Istituto Affari Internazionali

ISSN 2532-6570

IAI COMMENTARIES 23 | 54 - OCTOBER 2023

Setting the Standard for a Secure Digital Landscape: The Cyber Resilience Act

by Ottavia Credi, Michelangelo Freyrie and Federica Marconi

Electronic hardware has been vulnerable to malign cyber activities since the dawn of digital networks. However, the widespread adoption of the so-called Internet of Things (IoT) has led to a multiplication of cyber vulnerabilities in goods and pieces of infrastructure that were previously considered safe from digital threats.[1] The European Union witnessed this first-hand, with a significant increase in the number of cyberattacks to its hardware and software products in the last few years.[2]

Interconnectedness has been a boon to product efficiency, business opportunities and standard quality. Yet, it has also opened new avenues for malign activity, not only of the criminal kind. There are multiple examples of consumer goods bearing critical vulnerabilities, from webcams to pacemakers.[3] Amidst growing international tensions, such products will likely remain a playing field for state-sponsored and politically minded cyber actors. Since Russia's brutal invasion of Ukraine, the EU has

[1] Elizabeth MacBride, "The Dark Web's Criminal Minds See Internet of Things as Next Big Hacking Prize", in *CNBC*, 9 January 2023, https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html.

[2] Javier Espinoza, "EU to Impose Tough Rules on 'Internet of Things' Product Makers", in *Financial Times*, 7 September 2022, https://www.ft.com/content/cfa2e2be-8871-4b56-b7bf-c5d2c55e8ed5.

[3] Harold Kilpatrick, "5 Infamous IOT Hacks and Vulnerabilities", in *IOTSolutions World Congress*, 3 October 2018, https://www.iotsworldcongress.com/5-infamous-iot-hacks-and-vulnerabilities.

Ottavia Credi was previously a Researcher in the Defence and Security Programmes at the Istituto Affari Internazionali (IAI). Michelangelo Freyrie was previously a Junior Researcher in the Defence and Security Programmes at IAI. Federica Marconi is a Researcher in the Multilateralism and Global Governance Programme at IAI. *The authors would like to thank Paola Tessari (IAI) for her valuable contribution to this commentary. For the fruitful exchange of view, the authors would like to thank Anitec-Assinform, the Italian National Cybersecurity Agency (Agenzia per la cybersicurezza nazionale, ACN) and Microsoft. The views expressed in the commentary are those of the authors' only.*

observed a peak of attacks targeting digital service providers.[4] As a result of the conflict, cyberspace overall has registered an increase in offensive operations such as destructive malware, phishing campaigns and influence operations.

Cyber risks associated with the IoT are current, growing, cogent and critical – especially in the private sector and for small and medium-sized enterprises (SMEs). Recent reports have shown that 87 per cent of the companies affected by ransomware attacks in Europe are SMEs with under 50 employees.

Such companies are becoming progressively more connected; yet, each technological advancement entails an increase in vulnerabilities. Even though one of the main concerns lies with unmanaged devices, also devices that have been diligently managed can pose challenges. This can be because patches for vulnerabilities are simply not available or cannot be implemented, as the product was not designed with security in mind.

The exposure of IoT devices and connected goods has to be contextualised within a broader trend, which sees overall cybersecurity risks becoming endemic. The European Repository of Cyber Incidents reports 1,634 total politically relevant cyber incidents since 2015, with 2023 marking a peak of 486 recorded incidents.[5] Fifty-three per cent of attacks in this timespan were directed against government and political institutions, 39 per cent against critical infrastructures and the others against commercial actors, private citizens, social groups, media and other non-state actors. The political and strategic ramifications of such actions can be far-reaching, as recently exposed by the 2021 attack against Colonial Pipeline in the US, when a hacker group identified as DarkSide hit the infrastructure with ransomware.[6]

A fraught public-private relationship

The international debate has long pointed towards some forms of public-private partnership as the pillar of future cybersecurity governance, recognising the outsized role played by major businesses in shaping the digital commons and the supposed ease with which they could identify and act upon vulnerabilities in their products.[7] Yet,

[4] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, November 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[5] European Repository of Cyber Incidents, *Cyber Incident Dashboard*, last updated on 30 October 2023, https://eurepoc.eu/dashboard.

[6] Sean Michael Kerner, "Colonial Pipeline Hack Explained: Everything You Need to Know", in *Whatls Features*, 26 April 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[7] See, for instance: Kristoffer Kjærgaard Christensen and Karen Lund Petersen, "Public–Private Partnerships on Cyber Security: A Practice of Loyalty", in *International Affairs*, Vol. 93, No. 6 (November 2017), p. 1435-1452, DOI 10.1093/ia/iix189; Raphael Bossong and Ben Wagner, "A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union", in Oldrich Bures and Helena Carrapico (eds), *Security Privatization. How Non-security-related Private Businesses Shape Security Governance*, Cham, Springer, 2018, p. 219-247, DOI 10.1007/978-3-319-63010-6_10; Daniel R. McCarthy, "Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal

ISSN 2532-6570

the divergence of interests between the state and private actors has been identified as a major shortcoming of this model, with organisations often not sufficiently investing in cybersecurity practices.

The proliferation of state-sponsored cyber actors and bustling criminal activity on the one hand, and the reliance on privately owned, operated or produced infrastructures on the other, has led to an intense debate regarding who bears the responsibility for guaranteeing the safety and security of connected products. This discussion is becoming ever more important considering that critical vulnerabilities and zero-day exploits – namely, a vulnerability that is only discovered once exposed – are more and more in the crosshairs of malevolent state-sponsored actors, both as a way to compromise operational technologies and to penetrate networks violating office routers or VPNs.[8]
As a result, the policy debate seems to have decisively moved towards a stronger role of public authorities, both at the national and international levels. In the conclusions on the EU's Cybersecurity Strategy for the Digital Decade, the Council emphasised that cybersecurity is vital for the "functioning of public administration and institutions at both national and EU level and for our society and the economy as a whole".[9] In the US, the director of the Cybersecurity and Infrastructure Security Agency recognised that "For too long, we have sacrificed security for features and speed to market, leaving us increasingly vulnerable, with the burden of security placed on those least able to bear it."[10]

In an attempt to create a positive cooperation between the public and private sectors, the upcoming EU Cyber Resilience Act (CRA), which proposes some new measures specific to product vulnerabilities, can become a landmark for this approach.

The EU's Cyber Resilience Act

The CRA was first announced by European Commission President Ursula von der Leyen in the State of the Union address in September 2021, as part of the EU's toolbox towards a European Cyber Defence Policy.[11] Subsequently, the Council conclusions of May 2022 on the development of the European Union's cyber posture stressed the need for "a horizontal and holistic approach that covers the whole lifecycle of digital products, as well as existing regulation, especially

Political Order", in *Politics and Governance*, Vol. 6, No. 2 (2018), p. 5-12, https://doi.org/10.17645/pag.v6i2.1335.

[8] ENISA, *ENISA Threat Landscape 2022*, cit., p. 22-23; and *ENISA Threat Landscape 2023*, October 2023, p. 22-23, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[9] Council of the European Union, *Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade* (6722/21), 22 March 2021, point 2, https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf.

[10] Jen Easterly and Tom Fanning, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years", in *CISA News*, 7 May 2023, https://www.cisa.gov/node/18129.

[11] European Commission, *2021 State of the Union Address by President von der Leyen*, 15 September 2021, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701.

ISSN 2532-6570

IAI COMMENTARIES 23 | 54 - OCTOBER 2023
ISSN 2532-6570

in the area of cybersecurity".[12] Thus, the Council invited the Commission to propose common and horizontal cybersecurity requirements for all products with digital elements by the end of 2022.

On 15 September 2022, the Commission adopted the proposal for a Regulation aimed at mandating cybersecurity requirements for hardware and software products "with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network".[13] The focus of such requirements would include the products' design, development, production and availability on the market. At the same time, the CRA also complements the EU cybersecurity framework established by the EU Cybersecurity Act (Regulation (EU) 2019/881)[14] and referred to in the Network and Information Security (NIS) Directive 2,[15] which already includes measures to "introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU".[16]

The Council has made several changes to the Commission's CRA proposal, concerning the scope, the support measures for SMEs, the declaration of conformity and the reporting obligations of manufacturers. With regard to the latter, the manufacturers shall notify any actively exploited vulnerability contained in the product and any incident having an impact on the security of the product with digital elements that they become aware of. For example, changes include a shift in the recipients of cybersecurity information, as manufacturers shall notify the designated national Computer Security Incident Response Team (CSIRTs) and not the European Union Agency for Cybersecurity (ENISA), as in the Commission's draft. In addition, a two-step reporting process has been introduced. It involves an initial early warning notification to be made "without undue delay" and in any event within 24 hours of becoming aware of the actively exploited vulnerability or incident impacting the security of the product. The early warning is followed by a second notification within 72 hours, aiming to update the information already provided and indicate any available information about either the

[12] Council of the European Union, *Cyber Posture: Council Approves Conclusions*, 23 May 2022, https://europa.eu/!6VvGNk; and *Council Conclusions on the Development of the European Union's Cyber Posture* (9364/22), 23 May 2022, point 4, https://data.consilium.europa.eu/doc/document/ST-9364-2022-INIT/en/pdf.

[13] European Commission, *Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements...* (COM/2022/454), 15 September 2023, Art. 2(1), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52022PC0454.

[14] European Parliament and Council of the European Union, *Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification... (Cybersecurity Act)*, http://data.europa.eu/eli/reg/2019/881/oj.

[15] European Parliament and Council of the European Union, *Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union...*, http://data.europa.eu/eli/dir/2022/2555/oj.

[16] Maria del Mar Negreiro Achiaga, "The NIS2 Directive: A High Common Level of Cybersecurity in the EU", in *EPRS Briefings*, February 2023, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

status of remediation or any corrective or mitigating measures taken.

The CRA also provides for a sanctions regime for non-compliance with the essential cybersecurity requirements, that may have fundamental implications for those involved. The potential maximum fines for non-compliance could be either from 5 to 15 million euro or from 1 to 2.5 per cent of annual global turnover, whichever is greater.

Given the complexity and sensitivity of the issues at stake, there have been several moments of discussion between EU member states to find a compromise. The representatives of the member states (Coreper) finally reached a consensus on horizontal cybersecurity requirements for products with digital elements on 19 July 2023, allowing the Council to start negotiations with the European Parliament on the final version of the proposed legislation.[17]

A difficult balance

The CRA draft touches upon a diverse set of issues that need to be tackled to modernise and adapt Europe's cybersecurity governance. For the foreseeable future, this will likely remain a multilayered, complex affair which relies on two potentially fractious relationships: that between national cyber authorities and the ENISA, and that between cyber authorities and the private sector.

ENISA acts as an interface between the national and the European level: it promotes and participates in European working groups, it contributes to studies on practices at member state level meant to elaborate common guidelines, and it works to raise awareness on cybersecurity amongst European SMEs. ENISA also endures some undeniable difficulties stemming from its role as an EU organisation. For instance, it faces obstacles in maintaining an operational capacity to investigate and react to threats in real time, especially when political considerations are brought into the equation.

Each member state has its own national position on cyber security and defence. Similarly, different national Computer Security Incident Response Teams (CSRITs) have different approaches in dealing with cyber vulnerabilities and responding to emergencies. Their respective approaches largely depend on their internal security culture, both in terms of human resources and organisational habits.

The third protagonist to be factored in is, as mentioned, the private sector. The European information and communication technologies (ICT) industry does not seem to be inherently opposed to the CRA, but requires certain conditions to be met.

The CRA mandates that all manufacturers have resources and procedures in place to mitigate

[17] See the steps of Procedure 2022/0272/COD: https://eur-lex.europa.eu/procedure/EN/2022_272; and European Parliament, *Legislative Train Schedule: Horizontal Cybersecurity Requirements for Products with Digital Elements*, as of 20 October 2023, https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act.

IAI COMMENTARIES 23 | 54 - OCTOBER 2023
ISSN 2532-6570

vulnerabilities in products with digital elements and to ensure that vulnerabilities in their products can be addressed through security updates. Article 11 in particular sets a series of requirements that manufacturers have to comply with concerning the reporting of exploited vulnerabilities to the competent authority.[18] Such a development should significantly improve the cybersecurity of products placed on the market in the EU and elsewhere. At the same time, increasing the responsibility of manufacturers by obliging them to provide security support and software updates to address identified vulnerabilities may "undermine the security of digital products and the individuals who use them".[19]

Yet, the CRA is horizontal to almost all sectors of the economy: every product, device or software application that contemplates connection to a network falls within the scope of the Act. It affects industry sectors that are less accustomed to the digital sphere and which will have to go through a number of procedures for the certification of conformity of their products. As a consequence, the wider industrial sector is asking for some time to adapt and get acquainted with the legislation and its implications.

An additional argument put forward by the industrial players concerns the security of information. By sharing details on their products' cyber vulnerabilities, they worry they would unintendedly be feeding malevolent actors with information on ways to exploit such vulnerabilities. Moreover, whilst sharing information about significant cybersecurity incidents is deemed crucial to support collective defence actions, exchanging data about unpatched vulnerabilities before effective countermeasures are available can divert the attention of responders, as becoming aware of the presence of a vulnerability may compel those concerned with user protection to take hasty action rather than trying to identify the root cause of the incident and elaborate a structured response.

Looking forward

The adoption of the CRA represents a significant milestone in the EU's journey towards becoming a global leader in setting cybersecurity standards. Over the years, the cumulative effect of past initiatives at both EU and national levels had resulted in a somewhat fragmented legislative landscape within the internal market, underscoring the necessity for a comprehensive and global perspective. Legal developments such as the drafting of the CRA aim to standardise cybersecurity practices and certifications across the EU, thereby contributing to a more harmonised and robust cybersecurity landscape. Such legal efforts, however, must be complemented by other actions in order to achieve comprehensive digital security.

[18] To read the text of Art. 11, see European Commission, *Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements*, cit.

[19] Tony Anscombe et al., *Joint Letter of Experts on CRA and Vulnerability Disclosure*, 3 October 2023, https://www.centerforcybersecuritypolicy.org/insights-and-research/joint-letter-of-experts-on-cra-and-vulnerability-disclosure.

IAI COMMENTARIES 23 | 54 - OCTOBER 2023
ISSN 2532-6570

As known, cooperation and information sharing are key in order to prevent threats, also in the cyber domain. The adoption of a standardised vocabulary for threat intelligence – that is, evidence-based knowledge about existing cyberattacks or emerging cyber threats – would facilitate the sharing of threat intelligence both internally and externally, and both between public and private entities.[20]

As the virtual landscape exposed to cyber risks continues to expand, it is crucial to promote a corresponding increase in cyber awareness. A positive step in this direction is demonstrated by an increasing focus on coordination and information sharing by public and private actors working in cyber defence, as also stipulated by the CRA.

Furthermore, these efforts must be accompanied by a broader cultural shift. It will be important to promote an action of cultural mentoring to facilitate the transition of private companies, and especially SMEs, to the digital realm, ensuring that they not only meet compliance requirements but also become proactive contributors to the broader cybersecurity ecosystem.

By combining regulatory measures, threat intelligence standardisation, enhanced cyber awareness and a cultural mentoring approach, the EU is better positioned to fortify its cybersecurity posture and foster a more resilient digital landscape.

[20] Boning Feng, "Threat Intelligence Sharing: What Kind of Intelligence to Share?", in *Concordia Blog*, 20 August 2021, https://www.concordia-h2020.eu/?p=5655.

IAI COMMENTARIES 23 | 54 - OCTOBER 2023
ISSN 2532-6570

Istituto Affari Internazionali (IAI)
The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Global Politics and Security* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
Tel. +39 066976831
iai@iai.it
www.iai.it

Latest IAI COMMENTARIES

Editor: Leo Goretti (l.goretti@iai.it)

ISSN 2532-6570