AND MORE DISCRETE:

↗ A boom in the success rate of cyber extortion.

↗ Rise of attacks based on imitation of regulatory authorities and false fines.

↗ Increase in victim information sharing practices in cybercriminal networks.

↗ Increased number of attacks by non-professional and non-technical cybercriminals.

↗ Fall in reporting of cyber incidents by victims for purposes of discretion vis-à-vis regulators.

↗ Development of a «parallel world» that tries to escape regulations.

CONCLUSION

The future of our society in 10 years will not be exactly similar to one particular scenario identified here, but more probably a strong combination of the four.

Taken individually, the trends identified make it possible to highlight the major digital challenges and to better appreciate future threats.

Readers can apply this reading grid to their environment in order to identify and anticipate the consequences that these futures could have on political, public and private organisations, research institutes, or simply on the aspirations of individuals and citizens in society.

In the rest of this insight paper, the working group identified in a transversal manner what the priorities and the major challenges are the must be addressed to secure the world of 2030.

The group members did not analyse each scenario and identify each measure, but they cross-referenced the major security and trust needs related to the scenarios to identify the major challenges to be solved.

CHAPTER 02

5 PRIORITIES FOR THE FUTURE OF CYBER

PRIORITIES, CHALLENGES AND INVARIANTS

Based on the scenarios constructed beforehand and the proposals identified during the workshops, five major priorities were formulated. For each of them, one or two challenges to be resolved have been selected.

These challenges are both complex to solve, requiring the mobilisation of many players, and central to the definition of tomorrow's cybersecurity because of their technological or organisational implications. They can be integrated into the heart of the work carried out by the Cyber Campus.

The following summary is not intended to be exhaustive, neither in its analysis of the state of play nor in its proposals, it highlights the fundamental elements that emerged during the workshops.

→ **Inserting security by default in all digital systems.**

→ **Giving everyone back control over their digital life and data.**

→ **Enabling large scale resilience through automation and AI.**

→ **Fighting the impunity of cybercriminals.**

→ **Developing the attractiveness of the sector.**

INVARIANTS TO BE INTEGRATED IN THE WORK

↗ **As part of our reflections, three invariants have been identified.** It is essential to take them into account to respond to the various challenges in order to ensure the success and credibility of the solutions to be implemented, but also the definition of a responsible sector.

COOPERATION

- Cooperation, between all the private entities (academic, research, law enforcement, justice, etc.) is necessary to respond to all the issues at stake.

THE EUROPEAN PERSPECTIVE

- The European perspective must be considered in all decisions, to promote the emergence of pan-European cybersecurity initiative.

DIGITAL SOBRIETY

- In 2022, the reality of climate change requires all sectors to integrate the parameters of sustainable development into their progression. Digital and cyber technologies are particularly energy-consuming, both during the design of systems, in their daily use and during their decommissioning. The principles of sobriety must be part of their development model.

TOWARDS A MORE SUSTAINABLE CYBERSECURITY

REINVENTING THE FUNDAMENTALS OF CYBERSECURITY

↗ Our work has made it possible to identify three subsets for which the actors could minimise the use of resources and energy.

CRYPTOGRAPHY

↗ Its use is pervasive and extremely widespread. Therefore, even minor gains in energy consumption in our daily activities can have a determining effect on a large scale. Research is emerging, some even going so far as to position sobriety as a future factor of choice in algorithmic normalisation.

BACKUP

↗ This particularly concerns the phenomena of data duplication and infobesity. The mechanisms and techniques of sobriety in this area exist but must be scaled up by being integrated into daily organisational practices. We can mention, for example, the ability to deduplicate data between different individuals or to destroy unstructured information (e.g. erasure campaign of unnecessary data, automated deletion rules, etc.).

BLOCKCHAIN AND CRYPTO ASSETS

↗ Blockchain and crypto assets are becoming increasingly important, but the energy required to operate crypto assets can be optimised. Ongoing sobriety research should be supported.

ZOOM - CONSISTECY WITH THE NATIONAL CYBER ACCELERATION STRATEGY

↗ Finally, the proposed solutions take up the challenges presented in the French cybersecurity acceleration strategy below

TRUST:

C

“Users must be able to benefit from the possibilities offered by digital technologies without fear for the security of their data, for the availability of the services on which they depend or for their physical integrity“.

ECONOMIC:

E

«The competitiveness of companies is increasingly based on their mastery of digital tools. Thus, the ability to protect themselves against computer attacks is a vital issue both to guarantee their growth and to maintain the trust of their customers. Furthermore, the cybersecurity sector has significant economic potential and is a job providing sector”.

FRENCH SOVEREIGNTY:

S

«France must preserve its autonomy of action and have scientific, technical and operational skills, but also its own industrial capacities to face the challenges of the future».

In the rest of the insight paper, each solution presented is marked with the badge(s) of the issue to which it responds to.

PRIORITY

INSERTING SECURITY BY DEFAULT IN ALL DIGITAL SYSTEMS

THE SECURITY OF PRODUCTS AND SERVICES, A MAJOR OPPORTUNITY

↗ The subject of insertion of security “by default” in digital systems is not new, but so far presents a level of progress that is too relaxed. The concepts of security by default are still poorly understood, widespread and integrated.

The challenge is to ensure integrated security in digital products and services for both the general public and public or private organisations.

In order for manufacturers to integrate security from the design stage, it is important that it becomes a comparative factor when purchasing digital solutions. Thus, the level of security should be displayed and measurable in a transparent and simple way.

Several initiatives are underway, including the website security rating project, voted in November 2021 by the French Parliament. However, the criteria remain difficult to maintain and to assess over time and are limited to websites.

It is necessary to extend these types of measures. This indicates the need for easy and rapid evaluation mechanisms, applicable more widely and frequently. Ultimately, it should be possible to evaluate the entire construction chain of a product or software as a whole (third-party components, hosting, etc.).

Today, product security assessment is complex, long, mostly manual, and therefore expensive. Supply chains are difficult to grasp, with sometimes up to several thousand modules for a digital system, all from various sources.

If several scoring, qualification and evaluation mechanisms already exist, they present either difficulties of scaling up (ease, speed), or problems of quality and depth.

KEY CHALLENGE AHEAD

C E S

Build easy, reliable, and automatable methods and tools for assessing the security level of solutions, products, components and organisations (third parties, suppliers, customers, etc.) to enable the scaling up of cybersecurity assessments.

FIRST CAMPUS CYBER ACTIONS

Support the creation of an assessment standard, a cyber score, and its deployment

- **Benchmark of existing assessment solutions for products and organisations and their strengths and weaknesses.**
- **Identify and support research projects on the theme of product and organisational security.**

PRIORITY

GIVE EVERYONE BACK CONTROL OVER THEIR DIGITAL LIFE AND DATA

A STRONG NEED FOR THE CONTROL OF DATA

↗ The growth in number of attacks and scandals are today giving birth to the first movement of defiance towards digital services. How to trust when you provide your data? How to ensure your wishes will be respected? How to use key digital services (e.g. governmental and health) requiring identity validation while maintaining privacy when using less crucial services? These questions are more and more present in public opinion.

Everyday, people are facing the difficulties of managing multiple online identities and the associated authentication. Furthermore, providers have difficulties to implement easy and reliable security functionalities (for example in terms of authentication or protection of data using cryptography).

In the ultra-connected, ultra-fragmented and ultra-regulated societies, where citizens are extending their identity far into the digital world with metaverses, providing solutions to these issues (identity, authentication, data security and privacy) will be essential.

Today, even if regulations, the number of which are constantly growing, are aiming in the right direction, their contribution needs to be significantly expanded to avoid events that will negatively and permanently impact citizens' trust (e.g. scenario #2 "datastrophe") while staying realistic and remaining actionable by the providers of digital services.

The key challenge identified is articulated this time around three subthemes.

KEY CHALLENGES AHEAD

C

Identity control, using a reliable digital identity program, that is both interconnected and largely shared.
Its essential to be able to prove an individual's identity as well as use the most advanced digital services while catering for ease, decentralisation and in some cases anonymity. The technological innovations related to blockchain, and the associated technologies (Web3) present encouraging opportunities.

Data control, using devices and measures that give everyone back the control of their data.
Today, these platforms exist, the privacy centre, but they are not centralised (e.g. using API). They would allow citizens to get back visibility and control over their data and digital identities: centralised access to data localisation, activation of their rights to get back or delete data. It implies a good data management policies from the providers.

Protect more effectively, by simplifying and broadening the scope of cryptography.
Some progress on the topics are successful (e.g. laptop and smartphone encryption by default), but further innovations are required for these mechanisms to become simpler and adapted to the new usage of technology. Following the work done on encryption of data in transit and at rest, it is time to focus on encryption while processing. Research work is already ongoing, for example on homomorphic encryption, that allow to data processing while keeping it encrypted, making them inaccessible to service providers.

FIRST CAMPUS CYBER ACTIONS

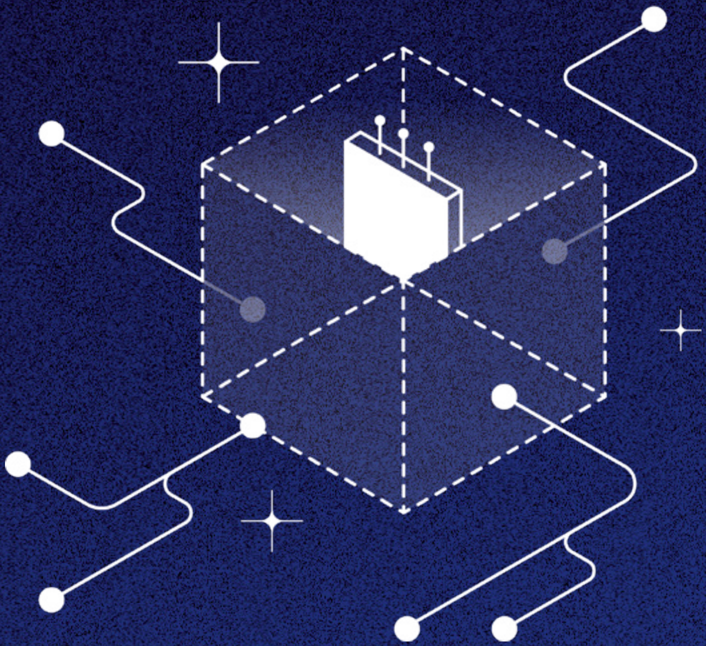
Contribute to the establishment of digital trust end-to-end

- **Evaluate the emergence of a centralised model for managing digital privacy (e.g. privacy centre).**

- **Launch a challenge on homomorphic encryption.**

- **Study the pros and cons of blockchain for digital identity.**

PRIORITY



ENABLING LARGE SCALE RESILIENCE THROUGH AUTOMATION AND AI

CYBER INCIDENT MANAGEMENT SOLELY HUMAN IS NO LONGER ENOUGH

↗ The sheer sum of cyber attacks are growing, becoming more complex and their effects are increasingly rapid. These impacts will be even broader in a society that is digitally transforming and interconnecting more and more systems.

In this context, the gap between the speed of action of cybercriminals and the detection times is still too long. The strengthening of solidarity between liable parties as well as the growth of human resources will not be enough to reduce the time gap.

New proven techniques are already making it possible to automate several processes. Among them, the detection of certain attacks, the implementation of simple reactions or the deployment of software during the reconstruction phases can be cited. These examples show the path to enhanced resilience based first on automation and then ultimately on artificial intelligence.

Initiatives are underway for many suppliers, in particular on the subject of attack detection and reaction, but also on the subject of information system reconstruction. However, the ideal solution has not yet been found. The subject is complex and requires significant research work.

KEY CHALLENGES AHEAD

E S

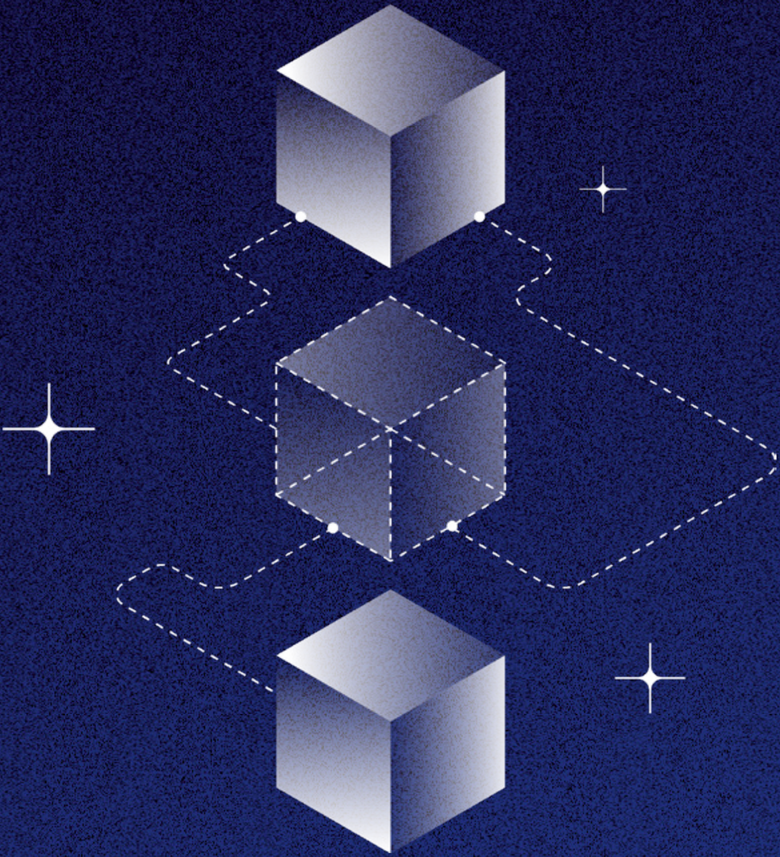
Effectively use artificial intelligence to improve detection, speed up response to attacks and automate reconstruction at scale.

FIRST CAMPUS CYBER ACTIONS

Facilitate the reconciliation of AI and cyber-security

- **Develop a platform to experiment with the use of AI in cyber.**
- **Join forces and develop cyber AI challenges.**
- **Provide data to facilitate experimentation.**

PRIORITY



FIGHTING THE IMPUNITY OF CYBER ATTACKANTS

ARDUOUS IMPUTATION PROCESSES

Despite the surge in arrests of ransomware groups in 2021, a strong sense of cybercriminal impunity remains.

The first legislative texts on the subject have been voted on in France and in Europe, the investigations are progressing, but the issue of identifying the perpetrators remain prominent and complex.

Today, assigning responsibility for a cyber crime is done via manual research that consumes a lot of time and money. Data is difficult to collect and to share because it is scattered, in various formats, and collecting it comes up against the difficulties of international law enforcement cooperation.

KEY CHALLENGE AHEAD

E S

Enhance the accuracy in identifying the guilty parties in the event of an attack by using artificial intelligence systems capable of cross-checking large masses of information. (attack tools, operating methods, infrastructures, tracing on anonymisation networks, financial transactions in digital currency or fiat money, open-source information, etc.).

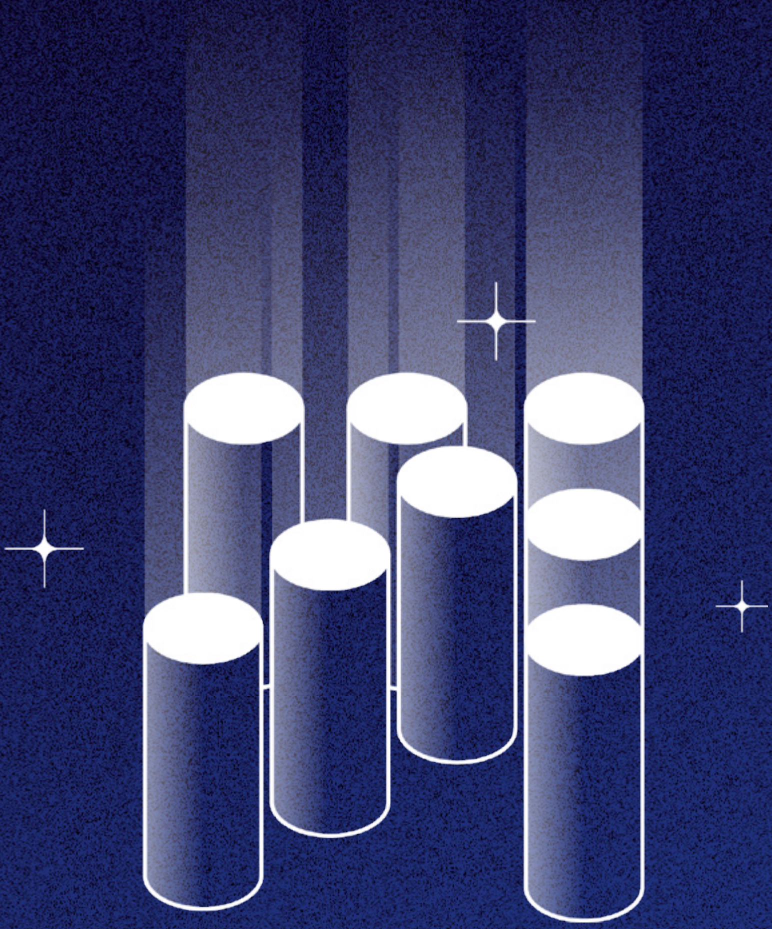
FIRST CAMPUS CYBER ACTIONS

Facilitate the emergence and modelling of AI to improve attack attribution.

+ **Create attack simulation environments and R&D projects on AI training to impute attacks.**

+ **Create R&D projects to trace or follow the movement of money and automate the seizure of crypto assets.**

PRIORITY



DEVELOPING THE ATTRACTIVENESS OF THE SECTOR

HUMAN RESOURCES AT THE HEART OF TOMORROW'S CYBER

↗ Beyond the global awareness of good practices, which is key and must be continued, the cybersecurity sector is experiencing an international shortage of skills. It constitutes a major problem for all organisations and their suppliers.

The challenge lies in the profession’s attractiveness and the need for diversification of the profile on all criteria, including education. Cyber is not only technical but touches on many different subjects: operational resilience, fraud, risks, governance. Increasingly diverse and interesting career paths exist.

Despite the multiplicity of initiatives for the general public, for organisations, or for the educational sector, we still perceive a lack of attractiveness for technological subjects, and in particular cyber. This is a major obstacle to the development of the sector that must be overcome.

KEY CHALLENGE AHEAD

E S

Ensure the accessibility to platforms that give a grounding in cyber skills and increase the sector's attractiveness.

FIRST CAMPUS CYBER ACTIONS

Centralise, promote and help with the consistent implementation of cybersecurity promotion systems.

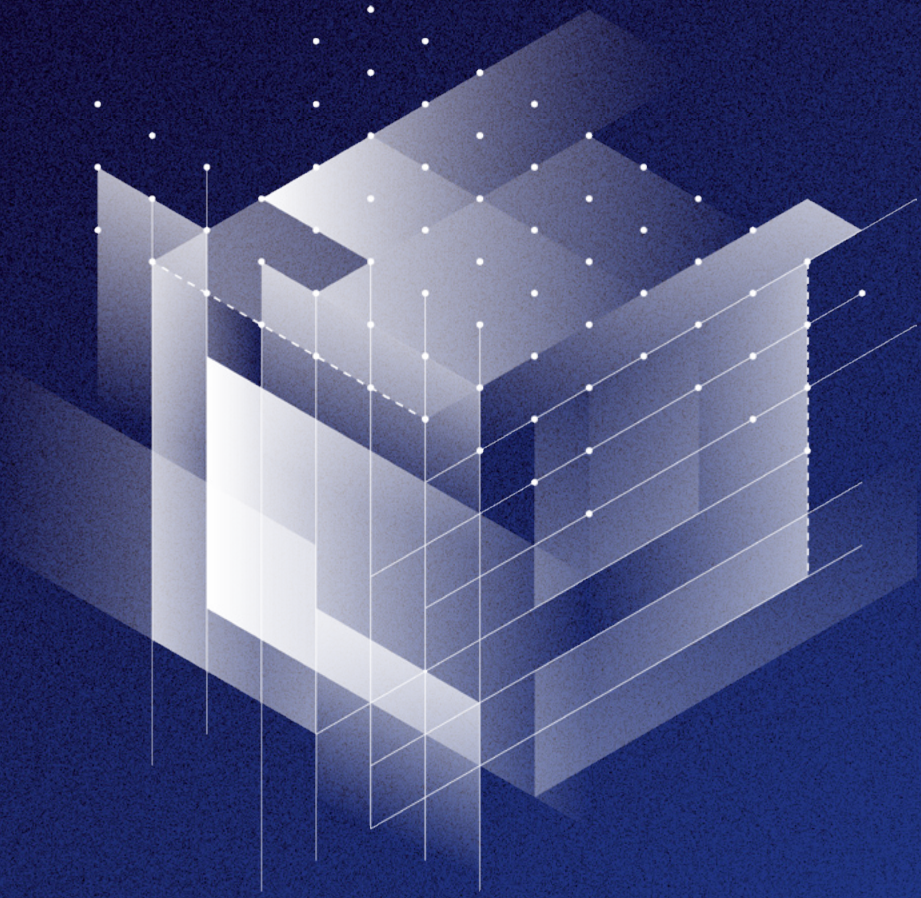
+ **Develop a cyber training and employment portal.**

+ **Strengthen cooperation with national education.**

+ **Set up the pooling of resources and communication actions.**

BEYOND 2030

QUANTUM'S ROLE



QUANTUM: BOTH A LONG-TERM THREAT AND A LONG-TERM OPPORTUNITY

Quantum might be a threat to cyber both due to the paradigm shift it implies and the potentially impressive results it presents for digital (e.g. due to its ability to easily break the encryption methods currently used). But it also represents an opportunity to rethink cybersecurity. In this context, the cyber campus will have to closely monitor its developments.

→ **Today, we can see the first uses of quantum properties to improve cybersecurity. Particularly on the transmission of encryption keys.**
The process is already functional and useful in some cases. Aware of these new capabilities, France launched its quantum plan in 2021. This plan aims at strengthening cooperation between industrial, educational, and research institutions as well as start-ups in terms of widening the scope of work carried out on quantum technologies and includes elements on cybersecurity. Europe is also engaged in similar initiatives.

→ **Tomorrow, there is no doubt that the initiatives will have to extend, potentially up to the creation of a «quantum internet» or a «digital quantum».**
The added-value and the effectiveness of quantum approaches remain to be seen. These approaches could make it possible to implement new mechanisms, with significant opportunities for cyber: transmission of encryption keys between «trusted» nodes, delegation of quantum calculations, distributed quantum computing. Even if much remains to be proven, the uses are various and their interests strong.

CONCLUSION & ACKNOWLEDGMENTS

A FIRST EXERCISE THAT MUST ANCHOR ITSELF IN TIME

In order to be assessed, the solutions proposed in this deliverable must be subjected to monitoring indicators. The Cyber Campus will be able to repeat the anticipation exercise to develop new scenarios and solutions.

In addition, it will be imperative to put in place mechanisms to observe threats, their transformation, and technological advances and usages in order to specify and develop the proposed solutions if necessary.

WE WARMLY THANK ALL THE CONTRIBUTORS

ABOULHADID Ahmed, **NUMERYX**

APOSTOLOS Malatras, **ENISA**

BACHELET Julien, **HERMÈS**

BARKAOUI Badr, **BPCE**

BESNARD Quentin, **ACE CAPITAL PARTNERS**

BLARD Sebastien, **SUEZ**

BLONDEAU Florent, **NAMESHIELD**

BOBIN Maxence, **SQUAD**

CAPRONI Nicolas, **SEKOIA**

CART-LAMY Laurent, **BPCE**

CAUDRON DE CAUQUEREAUMONT, Chantal **AGENCE L'INNOVATION DE DÉFENSE**

CHAILLEY Laurent, **BANQUE DE FRANCE**

CHARRAT Bruno, **CEA**

COLAS Jean-Baptiste, **AGENCE L'INNOVATION DE DÉFENSE**

COUTURIER Nataël, **RED ALERT LABS**

DE FRANCO Franck, **MINISTÈRE DE L'INTÉRIEUR**

DE LIEDEKERKE Arthur, **MINARM – COM.CYBER**

DEBAR Herve, **IMT**

DELPHA Luc, **ALMOND CONSULTING**

DESAMBLANC Thierry, **ENEDIS**

DRAME Aida, **GRTGAZ**

DUAULT Hubert, **INRIA**

DUPONT Sébastien, **CYBER4U**

FEIX Olivier, **GALILEO GLOBAL EDUCATION FRANCE**

FONTARENSKY Yvan, **THALES**

GAULIER Jean-Philippe, **OSSIR – CYBERZEN**

GIANNECCHINI Mathieu, **SIMPLON**

GRANGÉ Benoit, **HUB ONE**

GREMY Jean-Marc, **CLUSIF**

GUENAUX Dominique, **ALSTOM**

HASSAN Lucas, **DGE**

HERMAN Mathilde, **AGENCE L'INNOVATION DE DÉFENSE**

HEURE Jeanne, **CAPGEMINI**

HUMBERT Francis, **MINISTÈRE DE L'INTÉRIEUR**

IGLESIAS Pablo, **LFDJ**

KASSIANIDES Yoann, **ACN**

KIRCHNER Florent, **CEA**

KOLLA Vladimir, **OSSIR - GREENLOCK**

LE PIOLOT Bertrand, **LFDJ**

LECOQ Fabien, **SOPRA STERIA**

LEONETTI Xavier, **MINISTÈRE DE LA JUSTICE**
LEVASTRE David, **CYBERMALVEILLANCE**
LOUIS Nicolas, **SAFRAN**
LOURENCO Paulo, **COVÉA**
MARBAIX Jean-Pierre, **AXA**
MARZLOFF Bruno, **CHRONOS**
MEDA Phillipe, **INNOVATION COPILOTS**
ME Ludovic, **INRIA**
MESEGUER Ivan, **IMT**
NETZER-JOLY Philippe, **ARKEMA**
NGUYEN Vincent, **HS2**
PAVLOV ALEXANDRE, **CYCOVER**
PERETTI Walter, **ESILV**
PITON Thierry, **AXA**
PLASSAT Gabriel, **ADEME**
RIBEIRO Alina, **ORANGE CYBERDEFENSE**
RIBES Vincent, **EGERIE**
STEUNOU Julien, **ALMOND CONSULTING**
TABORET-AGNOLA Manuel,
MINARM – COM.CYBER
TOUBIANA Vincent, **CNIL**
TRIOLOT Benoit, **GATEWATCHER**
VALENTIN Yann, **BPCE**
VAN CAENEGEM Frank, **CNP ASSURANCES**
VINCENT Willy, **RISK & CO**

EQUIPE PROJET :

AJACQUES Jean Baptiste, **AXA**
ARGHERIA Thomas, **WAVESTONE**
BILLOIS Gérôme, **WAVESTONE**
BONNET Yann, **CAMPUS CYBER**
BRIOLAT Lucile, **CAMPUS CYBER**
COUSIN Mathieu, **AXA**
GAINIER Fabien, **CAMPUS CYBER**
QUICHAUD Marguerite, **WAVESTONE**
REGNIER Eleonore, **AXA**
Y BREH HWING Melanie, **CAMPUS CYBER**

FIND THE DETAIL OF ALL THE SOLUTIONS PROPOSED IN THE WORKSHOPS!

https://campuscyber.fr/
communs/

campuscyber.fr