Response of the EU-funded projects CC-DRIVER, CYBERSPACE, COPKIT, HEROES, INSPECTr, LOCARD, RAYUELA, ROXANNE, and TRACE as well as Trilateral Research and Coventry University to the EC consultation on a proposed Cyber Resilience Act

The European Commission (EC) has issued a call for evidence for an impact assessment in connection with its proposed Cyber Resilience Act.[1] In response to that call, this document represents the views of those listed at the end of this document. Principally, the list comprises the coordinators and partners of multiple EU-funded security projects, who participate in an LEA project cluster.

We note that in addition to the call for evidence, the EC is launching a public consultation to gather the views of a variety of individual stakeholders and various of those on the list below are also responding to that questionnaire.

In its call for evidence, the EC states that it "would like to gather:

- stakeholders' views on current and emerging problems related to the cyber security of digital products and associated services, including non-embedded software;
- stakeholders' views on the possible policy approaches to address such problems, the available options and their potential impacts; and
- evidence and data underpinning the identified problems."

Hence, in response to each point, we offer the following comments:

stakeholders' views on current and emerging problems related to the cyber security of digital products and associated services, including non-embedded software;

- There is a clear and obvious need for improving cybersecurity in the EU. The types and number of cyberattacks and cybercrimes is growing constantly and causing significant damage to our economy and society, as has already been demonstrated many times. To constrain the growth in cybercrimes, the EU needs (1) rules and standards governing the cybersecurity of all connected devices, services, processes and software,[2] (2) a regulator with the necessary resources and capacity to enforce the rules and (3) a huge increase in stakeholder and public awareness on the need for enhanced cybersecurity, all of which is less costly than dealing with the consequences of cyberattacks and cybercrimes currently being experienced.

- As explained in footnote 3, we support Policy Option 5. We favour a strong European regulator who interacts with strong national regulators. The model offered in the data protection domain of national data protection authorities who convene in a European Data Protection Board with the European Data Protection Supervisor could serve as a

[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, accessed on 25 May 2022.

[2] In his keynote from RSA'2017 (https://www.youtube.com/watch?v=b05ksqy9F7k), Bruce Schneier already made the point that IoT device manufacturers have no incentive to include any security, so regulators must force them. US states of Oregon and California released regulations in 2020 with specific requirements that IoT devices must meet, pioneering work along this line.

model in the cyber resilience domain. A regulator is needed as there is abundant evidence of the failure of self-regulation.[3]

- Putting in place rules implies being able to enforce the rules when someone breaks them. An EU regulator and national regulators must have the resources and capacity to enforce the rules.

- Most organisations, especially SMEs, have not considered what they need to do to ensure the cyber resilience of their products and services. Organisations need to continuously verify the security of their supply chain. In cases where this would be a disproportionate burden, the regulator or certification scheme could support the necessary checks. The EC should support the development of methodologies and tools supporting the process of certification that are open source or affordable for SMEs and small organisations to avoid entry barriers that would negatively affect the market. The European Cybersecurity Competence & Network Centre could be a vehicle for the development and dissemination of the tools and methods.

- Clarity will be needed on what certification means, as it may mean different things for different products, services, markets and domains. An effort is needed to harmonise regulation and certification, which may be especially important for SMEs. Based on https://arxiv.org/abs/2004.12179v1, there are more than 1,000 IoT security guidelines developed by standard bodies, governments and industry groups, which reduces their effectiveness. In addition, 70 per cent of such guidelines relate to early IoT device lifecycle stages, which highlights the critical position of manufacturers in addressing the security issues in question.

- The EC needs to distinguish between the rules established in the new Cyber Resilience Act and the requirements for cybersecurity certification (re the EU's 2019 Cybersecurity Act) and/or to manifest their complementarity, how to delineate between the two and how they work hand in hand. Certification could be voluntary or obligatory depending on the risk level. The proposed Cyber Resilience Act could adopt a proportionate, risk-based approach, as in the proposed AI Act.[4]

- Some cybersecurity certification rules could be mandatory, e.g., in areas such as critical national infrastructure, national security, health or where there is a risk of harm to humans. Furthermore, depending on the risk level of the digital devices' usage, the cybersecurity certification of the personnel who administer the devices should also be taken into consideration and in some cases should be characterised as mandatory.

---

[3] Yeung et al., among many other critics, cite the failure of self-regulation. They note that "self-regulatory standards have no legally binding force… it is naive to expect that they [industry] can be trusted to abide by voluntary standards when faced with such powerful commercial incentives… given the overwhelming evidence that the tech industry cannot be relied upon to honour its voluntary commitments." Yeung, Karen, Andrew Howes and Ganna Pogrebna, "AI governance by human rights-centered design, deliberation and oversight: An end to ethics washing", Chapter 4, in Markus D. Dubber, Frank Pasquale and Sunit Das (eds.), *The Oxford Handbook of Ethics of AI*, Oxford University Press, 2020, pp. 77-106 [p. 84]. Yeung et al cite the following example: "For a sobering account of Facebook's repeated failure to honor its publicly stated commitments", see UK House of Commons, Digital Culture Media and Sports Committee, Disinformation and "Fake News": Final Report, Eighth Report of Session 2017–2019, February 14, 2019, HC 1791. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf, accessed on 25 May 2022.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN, accessed on 25 May 2022.

- The EC should also clearly delineate the responsibilities between the regulators of the AI Act and the proposed Cyber Resilience Act.

- Adopting a meaningful cybersecurity certification scheme on an EU-wide basis poses many challenges and the EC needs to adopt such a scheme as soon as possible to address the lack of trust, reliability, safety and security of connected devices, services and technologies. A certification scheme should be focused on specific products and services, not organisations -- a company may offer various products and services, not all of them meriting the new EU cybersecurity certificate. The EC should give guidance to companies to not misrepresent what their cybersecurity certificate covers and impose penalties on those that do so.

- The certification schemes should cover the elements of the systems' cybersecurity that influence any resulting law enforcement investigations, availability and quality of related forensic data.

- There needs to be clarity on what resilience means, especially in the context of different products, services and software. There should be a clearer line between resilience, robustness and response. A challenge will be establishing some criteria for the resilience performance of products and services when they are attacked. Specific benchmarks will likely be needed for different products and services. Benchmarks will be useful in certification and establishing liability. Of specific interest is the forensics preparedness to allow for the collection of digital evidence when deemed necessary.

- In view of the millions or billions of connected devices and services, it will be a logistical challenge to put in place a network of certification authorities, to make the process of certification relatively easy and transparent. Self-declaration of compliance with a standard would be helpful here. If someone claims to be compliant and is not, there should be some penalties and consequences.

- The big tech companies are paying relatively large salaries for the technical expertise they want, leaving a huge shortage in cybersecurity capacity for SMEs who are not so well endowed. ENISA, regulators and relevant public bodies should increase their training and expertise-transfer activities[5] towards SMEs, public organisations and education bodies, including universities and schools. Addressing the shortage of talent in cybersecurity has to begin in schools.

- EU bodies (ENISA and any new regulators, in particular) should engage in more horizon scanning regarding what products, services or non-embedded software might pose some problems in cyber resilience.

- The rules in the proposed Cyber Resilience Act should apply to anyone putting a cybersecurity product, service or software on the European market. This is, among others, to avoid unfair competition from non-compliant bodies outside the EU.

- The proposed Act should explicitly take into account and address the specific considerations of products and services from the open source market, e.g., support the

[5] NoMoreRansom (https://www.nomoreransom.org/) is a positive example.

development of open source products and services as building blocks (including for the process of certification) for other open source activities.

- Any new rules in the Cyber Resilience Act should explicitly take into account ethical considerations, including privacy and other fundamental rights (such as freedom of expression and freedom of movement) according to the EU *acquis communautaire*.

- The proposed Act should emphasise the utility and value of information-sharing between LEAs and the public, especially victims, and of cooperation between LEAs within the EU and beyond the EU and especially with INTERPOL. Information sharing could be turned into specific certification and/or standardisation requirements. Big tech companies must put in place measures to protect their users and improve their online experience, closely collaborating with LEAs to achieve this common objective. They should invest part of their profits in research to develop tech tools to protect their users, especially when they are minors.

stakeholders' views on the possible policy approaches to address such problems, the available options and their potential impacts;

A principal approach to address the challenges identified above is to introduce new legislation, i.e., the proposed Cyber Resilience Act, with a regulator that has strong powers and the necessary resources to enforce the legislation at EU and national level. For this, a horizontal regulatory intervention is required.

If the regulator's role is not assigned to ENISA, the Cyber Resilience regulator should coordinate closely and interact frequently with ENISA, the cybersecurity certification community, and the proposed AI Act regulator.

The European Cyber Resilience regulator should interact regularly and frequently with its counterparts in all Member States.

The EC should fund Horizon Europe and ISF-P projects focused on cyber resilience and should encourage in its guidelines for funding proposals that cyber resilience be given appropriate consideration.

The EC should consider the need for and support new standards of cyber resilience via CEN/CENELEC, ISO and ETSI.

The European Multidisciplinary Platform Against Criminal Threats (EMPACT)[6] enables Member States to identify EU priority crime *threats* where collective action is needed. Its remit should be expanded to include *vulnerabilities*. The lack of resilience in many connected products and services should be identified as a serious vulnerability and an opportunity for attackers (threats). The Cyber Resilience Act should explicitly support the EMPACT platform.

ENISA, CERT-EU, CSIRTs and the new cyber resilience regulator should interact with Europol to understand which products and services are being reported to the LEAs as most

6 https://ec.europa.eu/home-affairs/policies/law-enforcement-cooperation/operational-cooperation/empact-fighting-crime-together_en, accessed on 25 May 2022.

frequently attacked and what certification requirements should be established to help in law enforcement investigations.

evidence and data underpinning the identified problems.

Research from EU-funded security projects

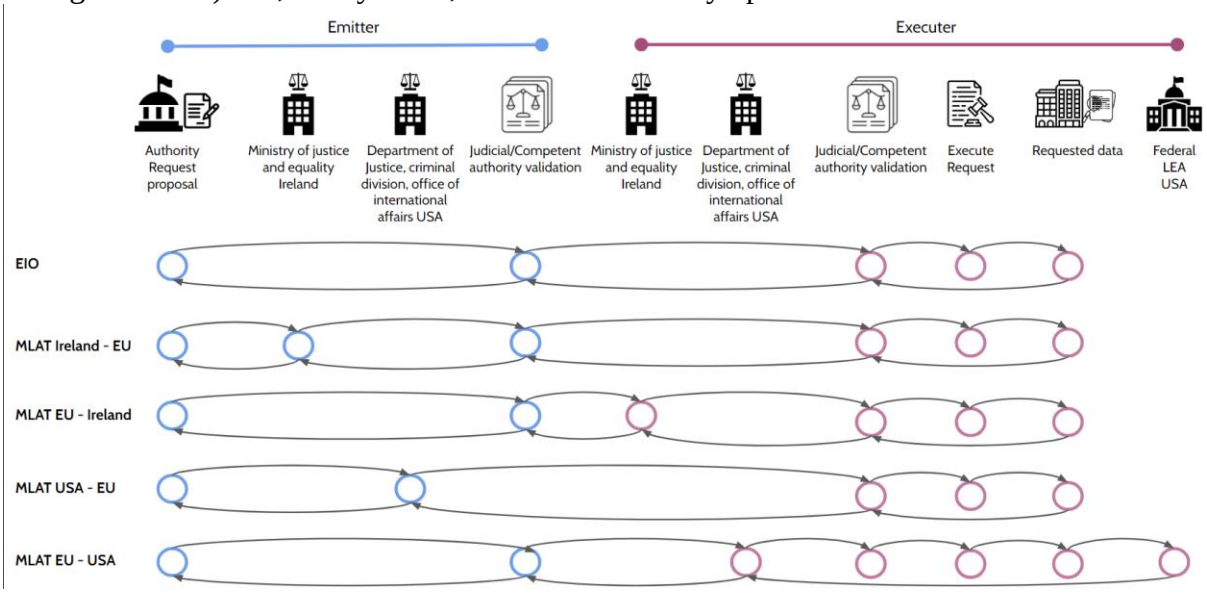
The case studies (D2.6) conducted by the ongoing TRACE project [1] indicate that there are new methods by which cyber extortion can take place. For example, using ransomware to deceptively market products online is one such new method. This dimension opens up grey areas that can undermine the capability of law enforcement authorities to effectively counter such criminal behaviour. It becomes even more challenging when a crime conducted by a legal person is approached more from an administrative angle than employing both criminal and administrative measures. TRACE case studies also evidence that:

- Cyber extortion as in ransomware is developing new ways to target its victims such that a holistic regulatory approach is required.
- In dealing with cyber extortion, new pathways of collaborative engagement are needed to undermine operating routes and financial objectives of perpetrators.
- Victims of cyber extortion can be re-victimised if care is not taken to build their capabilities to respond to such criminalities.
- Cyber extortion can be used to facilitate illegal money flows.
- Swift and comprehensive reforms are needed to capture the dynamic formations of cyber extortion.
- Capabilities of law enforcement authorities need to be enhanced particularly in AI and understanding the scope and dimensions of cyber extortion.
- Cyber extortion is versatile and can ride on other criminal activities such as money laundering and fraud to succeed against victims of such crimes.
- The uncertainties about the scope of operations and impact of the ransomware require innovative toolkits as proposed by the TRACE project, especially with respect to using a single platform-agnostic tool to automate complex analytical tasks and visually present combined results.

The chain of custody and the exchange of evidence among different stakeholders must be homogenised, at least across all EU Member States. Both INSPECTr [8] and LOCARD [2] have developed an immutable, transparent and auditable chain of custody platform to record all actions performed on digital evidence, facilitate their exchange, guarantee that the proper authorisations have been made, and allow their use in a court of law. LOCARD adopts the approach of blockchains to create an auditable trace of actions performed on the digital evidence and models the interactions among different stakeholders via smart contracts.

The tools that will analyse the collected evidence (which would be protected by the aforementioned immutable, transparent and auditable chain of custody) must generate reports that should include a detailed description of the scientific procedures used in the analysis: used algorithms, parameters, AI models and the evaluated metrics in the AI models. This would make the analysis process transparent, traceable and repeatable by both sides of a lawsuit. Every tool developed in HEROES [12] is being designed with such a target in mind.

Due to the nature of digital evidence, the collaboration of different entities and many jurisdictions may be necessary. However, the current legal framework is rather fragmented (see the figure below) and, in any event, some countries may opt not to collaborate.



Main flow of each existing collaboration instrument for the exchange of digital evidence and the corresponding institutions and authorities involved. Source: [9]

With regard to the aforementioned fragmented legal frameworks, the HEROES project is investigating the possibility of harmonising legal frameworks for undercover agents or other hidden methods to provide the possibility of their use, while bearing in mind all procedural safeguards and fundamental rights.

Cybercrime performed by state sponsored actors is likely to increase. Diplomatic intervention might be necessary, although the success of such interventions may be doubtful.

ROXANNE [3] collaborates with ZiTIS [10] on creating a unified approach to bringing lawfully intercepted data (tested on synthetic sets) to the research. The EU supports activities related to the international exchange of digital evidence from malicious operations (including those related to cyber attacks) in near real-time which could greatly help authorities to speed up the process of using this evidence in a court of law.

A recent study [4] by Vagelis Papakonstantinou suggests that the model of personal data protection could be of invaluable assistance, as data protection has preceded cybersecurity and now benefits from a comprehensive legal framework at EU and Member State level. The author additionally argues that the distinction between cybersecurity as praxis and as a state could perhaps assist understanding better and that it paves the way for introduction of a new relevant right. Another study [5] by Iain Nash identifies legislative and judicial shortcomings in relation to establishing liability, regarding the threats that are posed by the hacking of smart devices. In addition, it proposes remedies with the intention of establishing a solid legal basis and treatment for cybersecurity. In relation to encryption, a study [6] by Dizon and Upson examines illustrative examples of international and national laws and in particular export control laws, substantive cybercrime laws, criminal procedure laws, human rights laws and cybersecurity

laws, concluding that the legal framework is the key to discerning the present state and future direction of encryption laws and policies. The study [7] by Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert (2019) references the critical role of ENISA in implementing the NIS Directive on security of network and information systems and elaborates upon the inevitable relationship between the NIS Directive and the EU's General Data Protection Regulation, in addition to the examination of Member States' obligations regarding national strategy as well as cooperation at EU level. All of the above indicates current and emerging problems in cybersecurity from a practical and a legal framework and demonstrate the importance of regulation in the context of the proposed Cyber Resilience Act.

Regarding sharing of cybercrime information, the COPKIT project demonstrated the value of bridging the gap between strategic (threat level) analysis and investigative / case-base analysis for LEAs [11]. It seems likely that similar gains can be achieved in the interactions between LEAs and teams in charge of protecting organisations against cyber-attacks outside of LEAs (Security Operation Centre teams).

Entities associated with this document

EU-funded projects:

CC-DRIVER, https://www.ccdriver-h2020.com/
COPKIT, https://copkit.eu
CYBERSPACE, https://cyberspaceproject.eu
HEROES, https://heroes-fct.eu
INSPECTr, https://inspectr-project.eu/
LOCARD, https://locard.eu/
RAYUELA, https://www.rayuela-h2020.eu
ROXANNE, https://roxanne-euproject.org
TRACE, https://trace-illicit-money-flows.eu

Organisations

Trilateral Research, UK
Coventry University, Centre for Financial and Corporate Integrity, UK

---

[1] TRACE Project (H2020 Grant Agreement No. 101022004) https://trace-illicit-money-flows.eu
[2] https://locard.eu/
[3] https://roxanne-euproject.org
[4] Papakonstantinou, Vagelis, "Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?", *Computer Law & Security Review*, Vol. 44, 2022. https://doi.org/10.1016/j.clsr.2022.105653.
[5] Nash, Iain, "Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices", *Computer Law & Security Review*, Vol. 40, 2021. https://doi.org/10.1016/j.clsr.2021.105529.
[6] Dizon, Michael Anthony C., and Peter John Upson, "Laws of encryption: An emerging legal framework", *Computer Law & Security Review*, Vol. 43, 2021. https://doi.org/10.1016/j.clsr.2021.105635.

[7] Markopoulou, Dimitra, Vagelis Papakonstantinou and Paul de Hert, “The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 2019. doi:10.1016/j.clsr.2019.06.007
[8] https://inspectr-project.eu
[9] Casino, Fran, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas and Constantinos Patsakis, “SoK: Cross-border Criminal Investigations and Digital Evidence” [unpublished].
[10] ZiTIS, https://www.zitis.bund.de/DE/Home/home_node.html
[11] Pastor, Raquel, Franck Mignet, Tobias Mattes, Agata Gurzawska, Holger Nitsch and David Wright, “COPKIT: Technology and Knowledge for Early Warning/Early Action-Led Policing in Fighting Organised Crime and Terrorism”, in B. Akhgar, D. Kavallieros and E. Sdongos (eds.), *Technology Development for Security Practitioners*, Cham, Switzerland, 2021, pp. 121–133. https://doi.org/10.1007/978-3-030-69460-9_7
[12] HEROES, https://heroes-fct.eu/