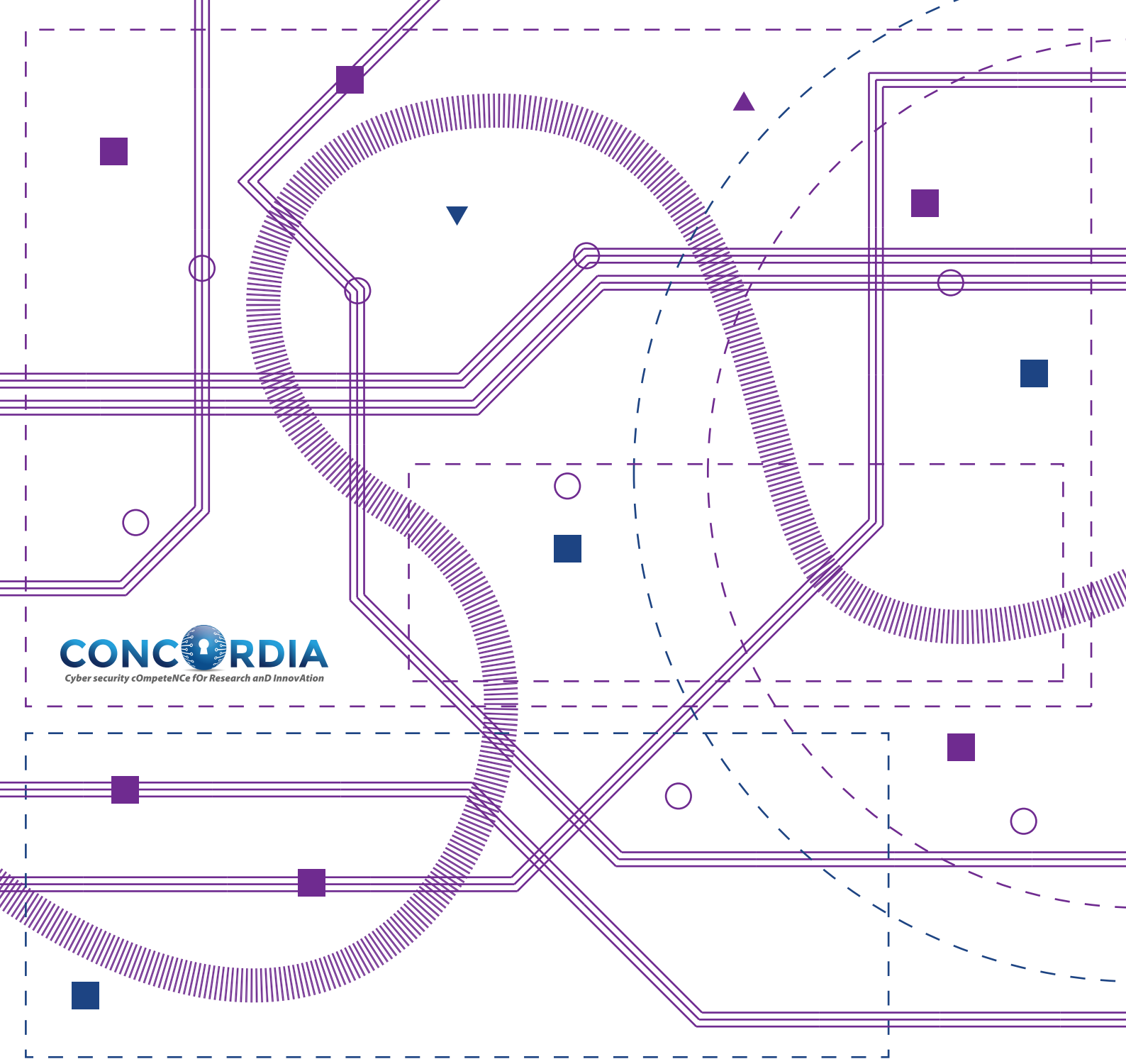


Roadmap for

Legal & Policy

8 Roadmap for Legal and Policy

For organisations in any and every sector in member states, the EU and around the world, implementing state-of-the-art security, privacy, cyber-physical safety, (personal and non-personal) data protection, cyber resilience, transparency, and accountability (using both technical and organisational measures) are now a must in this Digital Age. The level of dependability and the level of ever-increasing dynamics justify that and is proven daily. It is challenging our Digital Sovereignty and our Rule of Law, both on the European level and member statelevel.

This leads to many and various challenges to address, risks to mitigate, impact to avoid, re-organise or otherwise coordinate and orchestrate detrimental consequences and related responsibility, accountability, liability, and enforcement capabilities, as well as renewed or otherwise improved monitoring and supervising in this Digital Age. While the existing policy instruments of all sorts, the efficiency of governmental authorities, as well as existing legal structures, responsibilities, measures, remedies, and other capabilities are challenged, these are - in an improved, transparent and accountable way – for sure also part of thesolution.

8.1 Build, Achieve & Sustain Digital Sovereignty

However, it also leads to many and various opportunities to identify, grasp, embrace, incentivise, and otherwise organise, endorse, and augment. Policy instruments of all sorts, and related improvement of transparency, implementation, interpretation, living lab capabilities, inclusion, maturity and consistency of authorities and law enforcement, cross-sectoral and cross-member state public-private cooperation, co-creation, common understanding, joining forces and related trust and trustworthiness are very powerful – and prerequisite – tools and means to build, achieve and sustain Europe fit for the Digital Age including future-proof Digital Sovereignty.

Meanwhile, we have to accept – and embrace – constant change. The vast domain of cybersecurity amplifies this notion on a 24/7 basis. Developmentssuch as 5G further amply these with a factor of 100 or more. This also leads to the need to rethink what and how policy instruments

can be deployed and kept up to date with the ever-evolving and increasing dynamics of this Digital Age. Static (policy) instruments in a dynamic digital and cyber-physical world will generally not anymore be up for the job they were intended and designed for.

Said differently, in this Digital Age, digital technology and cyber--physical ecosystems have outstripped our societal, economical, and legal frameworks. How to catch up? And, how to keep up? For that, aiming to and supporting jointly creating, building, achieving, and sustaining European digital sovereignty (including the related intertwined symbiosis of collaborative resilience, research and innovation, education, skills and jobs, and economic development and competition) is definitely an excellent main mission to focus on. 21st century and future-proof legal and policy strategies are one the essential core components to make it work.

Figure 12: Ecosystem for technology & the Rule of law

For purpose of this CONCORDIA Cybersecurity Roadmap for Europe, various objectives, challenges respectively scenarios regarding or related to most-notable legal and policy strategies have been identified. Some of those are already high- lighted below where others are merely mentioned yet under development in a stage that these are expected to be incorporated more extensively in the next edition of the Roadmap.

For the avoidance of doubt, obviously numerous open source publications have been read and assessed (next to others for instance mentioned in D4.2), such as for example and in random order: (i) EPRS Ideas Paper Towards a more resilient EU, about Digital sovereignty for Europe [2], (ii) Report from the EU Court of Auditors[80] stressing that more EU action is needed to address inconsistent transposition or gaps in EU law (e.g. limited and diverse legal frameworks for duties of care; the EU's company law directives have no specific requirements on the disclosure of cyber risks), (iii) Consultation Paper by ENISA about EU ICT Industrial policy in cybersecurity context [4], (iv) Cyber Readiness Index Country Profiles [78] of the five member states that have been reported by Potomac Institute for Policy Studies,(v) the National Cyber Security Strategy paper by ENISA[81], and (vi) the draft Union Rolling Work Program for European cybersecurity certification, amongst many others.

8.2 Objectives, Challenges & Scenarios

Hereunder, the currently identified objectives, challenges respectively scenarios (also collectively described as initial "mini-roadmaps") are mentioned, each generally for local, sectoral, regional, member state, European Union team building, continuous improvement, and sustainment of European digital sovereignty and the related intertwined domains.

8. 2. 1 Objective: Trusted Experience Sharing

- **State of Play (SOP):** Within the EU and the member states and their respective regions and local public and private organisations in every sector, there is a wealth of knowledge, experience, lessons learned, and best practices (collectively: 'Experience') available in the EU, its member states and its organisations and individuals. Each has a particular Experience, but as per the dynamics of digital ecosystems, actors and the (mis)use it is not sufficient or otherwise run obsolete quickly, although each does not necessarily need the same amount of Experience as every- body else. This, as each context, is different and requires other Experience. Furthermore, some are more experienced, mature, or active in certain domains where others are not. Currently, there is no trusted Experience sharing ecosystem of ecosystems where omni-stakeholders can share, exchange, and otherwise take in the Experience of others. Most Experience therefore is not shared and not re-used. This wealth of Experience generally goes to waste.
- **State of Art (SOTA):** Trusted Experience sharing starts with transparency of stakeholders, and their various values, perspectives, and interests. Such insight and oversight in transparency and appreciation lead to trust. Consistency thereof will build and cater more trust down the road. Said otherwise, one of the main core components would be to have a clear stakeholder's landscape and based on that the stakeholders getting and learning to know, understand and appreciate each other, also cross-sectorial, cross-regional, and across networks. A next step thereafter enabled and facilitated will be the sharing trustworthy Experience in a trusted way: Trusted Experience Sharing.
- **GAP (SOTA -/- SOP):** The initial main GAP is the lack of mapping about the various stakeholders in this landscape. Trusted Experience sharing starts with transparency of and appreciation by stakeholders, and their respective and various values, perspectives, needs, and interests. Such insight and oversight lead to trust, necessary to discuss the multi-layered architectures that enable andfacilitate trusted Experience sharing. There needs to be a sufficient amount of trust before one will share. Thereafter, the sharing itself needs to be done in a trustworthy

and consistent way as well. With that one can take stock from member states level Experience regarding Digital Sovereignty & Collaborative Resilience, and also become future- proof and otherwise resilient on EU level, as well as vice versa: how to take stock from EU level Experience and become future-proof and otherwise resilient on a member state level. This wealth is to be organised, nurtured, structured, systemized, and built on for European digital sovereignty.

- **Timeline:** Short-Term to kickstart and assess, and both Mid Term and Long Term to scale, improve, and sustain are essential.
- Short-Term: For the Short-Term: for bridging the initial main GAP a member- state and cross-EU initiative is necessary to map and plot the landscape and its stakeholders. This is different than the current in-progress Cybersecurity Atlas initiatives. The Cybersecurity Atlas helps on certain identification and mapping on organization level and as per the current purposes of the Atlas mostly on research. The mapping and plotting with the purpose for Trusted Experience Sharing is as outlined in the paragraph GAP, above, including available, requested, required, and missing capabilities and competencies, including its needs and other related Expertise. Such should also not be in the public domain per se, such as the open-source parts of the Cybersecurity Atlas. The envisioned outcome of the short-term activities would be transparency of and appreciation by stakeholders, and their respective and various values, perspectives, needs, and interests.
- **Mid-Term:** For the Mid Term, insight and oversight will grow to a level where multi-layered Experience sharing architectures can be discussed and designed that enable and facilitate trusted Experience sharing. Starting relatively modest yet in a way that can scale and agility to evolve and be improved is recommended. Depending on the uptake, the Experience sharing network can hopefully be scaled in the Mid-Term.
- **Long-Term:** Where not yet achieved in the Mid-Term, the Experience sharing network can be scaled in the Long-Term. In any case, resilience, sustainability, and continuous enrichment, and other improvement should be part of the Long-Term efforts.
- **Conclusions:** Knowing what we already have, knowing where one can help and otherwise support the other, and knowing who to join forces with where white spots of Experience need to be addressed is a prerequisite for European digital sovereignty. Without knowing, in cybersecurity and another sovereignty context a malicious actor will find the weakest link or other weak access points for exploitation and the like. Regarding the latter, we all should be aware that those actors to collaborate with each other. It is up to us to do the same.

8. 2. 2 Objective: EU Landscaping of Products, Systems & Services

- **State of Play (SOP):** Cybersecurity is a very important and seen from all angles interesting domain; even the smallest connected device nowadays can add to major disruptions. As cybersecurity is a horizontal and cross-cutting topic, and as it is relevant in any and all layers of both the technical systems as well as organisational and societal ecosystems, there is no person or organisation – whether in the public or private sector – for which cybersecurity is not relevant and does not have a potential negative impact.
- However, the cybersecurity domain is vast, fragmented, and not well- defined. At the same time, attack strategies are constantly shifting, and the impact is becoming exceedingly high. While the urgency to understand and deal with these new attacks is increasing, there are not enough companies and other organisations that can formulate concrete responses to these new threats. To add to that, as digital and related technology in the connected, hyper-connected, converging world (physical, cyber, and cyber-physical) changes the world at such a fast pace, and is relatively new for organisations – whether on the supply side or on the demand or end-user side –, the maturity level of society is below par. Most of the member states have identified cybersecurity as not only an important and prerequisite domain and topic to address continuously, but also as an enabler and opportunity to build on, excel, and become digital sovereign as a member state and European Union Digital Single Market. However, it is not easy to landscape the vast and dynamic cybersecurity domain. Even ENISA, NIST as well as Gartner, and other organisations do not identify, landscape, and map all parts of this domain. Nor do they make their frameworks non-academic, i.e., readable for a wider audience. Furthermore, it is not easy to understand the various and generally not very transparent propositions of cybersecurity organisations and the products, services, and systems they factually develop and factually market. With that, it is also very hard to analyse these in-depth in such a way that is recognizable, practical, and useful to work with. Yet one can map out and execute strategies and tactics to take stock and convert this knowledge and experience into opportunities and enablers for companies, organisations, economy and to benefit European Union society, including without limitation economy, as a whole.
- **State of the Art (SOTA):** Adequate and comprehensive cybersecurity frameworks, also acknowledging that the cybersecurity domain continuously expands. Next to that, it is hard to spot and select the right players in the market, which makes diligent and effective matchmaking a tedious task. With this, both demand

side, vendor side, researchers and (other) academia as well as the public sector, member states, and the Commission and related agencies would know what European Union cybersecurity organisations actually and factually have to offer, what not, who could or should team up with whom, and where the gaps are that needs consideration, action or other (urgent or other) intervention. In this way, relevant stakeholders could and should be connected even more to prepare and continuously build resilience against both the threats of today and those in the future.

- **GAP (SOTA -/- SOP):** The initial main GAP is the lack of mapping about the actual, vetted cybersecurity capabilities and offerings of European organisations, starting with structured visualisation in identified cybersecurity domains and dimensions of (to be assessed and otherwise collaboratively and multi-angled vetted) cybersecurity products, systems and services of European cybersecurity companies that are active in the Cybersecurity Domain. Thereafter, certain analysis of the gaps between the identified cybersecurity domains and dimensions on the one hand and the various identified marketed cybersecurity products, systems, and services, on the other hand, will give oversight and insight in the gaps from angles such as without limitation risk, impact, geolocation, industry/market segment, compliance, best practices, standards, regulation, collaboration, market optimisation, market opportunities, research opportunities, competition, and other digital sovereignty relevance. This enables and also facilitates the SOTA, while being the basis for the supplement, keeping up to date, improvement and otherwise optimisation possible.
- **Timeline:** Short-Term to kickstart and assess, and both Mid--Term and Long- Term to scale, improve, and sustain are essential.
- **Short-Term:** For the Short-Term, bridging the initial main GAP a member- state and cross-EU initiative is necessary by mapping and plotting the land- scape of cybersecurity domains and dimensions on the one hand and the various identified marketed cybersecurity products, systems, and services on the other hand.
- **Mid-Term:** For the Mid-Term, building on the results – including themap- ping and plotting as set forth above – from the Short--Term activities: knowing what we already have, knowing where one can help and otherwise support the other, and knowing how to join forces where white spots of Experience need to be addressed is a prerequisite for European digital sovereignty.
- **Long-Term:** Where not yet achieved in the Mid-Term, such oversight, and insights as set forth above should be further pursued. In any case, these should be the basis for sustainment, supplement, keeping up to date, improvement, and otherwise

optimization.

- **Conclusions:** Knowledge provides insights and oversight. Without knowing, also in cybersecurity and another sovereignty context, no appropriate and contextual team building will be possible to help identify, assess, make aware, protect, detect, alert, respond, recover, report, and continuously improve products, systems, and services used, deployed, implemented, developed, pre-procured or procured. This would lead to a lower level of or no European digital sovereignty, which is obviously not recommended.

8. 2. 3 Objective: Member State NIS Directive Comfort & Capability Building

- **State of Play (SOP):** The current NIS Directive, which is under review, generally aims to enhance the readiness in particular sectors responsible for critical infrastructure, vital systems respectively essential services as defined therein. Compared to other critical infrastructure regulations outside the EU, the NIS Directive is state of the art. However, not all sectors mentioned in the NIS Director are covered by each member state. Even more, there is quite some difference in the sector- coverage by each member state under the NIS Directive. Some member states have up to four (4) times more sector-coverage than the other. In short, the levels of implementation differ substantially. This at least reduces the operational effectiveness of responses to large-scale cybersecurity incidents or zero-day vulnerabilities. It also reduces the effectiveness of the strategy of the NIS Directive, and any success to build, achieve, and sustain digital sovereignty within the European Union.
- **State of the Art (SOTA):** Vulnerabilities in critical infrastructure, vital systems, and essential services do not stop at any member state border (let alone the EU outer-borders). A particular challenge for the Commission and member state is encouraging other member states to adopt and implement the same level of sector-coverage as the other member states, or at least to a certain minimum yet sufficient level.

- **GAP (SOTA -/- SOP):** Identifying and addressing each reason for the difference in levels of implementation is the only way to support building, achieving, and sustaining digital sovereignty of European (member state and related) critical infrastructure vital systems and essential services. This, as the weakest link, can expect to be the main attack vector. But, also, as the systems are generally interdependent, influence each other, and can infect or negatively affect each other. Reasons could be the lack of expertise to implement in a particular sector, potential hurdles or other preconditions, or the lack of resources, funds, or other capabilities. Addressing these in a relatively modest way is recommendable. For instance, on a sector-by- sector basis, where the sector is addressed that adds the most appreciation to the respective member state where it may also be the one that brings synergies to the resilience of interlinked sectors in such member state or even augment resilience to the similar sector in other member states.
- **Timeline:** Short-Term to kickstart and assess, and both Mid--Term and Long- Term to scale, improve, and sustain are essential.
- **Short-Term:** For the Short-Term, identifying andaddressing each reasonfor thedifference in levels of implementation is recommended, including finding the true reasons and possible solutions to address those (including within limitation any precondition or impact such solution may have respectively created itself) and facilitating understanding and appreciation.
- **Mid-Term:** For the Mid-Term, support implementation in a non--intrusive and respectful way, where it is recommendable to initially have a relatively modest implementation speed, and only speed up where it may be possible and comfortable for the respective member state, sector, and related stake- holders. Meanwhile, it is also recommended to identify and visualise the output, synergies, and other results – including lessons learned –, also for potential (re)use in other NIS sector implementation, either in the respective or other member states.
- **Long-Term:** For the Long-Term, the sector-by-sector implementations can be completed to the extent agreed and continuously improved as the cat- and mouse game with the malicious actors will be continuous aswell.
- **Conclusions:** Supporting member states and related NIS sectors with the ap- propriate level of comfort and sufficient and adequate capability building is seen as a major contribution to digital sovereignty, both for member states, sectors – both public and private – as well as the European Union, and itsperiphery.

8. 2. 4 Challenge: How to Operationalise Europe's Championing of Human- Centric Values

- **State of Play (SOP):** In this Digital Age, and also because of that an increasingly globalised world, the European Union is generally seen as a leader regarding human-centric values such as those reflected and implemented in the GDPR. The GDPR is already either copied or inspired by many countries around the world. However, the GDPR is the successor of the 1995/46 EC Privacy Directive, so this human-centric regulation is already 25 years old and was implemented before the internet went from nice-to-have to a need-to-have and from an international network used by academia to a global network used by everybody. It is one of the indicators that the EU's normative power alone cannot guarantee the European digital sovereignty of its citizens, businesses, organisations, society, and economy. Neither can it guarantee that human-centric policy instruments give the European Union, its member states, citizens, and organisation a competitive edge both in the EU as well as when exporting abroad.
- **State of the Art (SOTA):** Leveraging the human-centric values approach to a level that can be operationalised, monitored and enforced – also by citizens and organisations themselves within the Rule of Law –, in a European Union-wide clear and transparent way. This, also to export these frameworks, good practices and lessons learned beyond the European Union, and to have the ability to market these value-centric digital products, systems, and services abroad. It strengthens both the digital sovereignty of within the EU as well as – at least on conceptual and principle-based level – of and within other countries and regions in the world. Furthermore, it can bring benefits to the European private sector, both vendor side as demand side, as more GDPR-proof or other human-centric digital products, systems and services can be exported or otherwise offered to (respectively can be procured from) a global market with the same of similar digital sovereignty objectives.
- **GAP (SOTA -/- SOP):** There are basically two main bridges possible to get to the SOTA, as each will take different efforts and have different timelines. One is to initially identify, mapping and plotting the member states, regions respectively states that have, in either substantial or certain parts, found inspiration from the GDPR and have or are working on implementing it locally, regionally, or nationally. This, to reach out, link up, and learn from choices make, lessons learned, improvements planned, and monitoring or enforcement made more efficient and transparent. The GDPR obviously is just one example of human-centricity, but currently the most mature to focus on. The other main bridge could be to use the first bridge

outcomes to discuss, identity and where feasible deploy and monitor improvements to means, measures, and other policy instruments (without revising the GDPR in any way) in order to enable European citizens, data protection authorities and other stakeholders to more effectively enforce their respective rights or help enforce the respective rights that are so essential for digital sovereignty. Digital sovereignty starts with sovereign citizens, communities, and local society.

- **Timeline:** Short-Term to kickstart and assess, and both Mid--Term and Long- Term to build appreciation and operational collaborations, develop future-proof measures, for deployment in living labs first with the ability to scale, and later on the scale, improve and sustain those are essential.
- **Conclusions:** The European Union, its member states, citizens, and organisation have something very valuable – and sought after globally – to offer: implemented human-centric value policy instruments such as the GDPR. It can both bring wealth and digital sovereignty to our allies and friends outside of the EU, as it can bring prosperity and digital sovereignty to EU's and member states' citizens, communities, society, and economy.

8. 2. 5 Objective: EU Pre-procurement of EU Products, Systems and Services

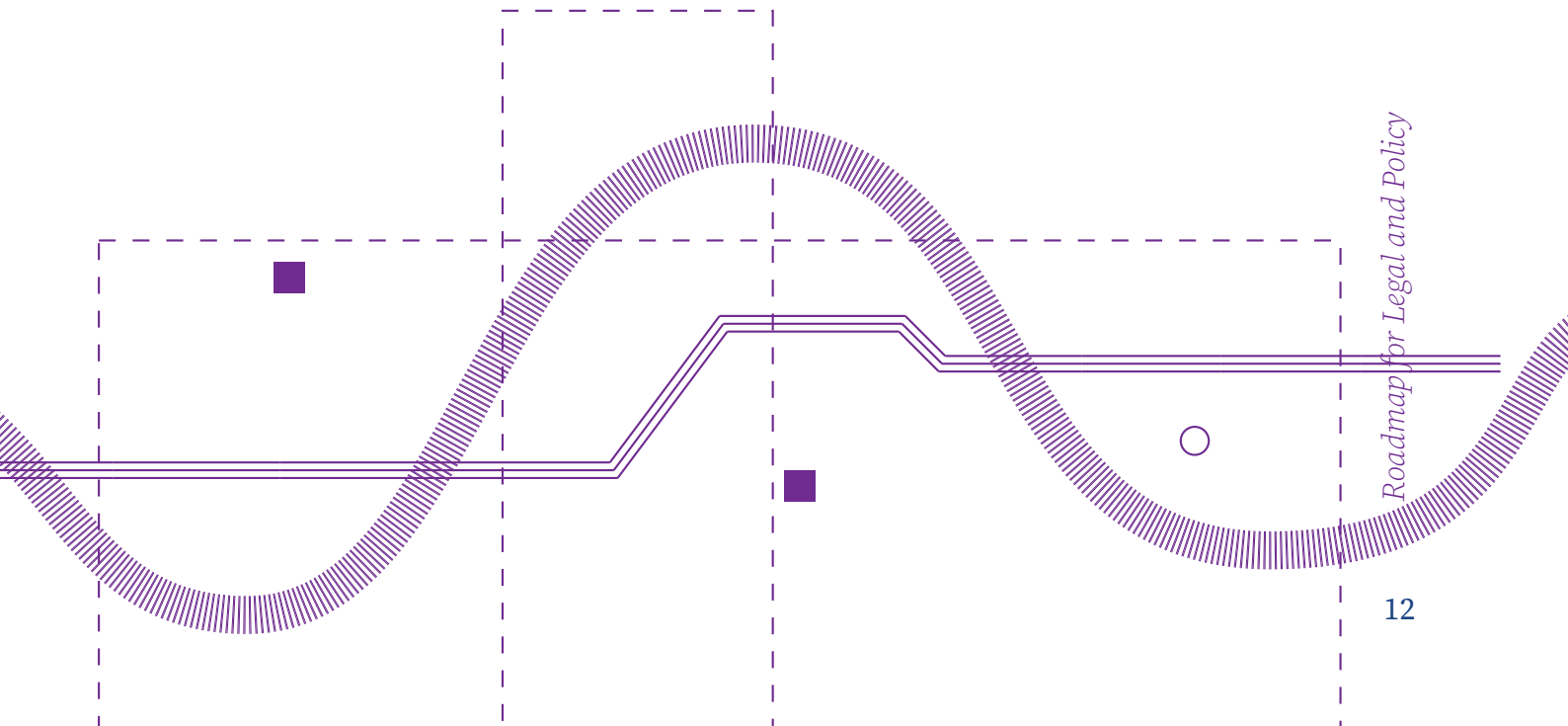
- **State of Play (SOP):** Whether one likes it or not, technology changes the world at a fast pace, so better embrace it. Digital ecosystems, cloud computing, edge, Internet of things, spectrum, cybersecurity, data management, and the like are what organisations are talking about daily and are increasingly assessing the opportunities, benefits, and risks. Technology makes innovation possible, and technology is a need-to-have in organisations, society, and the economy. It is essential for the successful and future-proof operation of an organisation. It can be the difference between an incumbent with no future continuity and no relevance, and one that is ready for the future. However, most organisations do not know what they need, what to procure, and how to procure including all relevant elements, components, functionals, and non- functionals –

including without limitation cybersecurity – to create its own digital sovereignty, and with that add and augment the digital sovereignty of its sector, market, member state, and the digital sovereignty of the EuropeanUnion.

- **State of the Art (SOTA):** There is no joint-procurement framework for cyber-security infrastructure, let alone a dynamic pre-procurement model with which one can make its own informed decision. The same goes for the essential and various combinations of digital functionals, non-functionals, and capabilities that make a digital ecosystem, platform, product, or service. Without such dynamic pre-procurement and procurement comfort and capabilities, there will be no successful engagement possible between organisations, vendors, staff, customers, and society. At the same time, given the increasing dependability on and complexity of digital technology and digital ecosystems, organisations generally do not know what they need, what to procure (pre-procurement), how to procure it, how to negotiate out such technology arrangements (either platforms, digital ecosystems, networks, technology-as-a-service (xaaS) or otherwise) and how to keep it optimized and to monitor it continuously.
- **GAP (SOTA -/- SOP):** Applying easy to implement good practices such as a three-phases methodology visualised below, and using proven common reference models about performance, cybersecurity, data protection and data management, and negotiation capabilities to pre-procure and procure 21st-century technology including the appropriate levels of trust, security, safety, protection and management capabilities can help to navigate organisations during their effort to both stays or become more resilient and competitive as well as support the digital sovereignty of such organisation as well as its network, sector, member state, and the European Union. It enables and facilitates making informed decisions and a decision model that helps to ensure compliance with regulatory frameworks and industry standards, and, thus, facilitates increasing trust and trustworthiness.

Figure 13: Three Phase Methodology

- **Timeline:** Short-Term to kickstart and assess, and both Mid--Term and Long- Term to scale, improve, and sustain are essential. A well-defined strategy concerning pre-procurement, procurement, and continuous monitoring and optimisation for the short, mid-, and long term is recommended.
- **Short-Term:** For the Short-Term, the various methodologies and other best practices should be identified, vetted, tested, and further improved, where- after a controlled, relatively modest deployment is recommended to commence, for instance in a certain sector or a certain group of organisations.
- **Mid-Term:** For the Mid-Term, focussing on certain sectors or groups of organisations is recommended to help increase both the appreciation of these pre-procurement capabilities as well their competitiveness on the market, including mitigating becoming an irrelevant market player, and their ability to offer European, superior, state-of-the-art products, systems and services and the resulting increased consumer and other market trusts.
- **Long-Term:** For the Long-Term, the more challenging sectors, or groups of organisations can be enabled and facilitated to deploy these pre-procurement capabilities, including structured, modular architectures, data-centric, technology- & vendor--neutral and by-design approach following the most demanding regulatory frameworks and industry standards.
- **Conclusions:** The objective is to support European organisations, whether public or private sector, and whether small, SMEs, midsized or large, to make informed decisions and give them future-proof capabilities to prepare, create transparency and trust and build agility and resilience for the Digital Age and new markets, transformation, convergence, and competition. Hence, an organisation will be able to remain relevant with the potential of becoming a market leader in fields that shape the future, and the future of your organisation, both in the European Union as well as globally.



8. 2. 6 Other Objectives, Challenges or Scenarios

Other objectives, challenges, or scenarios that are under investigation and development as a mini-roadmap, and that are anticipated to reach a certain level of maturity and detail to be included in subsequent Roadmap edition(s) currentlyare:

- **Objective: Trust & Trustworthiness by Design for Cross--Sectorial Convergence.** This mini-roadmap is envisioned to focus on digital ecosystems in multiple sectors, and how to go from a trusted and trustworthy single component to a trusted and trustworthy end-to-end system, where multi-use (other than a single intended use approach) – including unintended use – is the default.
- **Objective: Data-Supported, (Near)Real-Time Transparency & Accountability.** This mini-roadmap is envisioned to focus on both (A) digital sovereign authorities, that are well-equipped for the Digital Age (including without limitation with transparent and trustworthy digital means), well-sourced, well-endorsed and can operate independent yet accountable (also while addressing the vault-lines between privacy and freedom on the one hand and surveillance and national security on the other) in accordance with their mandate, and (B) means that support with data- supported transparency and accountability of digital products, systems and services for the benefit of member states, citizens, society and economy (either demand or supply-side) and within the Rule of Law.
- **Objective: Interconnecting & Balancing Security Policies.** This mini- roadmap is envisioned to focus on how to introduce general security principles and generic cybersecurity controls and measures in horizontal regulations (such as the Cybersecurity Act (CSA) but also, Radio Equipment Directive (RED), General Data Protection Regulation (GDPR), General Product Safety Directive (GPSD), Machinery Directive, NIS Directive, eIDAS Regulation (EUid), Sales of Goods Regulations and the like, while avoiding overlap or at least avoiding conflicts between specific vertical regulations (such as for instance the Medical Device Regulation (MDR), regulatory standards such as the RTS of the Second Payment Services Directive 2 (PSD2) and many others), avoid conflicts, confusion or other discussion – and therefor delays in implementation and also in the Enforcement capabilities, as well as delay in building and achieving digital sovereignty – in the respective markets and between respective stakeholders on what applies, prevails, how to address conflicts, who is allowed to enforce what.

8.3 Further Backgrounds regarding Legal & Policy Strategies

8. 3. 1 Making EU Regulations Fit for a Digital Sovereign Europe

Despite the indisputable benefits of the Digital Age for individuals, organisations of all sizes, member states, and society at large, Digital Age also raises risks, thus, surfacing aspects of critical importance within the Rule of Law outlined under Section 8.1, such as the complexity in attributing responsibilities.

In this context and bearing in mind how to best protect vital societal interests, the European Regulator has been quite active over the last years focusing on how to best protect the interests of individuals acting under multiple personas (e.g., data subjects, consumers), business interests of organisations (e.g., trade secrets) and interests of Member States, therefore, focusing -also- on how to best protect critical infrastructure (e.g., hospitals) and products (e.g., IoT devices).

Figure 14: Digital & data regulatory landscape

Taking into account that the above figure produces merely an overview of the most relevant regulation at the EU level pertinent to the scope and the objectives of the present Roadmap, the discussion below provides the most up to date considerations regarding the status of implementation of GDPR, NIS, and CSA (cf. Deliverable D4.1 [82] and upcoming Deliverable D4.2, as well as in this Deliverable D4.4).

May 25, 2020, marked the second anniversary of the application of Europe's General Data Protection Regulation which, as discussed in Chapter 4 of Deliverable D4.1 [82], was enacted to harmonise and strengthen the fundamental rights of individuals pertaining to the processing of personal data. The Communication published by the European Commission regarding the evaluation of the GDPR did consider input from the European Parliament, the European Data Protection Board, individual data protection authorities and other stakeholders [83]. As per the said

report, the general view was that the GDPR was able to successfully achieve the objectives of strengthening individuals' right to personal data protection as well as guaranteeing the free flow of personal data within the EU, however, areas for future improvement were also identified.

In this Communication, the Commission highlights that while the GDPR provides for a consistent approach pertaining to data protection in the EU, it does give Member States discretion in certain areas. This has resulted in diverging approaches and fragmentation that has subsequently created challenges for conducting cross-border business, innovation, in particular as regards new technological developments and cybersecurity solutions. As a part of its action items necessary to support the application of the GDPR which is relevant for the purpose of this deliverable, the Commission has stated that it will support standardisation/certification in particular on cybersecurity aspects through the cooperation between the European Union Agency for Cybersecurity (ENISA), the data protection authorities and the European Data Protection Board.

8. 3. 2 NIS Implementation Status Update

The Directive on security of network and information systems (NIS Directive) aims at enhancing cybersecurity across the EU and is also the first piece of EU- wide cybersecurity legislation. The NIS Directive requires operators in critical sectors (such as banking, health, finance, transport) and enablers of information society services (such as app stores, social networks, and search engines) to implement effective risk management practices. It also requires Member States to set up at least one Computer Security Incident Response Team (CSIRT) that will be responsible for monitoring threats and incidents at a national level and to create appropriate response mechanisms. At an EU level, the Directive establishes a Network of the national Computer Security Incident Response Teams (the network of CSIRTs) to build trust and confidence between the Member States and enable effective communication.

Given that since its enactment in 2018, the cyber threat landscape has been constantly evolving and becoming more widespread, the European Commission published an initiative involving the review of the NIS Directive [84]. Based on evidence gathered, the Commission is of the view that while the NIS Directive immensely contributed to improving the cybersecurity capabilities within the Member States, there were various issues relating to its implementation.[85] Firstly, due to the minimum level of harmonization and the identification process applicable to operators of essential services, Member States have given a lot of discretion, which has resulted in fragmentation in the regulatory landscape and several inconsistencies [86]. This has also resulted in various sectors

and actors with critical societal and economic activities and which are susceptible to cyber risks to be left outside the scope of the Directive. Hence, to achieve a 'Europe fit for the digital age' as envisioned by the EC, the Initiative aims to identify suitable policy options including non-legislative measures and possible regulatory interventions, as well as a combination of the two.

The EC recently sent out reasoned opinions [87] to Belgium, Hungary, and Romania referring to their failure to comply with their obligation set out in the Directive on security of network and information systems (NIS Directive). As per the NIS Directive, Member States were required to provide the Commission with information regarding the identification of operators of essential services in their respective jurisdictions, the deadline for which was 9 November 2018. For Belgium, identification of operators in critical sectors such as energy, transport, health, and drinking water supply and distribution is pending while Hungary is required to notify about the operators of essential services for the transport sector. Romania's authorities need to provide information on national measures allowing for the identification of operators, the number of operators of essential services, and thresholds used in the identification process. The Member States have been given two months to comply with their respective obligations.

8. 3. 3 Cybersecurity Act Implementation Update

In recent years, the EU has taken great strides to bolsters its resilience and its capabilities to identify, prevent, deter, and respond to cyberattacks and other malicious activities. The enactment of the EU Cybersecurity Act (CSA) in 2019 was one such initiative by the Commission to strengthen the EU Agency for cybersecurity (ENISA) and to create an EU-wide cybersecurity certification framework for digital products, services, and processes.

According to the CSA, ENISA also launched a month-long public consultation in July 2020 for the first candidate cybersecurity certification scheme, the Common Criteria based European cybersecurity certification scheme (EUCC). The EUCC scheme will replace the existing SOG-IS MRA and extend the scope to cover all EU Member States. To assist with this transition as well as to ensure consistent application of the CSA, the European Cybersecurity Certification Group (ECCG) was established. The ECCG comprises of representatives of national cybersecurity certification authorities or the representatives of other relevant national authorities.

ENISA has also set up a 15-member working group on Cybersecurity for Artificial Intelligence to advise ENISA on matters and developments relating to AI cybersecurity and to support ENISA in creating risk-proportionate cybersecurity guidelines for AI.

8. 3. 4 The Data Governance Act

On 25th November 2020, the European Commission published a Proposal for a Regulation on European data governance (Data Governance Act) [88]. The overarching objective of the proposal is to strengthen the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU.

Data sovereignty as an essential component of digital sovereignty is well- represented in the Data Governance Act. For instance, the proposed Regulation introduces many measures to increase trust in data sharing, creates new EU rules on neutrality to reinforce the role of data intermediaries concerning data sharing, and provides for measures to facilitate the reuse of certain data held by the public sector. Moreover, the proposal facilitates companies and individuals to voluntarily make their data available for the wider common good under specific conditions.

The proposal is aimed to incentivise data sharing, especially in the public sector, thus fostering a culture, which is anticipated to encourage, without limitation, threat intelligence sharing, which is particularly relevant for the scope of CONCORDIA.

8. 3. 5 Making Contracts Fit for a Digital Sovereign Europe

As mentioned earlier, cybersecurity relates to numerous layers including hardware, software, data, and service. This multi-layered structure often requires numerous different manufacturers and providers to participate, for example, in the manufacturing of a product, as well as in the provision of services during its life- time. This setting accounts for a large number of contractual documents, licenses, notices, declarations, and/or reports to be in place and effective, not only between the supply-side actors themselves, but also vis-a-vis the customer. The resulting relationships tend to be very complex and bear a great deal of challenges in achieving transparency in allocating responsibilities and risks, as well as issues concerning jurisdiction and remedies.

One of the main challenges stakeholders with a role in the delivery of a system, product, or service is repeatedly faced with is the difficulty to understand applicable contracts, agreements, and other legal documents. Numerous reasons account for this issue, but for purposes of further discussion, it is mainly worth noting that, aside from the European versions of contracts often being verbatim reproductions of their US counterparts, (which may not be necessarily suitable), identifying all the applicable documents may be a challenge in itself. For example, in the case of Nest connected thermostat produced by Nest Labs owned by Google, this challenge is illustrated by about 13 legal documents which a user has to read to get a 'clear' picture of the rights, obligations, and responsibilities in the supplychain. Having a clear picture of legal relationships is also challenging from the perspective of the scope of the documents. While they may claim that they are only applicable to one

separate part of a product or service, in the Digital Age, it is difficult to imagine a part of the system or a separate layer functioning irrespective of the remaining parts or other layers, i.e. without affecting the whole ecosystem. However, to provide a sufficient amount of transparency and accountability, consumers and organisations (both private and public) must have an accurate and transparent account of how the layers (and the respective contractual documents) interact and who becomes relevant (not only active) in what layer. Just as the consumer or organisation should be able to identify the parties upon whom the service is dependent and who are the processors and sub-processors of data. Not only does this information provide the customer with greater transparency; it also helps them establish the extent of liability of various suppliers should a problem arise that requires legal redress.

Further questions concerning liability and other complex contractual issues arise in our Digital Era, for example, concerning the cybersecurity of IoT devices that can make autonomous decisions and enter into legally binding agreements with third parties (e.g., connected home appliances purchasing products from third parties). On the one hand, questions of liability for the actions of these autonomous devices are inevitable. On the other hand, although our traditional understanding of property is a static one, it will likely need to change and respond to the dynamic nature of IoT devices which can evolve and mature over time. Note that the latter has been considered by the European Regulator, who – in the context of the revision of the Product Safety Directive- provides for a new definition of "product".

From a separate perspective, it is also important to consider the status and the role of the customer in the ecosystem. It has been argued that two further distinctions of legal consequence can be made that are particularly relevant for consumers. 'First, the end-user may be the contracting customer or a third party, such as a family member. Second, the device itself may be owned by the customer or maybe leased to the customer by the supplier (or provided as part of rented or leased premises).' Considering the latter, 'the distinction between the device and the associated services becomes critical because the Nest Terms of Service states that if the device owner does not agree with the terms 'you should disconnect your products from your account and cease accessing or using the services'. However, in some jurisdictions, a disconnected IoT device would potentially breach the law. For example, according to the Sale of Goods Act 1979 of England and Wales, the purchasers of goods

will 'enjoy quiet possession', which term would be potentially breached if when the Nest device was disconnected it loses most of its functionality.

Last but not least, complexities also arise in the context of clauses relating to the selection of jurisdiction in contracts. Most commercial contracts explicitly stipulate applicable law and jurisdiction governing them, to the maximum extent permitted by law. However, in cases where mandatory national laws apply, judges will have to abide by those. As a consequence, cases may arise in which the judge will have to apply different pieces of legislation, for example, to the same product. Already in today's connected world, it is not difficult to imagine a scenario in which a Dutch customer uses a US-manufactured product during their holiday in Tunisia, where the product was purchased in Venezuela, consists of software running in Ireland and uses applications developed by a Chinese company. This presents a very complex setting where the judge is expected to decide, for example, on damages that occurred due to cybersecurity incidents, based on different pieces of legislation that are likely to apply concerning the acquisition and functionalities of a given product.

Based on the above, there are considerable limitations on whether contracts are fit, also, for effectively providing for cybersecurity in the Digital Age. Those considerations, therefore, stress the necessity to look into the role self-regulatory instruments may play in relation to the protection of products, systems, and services from cybersecurity threats.

8. 3. 6 Making Self-Regulatory Instruments for a Digital Sovereign Europe

Within the Rule of Law as depicted earlier under Section 8.1, there are several legal and policy instruments shaping behaviour that are all meant to synergize to best protect individual and societal interests in practice. This entails that, for instance, European Regulations cannot provide guarantees in absolute for the protection of those interests, as there are inevitable occurring gaps and challenges at the level of implementation that, subsequently, render of key significance the complementing role of contracts and policy instruments, such as the codes of engagement. Commitment to the latter may, also, reveal – especially – the social corporate responsibility of organisations to run the extra mile, potentially, mitigating the uncertainties resulting from regulation.

An appropriate code of engagement to strengthen cybersecurity in the Digital Age entails utilizing all relevant concepts found in a regulation, contract law, and other policy instruments to best serve stakeholders' interests concerning the safeguard of cybersecurity while safeguarding the vital societal interests associated with cybersecurity. In this respect, a balanced approach underlying a code of engagement for cybersecurity presumes to abstain from overreliance on mandatory regulations, as these may be quite generic. Similarly, an effective code of engagement in the field of cybersecurity entails avoidance of overreliance on a single

Remark: This section is largely based on ***IERC Handbook 2017, Cognitive Hyperconnected Digital Transformation, IoT Standards Landscape – State of the Art, Analysis and Evolution, 2017***, accessed Nov 27, 2020

standard, as this would merely further foster the already existing market fragmentation linked to the use of standards. Moreover, a code of engagement relevant for cybersecurity in the Digital Age could exceed the limitations of contractual arrangements between two parties (as common agreements are signed and sealed), while in a multi-stakeholder environment that would lead to the creation of a massive amount of paperwork, red tape and delays hampering -inevitably- daily business activities. Finally, a code of engagement fit for the Digital Age along the lines discussed, would not set terms and conditions (T & C) or similar of one company or organisation, which probably is the larger, unfair one that is non-negotiable, or the one that one has not been able to read, or the one that is unilaterally changed to your detriment (so no freely contracted-out and no balanced relationship, while pushing all liability to another); on the contrary, it would consider the interests of the wider community of stakeholders possibly adhering to the said code of engagement.

Note that at the moment of the present deliverable, there is work conducted within the CONCORDIA project, led by the legal partner and the relevant technical partners, that is directed towards the creation of a code of engagement -specifically- addressing the matter of Threat Intelligence Sharing.

8. 3. 7 Making Internal Policies Fit for a Digital Sovereign Europe

As mentioned in Section 8.1, also, policies have a role to play within the Rule of Law. By putting forward specific approaches in their internal policies, organisations are in the position to play a critical role concerning how regulations, contracts, and other policy instruments are implemented in reality. In light of this and in line with the overarching objectives of CONCORDIA, this section argues that for internal policies to be Fit for the Digital Age, they have to address how employees behave, therefore, focusing -also- on skills development. To this end -and given the dynamic nature of the cybersecurity field-, it is deemed both necessary and appropriate that cybersecurity skills are developed and sharpened in parallel inthree layers, namely, at an individual level, at an organisational level, and a community level. Taking, also, into account that community building per se is addressed under Chapter 10 of the present Roadmap, the discussion below addresses skills in relation to the first two layers, meaning, at an individual level and an organisational level.

8. 3. 8 Skills at an Individual level

Considering the work conducted under T3.4 and, in particular, the findings captured under the post-workshop report of CONCORDIA Workshop on Education for cybersecurity professionals, which took place in June 2020, internal policies could provide for the separate role of the Cybersecurity Consultant. This role has been internationally identified,

but there is a lack of a concrete definition of the profile in all identified frameworks. Notably, in the related survey [15] that was conducted under T3.4 the acquisition of a basic understanding of the legal aspects of cybersecurity was considered as a key element of the Cybersecurity Consultant profile.

Furthermore, taking also into account the findings of a relevant JRC report [89], it is recommended that Cybersecurity Consultant professional has a basic under- standing of the fundamentals of each cybersecurity domain identified, namely, on Assurance, Audit, and Certification, Cryptology (Cryptography and Cryptanalysis), Data Security and Privacy, Education and Training, Operational Incident Handling and Digital Forensics, Human Aspects, Legal Aspects, Theoretical Foundations, Identity and Access Management (IAM), Security Management and Governance, Network and Distributed Systems, Security Management and Governance, Software and Hardware Security Engineering, Security Measurements, Trust Management, Assurance, and Accountability.

In-depth knowledge of a certain domain will -naturally- depend on each professional's background and working experience.

8. 3. 9 Skills at an Organisational level.

Although in practice this is hardly the case, there is a wide consensus in theory that cybersecurity should not be dealt with in splendid isolation within organisations. On the contrary, several departments should be involved and different levels of the hierarchy engaged.

In this spirit, the ENISA report 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity' [90] provides a set of specific recommendations relevant for certain functions within an organisational structure, as illustrated in Figure 15.

Figure 15: Cybersecurity Culture Guidelines: Behavioural Aspects

[15] More information on a ***Code of Engagement for IoT, see CREATE IoT H2020 Project, Deliverable 05.01 IoT Policy Framework***, accessed Nov. 27, 2020

With respect, the skills development, the present input to the Roadmap endorses the specific recommendations listed for each function addressed in the above- mentioned report, including, those pertaining to the role of soft skills. The latter could act as a catalyst, especially with respect to the effectiveness of cybersecurity practices.

Based on the earlier discussion and given the challenges raised by the dynamic nature of cybersecurity, internal policies of organisations to best provide for how regulations, contracts, and other policy instruments are implemented in practice could put special focus on skills development. It is of significance that the development of skills is seen both in micro-scale (on an individual basis), but also in macro-scale (based on the organisational structure).

8.4 Roadmap for Legal and Policy

The visualized current roadmap for research and innovation is shown in Figure 16.

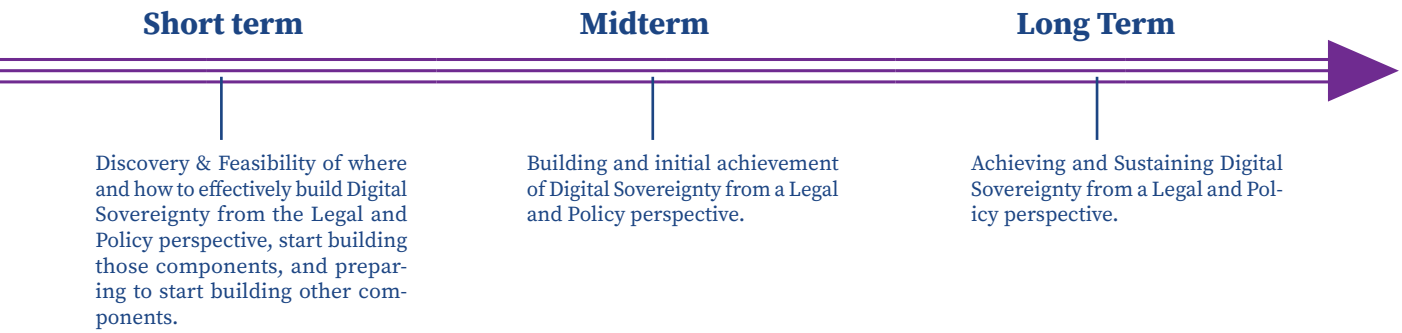


Figure 16: Overview from a Legal and Policy perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines

8.5 Taking Stock: SOTA & the CONCORDIA Leadership

This Chapter of the CONCORDIA Roadmap covers both (a) the stock--taking of state of the art and GAP recommendations that resulted from CONCORDIA project tasks and deliverables during the project that are

recommended to further after the project that can make the cybersecurity landscape in the EU more resilient, agile and future proof on various fronts, as well as (b) other state of the art and GAP recommendations that are not part thereof yet highly recommended as well.

Regarding the first, the six (6) most notable domains and dimensions coming from such stock-taking are visualized below.

CONCORDIA Project Stock-Taking for Legal & Policy

The above domains are further elaborated upon within this Roadmap and in some other deliverables of CONCORDIA as well as and can be found in:

- **Digital Sovereignty:** Chapter 2, Chapter 8 (Section 8.1) & CONCORDIA D4.2 (Chapter 4).
- **NIS Infrastructure Security & Capability Building:** Chapter 8 (Section 8. 3. 3), CONCORDIA D4.1 (Chapter 4) and CONCORDIA D4.2 (Chapter 4).
- **Championing Human-Centric Organizations & (Eco)Systems:** Chapter 8 (Section 8. 2. 4)
- **Trustworthiness by Design for Cross-Sectorial Convergence:** Chapter 8 (Section 8. 2. 6)
- **Data Supported (Near) Real-Time Transparency & Accountability:** Chapter 8 (Section 8. 2. 6)
- Cybersecurity Act Implementation & Dynamic Assurance: - Chapter 8 (Section 8. 3. 1) and Chapter 9.

The 6 domains and dimensions consider critical considerations in order to take a holistic overview of cybersecurity from an EU perspective and need to be continuously built upon after completion of project CONCORDIA as well. The need for Digital Sovereignty in the EU has gained significant traction in the last few years in order to reduce dependencies on other countries and to enable the EU to have more control over its technology and data. On similar lines, the NIS Directive is an essential dimension as it is bolstering cybersecurity capabilities in the EU in tandem with the Cybersecurity Act. Lastly and more importantly, creation of an overarching cybersecurity landscape in the EU would be

incomplete without focus on human-centric organizations & ecosystems, trustworthiness and transparency and accountability.

8.6 Contributions for EU Policies: Roadmap for Legal and Policy

This Chapter Roadmap for Legal and Policy – obviously – has integral and critical EU policy relevance from all perspectives, including to build, achieve and sustain digital sovereignty and otherwise be fit for the further expanding and evolving Digital Age, both for the EU, the member states, but also society, economy, public and private sector including SMEs, citizens, educational institutes and other organisations, and both for the short, mid, long and extreme long term. For that, the recommendations highlighted or otherwise mentioned in this Chapter can help identify, further, improve, augment or otherwise support valuable policy initiatives and instruments, and provide a valuable roadmap and various mini-roadmaps supporting the discussion of priorities and paths to follow, and nuances to observe and cater for.

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

[2] European Parliament Research Service. ***Digital Sovereignty for Europe (July 2020).*** Accessed Dec. 18, 2020.

[4] European Union Agency for Cybersecurity (ENISA). ***Consultation Paper – EU ICT Industrial Policy: Breaking the Cycle of Failure (August 2019).*** Accessed Dec. 18, 2020.

[80] European Court of Auditors. ***Challenges to Effective EU Cybersecurity Policy. (March 2019)***. Accessed Dec. 18, 2020.

[81] European Union Agency for Cybersecurity (ENISA). ***National Cyber Security Strategy.*** Accessed Dec. 18, 2020.

[82] CONCORDIA Consortium. ***Deliverable D4.1: 1st Year Report on Cybersecurity Threats.*** (April 2020). Accessed Dec. 18, 2020.

[83] European Union Law. ***Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM/2020/264.*** (June 2020). Accessed Dec. 18, 2020.

[84] European Commission. ***Cybersecurity: Review of EU Rules on the Security of Network and Information Systems.*** (June 2020). Accessed Dec. 18, 2020.

[85] European Commission. ***Combined Evaluation Roadmap/Inception Impact Assessment,Revision of the NIS Directive.*** (2020). Accessed Dec. 18, 2020.

[86] European Union Law. ***Report from the commission to the European Parliament and the council assessing the consistency of the approaches taken by member states in the identification of operators of essential services in accordance with article 23(1) of directive 2016/1148/eu on security of network and information systems .COM/2019/546 final.*** (October 2019). Accessed Dec. 18, 2020. European Commission. ***Cybersecurity: Commission urges Belgium, Hungary and Romania to Comply with Their Obligations Regarding Operators of Essential Services.*** (October 30, 2020). Accessed Dec. 18, 2020.

[87] European Commission. ***Proposal for a Regulation on European Data Governance*** (Data Governance Act). (November 25, 2020). Accessed Dec. 18, 2020.

[88] Nai Fovino, R. Neisse, A. Lazari, G.-L. Ruzzante, N. Polemi, and M. Figwer. European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. Technical Report EUR 29332 EN OPOCE KJ-NA-29332-EN-N, European Commission, Brussels, Belgium. (2020). Accessed Dec. 18, 2020.

[89] European Union Agency for Cybersecurity (ENISA). ***Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.*** (April 2019). Accessed Dec. 18, 2020.

[90] ISO. ***ISO in brief - Great Things Happen When the World Agrees.*** (August 2019). Accessed Dec. 18, 2020.