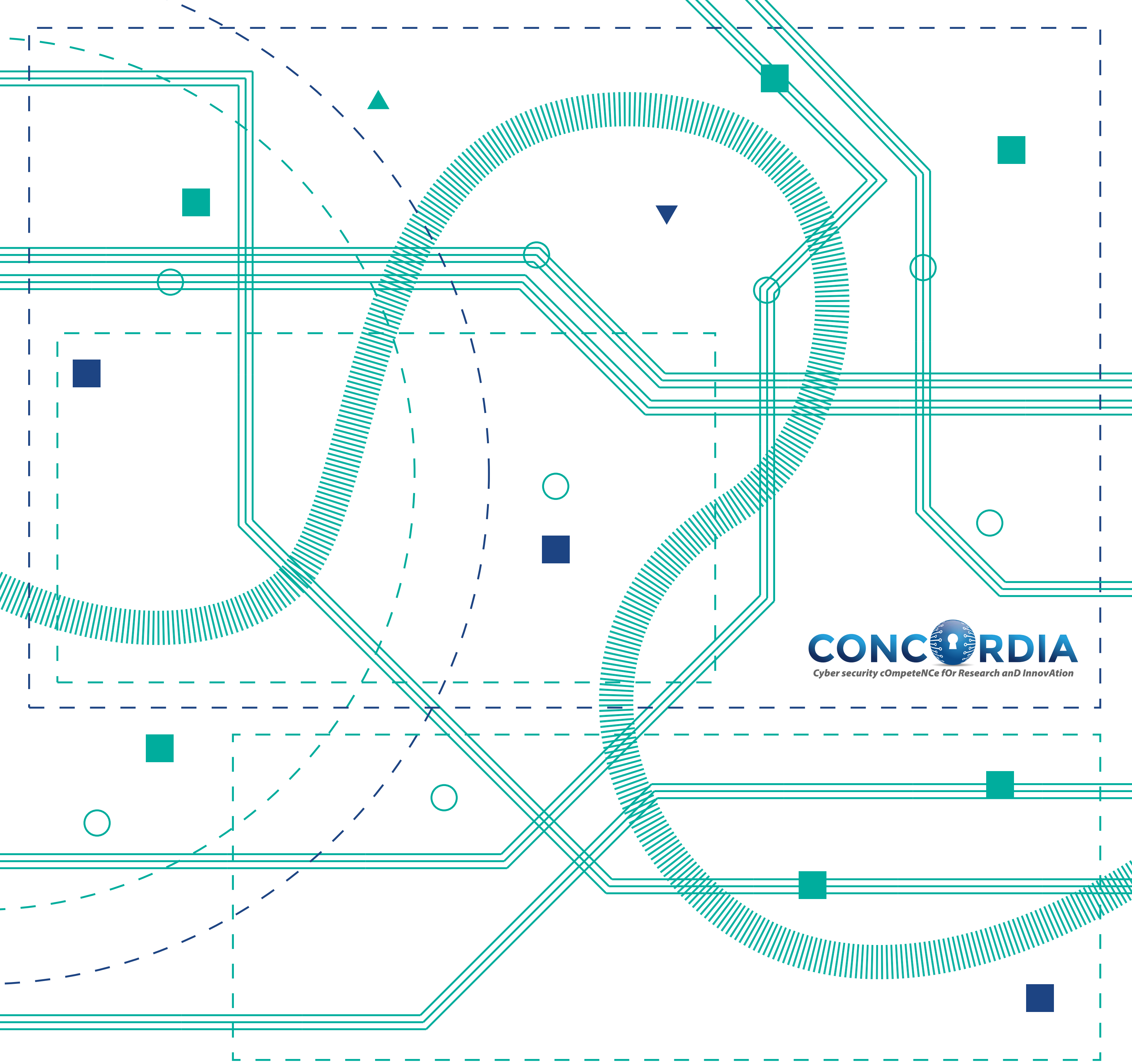


CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Roadmap for Research & Innovation

4 Roadmap for Research and Innovation

As pointed out by Commissioner Breton, the digital sovereignty of Europe rests on three inseparable pillars: computing power, control over our data, and secure connectivity [47]. Computing power means that Europe should have the means to design and manufacture current and future computers, ranging from high- performance microprocessors [48] to quantum computers [49]. Control over our data means that European citizens should be able to trust that their data will be stored on cloud servers operating under EU law [50]. Secure connectivity means that data will be exchanged over a responsible Internet that increases the trust of our citizens [51].

In the next sections, we will identify some of the short-, mid-, and long-term research and innovation challenges we will be faced with. The focus hereby will be on challenges that are novel and therefore not (yet) sufficiently addressed by running EU activities. The results of this discussion will form the Roadmap of Research and Innovation, i.e., the technological roadmap.

CONCORDIA takes a holistic view on cybersecurity and identifies five layers (Figure 3), as from the analysis of the threat landscape:

1. Device
2. Network
3. Software/Systems

4. Data/Applications
5. the User's layer

4.1 Device

The need to improve the security of devices is to a large extent motivated by the dramatic growth of the IoT. As part of their home automation, end-users will connect tens of billions of consumer devices to their Internet. To protect the privacy of these end-users and to avoid that these devices become part of a botnet, security awareness and measures should be strengthened. Less visible, but from a digital sovereignty point of view probably more important, are the devices that are embedded within cars, drones, and the devices that control our critical infrastructures and industrial systems.

To ensure Europe's digital sovereignty, Europe must keep its ability to develop its own hard- and software infrastructures. In the past Europe always had a strong chip industry, and for the future, we should ensure that Europe remains the ability to design and manufacture its own high-performance microprocessors and other chips. In the next decades, we may expect that traditional computers will partially be replaced by quantum computers, which implies that Europe should strengthen its research in the area of quantum computers.

Traditionally, Europe has been strong in developing new devices such as mobile phones, as well as in developing software, including programming languages (such as Simula, Prolog, Pascal, Eiffel, Haskell, Python, PHP) and operating systems (Linux). However, for more recent developments, such as Artificial Intelligence (AI) and Machine Learning (ML), the European influence seems to diminish, despite some positive developments such as the European Laboratory for Learning and Intelligent System (ELLIS Society).

4.1.1 Transparency in the Software Supply Chain

To improve the security of devices, the software supply chain must become transparent. An enhanced level of transparency will also reinforce trust between the various parties and other relevant stakeholders. These notions have for instance been formulated by Allan Friedman, who is director of Cybersecurity Initiatives at the National Telecommunications and Information Administration at the US Department of Commerce. The problem with current device software is that it comes from many different sources, and even device developers do not oversee the origin or supply chain of the software that is included in the device.

Actions: *To make the chain of components and their relationship transpar-*

ent, a Software Bill of Materials should be included with each device. Such Bill of Materials can be expressed in terms of a Software Package Data Exchange (SPDX), as being developed by the SPDX workgroup of the Linux Foundation.

4.1.2 IoT Device Updates

Even if devices are tested and certified to be secure, and vulnerabilities will be discovered sooner or later. It is therefore important that each device includes facilities to be updated. To make such updating straightforward, current devices can be updated automatically over the air. For that purpose, consumer devices regularly contact servers at the vendor, to check if security updates areavailable.

A problem with this approach is that vendors can take over any device, by in- stalling a prepared "security update". Current approaches to update devices provide a backdoor to vendors and nation-states to take over devices. By taking control of such devices, vendors and nation-states can have the ability to spy on individual citizens and to misuse devices for large-scale attacks. This is particularly worrying since most IoT devices, or part of them, are not manufactured by European vendors Actions: To deal with this problem, all consumer devices must provide secure software update mechanisms. Besides, software updates should not only be triggered by the vendor, but they should also be certified. European researchers and regulators should therefore develop novel approaches and techniques to make such double certification possible.

4.1.3 Continuous Re-certification with Open Hardware and Software

The EU Cybersecurity Act aims to introduce for the first time an EU-wide security certification scheme for electronic devices. This presents unique challenges for research and industry. In the case of safety certification, a rigorous process of testing and documentation endows a high level of confidence that a device will behave as expected. In contrast, history has shown time and again that every complex software system contains exploitable vulnerabilities. Hundreds are discovered in the Linux kernel every year.[3]

In practice, security depends on our ability to issue software update patches as soon as vulnerabilities are discovered. There are three basic building blocks required to automate this process on IoT devices, namely:

6. Digital certificates backed by a reliable PKI are needed to sign firmware images. For encrypted updates, digital certificates also provide the basis for end-to-end security between devices and update authors.

[3] ***CVE Details, Linux Kernal***, accessed 14/12/2020

7. A trusted execution environment (TEE) on each device provides hardware- enforced isolation of security-critical software.
8. A small amount of trusted immutable code (i.e., the trusted computing base, or TCB) with exclusive access to the device hardware root of trust.

The TCB code executes in a TEE and is responsible for installing firmware updates on the device, and for providing the device owner with cryptographic proof that this has been done correctly – a process known as remote attestation. The advantage of this approach is that only the TCB and the hardware itself is fully trusted. The operating system and application code are complex and therefore likely to require security patches.

Actions: *Ultimately, our objective is to create an automated re-certification solution, whereby devices can be issued with an EU-backed security certification that is valid until a vulnerability is discovered. When this occurs, devices must be patched and re-certified without any physical interaction. There are already ongoing efforts in the IETF SUIT working group to standardize the distribution of firmware updates and metadata.[4] One of the prime research focuses could be the implementation of TEEs on open-source RISC-V architectures that suits low- power IoT. With automated PKI, software updates, TEE, remote attestation, and dynamic AI-based code analysis, the vision of automated re-certification can become a reality.*

4.1.4 Device Identification and Assessment Mechanisms

Secure device identification is an essential step for establishing trust in a distributed computing environment. Being able to distinguish a clone from an expected genuine device is essential but not trivial. One approach is to design hardware components that can safely store device identity information (e.g., a device key) such that it is impossible to clone the stored information. The current trend is to make these hardware components more flexible and programmable, which will lead to a situation where the complexity of the security software grows to a point where its correctness the security software cannot be guaranteed any more. An alternative approach is to use physically unclonable properties of a device to establish the identity of the device.

Related to the identification of the device is the identification of the software components that are installed and/or running on a device. It is necessary to continuously assess the integrity of the software components and to detect attempts to compromise a device, including attacks exploiting so called zero-day vulnerabilities.

Device identification and assessment mechanisms need to be complemented by remote attestation protocols, which enable authorized third parties to assess the integrity of a device and its software and to detect changes. These protocols should be standardized, and the industry will benefit from openly available reference implementations.

Actions: *Develop device identification mechanisms that exploit physically*

[4] ***Datatracker***, accessed 14/12/21

unclonable properties of devices. Develop novel techniques to continuously assess the integrity of installed and running software and that can detect deviations from expected normal control flows. Create standards and reference implementations of remote attestation protocols that enable applications to assess the identity and integrity of devices.

4.1.5 Embedded Operating Systems Utilizing Hardware Security Features

Hardware designed for embedded systems is nowadays being extended with special hardware security features that enable the separation of the execution of un- trusted code running in a "normal world" execution context from the execution of trusted code running in a "secure world" execution context. Many new embedded operating systems have recently appeared but only a few exploit hardware security features to their full extend. While some embedded operating system projects are truly open source, others are driven by vendors promoting specific hardware designs.

As embedded hardware becomes increasingly powerful, it will be useful to converge on a common embedded software framework that supports a larger number of embedded hardware designs. Hence, it is highly desirable to develop a common European open-source embedded operating systems utilizing hardware security features from the ground up. Ideally, this builds on existing expertise with open-source embedded operating system activities that are not controlled or driven by a single vendor.

Actions: *Development of open-source embedded real-time operating systems that fully exploit hardware security features and that are not bound to vendor- specific and proprietary hardware solutions.*

4.1.6 Microkernel Isolation and Virtualization Mechanisms

In industrial environments and modern vehicles, the number of embedded control units is steadily increasing and reaching a point where consolidation is desirable since having separate embedded control units for each function is expensive and not scalable. Virtualization systems based on microkernel architectures start to become feasible and affordable for virtualizing embedded control units. However, more research needs to be done to achieve the level of isolation required for safety- critical functions. Besides, functions need to be integrated that can continuously measure the integrity and separation that is being achieved.

Actions: *Development of light-weight virtualization mechanisms for the embedded devices that provide isolation and resource control satisfying the requirements for virtualizing safety-critical functions.*

4.1.7 Open-source Secure Processor and Hardware Designs

Critical infrastructures require trust in all software and hardware components. The availability of well-maintained open-source software has enabled the software industry to build software, including the software necessary to build software, from scratch using open-source components. On the hardware side, the industry typically relies on closed hardware designs and it has very limited tools at hand to verify whether a given piece of hardware is free from hidden functions or possible backdoors.

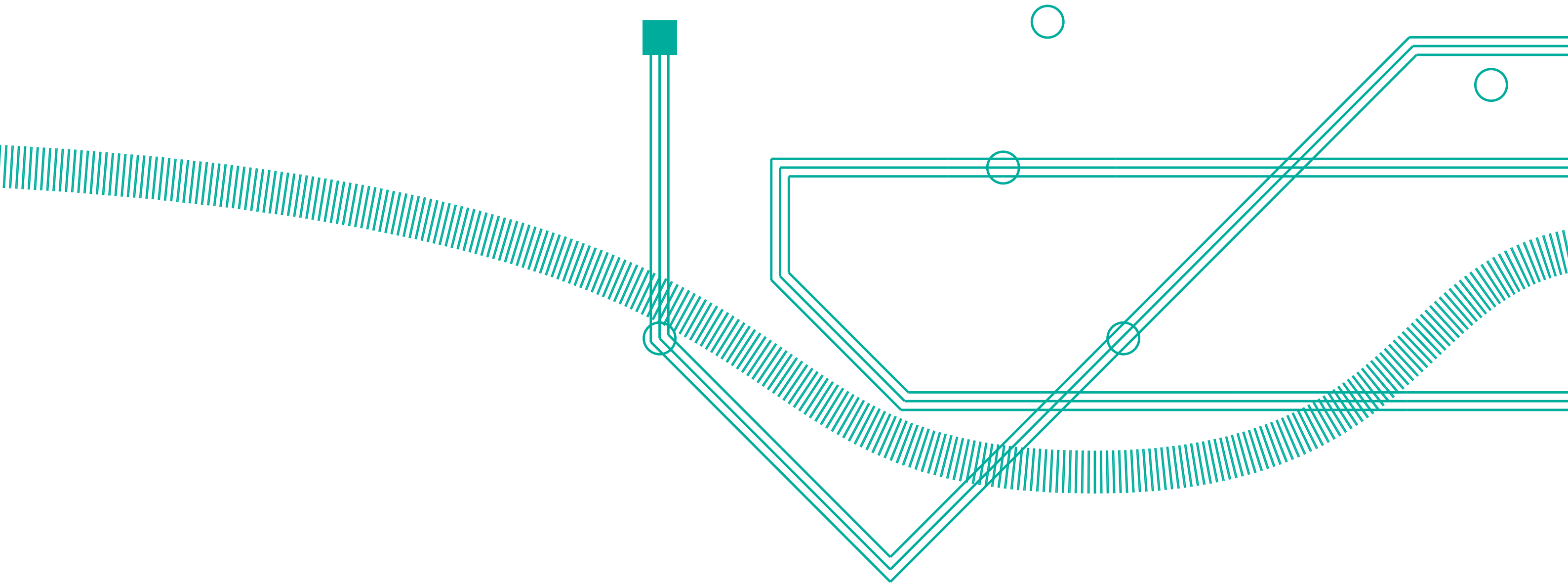
There is a movement towards open hardware designs. A prominent example at the processor level is the RISC-V project, providing an open-source CPU instruction set architecture enabling everybody to create RISC-V processors. Developing security extensions for RISC-V and hardware designs based on RISC- V technology will enable the industry to obtain hardware components from a variety of hardware components vendors, providing eventually the same control over the hardware components that are already possible on the software side.

Actions: *Create an ecosystem of open-source hardware designs enabling vendors to fully control the production of hardware components, which are used in products controlling critical infrastructures.*

4.1.8 Postquantum Cryptography Schemes on Constrained Devices

As quantum computers evolving to a real computational reality in the next few years, modern cryptography solutions (especially public-key cryptography) need to be reinvented to avoid quantum processor-based cryptanalysis that can lead to full disclosure of secrets in a reasonable amount of time. Thus, the cryptography research community in the past few years has invested time and effort to design and promote postquantum cryptography schemes that withstand quantum cryptanalytic attacks. NIST has launched a competition to award a standardized postquantum cryptography solution for Key Encapsulation Mechanisms (KEM) as well as Digital Signatures. The European research community has a prominent role in this process with several PQC (Post Quantum Cryptography) schemes reaching the final competition round. The competition will be concluded in the upcoming years and the winner schemes will be broadly adopted by the security community. How- ever, when such schemes are transferred to the IoT environment and especially in resource-constrained end nodes, several implementation aspects need to be considered that is not originally included in the postquantum cryptography algorithm definition. The relatively big cryptography keys used by the PKE schemes as well as the computational complexity of those schemes may drain the resources of the existing IoT end node devices. The devices themselves may be deployed in a "hostile" environment where they may be attacked using side- channel attacks. Furthermore, security schemes for the IoT domain, like CoAPs do not consider PQC solutions and further adaptation at the protocol level should be made (e.g., on TLS or DTLS).

Actions: *The PQC solutions should be adapted to the IoT and Industrial IoT environment so that it can become deployable on resource-constrained devices. Also, PQC scheme implementations should be protected against side-channel attacks, including high order side-channel attacks. Existing IoT protocols that support security, should be adapted to the postquantum era by supporting PQC ciphers for KEM and digital signatures. Lightweight PQC scheme versions should also be researched and promoted to match the non-functional requirements of IoT end nodes and cyber-physical systems employed in the IoT/IIoT paradigm.*



4.2 Network

Europe has an excellent track record in the area of networks. Europe has played a major role in the standardization and development of mobile networks, with companies such as Siemens, Alcatel-Lucent, Ericsson, and Nokia and the like. Technologies such as Wi-Fi and Bluetooth were developed in Europe. Three of the largest Internet Exchanges are located in Europe (DE-CIX, AMS-IX, LINX), and connectivity for citizens and companies is world-class.

Europe is challenged, however, by the US and China (Huawei). If Europe loses control of its own networks, it runs the risk of becoming a digital colony of the US and/or China. Such development would not only have severe consequences for European companies (manufactures as well as operators), but ultimately our society and European values are at stake.

As Thierry Breton, the European Commissioner for the Internal Market already said, the digital sovereignty of Europe rests on three inseparable pillars: computing power, control over our data, and secure connectivity (=networks). Whereas major European programs already exist for computing (processors, quantum) and data (GAIA-X), a major program for networking seems to be missing. In this section, we will therefore identify some challenges to improve the security of European networks. Probably Europe's biggest problem is that of fragmentation. Worldwide, we witness a consolidation phase, where big companies take over smaller competitors. At this moment Europe has more than 50 mobile operators [5], of which only Deutsche Telekom, Telefonica, and Vodafone are within the top-ten [52]. The revenue of these three operators together is comparable to that of the biggest US operator (AT&T).

Because of this fragmentation, the security groups at most individual operators are relatively small and just able to follow the market. Real innovations often come from outside Europe, as is the case with DDoS protection services, DNS over HTTPS (DoH), and, more generally, the collection of network data that may be relevant for security.

A long-term solution for these problems would be the consolidation

[5] ***List of mobile network operators of Europe*** – Wikipedia, accessed 14/12/2020

[6] Note: *the term 5G security is sometimes used as an umbrella to denote the various steps that Europe needs to take to make its networks secure. The problem with such a term is that 5G is generally associated with mobile networks, leaving fibre and cable infrastructures aside. Besides, umbrella terms are generally not specific enough to identify the exact actions that need to be taken.*

of smaller EU companies into bigger, more powerful companies. Due to the federated nature of Europe, such development would be politically extremely sensitive, and therefore, not attainable in the short term. Fortunately, there are also many research and innovation actions that Europe could take now to strengthen its digital sovereignty and to ensure the security and privacy of its citizens.

One of the keys to all actions is to implement and monitor data sharing such as reflected in the Data Strategy of the Commission and making infrastructures transparent.[6]

4.2.1 Open Networking: The Responsible Internet

The problem of declining digital sovereignty is being addressed in several ways and different areas of technology, [51]. For example, Artificial Intelligence (AI) researchers have developed design guidelines to make the decisions of AI algorithms more transparent and explainable through what they call ‘responsible AI’. Similarly, the European Commission is driving the development of a European federated cloud service called ’GAIA-X’ that aims to improve Europe’s data sovereignty. The European Commission recently also mapped out various policy instruments for areas such as 5G cellular access networks and the Internet of Things.

While these developments illustrate that digital sovereignty is a widely acknowledged and urgent problem, we observe the discussion largely overlooks the Internet infrastructure: the technical systems (e.g., routers, switches, and DNS servers) that enable remote internet devices to communicate with each other and that all of the other ‘layers’ (policy-making, AI, data) depend upon. The exception is the debate around the alleged security weaknesses in 5G equipment. According to the EC, these pose a risk to the strategic autonomy of the European Union, but 5G networks only cover the cellular access part of the internet infrastructure.

The specific sovereignty problem in the Internet infrastructure is that users have no insight in, or control over how they depend on network operators and their systems, which ultimately poses a serious limitation for governments, institutions, companies, and individuals to decide how they can securely communicate. This is particularly relevant for critical service providers (e.g., power grids, transportation systems, mobile networks, and manufacturing facilities), which have become increasingly dependent on computer networks. For example, such providers want to know if the internet routes their traffic through networks with equipment that might have backdoors. At the same time, internet users by design depend on third parties because the Internet is a massively distributed and global system of some

70.000 autonomous networks. For example, during a typical website visit, users unknowingly make use of the services of several DNS operators, transit providers, cloud services, and content distribution providers, all of which may reside in different geographical locations and jurisdictions.

Actions: *To fill this gap in the digital sovereignty discussion, we propose the notion of a* ***Responsible Internet****, a novel security-by-design extension of the Internet (or future networks) that offers users (e.g., providers of critical services or individuals) additional security-related options that give them a better grip on their dependencies on the internet, thus increasing their trust in and their sovereignty over internet communications. A Responsible Internet accomplishes this by making its networks more transparent, accountable, and controllable. This means users can ask a responsible internet to provide high-level descriptions of the chains of network operators (e.g., ISPs, data centres, and DNS operators) that potentially handle their data flows, for instance in terms of security and administrative properties, their interrelations, and the management operations they carried out (transparency). A Responsible Internet allows users to verify that these details are accurate (accountability) and to subsequently instruct the responsible infrastructure to handle their data flows in a specific way, for example by allowing them to only pass through network operators with certain verifiable security properties (controllability). The notion of a responsible Internet is inspired by responsible AI, a design paradigm that focuses on giving people more insight into how AI systems reach decisions and why.*

4.2.2 Trustworthy DNS Resolver Infrastructures

The DNS system takes care of translating domain names into IP addresses (e.g., `www.concordia-h2020.eu` – 139.91.90.171). Since DNS data provide a high- level overview of what network services exist and are used, DNS data is crucial for security purposes. However, in the absence of proper privacy protection rules, DNS data can also be misused to monitor the behaviour of individual users. Fortunately, Europe has strong rules to protect the privacy of its citizens.

In the US such rules are lacking, and Internet providers are allowed to monitor the websites that their customers visit and sell that information to an advertisement and other companies. Since many customers do not like this, many US companies, most notably Google and Cloudflare, introduced the possibility to use DNS over HTTPS (DoH). By using DoH, Internet providers can no longer monitor the websites that their customers visit.

DoH is aggressively promoted by companies such as Google, and in the US browsers like Chrome and Firefox use DoH by default. However, migration towards DoH introduces the following problems:

- US companies like Google and Cloudflare collect even more data of European citizens,
- For European Security Operation Centres (SOCs) and national intelligence services it becomes harder or even impossible to detect security breaches,
- One of the most important Internet services, DNS, thus becomes under the control of a small number of (US) companies. This introduces vendor lock- in and potential single points of failure.

Actions: *Although some aspects of DoH could potentially improve security, it is clear that changes are needed to solve the problems mentioned above. Research is therefore needed in the short term to address these challenges and make the necessary improvements.*

4.2.3 DDoS Protection Services

In a relatively short period, the Internet has become one of the, or probably the most important infrastructure(s) that our society relies upon. If the Internet would fail, airports, harbours, and shops should be closed, payment systems will fail, and working from home (in these times of COVID-19) becomes impossible.

In the last decade, we have witnessed an immense growth regarding the number as well as the strength of Distributed Denial of Service (DDoS) attacks on this vital infrastructure. Only five years ago most attacks were initiated by youngsters, spending a few Euros on a DDoS as a Service website (booter, stresser) to attack their favoured bank. Fortunately, the mitigation of such attacks is relatively straightforward. Nowadays, however, we see ransomware attacks by criminals with strong technical skills on the Internet and Service Providers. These new attacks are quite challenging and therefore have the potential to disrupt parts of our society for longer periods.

To defend against DDoS attacks, many companies and organisations have outsourced their protection to Akamai, Cloudflare, and similar services. Although on average these DDoS protection services perform well, the fact that many of them are US-based creates new problems.

First, protection against layer 7 attacks often require that these companies should decrypt all data, including sensitive data such as medical health records and online payments. In principle, this gives Intelligence Services from outside the EU access to private information from EU-citizens. This is not only undesirable but might in some cases even be illegal.

Second, it creates a dependency on vital EU-services (such as healthcare end payments) on services from outside the EU. From the point of view of digital sovereignty, this is not what Europe should aim at.

Actions: *It is important to further develop open and European approaches towards DDoS protection. The DDoS clearinghouse, as being developed within the EU CONCORDIA project, is a good first step. However, the focus of the DDoS clearing house is to share fingerprints of previous attacks, and not to protect against possible future attacks. Therefore, it is important to the extent the Clearinghouse with protection capabilities.*

To cope with Terabit per second attacks, protection should be distributed over many locations, using technologies such as Anycast. In fact, a collaborative or federated protection architecture can be envisioned, in which similar services (for example banks or ISPs) share their DDoS protection capabilities to create a scalable DDoS protection service. More research on collaborative DDoS protection mechanisms is therefore needed now.

4.2.4 Monitoring and Data Collection Infrastructure (Data Lakes)

The key to secure systems, services, and infrastructures, is the availability of data. Examples of data relevant for (network) security include DNS data, BGP data, location data, log files, traffic traces (pcap and flows), open ports, etc. Data is not only needed to detect future threats but also to understand trends. Data should therefore be stored for later analysis in so-called "data lakes".

Every day the Internet is scanned by many parties. For example, criminals scan to find potential ransomware victims, nation-states scan to understand the state of the art, commercial organisations scan to share and sell data to interested customers. Examples of projects and organisations that scan the Internet include shodan.io, censys.io, RIPE Atlas, and OpenINTEL. But also, passive data is important for security; examples include BGP data from Hurricane Electric, traffic traces from CAIDA, and security incidents by Shadowserver.

Actions: *Europe should have the ability to collect, analyse, and archive the data that it considers important to secure its citizens and society. Of course, such activities should protect the privacy of its citizens by fulfilling the requirements of the GDPR, which means that critical analysis is always needed to decide which data is collected, and which not. Such analysis needs to be transparent for the general audience.*

From a research perspective, the challenges include questions like:

- *how to perform scanning in a scalable and privacy-sensitive way,*
- *how to quickly analyse huge data sets (big data analysis),*
- *how to correlate different and sometimes incompatible data sets (Machine Learning),*
- *how to condense and archive historical data, without losing precision, how to federate smaller data lakes to create bigger and therefore*

richer data lakes, without violating legislation or losing trust.

4.2.5 Network Assurance & Certification

The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services, and processes to ensure security and trust in ICT systems, including mobile networks, across development, deployment, and operations. ENISA has a key role in setting up and maintaining European cybersecurity certification schemes. For instance, ENISA is currently considering adopting the GSMA/3GPP NESAS/SCAS [53, 54] certification scheme that has been jointly developed by GSMA and 3GPP for the certification of mobile networks equipment.

On the other hand, ICT technologies are developing at a fast pace and rapidly introduced in ICT systems, which in turn are increasingly being developed and released and deployed following the Continuous Integration & Continuous Deployment (CI/CD). However, Security Assurance Frameworks (SAF) have not evolved at the same pace as ICT systems:

- **Stasis:** SAF processes are defined for static targets with limited borders and features at a given point in time. Assurance for targets in development & operations is not sufficiently defined.
- **Slow and expensive:** SAF takes a long time to conduct with human-based evaluation work by skilled experts from various security fields in addition to the target's domain of application.
- **Inertia:** Upgrades or patches are either ignored or heavily delayed in domains with strict security SAF policies. Otherwise, vendors upgrade products but refer to outdated SAF proofs.
- **Waterfall:** SAF follows conventional waterfall process whereas ICT systems are engineered increasingly by Continuous Integration Continuous Deployment (CI/CD) practices.
- **Blurred targets:** SAF is equipment/device-oriented for bundled software and hardware. But ICT softwareization and virtualization decouples software from infrastructure blurring the target's borders across software, infrastructure and service providers.
- **Technology (dis)trust:** There is a growing distrust on technology (origin) fearing backdoors in systems or components. It is not clear whether SAF can provide trustworthiness in this case.
- **Artificial Intelligence:** ICT systems are becoming AI-assisted. It is not clear how to evaluate AI unexplainable internals and its robustness against a new class of "intelligent" AI-based threats [55].

Actions: *To enable an agile and trusted EU digital market, where the latest technology can be leveraged in ICT systems that in turn can be trusted based on evidence from agile security assurance frameworks, it is imperative* *to perform further research and foster innovation.*

Short-term actions:

- ***Metrics:*** *SAF should develop better quantitative metrics for measuring ICT trustworthiness.*
- ***Explainability:*** *SAF outcome is written for experts, but difficult to understand by stakeholders, not in the security field. Explainable and comprehensive assurance is needed for legal purposes, business decisions, and policymakers.*
- ***Automation & formal proofs:*** *SAF should leverage the latest advances in AI for automation of the assurance and re-assurance process to reduce the human-factor that is subject to subjectivisms or prone to errors. Automation is also an enabler towards formal proofs of assurance.*

Long-term actions:

- ***Embedded:*** *SAF should be agile and possible to embed in the ICT CI/CD lifecycle: development, deployment and operations. This would reduce theassessment and re-assessment burdens.*
- ***AI:*** *SAF shall include best practices end methodologies for evaluating the robustness of AI-based ICT systems that may contain bias or vulnerabilities against adversarial AI attacks.*
- ***Softwarization & Virtualization:*** *SAF should provide methodologies for assurance of virtualized and softwarized targets that are decoupled but still dependent on hardware and infrastructure.*

4.3 System

Future research to improve the security of systems includes research on Quantum Technologies and Artificial Intelligence.

4.3.1 Quantum Technology

Quantum Technology (Q-tech). Q-tech is receiving high attention in research, industry, and governmental agencies. It is therefore important to outline an informed strategy based on a good understanding of the current status of the Q- tech and prioritize the right topics.

Based on existing research in Q-tech related initiatives [56] we can summarize the current status as follows:

- **Quantum Computers:** building a quantum computer is highly expensive and difficult. Its application is not general yet, i.e., it can efficiently solve a few specific problems (e.g., optimization problems).
- **Quantum attacks on crypto:** A recent report by experts from academia and industry judged that the construction during this decade of a quantum computer capable of breaking currently used public-key crypto would be highly unexpected. Symmetric crypto is quantum-safe, e.g., SIM card authentication. The business case for quantum adversaries is thus questionable. How- ever, quite a lot of research and development is focused on post-quantum cryptography (sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant).
- **Quantum crypto:** Evaluating and standardizing new crypto-systems necessarily takes time. The industrial benefits of quantum crypto are not directly applicable to all industries. Each industry sector needs to assess its suitability and feasibility.
- **Quantum key distribution (QKD):** QKD is suitable in quantum communications and research shall remain in this quantum domain. QKD is primarily seen as a replacement of currently established key distribution protocols used for authentication, signatures, or integrity. Projects such as the EU H2020 project OPENQKD are building the EU's sensitive data and digital infrastructure for years to come.
- **Governmental intelligence agencies:** Based on authoritative sources, they are not in a hurry replacing commercially used public-key encryption.
- **Quantum simulators:** while useful in some domains, quantum simulation environments for cybersecurity purposes are questionable and no meaningful use case has been identified.
- **Quantum Internet:** The Quantum Internet is a network that will let quantum devices exchange information (Qubits) across a network with multiple quantum devices that are physically separated. The US Department of Energy [57] lays out a blueprint for the development of a national quantum Internet.

Actions: *Based on the current state of the art and estimations about the expected progress the following research is needed:*

- ***Open post-quantum crypto:*** *Research in post-quantum crypto (aka quantum- safe) is of high-importance including wide and active participation in relevant standardization bodies such as IETF, NIST, 3GPP to ensure many-eyes expert reviews in an open transparent process. We need to avoid lock-in proprietary schemes taking over the market.*
- ***Resilience:*** *For industries relying on public-key cryptography (PKC), prepare risk-based recommendations on: i) develop post-quantum systems based on authoritative upcoming NIST standards; ii) prepare timed transition processes based on the progress of the authoritative research community; iii) prepare replacement, contingency, and containment strategies. For industries, this includes inventories of PKC-based protocols used (TLS, IPSec, S/MIME, SSH) and its base deployment in devices, appliances, networks, and services.*

4.3.2 Adversarial Artificial Intelligence Attacks and Countermeasures

A very important aspect to be considered in AI usage for security purposes is the intrinsic vulnerability of AI data, algorithms, and models to adversarial AI attacks. This new attack surface can be considered hard to mitigate. AI adversarial attacks cannot be fixed since they rely on the learning nature and unavoidable use of data of an AI algorithm. AI technologies can be used as weapons for performing cybersecurity attacks by generating malicious traffic, malicious code as well as automating the hacking process. This weaponization of AI can be very potent since it is adaptable to the countermeasures provided by defenders. In parallel to this type of attack, data poisoning and model poisoning can also be performed to attack an existing AI infrastructure. These adversarial attacks on legit AI systems aim to render such systems blind to a specific type of inputs or reduce the AI systems' accuracy as a whole. The current threat landscape is very broad and has been identified as critical for the secure use of AI in European security and privacy sensitive domains (Law Enforcement, Health, Critical infrastructure domains, etc.). Also, it should be mentioned that there exists no well-structured detection framework that can assess vulnerabilities of AI systems against adversarial AI attacks or weaponized AIs. Given the growing usage of AI solutions, the need for such an assessment mechanism becomes great.

Actions: *Acknowledging the potency of the above-mentioned attacks, agencies, organisations as well as industries across Europe should establish a "security net" for detection, response, and mitigation. The goal should be to create the means to: i) reduce the risk of attacks on AI systems, and ii) mitigate the impact of successful attacks.*

AI adversarial attack protection (security net) can be structured in three *layers, planning, implementation, and mitigation:*

- ***Planning:*** *At the design phase of an AI solution, including evaluation of possible training datasets as well as a choice of AI classifier and modelling algorithms, an AI risk assessment process could be formalized to perform "AI Suitability Tests" that assess the risks of current and future application of AI datasets and algorithms. An acceptable level of AI use within a given application could be provided as an outcome. These tests should weigh the application's vulnerability to attack, the consequence of an attack, and the availability of alternative AI-based methods. Apart from the above, the AI risk assessment can also perform a formal validation of data collection practices and suggest mechanisms for protecting data and restricting data sharing to trusted entities only. Finally, in the planning layer, best practices should be extracted to manage the entire lifecycle of AI systems in the face of AI attacks. These practices apart from technical aspects they will include strategic, operational as well as legal/ethical aspects of AI deployment.*
- ***Implementation:*** *During this layer, the best practices should be further consolidated into adopted IT-related reforms on ATI solutions to make AI attacks more difficult to execute. The process relies heavily on setting up security/cybersecurity mechanisms that will protect the assets which are used to craft AI attacks, such as datasets and models e.g., by improving the cybersecurity of the systems on which these assets are stored. This includes installing cyber defence mechanisms that support the CIA triad and detect cyberattacks (intrusion detection, anomaly detection, etc.) using hardware and software means.*
- ***Mitigation:*** *Mitigating AI attacks is not an easy task since such attacks are advanced and have very recently appeared in the security domain. Existing research proposals should be extended to mature solutions. Detection and Mitigation techniques could rely on decreasing the success rates of back door (harder to identify and track) attacks also known as poisoning attacks (e.g., "pruning method") but also techniques that introduce defence mechanisms (for detecting AI-based attacks) like Adversarial Training, Defensive Distillation, Generative Models and Regularization of datasets. The goal of the mitigation layer should be to:*
    - » *Harden AI models to be resistant to fault data injection and poisoning attacks (during design).*
    - » *Infuses the AI models with detection mechanisms so that they can classify (apart from valid data) also malicious data (during AI operation).*
    - » *Record the cybersecurity incident related to the detected attacks and report it to the cybersecurity community.*

4.3.3 Malware Detection and Analysis

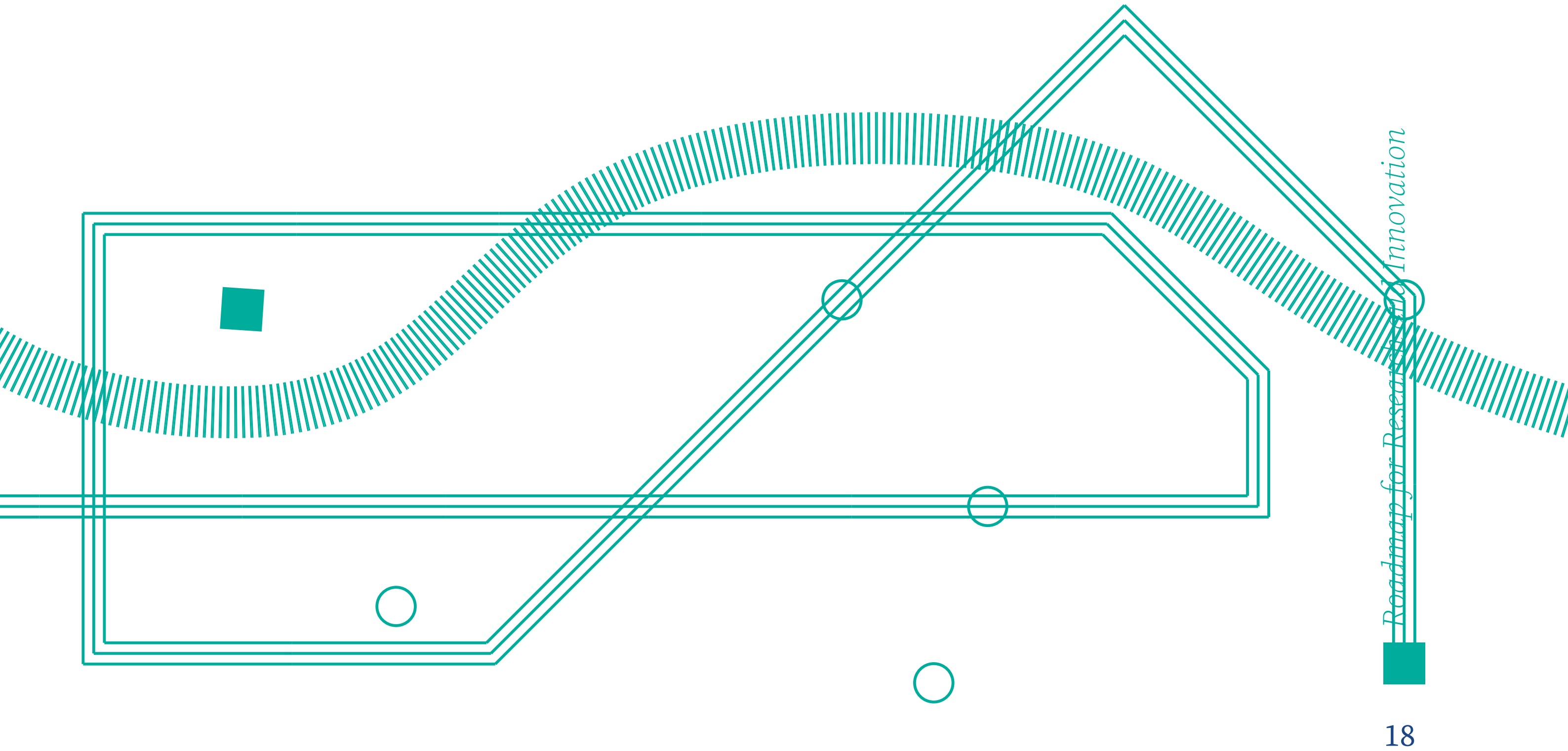
Ransomware, and more generally malware encompassing a lot of other threats like spyware and botnets that weaken our digital systems. The surface of attacks of malware are broader and broader, it includes all IT infrastructures: computes, smartphones & tablets, IoT devices, cars, and industrial infrastructures. They are aimed at the ordinary citizen as well as companies and administrations, even hospitals. The design of these malicious codes is increasingly complex. That is why even old malware strains can be undetected, like recent Emotet attacks. The consequences are financially huge and can also lead to a malfunction of our critical infrastructures.

Actions: *In this arms race, it is necessary to develop new malware defence concepts. A holistic approach that considers a broad set of information, is necessary. That said, there is also room for improvement to devise newcutting-edge anti-virus products by combining machine learning and formal methods along with system events augmentation.*

Lastly, it is crucial to have access to a shared platform of malware collection and their related information.

4.3.4 Explainable Security Deep Analysis

Nowadays, ML approaches are more and more prominent as methods to analyse, classify, and then take action. This is quite well-known in systems like face recognition, but there are other applications like network traffic analysis or malware detection. In each case, it is important to be able to explain an analysis performed by AI systems and give reasons justifying actions taken (i.e., explainable AI). Thus, in forensics, proofs or attribution of an attack is a key issue, and so analysis should be returned enough explanations. Another field is one of the embedded systems. Decision systems in a car should be able to provide a reason for a decision.



Actions: *In the domain of cyber-security, it is worth to develop Explainable Security Deep Analysis. This domain is already an important subject in AI, so we should have a closed loop in this direction.*

4.3.5 Service Dependency Roadmap

The complexity and a plethora of services involved in distributed systems such as the Cloud entails significant and often manual work to understand the interconnection and the behaviour of the services in the system. This hinders the profiling of threats and their propagation in the system. We plan to automate this process by using the capabilities of model checking that would essentially enable profiling and analysing the potential paths that could be taken by a threat to propagate in the system.

Actions: *The midterm goal for the service dependency task is to develop techniques to perform automated multi-level threat detection in a large-scale data centre or cloud systems. This inherently enables the cloud providers to assess the potential propagation paths of the threat and consequently, prioritize the services accordingly.*

4.4 Data

To achieve digital sovereignty and increased levels of information technology security at the European level, it is important to identify research challenges that can act as enablers for the European industry to build the most secure products in the world (Security made in Europe). Here we present future research directions that are specific to data/ application security.

4.4.1 EU-Controlled Cloud Infrastructure (GAIA-X)

The EU aims to create GAIA-X, a secure and federated cloud European infrastructure that meets the highest standards of digital sovereignty by combining existing central and decentralized infrastructures. Consequently, common requirements derived from all European partners, openness, transparency, and use of secure, open technologies are important and will be used as foundations on which the framework aims to be built. It is thus necessary to provide access to secure, trustworthy and automated services and API-controlled infrastructures. Solutions must be able to minimize the leak/loss of data and increase security in software/applications development, to facilitate increased data value and support cross-sector cooperation.

4.4.2 Smart Technologies

The future of the facilitation of everyday life lies in smart technologies. Smart and green energy systems will generate electricity, store it, and interact with the power grid to provide the necessary energy. Smart health monitoring systems will provide care based on distributed data and intercommunication with other systems or actors (e.g., medical personnel). Smart commerce will facilitate international activities based on multiple types of data as well as numerous stakeholders. Hence, it becomes increasingly necessary to develop the means to manage and audit the security of such a system and continuously re-assess the security risk of the systems they form. The boundaries between end-user systems and infrastructure are increasingly blurring, raising the prospect of critical services being impacted by vulnerabilities at the edge. Increasingly, smart technologies embed various forms of intelligence, machine learning being the most common one amongst them. This enables us to adapt services to the current context and to create new ones. However, ML and AI also have new vulnerabilities that are as yet poorly understood. It is important to uncover and develop means of mitigating them. Best practices for interconnecting smart devices must include end-to-end security of an application and its communication with external services, data confidentiality/ integrity/availability/anonymity, privacy controls over accessibility at different levels concerning actors and compliance with related assurance and certification standards.

4.4.3 Securing Data/Software in Distributed Computing Environments

The IoT ecosystems are on the rise and with the imminent adoption of 5G, it will continue to grow, even more, creating multitudes of networks where data is being exchanged among and applications are executed on the different components. In this multi-device distributed environment, data can be used to provide integrity and trust among the communicating entities/running software, by securely identifying all involved parties. Operating systems driving such data/software, as well as the ability to securely update them, also play an important role in such environments. Thus, it is important to be able to provide solutions that secure this kind of data, their exchange, and the applications that depend upon them. We expect research in the future to tackle these important subjects as well.

4.4.4 Inter-Networking in the Future

Data flows through the Internet in massive amounts. However, users do not usually have a say in how their data is being processed and handled: who is responsible, where it is stored, in what format, under what security measures, etc. Furthermore, data can be intentionally mishandled or even used to launch cyberattacks (DDoS, phishing, etc.). It is important to provide security mechanisms that can assure the proper handling of data based on advertised security properties. Additionally, solutions need to provide users with the ability to verify that their data is being processed in the way they want.

4.5 User

To protect the security and privacy of European users, we concentrate in the first observation on three research challenges that are of eminent importance:

- Fighting disinformation in Europe
- Data ownership and Data Privacy
- Dynamic Attribute-Based Trusted Digital Identify Management
- All challenges should be addressed to lead to short-, mid-and long-term research activities.

4.5.1 Fighting Disinformation in Europe

Online social networks and online media platforms enable individuals from remote corners of the globe to share ideas, news, and opinions in an almostinstantaneous manner. Social networks such as Twitter and Facebook have become a primary source of information for billions of users and the media where new cultural and political movements are formed and promoted. This high level of reliance on social media opened the field to malicious actors to pose new kinds of threats, which can have severe consequences at a societal level. Disinformation diffusion in social networks is one such threat carried out by diverse users who have various motives. For example, terrorist organisations deliberately diffuse false information for propaganda purposes, trying to inflict conflict or to cause extreme emotional reactions. Foreign interference of actors with motives against the EU using human or automated operated accounts (bots) can slander a candidate, trying to shift the outcome of national elections or impede the policy-making process in general.

Challenges:

- ***Understanding the disinformation diffusion:*** *The multiplatform diffusion: The mechanism, the channels, and dynamics of disinformation diffusion are neither clear nor easily assessable for analysis. The disinformation content can become viral following a complex path of transmission and through many online communication platforms. The disinformation content could first be originating in the "periphery" of social platforms and become viral in mainstream media. QAnon conspiracy theory is such an example. It is a unified-conspiracy theory consisting of several other conspiracy theories such as Pizzagate. It originated on 4chan (by the anonymous user "Q") and then spread through multiple social media platforms.*
- ***Official malicious actors:*** *Elected politicians: Often, there is a symbiotic relationship between elected politicians and conspiracy theory promoters. Often, political parties are the source of disinformation – using as a tool the conspiracy theories aiming to create a political polarization which will consequently lead to a loyal political base. Hence, individuals who support reactionary and anti-scientific narratives can become part of the elected government. Although this is a mainly political challenge for the European democratic system, countermeasures against disinformation campaigns employed by the social platforms themselves could suppress political extremism.*

Actions:

- ***Early detection of disinformation:*** *Classify the content and identify the actors. One of the main challenges is detecting disinformation and mis- information operations at an early stage before becoming viral in the mainstream media. Therefore, research should be conducted on developing novel machine learning techniques that will classify the spread of information and identify the source of disinformation – the influential users who were responsible for the information diffusion.*
- ***Countering disinformation:*** *During crises such as the COVID-19 pandemic, false information such as pseudoscientific conspiracy theories can result in wide-spread panic and chaos. Hence, not only*

early detection but also countering the disinformation is crucially important. Conspiracy theories related to the origin of COVID-19 and the anti-vaccine movements could play a negative role in the fight against the pandemic. Therefore, it is crucial to develop countermeasures against conspiracy theories that will be, at the same time, in line with the democratic values of Europe, such as the freedom of speech. Research on the early identification of malicious users that lead to their suspension from the social platforms is one such direction. Also, it is not enough to suspend accounts spreading disinformation. It is of paramount importance to research social media dissemination strategies that increase the influence of correct fact-checking information by employing graph-theoretical, game-theoretical, and human factor principles.

- ***Coordination, European disinformation observatories:*** *An integrated or federated European observatory of disinformation that will monitor the social media streams and disclose disinformation activities should be a long-term. The observatories are currently being established in any European country to form an internal interconnected network of national institutions. Each network hub collaborates with national authorities, fact- checking organisations, and research institutions. Research on how to properly share and aggregate information from multiple observatories could prove highly beneficial in the observatory integration effort.*
- ***Detection and Mitigation of Social Bots, resp. the Social Bot Pandemic:*** *Social bots are a long studied, yet unsolved problem in the online social ecosystem. Detection is still a key challenge. Adversarial machine learning is a promising approach to be used in the fight against all forms of online manipulation. Deep fakes and other recent advances in AI can support the identification of social bots.*

4.5.2 Data Ownership and Data Privacy

The initial design requirements of the Internet and the Web in the early 60s and 90s were far different than those of today (i.e. Connecting servers between academia, sharing content through simple websites, email exchange, etc.). Today, both the Internet and the Web have managed to exhibit tremendous evolvability and extendibility. They have succeeded in supporting services (e-commerce, e- banking, content distribution, video streaming, Web conferencing, etc.) and capabilities (broadband connection, mobility, satellite, etc.) that could hardly be imagined.

Online advertising and marketing appeared soon after the Web's appearance in the 90s and grew into an entire industry that is currently funding a large part of the so-called free services of the Internet. Advanced versions of web advertising and recommendation systems, in general, are heavily based on detailed personal data collected online from millions of individuals to offer tailored ad impressions and recommendations to maximize profits of the so-called "Tech Companies," such as Google, etc.

Of course, the uncontrolled user tracking and personal data collection of individuals lead to data protection and privacy problems that have challenged the Internet and the Web today.

Actions: *New research efforts are required to mitigate and control the challenges mentioned above. Below we identify different directions that we need to turn to our attention:*

- ***Data protection regulations:*** *In recent years, we have witnessed new data protection regulations such as the GDPR in Europe and the California Consumers Act in the US, to name some. Since new regulations are now in place, the challenge now is shifted towards how we can apply them in practice by proactively monitoring and detecting violations in an automated way. As a result, new tools and methodologies need to be implemented to automate such regulations' enforcement. Some examples include tools related to web tracking and personal data leakage detection, website classification to identify sensitive content websites as defined by GDPR and similar legislation, Cookie consent (opt-out) automation and monitoring, browser fingerprinting mitigation, personal data handling, storage, and localization monitoring, etc.*
- ***Personal data ownership:*** *New research needs to be conducted to allow users to have full control of their data, including their browsing patterns, shopping activities, social network activities, etc. The main focus of such tools should be but not limited to the following functionalities:*
  - » ***Data portability:*** *Data owners should be able to move their data across different online services of their choice (i.e., move financial data from one online banking service to another). As a result, new research should be focusing on novel portable data structures and mechanisms to allow the above functionality.*
  - » ***Right to be forgotten:*** *Data owners should be able to block access and delete their personal data across different online services (i.e., remove their data from a social network). New tools and methodologies need to be invented to ensure that personal data collected and stored online are under the full control of the data owner (users), rather than the data collector (online service), which is the current state that we are facing today.*
  - » ***Furthermore,*** *we need to provide technologies and tools to allow users to benefit from their personal data (i.e. create new monetization schemes based on personal data sharing).*
- ***Personal data value and Human-Centric Data economy:*** *Most online services utilize personal data to increase their profits. For example, e- commerce websites can use personal data to train machine learning algorithms to optimize their inventory and product recommendations. The ad industry uses personal data at a massive*

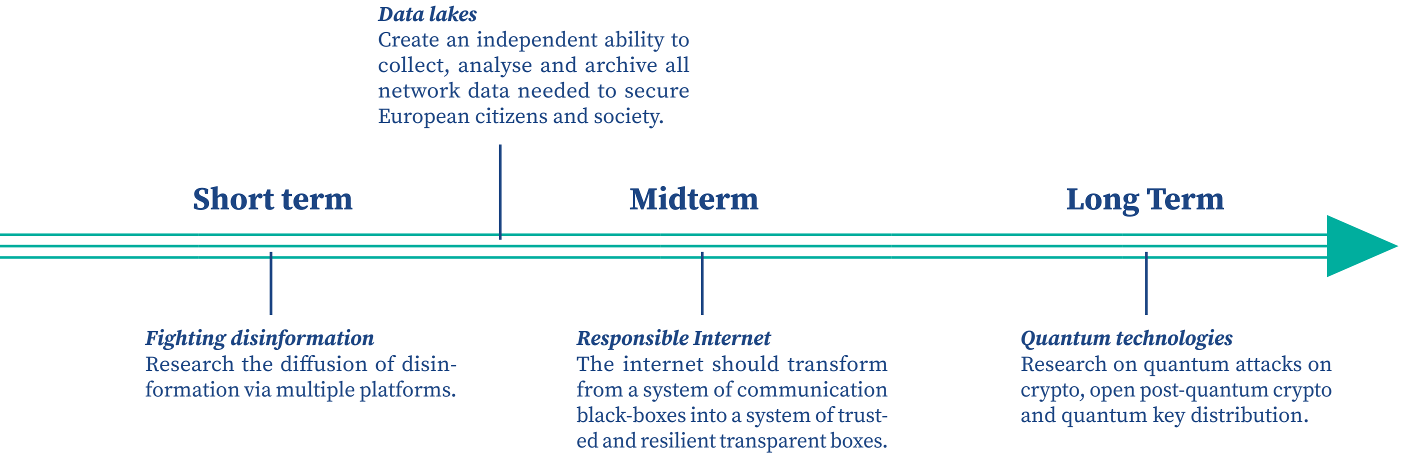
scale to serve targeted and re- targeted advertisements at a higher premium, etc. In all the above scenarios, the data producer (user) is only compensated by getting access to the corresponding online service for free in exchange for being tracked. Instead, it would be fairer for end-users to have direct financial benefits for their data. To provide economic benefits based on personal data, the following research questions need to be answered: What is the actual value of personal data? How can we estimate such value? What factors influence data value based on how data consumers use them? Based on what frameworks do the data owner and data user value them?

- ***Personal Information Management Systems (PIMS):*** *A more recent trend towards addressing privacy and cybersecurity threats around personal data is introducing an additional entity between online services and end-users. The so-called Personal Information Management Systems (PIMS) or Data Vaults. Towards that direction, we need to investigate different paradigms, such as centralized vs. decentralized PIMS, distributed open source or centralized closed source approach, and what the pros and cons of each paradigm are to achieve adaptability and global acceptance. Besides, we need to identify what the critical parts of such an ambitious approach are (i.e., data integrity, trust between nodes, data access control, etc.)*

4.5.3 Dynamic Attribute-Based Trusted Digital Identity Management (Decentralized Identifiers – DIDs)

Data structured at a contextual-appropriate level of abstraction, an attribute, can be a very powerful means and an asset to contribute to digital trust. Especially, if these attributes are dynamic, these can constitute part of a digital pulse and another unique identifier. With that, it has a strong digital identity, authentication, and authorization capabilities that are needed in this Digital Age. Having a trusted and trustworthy digital identity is essential. Without a 'strong' digital identity, and without being able to authenticate both the identity of a person, the identity of organisations, and the identity of the persona and related mandate of the person within the organisation ('authorization'), digitising systems and building, achieving and sustaining digital sovereignty will not be very successful.

Authentication and authorization are security challenges that need to be factored in given that the digitalisation of our societal, economic, governmental, and other systems within the European Union will result in the creation of digital identities of the relevant stakeholders that need to be safeguarded. With the increasing number of risks such as identity-related fraud and mass data breaches, people are becoming more and more hesitant to trust these systems and organisations, whether public or private sector, with their data. Therefore, the digitalisation processes in this digital age will have to establish a higher threshold when it comes to authenticating and authorizing the identities of the relevant persona.



Data lakes
Create an independent ability to collect, analyse and archive all network data needed to secure European citizens and society.
Short term
Midterm
Long Term
Fighting disinformation
Research the diffusion of disinformation via multiple platforms.
Responsible Internet
The internet should transform from a system of communication black-boxes into a system of trusted and resilient transparent boxes.
Quantum technologies
Research on quantum attacks on crypto, open post-quantum crypto and quantum key distribution.

Figure 5: Overview from a Research & Innovation perspective of most important directions, steps, and threats for short-, mid-, and long-term

As a basic standard, users must be authenticated and authorized access to their digital identity using multi-factor authentication (MFA) and is in scope and compliant to the eIDAS Directive, for instance, taking inspiration from the guidelines regarding the implementation of secure authentication such as established by FIGI (Financial Inclusion Global Initiative), and the like. Such and similar (and preferably post-quantum proof) identity, authentication, and authorisation are needed based on the principles such as user-centric design, dynamic, and risk-based continuous authentication, a fine-grained authorisation that is serving both the private and public sector across all vertical industries and cross-border.

4.6 Roadmap for Research and Innovation

It is expected that certain recommendations and other details will be incorporated more extensively in the next edition of the Roadmap for Research and Innovation. The visualized current roadmap for research and innovation is shown in Figure 5.Figure 5: Overview from a Research & Innovation perspective of most important directions, steps, and threats for short-, mid-, and long-term.

4.7 Taking Stock: SOTA & the CONCORDIA Leadership

Europe's digital sovereignty demands for secure digital infrastructures. Such infrastructures should be built upon three inseparable pillars: computing power, control over data, and secure communication. Computing power means that Europe should have the means to design and manufacture current and future computers, ranging from industrial controllers, high-performance microprocessors to quantum computers. Control over our data means that European citizens should be able to trust that their data will be stored on (cloud) servers operating under EU law. Secure communications mean that data will be exchanged over a trustworthy Internet.

The leadership of CONCORDIA becomes especially apparent when it comes to secure communication. Not only are many of Europe's major telecom operators and manufacturers collaborators within CONCORDIA, but also CONCORDIA's research in this area is of world-class. Finally, novel research ideas, such as the DDoS clearinghouse, are transformed by CONCORDIA into exploitable results. Research on secure communication ranges from research on human behavior to high tech systems.

4.7.1 Fighting Misinformation

Probably to most urgent topic to address is the misuse of social networks and online media platforms by malicious actors. These actors may be individuals, such as believers in QAnon and other conspiracy theories. But even more worrying are state actors, who's goals are to destabilize other nation states, by influencing elections or spreading fake news. Cyberspace is not only used for economic warfare, but also for an information war to weaken democracies. To fight disinformation in Europe, research is needed on early detection of disinformation, countering disinformation, coordination of disinformation sources and monitoring social bots. For details, see Section 4.5.1

4.7.2 Data Lakes

To strengthen Europe Europe's cyber security information position, it is crucial to have adequate facilities to collect and analyze security related data. At this moment many of the security data sources are located within the US. Examples include shodan.io, censys.io and Shadowserver. It is important that Europe extends its own collection infrastructures for attack data (data lakes), and facilities to analyze such data (possibly by using AI and ML techniques). For details, see Section 4.2.4.

4.7.3 Responsible Internet

The problem of declining digital sovereignty is being addressed in several ways and different areas of technology. For example, Artificial Intelligence (AI) resear chers have developed design guidelines to make the decisions of AI algorithms more transparent and explainable through what they call ’responsible AI’. Similarly, the European Commission is driving the development of a European- federated cloud service called “GAIA’ that aims to improve Europe’s data sovere ignty. Although these developments illustrate that digital sovereignty is a widely acknowledged and urgent problem, it is remarkable that the discussion largely overlooks the core Internet infrastructure, thus the technical systems (e.g., routers, switches, and DNS servers) that enable remote internet devices to communicate with each other and all services depend upon. To fill this gap, the notion of a Responsible Internet is proposed, a novel security-by-design concept that offers additional `Internet transparency` for critical users and services. For details, see Section 4.2.1.

4.7.4 Quantum Technologies

On the long-term Europe should investigate in quantum technology to ensure it remains secure and competitive compared to the US and China. In the area of cyber security at least research in open post-quantum crypto is necessary. It is important to avoid that lock-in proprietary schemes will take over the market.

Please note, that this is a part of the CONCORDIA Roadmap. If you are interested in the whole document, you can download it ***here.***

[48] European Processor Initiative. ***First Steps Towards a Made-in-Europe High- Performance Microprocessor.*** (June 4, 2019). Accessed Dec. 18, 2020.

[49] European Commission. ***Quantum Technologies Flagship.*** Accessed Dec. 18, 2020.

[50] Federal Ministry for Economic Affairs and Energy. ***GAIA-X: A Federated Data Infrastructure for Europe.*** Accessed Dec. 18, 2020.

[51] Federal Ministry for Economic Affairs and Energy. ***A Responsible Internet: Increasing Trust in the Foundation of Digital Societies.*** (November 5, 2020). Accessed Dec. 18, 2020.

[52] Investopedia. ***10 Biggest Telecommunications Companies.*** (Nov, 2020). Accessed Dec. 18, 2020.

[53] GSMA. ***Network Equipment Security Assurance Scheme (NESAS).*** Accessed Dec. 18, 2020.

[54] Pope, ***M. Security Assurance Methodology (SCAS) for 3GPP Network Products.*** (September 2020). Accessed Dec. 18, 2020.

[55] Federal Ministry for Economic Affairs and Energy. ***A Taxonomy and Terminology of Adversarial Machine Learning.*** (October, 2019). Accessed Dec. 18, 2020.

[56] F. Cavaliere, J. Mattsson, and B. Smeets. 'The Security Implications of Quantum Cryptography and Quantum Computing'. Network Security, 2020(9):9 – 15 (September 2020).

[57] U.S. Department of Energy. ***U.S. Department of Energy Unveils Blueprint for the Quantum Internet at 'Launch to the Future: Quantum Internet' Event.*** (July 23, 2020). Accessed Dec. 18, 2020.