Alliance for Internet of Things Innovation

Brussels, 25 May 2022

AIOTI Input to Call for Evidence for an Impact Assessment on the initiative: Cyber Resilience Act (CRA)[1]

I. INTRODUCTION

a. Security of and related to IoT ecosystems is one of the main trust components that AIOTI is and has been focussing on since it was founded. A substantial part of IoT ecosystems are already, or will become part of critical infrastructure, vital systems and essential services.

b. IoT is one of the main areas where physical and digital realities meet, in the meanwhile more than 20B times. Thus, the relationship between IoT and cybersecurity is crucial from the security point of view where a holistic perspective that includes a joint approach to physical, cyber-physical and digital security is required.

c. As the Commission has opened consultations on the Cyber Resilience Act, the aim of this new initiative seems to be to ensure that cybersecurity is taken into account during all phases of the development process (security by design) as well as that products are placed on the market with the most secure settings enabled by default (security by default). It also seems to be to improve the internal market's functioning by streamlining and supplementing existing rules applicable to digital products and preventing further fragmentation of cybersecurity requirements for digital products and ancillary services in the market.

d. This new proposal seems to adopt a horizontal approach to cybersecurity, namely it will be applicable across sectors. Moreover, there is awareness that emerging technologies pose new risks throughout their whole life cycle. One specific example concerns software security, which is seldom addressed in EU law. The new proposal seems also to aim to complement the certification framework envisaged in the second part of the Cybersecurity Act (CSA).

e. AIOTI therefore endorses the intended objectives and welcomes the possibility to respond to the call for evidence, and in the following paragraphs will expand on several aspects of this initiative.

f. Regarding IoT Security, in 2016 and 2017 AIOTI together with the Commission, ENISA and other relevant AIOTI members and other stakeholders has organised two workshops in which these and related topics has been extensively discussed and resulted in outcomes as published in two reports, which are encouraged to be taken good notice of and form the basis of the observations made below.[2]

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

[2] AIOTI Workshop on Security and Privacy in IoT of 16 June 2016: https://ec.europa.eu/digital-single-market/en/news/aioti-workshop-security-and-privacy-etsi-security-week; Final Report Workshop on Security and Privacy in IoT of 16 June 2016: https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf; Final Report European Commission of 13 January 2017 Workshop on Internet of Things Privacy and Security: https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshops-report.

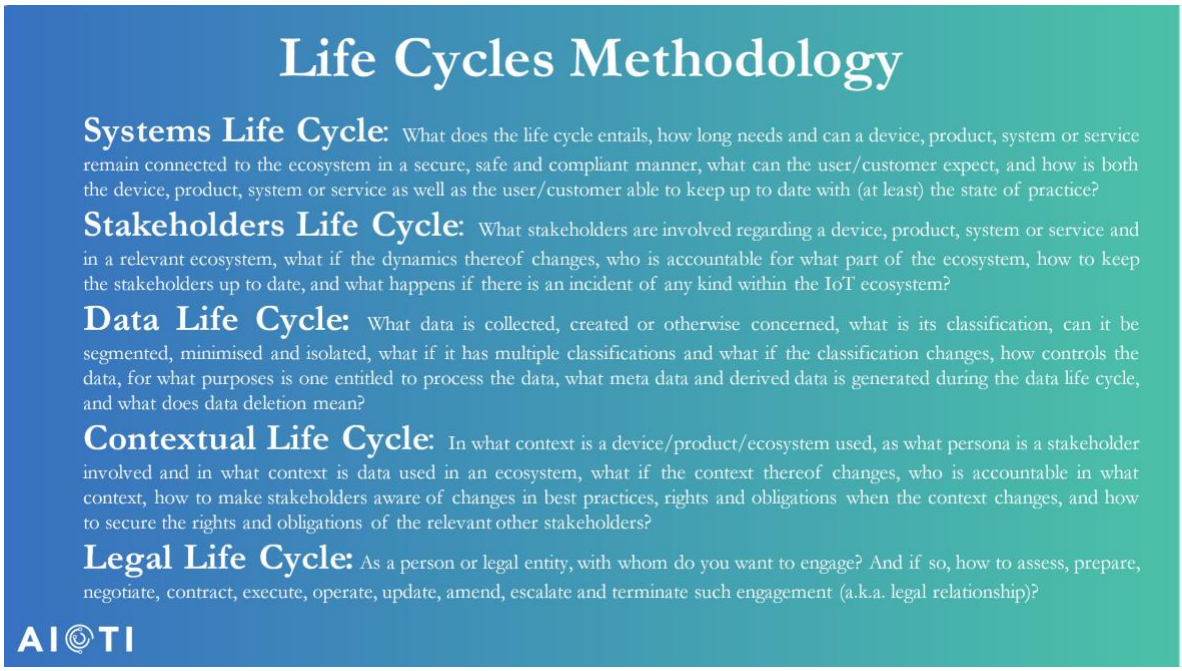
II. MAIN OBSERVATIONS

Horizontal, Cross-cutting & cross-sectorial

1. There is a need for a horizontal, cross-cutting & cross-sector approach. Sectors are not isolated or otherwise silo-ed, and as per the ongoing and expediting convergence become more and more
2. interconnected and hyperconnected, bringing greater opportunities, cross-fertilisation on best practices, data and intelligence sharing, but on the other end also augment known and unknown threats and vulnerabilities when they arise. Therefore, devices and components are used cross-sector or often connected devices are simply 'mis-used' in a non-intended use case if they fit for purpose.
3. Ecosystem thinking, end-to-end, holistic and data-centric, is a prerequisite. For instance the harmonisation of 'identification' in different critical, vital or essential IoT ecosystems is necessary. This is for instance particularly important, for instance, in healthcare, (commercially of the shelf or other) especially wearables used in for health related purposes, and UAVs (whether transporting people or goods, proving incident support, or sensing or performing inspection tasks) within these critical, vital respectively essential physical, cyber, cyber-physical domains. In this context, uses of IoT devices in safety-critical and liability-critical systems need to be properly considered.
4. IoT is one of the links of the digital world with the physical one, being a combination of the cyber-physical and physical worlds. Therefore, IoT is where cybersecurity meets security and safety and both have to be addressed from an integral perspective and with a duty-of-care principle in mind. Cybersecurity threats can impact in the real world through IoT systems and physical actions over IoT can be part of cybersecurity attacks. Said otherwise, this creates or otherwise extends and augments the attack surface. As mentioned in the introduction, AIOTI has been actively contributing and will further contribute on this topic.
5. Similar to the General Data Protection Regulation, the CRA should also implement a horizontal methodology wherein it takes a risk-based, impact-based and principle-based approach to cybersecurity. By outlining basic principles as well as establishing a standard minimum threshold for security assessment, the CRA can enable organisations across different industries to implement resilient and future-proof digital products and ancillary services. Ultimately, doing so will also boost the overall level of cybersecurity in the EU (and its neighbouring countries) and have a positive effect on the level of trust in the European market and Its digital and connected products.

Entire & Dynamic Life Cycles

6. A life cycle approach to cybersecurity does not imply that one sole party such as for instance an upstream manufacturer, midstream integrator or downstream customer is responsible for a whole life cycle. Yet, the CRA is aiming to establish for each actor their roles, (co)responsibilities and related (co)accountability in order to ensure legal certainty. The figure below represents the different life cycles that an organisation must account for in order to take a holistic and overarching approach to cybersecurity, which have been discussed and established in various AIOTI workshops together with internal and external stakeholders.



7. In addition, it is essential that the CRA stresses the cyclical nature of designing and implementing security processes and systems given that they should not be viewed in a stand-alone manner but should be constantly re-assessed and re-aligned. It should consider functionality, performance, adaptability to emerging technologies, cost effectiveness and most importantly flexibility.
8. Cybersecurity incidents that have taken place worldwide in the last few years including the recent SolarWinds supply chain attacks[3] are evidence of how complacency can be catastrophic for a company's security processes and ultimately the company's reputation, market standing and similar for its affected customers in the public sector and private sector.
9. Hence, using approaches such as the Life Cycle Methodology shown above, companies must strategically assess the efficiency of their existing processes, controls and systems in line with the different facets that impact them including technological innovation, evolving threat landscape, regulatory changes and the like.

[3] https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

Coherence

10. Since multiple relevant regulations in the digital domain have been proposed or already adopted, there should be an increased coherence between those. For instance, it should be clarified the relationship with the European Cybersecurity Act (CSA), Radio Equipment Directive (RED), General Data Protection Regulation (GDPR), General Product Safety Directive (GPSD)/proposed Regulation, Machinery Directive/ proposed Regulation, Medical Device Regulation (MDR), eIDAS Regulation (EUDI), Sales of Goods Regulations (Art. 7(3)), proposed Digital Operational Resilience Act (DORA), proposed Regulation European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres or other current or upcoming or (to be revised or otherwise refitted) directives and regulations.
11. In consideration of the horizontal scope of the CRA, the policymakers should ensure seamless and clear application between other horizontal legislative proposals and relevant *lex specialis*. In order to support Member States in strengthening their respective capabilities and competences, and improve (cyber)security and resilience, the CRA should ensure that there are no overlaps or double reporting required amongst all cyber related legislative proposals, while at the same time acknowledging the attributes of different sectors.
12. In the context of privacy, the CRA should also support the GDPR. As §25 of the GDPR asks 'to implement appropriate organization and technical measures' to secure Personal Identifiable Information (PII) the CRA could act as a means to secure such PII in digital products while storing, transferring or processing PII.
13. As adversarial attacks are usually not focusing on the intended use of digital products and ancillary services the CRA should generate coherence between legislation addressing only the intended use and legislation addressing the challenge related to cybersecurity also taking the non-intended use into account.
14. The essential cybersecurity requirements are intended to be translated into harmonised standards specific for the different categories of products. One of the policy options considered by the Commission in the call for evidence is introducing voluntary measures: "voluntary certification schemes under the Cybersecurity Act could be further developed and applied. Soft law measures such as guidelines or recommendations could also be considered, in particular on the cybersecurity of non-embedded software".
15. Soft law is the term applied to EU measures, such as guidelines, recommendations, declarations and opinions, which in contrast to regulations, directives, and decisions are not binding on those to whom they are addressed. Soft law usually affects policy development and practice through an informal persuasive influence. Member States and other actors might undertake to do something voluntarily which they would be less willing to do if legally obligated. Soft law, therefore, is a more flexible instrument in achieving policy objectives.
16. As an example of such an approach can be cited the Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification where the key element was the establishment of the European cybersecurity certification framework. It lays down the main horizontal requirements for European cybersecurity certification schemes to be developed.

17. The purpose of the certification schemes is to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data throughout their life cycle. The Cybersecurity certification is voluntary. The certification and evaluation shall be performed by a conformity assessment body, which is accredited by its National Accreditation Body.

18. Soft law instruments on cybersecurity issues provide for more flexibility compared to hard law. They allow for less politicized compromises and are developed more quickly and at lower cost. Also, soft law instruments are very well suited to developing ethical (and professional) standards, supporting coordinated action where hard law is lacking, and their use does not diminish a states' (or a court's) sovereignty.

Harmonisation & International Standards

19. Next to legal coherence mentioned in the previous paragraphs, the importance of harmonisation and (international) standards cannot be overstressed. Fragmentation is one of the main challenges, also in the various IoT security dimensions in scope of the CRA. While different sectors may have unique cybersecurity standards, there are a set of principle-based cybersecurity measures and controls that are common across sectors. These can be found in various standards, such as for instance ISO/IEC 27000 Series, IEC 62443 and other information security and other security and safety open standards and other guidelines that either already exist or are under development by ESOs and other SDOs, including without limitation the recent guidelines by OECD on digital security of products4.
20. Furthermore, to enable security and privacy functionality while facilitating integration and interoperability to related sectors, domains and dimensions, open standards should be preferred, where available, for security spending and solutions.
21. Harmonisation is not necessarily a matter of coming to one standard or the like, but also to find ways to co-exist and work to strengthen each other, such as between for instance a NLF-Approach and the current CSA. For an example, a NLF-Approach does address the lifecycle focusing on a go-to market day perspective, while a traditional certification approach looks only at the timeframe of the certification; a NLF-Approach already include surveillance during the whole product life and takes the manufacturer accountable for it.
22. Collaboration as part of the harmonisation approach may include sharing positions and ideas with international stakeholder also working on future cybersecurity requirements like the US Cyberspace Solarium Commission5 (of which 27 of its recommendation have been put into law in January 20216), Japanese METI or Indian TEC7.

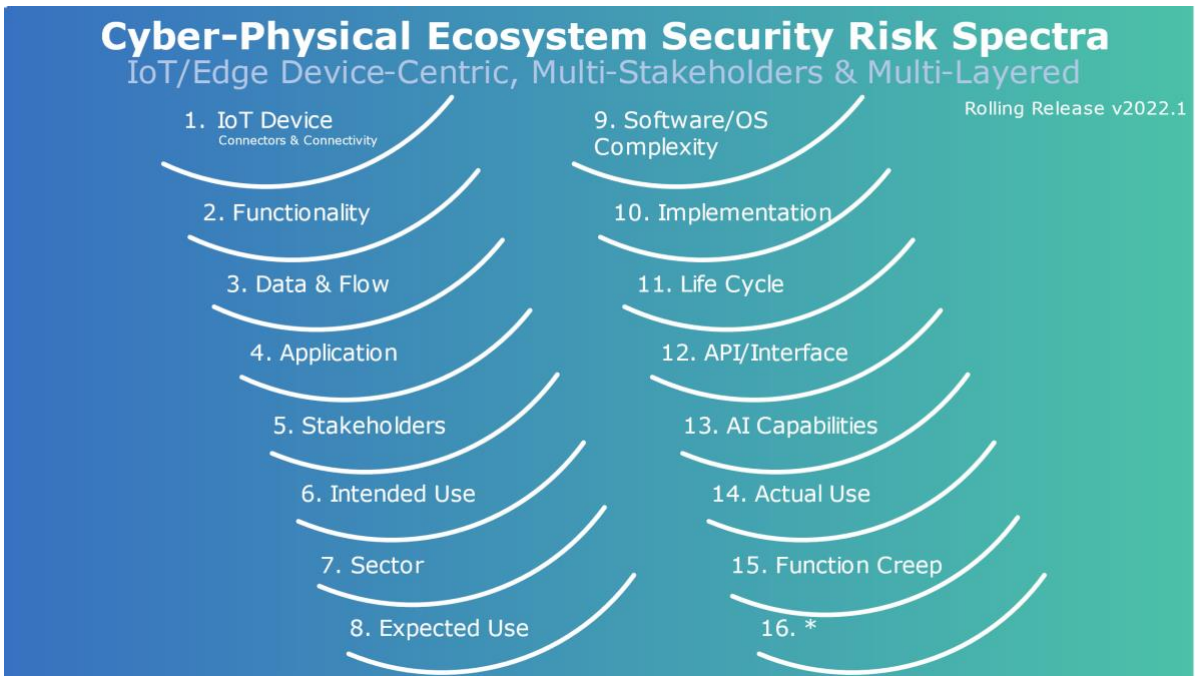
[4] http://www.oecd.org/digital/ieconomy/digital-security/
[5] Cyberspace Solarium Commission Legislative Proposals (July 2020): https://www.solarium.gov/report/legislative-proposals
[6] NDAA Update: https://www.solarium.gov/press-and-news/ndaa-override-press-release
[7] India TEC: https://www.tec.gov.in/inviting-comments-on-draft-guidelines-for-consumer-iot-security/

23. AIOTI encourages the Commission to propose a maximum harmonisation framework. This would contribute to legal certainty as well as to make implementation more efficient and related costs possibly lower. Currently, the implementation of standards as envisaged in the CSA may lead to fragmented approaches on mandating certification in individual EU Member States which would not strengthen cybersecurity in Europe as a Digital Single Market. Establishing a pan-EU framework for certification would enhance legal certainty, which is indispensable for businesses and other economic operators in the EU market.
24. Harmonization also means a levelled approach in the context of risks as well as assurance levels. While there will be self-declaration of conformity acceptable for a low assurance level for low-risk products and ancillary services and mandatory certification for high-risk applications there is a huge amount of use cases in between which fit to a 'substantial assurance level' as defined in the CSA.
25. The CRA should also take into account the specificities of certain categories of products, namely software. Indeed, the context in which a piece of software is used affects its risk profile, and its components vary throughout its development, integration, and use. This is why the author of a software component cannot control the environment in which it is executing. More specifically, the component author could design a software for use in one environment, but it might end up being deployed, unbeknownst to the author, in a completely different environment for which it is ill-suited. Additionally, software will be updated many times and the same piece of software may present a different risk depending on which product it applies to (for example a similar SaaS component in a smart coffee machine vs. usage of the same software building block in a medical device). This is especially true in the B2B world and in the case of Open-Source development platforms, which are key for supporting strategic autonomy and digital sovereignty, as the supplier/developer typically would have no means of knowing which parts of their product software the client had used, modified, or not utilized, and might also be limited to intervene by contractual agreements.
26. To reduce costs of conformance, certification composition is an important mechanism to make use of existing certificates of components and 'sub-products' used in digital products also in order to support SMEs.
27. The CRA has also the chance to harmonize recall mechanisms of vulnerable digital products In the Digital Single market and avoid Individual procedures per Member State.
28. 'End of life' security requirements related to destruction or disabling of digital products and deletion of credentials should be harmonized in order to avoid fragmentation.
29. Additionally, the CRA could be prepared in order to provide relevant cybersecurity related data for the planned *Digital Product Passport* in a digital and structured format.

Linear is not necessarily enough

30. In line with the outcomes of the abovementioned workshops, standards or other policy instruments that have a linear or otherwise process-based approach - such as for instance ISO 27001 - are good to have. However, these do not establish the dynamic and contextual appropriate levels of trust, trustworthiness, security and related end-to-end or ecosystem life cycle resilience that is required in real-life for and in critical infrastructures, vital systems and essential services. This for once as hackers and other malicious actors change their ways on a daily basis and can easily manoeuvre around these instruments. Compliance to paper processes does not mean security effective security, which should be CRA's end goal. For instance, the GDPR is a valid reference, as it envisages these concepts, including in Article 32 GDPR about the requirement of state-of-the art security and related continuous dynamic accountability.

31. The CRA should establish a certification mechanism that considers several dimensions, such as, but not necessarily limited to, the characteristics of the product, its functionality, the quality and quantity of data and data flow it processes, its application, the stakeholders directly and indirectly affected, the intended use, the expected use and the actual use.



32. Therefore, it is for once recommended to assess and refer to the European Cybersecurity Certification Framework and its certification schemes (such as the upcoming EUCS) to cover the risks from a product, services (including without limitation cloud services) and (edge, IoT and other) systems view and be able to adapt the assurance levels according to the risks. Certification to demonstrate conformity of highly critical products, services and systems shall be done on assurance level 'High' to generate trust. In this context conformity assessment bodies should be taken into account to be able to leverage the European cybersecurity certification schemes also for critical infrastructures.

Emerging Threats & Opportunities

33. The development of autonomous systems, artificial intelligence, quantum computing and other emerging technologies in the broad sense of the word should be taken into account in the CRA, and national, regional and Union strategies (for instance AI or IoT devices used to attack and to defend). This for once as the related risk and impact may be affected, either positively or negatively. This in particular taking into account the expected amount of IoT devices in critical infrastructure, vital systems and essential services, whereby such IoT devices are or may not initially be designed for use in these domains.
34. It is important to be clear about the potential risk and impact of intended, expected respectively actual use, and how to both classify those and mitigate, monitor or even eliminate these. In this context, but also related to other existing or evolving technology, the duty of care and related accountability should be added as a main principle related to cybersecurity requirements, same as in the GDPR.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.