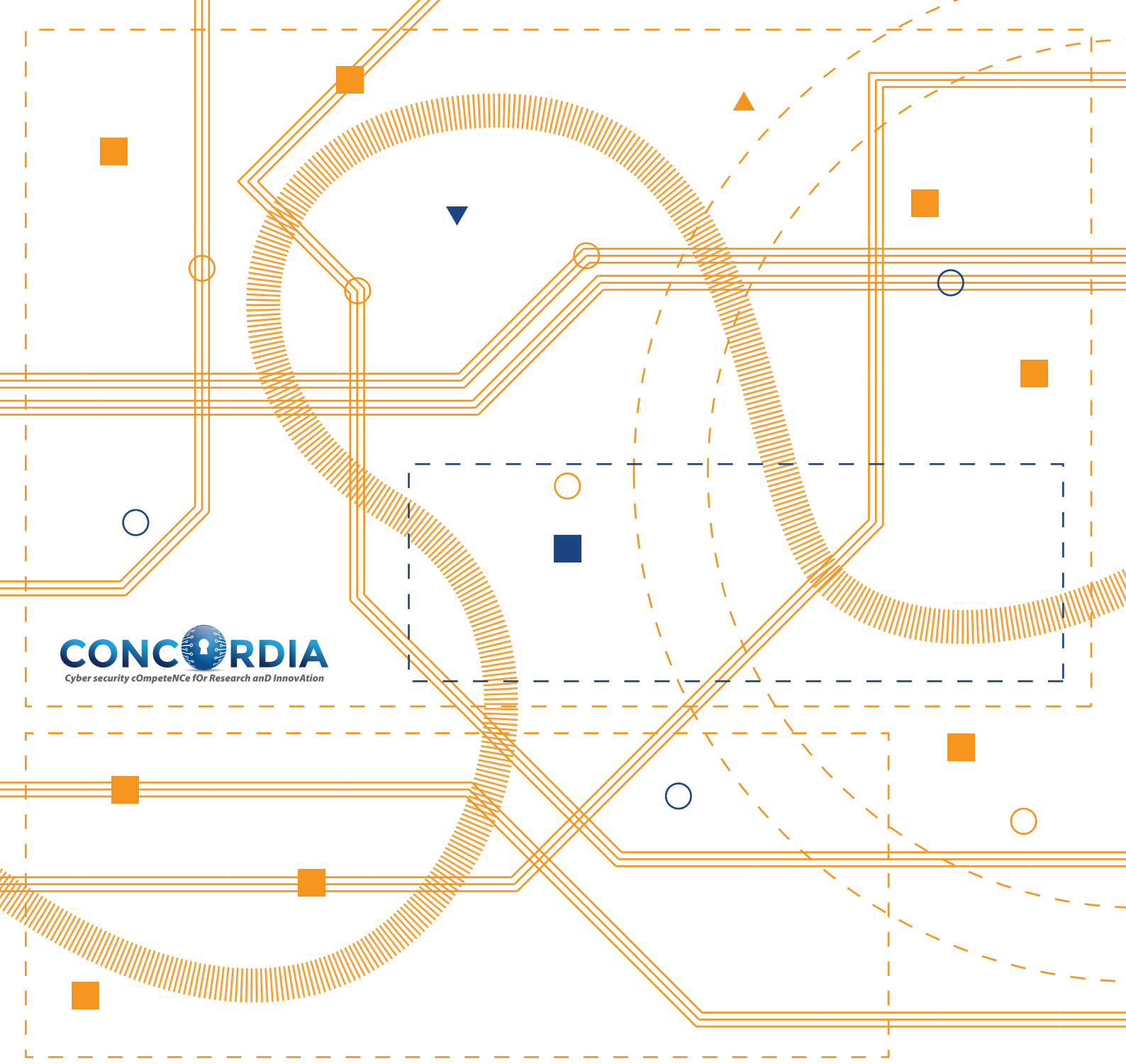
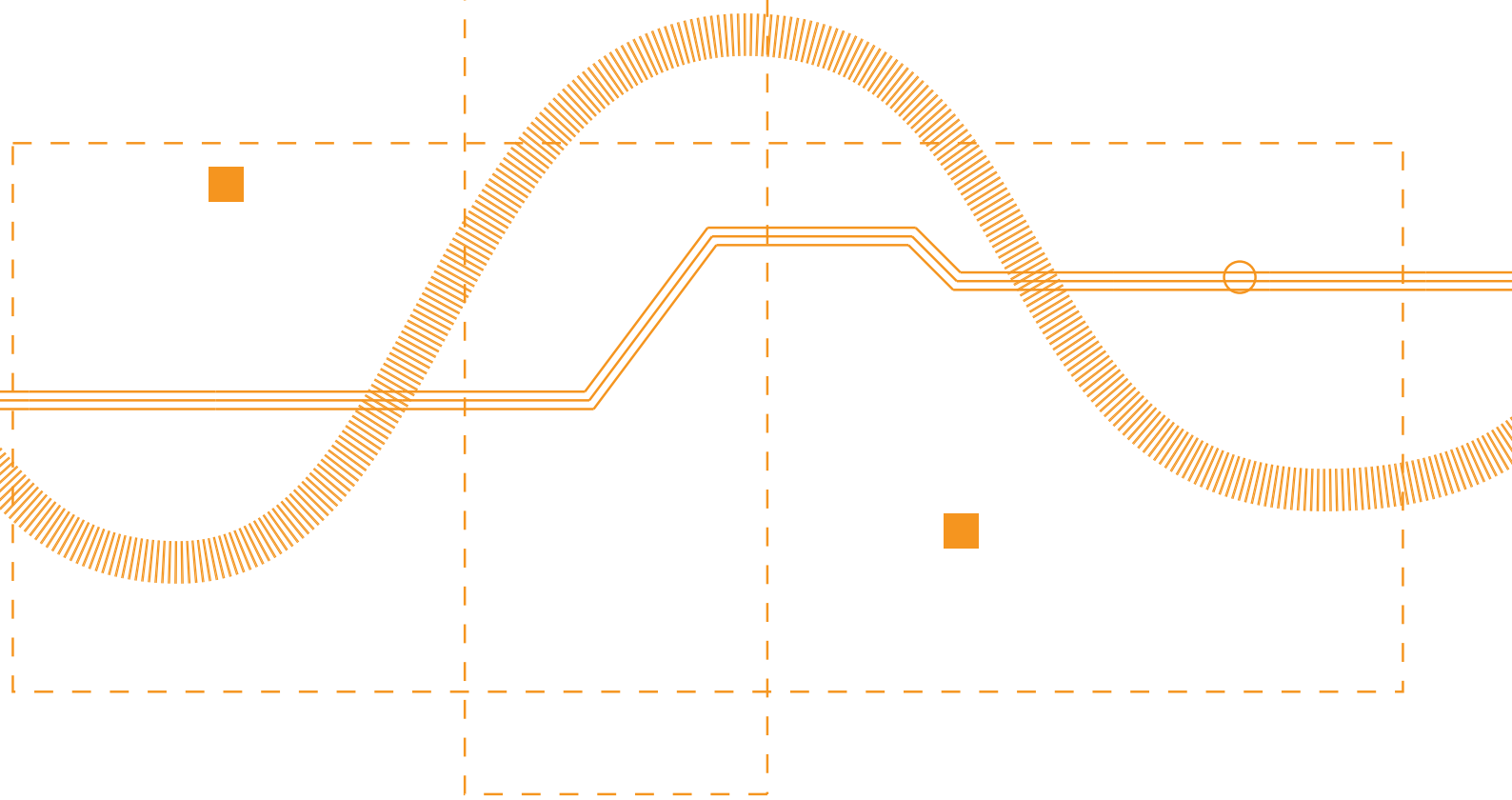


Roadmap for
Community Building



10 Community Building

'If you want to go fast, go alone. If you want to go far, go together' is a famous universal wisdom. The proposal for Regulation establishing the European Cybersecurity Indus- trial, Technology and Research Competence Centre and the Network of National Coordination Centres [101, 102, 103, 104] is one of the excellent mission instruments, as for once it is designed to fragmentation and convert duplication of efforts to synergies of coordination and cooperation, including the ability to supportvarious development of European cybersecurity competences and capabilities, also to help built, achieve and sustain digital sovereignty.

10.1 Hybrid Interconnected & Intertwined Ecosystem of Ecosystems

However, although the vision and mission are clear, and everybody agrees that collaboration is essential, the question how to collaborate is generally not addressed let alone operationalised. This, for instance, as per the multiple values, needs, interests, maturity levels, focus areas, each with their own short-term, mid- term and long-term characteristics and preconditions. Furthermore, the proposed Regulation will be focussing on four main domains that are intertwined per context, per addressed objective, stakeholders' group, impact, challenge, opportunity and life cycle phase.

Those four main domains are already mentioned and visualised in Figure 18, being (i) Sovereignty & Collaborative Resilience, (ii) Economic Development & Competition, (iii) Research & Innovation, and (iv) Education, Skills & Jobs. These are intertwined as one affects the other, as one requires the other, and as one adds to and augments the other.

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

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

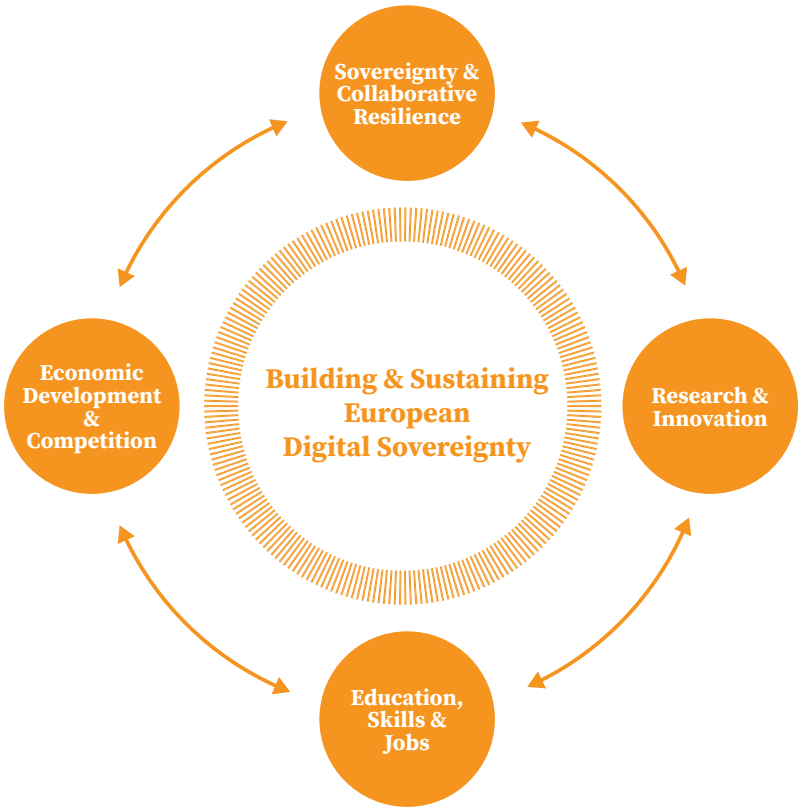


Figure 18: Contextual, impact-based symbiosis of four intertwined main domains

10.2 Objectives, Challenges & Scenarios

10.2.1 Objective: Know (Your Enemy and Know) Yourself

- **State of Play (SOP):** As stated in the Commission Staff Working document Impact Assessment related to the Proposal for Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, as well as reconfirmed in June 2020 by the Council, Cybersecurity is an issue local, national and cross-border issue of common interest of the European Union, and it needs to make sure that it has the capacities to secure its economy, democracy and society. For Europe to be prepared it needs to have a thriving cybersecurity ecosystem, including industrial and research communities. However, do we truly know the ecosystem and its communities, and do we and they know, understand and appreciate each other's capabilities, experience, offerings, challenges and needs to build, achieve and sustain future-proof digital sovereignty? Currently, one cannot represent that we really know 'ourselves' as existing European Union cybersecurity ecosystem and existing communities, also as cyber-security is a vast and constantly evolving and expanding domain, horizontal and multifaceted dimension, which nowadays relevant almost in any sector, vertical, separate or converging markets and basically any part of society, economy and daily life.
- **State of the Art (SOTA):** 'If you know the enemy and know yourself, you need not fear the result of a hundred battles.' is a famous quote allotted to Sun Tzu from his publication the Art of War. The state of the art should be to know 'ourselves' as cybersecurity universe, know what and where our weakness and strengths are, who we are missing out of to complement and optimise. It should clear and continuously challenged, updated and improved – what such cybersecurity ecosystem and its communities should consist of to build, achieve and sustain future-proof digital sovereignty, what and who we are missing in existing communities, how to complement and cater for a full-spectrum, intertwined, multi-tiered and multi-layered ecosystem.
- The state of the art should include taking into consideration – on a scenario by scenario basis, respectively objective/challenge by objective/challenge basis – the numerous stakeholders that are either directly or indirectly part of (whether desired, knowingly or otherwise) any scenario respectively objective, challenge or other situation or case. Some examples of such

stakeholders are set forth in the visual below (Figure 19). In each case, the landscape of the various relevant stake- holders and various influences each may of will have, will be different. Therefore, a contextual approach is pre-requisite.

Human-Centric Digital Ecosystems & Multi-Angled Omni-Stakeholders & Influencers

1. **The User** (Convenience-Focused, Cheap, Curious, Creative, Opportunistic)
2. **Customers** Who Are Willing To Pay (B2x, x2x)
3. **Suppliers & Value Ecosystem** (Secure In, Secure Inside, Secure Out, Secure After)
4. **Physical, Cyber-Physical & Cyber Ecosystems and Society** (including Non-Users)
5. Act First Seek Forgiveness Later **Technology & Data Titans**
6. **Investors & Financers** (they invest, and want return on investment)
7. **Policy Makers**, Standardisation Development Organisations & Markets
8. **Authorities** (Who is responsible for what, and are they capable?)
9. **Data Acces:** Law Enforcement, Intelligence Services & Defence

Figure 19: Overview of different stakeholders and influencers of digital ecosystems

- **GAP (SOTA -/- SOP):** The basis query 'How', which is generally been mentioned as the current main challenge, the first part of the GAP actually starts with 'Who'. Based on that, one can identity, assess, discuss and organise what binds or could bind the member states – in all their various facets and in the various domains and sectors relevant for government and society – and its national stake-holders together, which is for the benefit of the member states as well as others – and therefor the European Union –, both top-down and bottom-up. Furthermore, as per the ever evolving and expanding domain that is or relates to cybersecurity and digital sovereignty, this will need to be a continuouseffort.
- **Short-Term:** For the Short-Term, bridging the initial main GAP cross-EU initiative is necessary to discover, identify, map and plot the various current and potentially near-future and future stakeholders and their various interests, values, expectations and the like, including identity the various common grounds, benefits and preconditions each may foresee or seek for, either with scenario's and impact plotting or otherwise.
- **Mid-Term:** For the Mid Term, insight and oversight will grow to a level (1) where European stakeholders that wish to actively contribute to European digital sovereignty can start to understand and appreciate each other, and (2) where scenarios can be operationalised, and deployed. Starting relatively modest yet in a way that has the ability to scale and agility to evolve and be improved is recommended. As appreciation within the

EU is sought after, some traction and growth of the willingness to collaborate is expected to increase. Further organising, executing, monitoring and improving are essential.

- **Long-Term:** Where not yet achieved in the Mid-Term, getting to know and appreciate the various European stakeholders, both locally, regionally, nationally and otherwise can be scaled in the Long Term. As mentioned, narrowing this will be a dynamic and ongoing effort that will need constant attention and agility.

Conclusion: *Getting to know yourself is the first step to any next step. This is the way to start building trust, and thereafter add further trust layers on top of that. For all that we did not know before, we should not want to explain the notion of building, achieving and sustaining European digital sovereignty to them; they should understand it themselves. The above-mentioned proposed Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres offers a possibility to cater for such a meta-framework to take in the recommendation set forth above.*

10.2.2 Challenge: Short-, Mid- & Long-Term Community Engagement

- **State of Play (SOP):** Connecting and collaborating with each other sounds easy, including – seemingly – the start, yet it has probably one of the most underestimated and difficult things to achieve and sustain. One if the reasons, next to the objective set above in Section 10.2.1: 'Know (your enemy and) know yourself', is that the start looks so easy that the initial architecture, stakeholders and governance are generally too rigid, too centralised and not omni-stakeholder enough, where down the road it is impossible or nearly impossible to change let alone pivot and other improve. Another reason is that intentions and horizons tend to be dynamic and therefor subject to change, even those of the initial group of stakeholders, as well as for those stakeholders that generally appear on the horizon in the mid-term and long-term. Particularly in the cybersecurity domain and regarding digital sovereignty, this all in all is a challenging problem set.
- **State of the Art (SOTA):** The state of the art could be that each and every stakeholder understands that there is no one solution, there is no one group with the answer, no one technical fixture, and that is this all about working together,as teams, to achieve outcomes. The state of the art is that this is a team sport

of sports, and that each sport has its own rules of engagement, has its own particulars, need sits own capabilities, and diverse groups of people – both in the field and outside the field, and that each has different phases that requires different competences and capabilities.

- **GAP (SOTA -/- SOP):** Part of the GAP is to have a mission-centric focus, while appreciating that the point on the horizon will never be met as a new horizon will appear while nearing the initial horizon. Based on this notion, one can reverse engineer how, with whom, and with what to manoeuvre towards the intended yet dynamic point on the then relevant horizon which will probably not be led to a navigation in a straight line. With that, one can work to organising living labs (as well as field labs and otherwise) competence centres & deployable capabilities.
- **Short-Term:** For the Short-Term, these are examples of topics to consider:
  - » Identify community and other stakeholders needs and expectations, from all perspectives, and in the various phases;
  - » Identity awareness, acceptance and adoption metrics and KPIs;
  - » Identify skills, capabilities and experience that can contribute best to individual's readiness for 21st Century interdisciplinary challenges;
  - » Engage a diverse group of individuals to take a 360-degree view;
  - » Stimulate collaboration, innovation and co-creation;
  - » Invest in technical and organisational skills and creation of more jobs that add value to society and economy, and digital sovereignty in particular;
  - » Develop human-centric technology by involving stakeholders and the community from the very beginning, and;
  - » Build trust and trustworthiness.
- **Mid Term:** For the Mid-Term, these are examples of topics to consider:
  - » Creation of living labs and local, regional, national and (European) sectorial competence centres to attract diverse ideas and perspectives to relevant challenges;
  - » Start small scale pilots;
  - » Facilitate public participation to identify threats and vulnerabilities caused by use of certain technologies and processes;
  - » Devise innovative strategies and measures to counter potential threats and vulnerabilities;
  - » Strengthen capability building;
  - » Initiate medium-scale pilots that will include more than one- member state;

- Identify skills and enhance participation from the additional member states;
- Identify and map the outcome, challenges, hurdles and interdependencies of small-scale pilot;
- Evaluate the takeaways, build on previous deficiencies and expand the results of small-scale pilots;
- Develop tailor-made solutions and strategies;
- Ensure seamless collaboration and communication in the region and beyond, and;
- Present results of pilots, needed skills and strategies to policy makers.

- **Long-Term:** For the Long-Term, these are examples of topics to consider, where the focus is to expanding, sustaining and improving the various living Labs, competence centres and further capability building.
  - Initiate large-scale pilots that will include all member states;
  - Identify skills and enhance participation from all member states;
  - Identify and map the outcome, challenges, hurdles and interdependencies of small-scale and medium-scale pilots;
  - Evaluate the takeaways, build on previous deficiencies and expand the results of small-scale and medium-scale pilots;
  - Develop tailor-made solutions and strategies;
  - Ensure seamless collaboration and communication in the region and beyond;
  - Incorporate results of pilots, needed skills and strategies to policies.

Conclusions: *In most of the community building scenarios it is relevant to start in a diligent, mission- and principle-based yet solid way without bias or assumptions, and reverse-engineer how to complete the mission, how should be in the team, what does the team needs and how to distribute the contributions, work, risks, fruits and other benefits. Without teamwork, co-creation and co-allocation on a phase- by-phase basis one would miss out on a prerequisite success factor and main enabler and facilitator to build, achieve and sustain European digital sovereignty.*

10.2.3 Other Objectives, Challenges or Scenarios

Other objectives, challenges or scenarios regarding community building are under investigation and development as a mini-roadmap, and are currently anticipated to reach a certain level of maturity and detail to be included in subsequent Roadmap edition(s), including the following:

- **Objective: How to move from communities to a hybrid, interconnected and intertwined ecosystem of ecosystems?** This mini- roadmap is envisioned to move beyond the generally fragmented, unconnected, unbalanced and in- complete communities towards hybrid interconnected hypercube ecosystem of ecosystems, where those communities are part of but will learn to understand and appreciate the synergies and inter-dependabilities and merits of ecosystems;
- **Objective: How to build a NSG Ecosystem of ecosystems?** This mini roadmap is envisioned to be built within the current framework of the propose Regulation mentioned in the introduction of this chapter. If will consider a hybrid, dynamic, distributed yet coordinated and transparent multi-layered meta-architecture of multiple communities in multiple ecosystems with an underlying European Union level ecosystem to enable and facilitate both digital sovereignty for member states, its citizens, society and other stakeholders as well as digital sovereignty for the European Union at large. This, included without limitation (i) Research & Innovation community building, (ii) Education, Skills & Jobs community building, (iii) Economic Development & Competition community building and, last but not least: (iv) Sovereignty & Collaborative Resilience community building, as visualised in Figure 18.
- **Objective: Cybersecurity community building for, with and by EU periphery countries, regions and partners.** This mini-roadmap is envisioned to enable the European Union, member states and other stakeholders to connect and collaborate with the periphery, as digital, cyber and related matters to not stop at the borders of the European Union and vice versa, and;
- **Some objectives, challenges or scenarios that are defined elsewhere in this Roadmap**, but then where relevant developed from the community building angle, such as for instance the objectives set forth in Section 8.2.1 (Trusted Experience Sharing), Section 8.2.3 (Member States NIS Directive Comfort & Capability Building), Section 7.2.1 (Landscaping H2020 Cybersecurity Deliverables, and Section 7.2.2 (Narrowing the Investment Gap), to name a few.

10.3 Roadmap for Community Building

The visualized current overview from a Community Building perspective is shown below, in Figure 20.

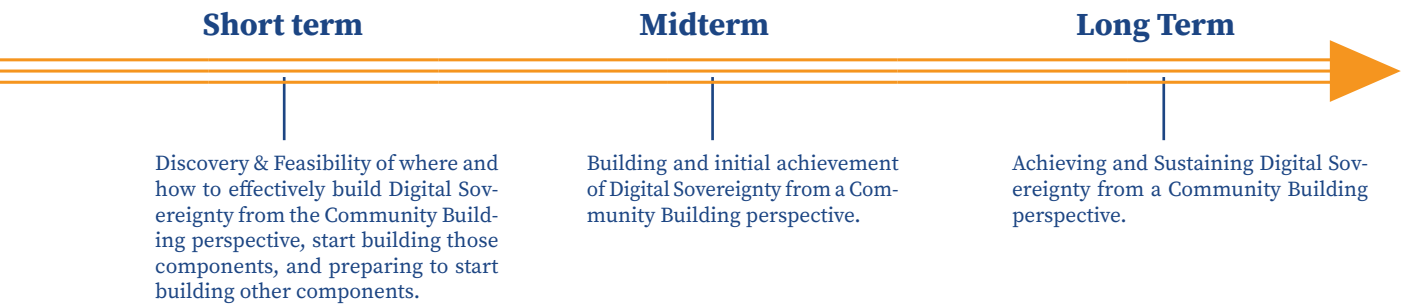


Figure 20: Overview from a Community Building perspective of most important directions, steps, and threats for short-, mid-, and long-term timeline.

10.4 Taking Stock: SOTA & the CONCORDIA leadership

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 most notable domains and dimensions coming from such stock-taking are visualized below.

CONCORDIA Project Stock-Taking for Cummunity Building

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:

- **Hybrid Interconnected & Intertwined Ecosystem of Ecosystems** - Chapter 10 (Section 10.1)
- **Plotting Stakeholders & Other Influencers** - Chapter 10 (Section 10.2.1)
- **Short-, Mid- & Long- Term Community Engagement** –Chapter 10 (Section 10.2.2)
- **Cybersecurity For, With & By EU Countries, Regions & Partners** - Chapter 10 (Section 10.2.3)
- **Education, Skills & Jobs** - Chapter 5, Chapter 8 and Chapter 10 (Section 10.2.1, Section 10.2.2 & Section 10.2.3)
- **Building Societal Trust & Collaborative Resilience** – Chapter 8 and Chapter 10 (Section 10.2.1 & Section 10.2.2)

The Cybersecurity landscape in the EU cannot be built & bolstered by one person, one organization or even one country and certainly requires contributions from the entire EU community to create a hybrid, interconnected and intertwined ecosystem of ecosystems. Moreover, in doing so understanding and appreciating the capabilities, experience, offerings and competencies of the stakeholders and other influencers involved is essential while also ensuring that the said symbiotic ecosystems can be sustained in the short, mid and long run. The focus on education, skills and jobs in the cybersecurity landscape is essential and needs to be supported after project CONCORDIA given that it creates immense value to society and the economy. Lastly, societal trust and collaborative resilience are critical layers that need to be continuously assessed, evaluated and improved in line with the dynamic cybersecurity landscape.

10.5 Contributions for EU policies: Community Building View

This Chapter Roadmap for Community Building – 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.***

[100] European Parliament Legislative Observatory. European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres - 2018/0328(COD). (2018). Accessed Dec. 18, 2020.

[101] European Union Law. ***COM (2018) 630: Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.*** (2018). Accessed Dec. 18, 2020.

[102] European Commission. ***Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.*** (September 2018). Accessed Dec. 18, 2020.

[103] European Commission. ***Commission Staff Working Document Impact Assessment.*** (September 2018). Accessed Dec. 18, 2020.