Computer Law & Security Review xxx (xxxx) xxx

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Editorial

A cybersecurity strategy fit for purpose? Introducing the special issue on EU cybersecurity: Collective resilience through regulation

In 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the 'EU's Cybersecurity Strategy for the Digital Decade'.[1] The strategy contains proposals for regulatory, investment, and policy initiatives in three areas of EU action:

1. Resilience, technological sovereignty, and leadership
2. Building operational capacity to prevent, deter, and respond; and
3. Advancing a global and open cyberspace through increased cooperation.

This Special Issue, which is the product of a conference held on 22 June 2023 in Brussels, co-organized by Radboud University, Tilburg University, and Maastricht University,[2] reflects on the strategy from legal and technical perspectives. It consists of thirteen engaging papers.

The conference was inspired by the need to take stock of progress to date on the EU Cybersecurity Strategy. The strategy promised to bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. Furthermore, it intended to enable the EU to lead international norm and standard setting initiatives and to strengthen cooperation around the world to "promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values". The EU Cybersecurity Strategy also announced changes in the regulatory landscape in the field of cybersecurity: the revision of the Network and Information Security Directive, which is now adopted (NIS2),[3] as well as horizontal rules for connected products, namely the EU Cyber Resilience Act (CRA).[4] The strategy emphasized the need for upscaling operational capacity and skills development in Europe, while it also positioned the EU in the international landscape as regards initiatives such as the cross-border exchange of electronic evidence with the 2nd Additional Protocol to the Council of Europe Cybercrime Convention.

The conference brought together academics, policymakers, and practitioners with different specializations to discuss the merits and shortcomings of the strategy as well as features of its ongoing implementation. The discussions at the Brussels conference, much like the papers that form this Special Issue, evaluated whether the strategy is succeeding in its original goals, but also whether it is still fit for purpose in an ever evolving and increasingly complex digital society. In this introduction, we summarize the papers comprising the resulting Special Issue.

Bygrave [3], in his contribution, lays out how EU cybersecurity law has developed over time. He points to the explosion of legislation, from three legislative instruments in the 1990s to over twenty in the 2000s, particularly in the last decade, not including standards, guidelines, and (other) soft law instruments. Bygrave typifies EU cybersecurity as more of a jungle of regulatory instruments than a well-kept forest. He explores why EU cybersecurity law has expanded as it did, identifying three main drivers:

1. Lemons: describing the bitter taste of working on cybersecurity because the Internet was not being built with security in mind as well as the lack of economic incentives for up-front investments in cybersecurity, also because of initially weak legal incentives;
2. Angst: resulting from digital infrastructures becoming more vital and security breaches more frequent, and;
3. Turf: denoting the desire for greater control with EU institutions and EU Member States claiming sovereignty.

Mirzaei and De Busser's [8] contribution picks up on a lemon: the alleged fragmentation of the Dutch cybersecurity landscape. To determine whether and to what extent there is actual fragmentation, the authors investigate how cybersecurity governance is organized and which organizations are involved in the various aspects and phases of cybersecurity policies. Based on theories on fragmentation, and distinguishing between vertical fragmentation (the number of layers or levels in a government, with different responsibilities and powers) and horizontal fragmentation (organizations at the same level operating at similar levels of authority or responsibility), Mirzaei and De Busser find

[1] European Commission, Joint Communication to the European Parliament and the Council, 'The EU's Cybersecurity Strategy for the Digital Decade', JOIN(2020) 18 final.

[2] The conference was supported by the sectorplan Digital Legal Studies, an interuniversity research initiative on law and digital technologies. https://www.sectorplandls.nl/wordpress/ (accessed 19 November 2024).

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022.

[4] The Cyber Resilience Act was recently adopted by the Council: https://www.nldigitalgovernment.nl/news/european-council-approves-cyber-resilience-act-cra/ (accessed 19 November 2024).

https://doi.org/10.1016/j.clsr.2024.106104

support for a fragmented cybersecurity landscape in the Netherlands and call for additional research on whether fragmentation impacts organizations (negatively or positively).

Miadzvetskaya's [7] contribution addresses another lemon. She dives deeper into the sanction regime, specifically the emergence of administrative measures compared to crime-based sanctions. Discussing trends in EU sanctions vis-à-vis cyberattacks, Miadzvetskaya finds a trend toward individualization of sanctions. This explains the increased popularity of administrative sanctions, although the boundary can be blurry. She analyzes the different purposes these sanctions serve. Compared to criminal measures, administrative measures are often fast responses that require minimal evidence and are considered suitable for addressing cyber-attacks such as hacking and unlawful interception. Miadzvetskaya draws comparisons to the US, where administrative measures and criminal charges are often imposed together, unlike in the EU.

Sanctions can also emerge from non-compliance with the Corporate Sustainability Reporting Directive (CSRD). This Directive, adopted in 2022, has introduced more non-financial disclosure obligations through the European Sustainability Reporting Standards (ESRS), including in ESRS 4, which deals with obligations regarding data breaches. Boggini [2] analyzes the CSRD and its reporting obligations, focusing on the extent to which the General Data Protection Regulation (GDPR) and NIS2 improve the disclosure of cybersecurity information in risk disclosure reports of listed companies. Boggini finds that the existing EU cybersecurity regulation improves the reporting of cybersecurity-related matters and activities in companies' sustainability reports. Her contribution discusses in detail which provisions have this effect.

Turf wars can, in turn, be observed in Serini's [10] contribution on the organization and procedures regarding information exchange to counter cyber threats. He departs from the observation that the EU lacks collective situational awareness concerning cyber threats due to the private sector's lack of involvement in information-sharing practices and Member States' unwillingness to share information. In his contribution, Serini analyzes the reporting entities and the tools and processes they have available, focusing on the gap between political desires for more and better cybersecurity information sharing on the one hand, and the legal obligations and instruments on the other. Serini finds that despite institutions, partnerships, legislation, and technical remedies, a joint decision-making process is lacking due to the freedoms of the EU, including the free flow of information, that Member States can and do invoke.

Tridgell [13] examines the EU's use of 'digital sovereignty' as a core principle in its Cybersecurity Strategy, particularly in the context of open-source software. She critiques the tension between open-source software's open nature and the control prioritized in digital sovereignty's closed rhetoric. Tridgell discusses the aspect of open-source software's being a foundation for the global digital infrastructure on the one hand and its vulnerability to cybersecurity threats on the other. After analyzing the Cyber Resilience Act, she identifies a trend towards regulatory control through initiatives such as a stewardship role for open-source software entities. Additionally, she raises questions about their compatibility with open-source software's underlying philosophy. Tridgell argues that the EU seems to be adopting an open-source software cybersecurity approach that avoids strict controls on open-source software and promotes an open-source software culture within the EU while exploring global or bilateral collaboration.

Turf wars relate not only to whether the EU or Member States should have competence over which matter or issue, but also to whether rule-making and compliance should be left to technical standards. Rampášek, Mesarčík, and Andraško [9] discuss whether the adoption of conformity assessment and certification for both AI systems and AI products and services would improve cybersecurity. They reflect on whether the EU's regulatory approach, including the Cyber Resilience Act, NIS2 Directive, and AI Act, risks creating burdensome or outdated requirements and argue that a certification framework can better adapt to AI systems' rapid technological advancement as opposed to regulation. Their work complements the other contributions in the Special Issue by addressing AI's challenges and potential within cybersecurity in the EU.

Jacobs [5], focusing on information security, touches on the topic of angst. Misinformation or disinformation, such as fake news and, more recently, AI-generated (i.e. synthetic) content and deep fakes, have been at the center of scientific, societal, and political debates. Detecting and combatting mis-/disinformation has proven increasingly challenging. In his contribution, Jacobs approaches mis-/disinformation from an authenticity angle: he explores how digital signatures in particular could be used to combat mis-/disinformation. Jacobs distinguishes in this respect between source-authenticity (having certainty about the message's source) and message-authenticity (having certainty about the message's integrity). His paper offers a way forward on further embedding digital signatures in regulation to ensure authenticity.

Toftegaard, Grøtterud, and Hämmerli's [12] contribution addresses angst that has become more prominent, namely attacks on and disruptions of cross-border power grids, which are managed through Operational Technology (as opposed to Information Technology). The authors investigate whether Operational Technology is covered by current legislative instruments, particularly the (draft) delegated act on cybersecurity for the European power sector. They find that the delegated act does not, or limitedly, address Operational Technology, and assert that this will leave the sector vulnerable to attacks. Their analysis reveals that the lack of rules likely stems from a stronger position of Information Technology communities than of Operational Technology communities. In their paper, the authors propose three measures to increase Operational Technology resilience.

In his contribution, Shaffique [11] analyzes the cybersecurity challenges stemming from Internet of Things (IoT) devices from the perspective of the Cyber Resilience Act (CRA). After describing IoT cybersecurity challenges and the EU cybersecurity framework, Shaffique identifies areas where the CRA is expected to be effective, such as encryption, security during updates, and user awareness, as well as areas where it may be less effective, such as in security during manufacturing, identification and authentication, and the challenges associated with IoT's large attack surface. He offers several ways in which the CRA could provide more legal certainty and, hence, improvements to address the cybersecurity challenges emerging from the proliferation of IoT devices.

The IoT inspires Chiara [4] to explore the need for a new fundamental right to cybersecurity in EU law, the content of such a right, and how it may be implemented. The convergence of our digital and physical realities, or at least their increasing connectedness, could give rise to such a right. Chiara draws inspiration from the European Declaration on Digital Rights and Principles for the Digital Decade to define the right, in particular its 16th principle, which results in the fundamental right for individuals to enjoy a secure digital life, protecting individuals in their digital activities. The competence the EU would gain from enacting such a right could also offer the potential for addressing or resolving challenges identified by other contributors to this Special Issue, such as the lack of information exchange.

Boeken [1], instead of addressing the adoption of new rights, legislation, or standards, focuses on the actors involved. With legislators having difficulties keeping up with the pace of technological developments, she explores a different route than through legislation: stakeholder theory. Boeken advocates for a stakeholder model with shared responsibility by governments and companies and with care ethics at its core, which requires moving from conventional risk assessments to incorporating ethical values by shifting part of the responsibility for achieving cybersecurity from governments to companies.

In his contribution, Kun [6] similarly does not introduce new rights. Instead, he addresses the issue of the legal basis for processing personal data in relation to cybersecurity measures taken under the NIS2 Directive. Operators of Essential Services like energy, transportation, and banking, and Digital Service Providers have a variety of cybersecurity

responsibilities under the NIS2 Directive that may involve personal data processing, such as processing IP addresses and log data. From the four potential legal grounds of Article 6 of the GDPR (consent, legal obligation, public interest, legitimate interest), he concludes that legal obligation and legitimate interest seem to be the most suitable grounds for processing personal data. Non-special and special categories are discussed, as well as automated decision-making. Kun illustrates his analysis with the example of insider threat detection technologies.

From examining regulatory proliferation and fragmentation to proposing new frameworks for stakeholder responsibility and digital rights, the contributions in this Special Issue show how the EU's cybersecurity initiatives are shaping and are shaped by legal, technical, and ethical challenges. By analyzing issues such as authenticity, operational technology vulnerabilities, and the evolution of sanctions, this Special Issue provides insights into how the strategy's objectives are being realized and where further development is needed or desirable. We invite readers to explore these contributions and to join the ongoing dialogue on the future of cybersecurity in Europe.

References

[1] Boeken J. From compliance to security, responsibility beyond law. Comput Law Security Rev. 2024;52:105926.
[2] Boggini C. Reporting cybersecurity to stakeholders: a review of CSRD and the EU cyber legal framework. Comput Law Security Rev. 2024;53:105987.
[3] Bygrave LA. The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. Comput Law Security Rev. 2025;56:106071.
[4] Chiara PG. Towards a right to cybersecurity in EU law? The challenges ahead. Comput Law Security Rev. 2024;53:105961.
[5] Jacobs B. The authenticity crisis. Comput Law Security Rev. 2024;53:105962.
[6] Kun E. Searching for the appropriate legal basis for personal data processing for cybersecurity purposes under the NIS 2 directive: legal obligation and/or legitimate interest? Comput Law Secur Rev 2025;56:106098.
[7] Miadzvetskaya Y. EU sanctions in response to cyber-attacks as crime-based emergency measures. Comput Law Secur Rev. 2024;54:106010.
[8] Mirzaei P, De Busser E. The new F-word: The case of fragmentation in Dutch cybersecurity governance. Comput Law Secur Rev 2024;55:106032.
[9] Rampášek M, Mesarčík M, Andraško J. Evolving cybersecurity of AI-featured digital products and services: rise of standardisation and certification? Comput Law Secur Rev 2025;56:106093.
[10] Serini F. Collective cyber situational awareness in EU. A political project of difficult legal realisation? Comput Law Secur Rev 2024;55:106055.
[11] Shaffique MR. Cyber Resilience Act 2022: a silver bullet for cybersecurity of IoT devices or a shot in the dark? Comput Law Secur Rev 2024;54:106009.
[12] Toftegaard Ø, Grøtterud G, Hämmerli B. Operational Technology resilience in the 2023 draft delegated act on cybersecurity for the power sector—An EU policy process analysis. Comput Law Secur Rev 2024;54:106034.
[13] Tridgell J. Open or closing doors? The influence of 'digital sovereignty' in the EU's Cybersecurity Strategy on cybersecurity of open-source software. Comput Law Secur Rev 2025;56:106078.

Gijs van Dijck[a], Irene Kamara[b], Aaron Martin[c], Aurelia Tamò-Larrieux[d], Pieter Wolters[e,*]

[a] *Maastricht University, the Netherlands*
[b] *Tilburg University, the Netherlands*
[c] *University of Virginia, United States*
[d] *University of Lausanne, Switzerland*
[e] *Radboud University, the Netherlands*

[*] Corresponding author
E-mail address: pieter.wolters@ru.nl (P. Wolters).