Defining security by design: a stakeholder's perspective

Real, C. del; Busser, E. de

2023 Report Cyber Security by Integrated Design

DEFINING SECURITY BY DESIGN

A STAKEHOLDER'S PERSPECTIVE

Cristina Del-Real and Els De Busser

Project C-SIDE
Cyber Security by Integrated Design

Universiteit Leiden

This report is part of the project “Cyber Security by Integrated Design” (C-SIDE) funded by NWO (the Dutch Research Council) and is part of the Dutch Research Agenda 2018: Cyber security – towards a secure and reliable digital domain

Universiteit Leiden
The Netherlands

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

SURF

LUMC Leiden University Medical Center

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Suggested citation:
Del-Real, C., and De Busser. (2023). *Defining security by design: A stakeholders perspective*. Cyber Security by Integrated Design. December 2023.

Introduction

SbD is an approach that originated at the end of the 20th century to describe the practice of considering security already in the design of technology rather than at a later stage of the development process. SbD, born out of the recognition that digital harm stems from software design and coding errors, strives to instil a proactive mindset among developers. Since then, many companies have adopted the SbD approach, and have generated their own solutions based on it. For example, the Microsoft's Security Development Lifecycle (SDL) is a technology design methodology that contains twelve practices aiming to improve the security of their products.

While SbD presents a promising avenue for curbing the frequency and impact of cybersecurity incidents, it predominantly addresses technical aspects. The traditional pitfall shadowing SbD lies in assuming that once a system or application is technically secure in its design, its operations and user interactions should unfold seamlessly. Invariably, when a system encounters glitches, the blame often centres on the technical setup. Yet, this perspective overlooks three critical dimensions of contemporary cybersecurity:

(1) Expansion of the concept of cybersecurity

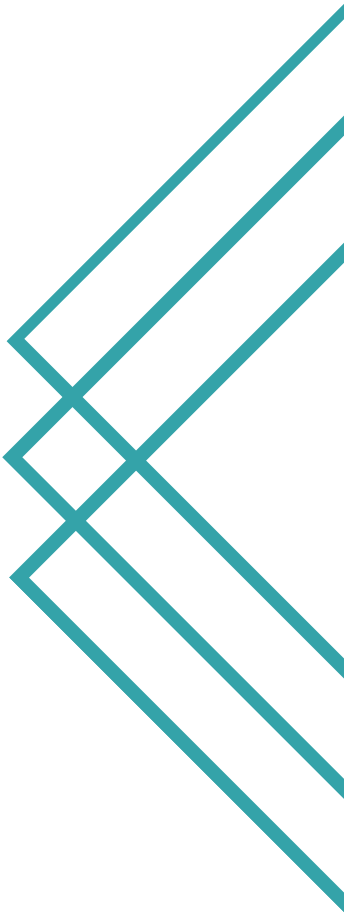
Since Fernando "Corby" Corbató pioneered the Compatible Time-Sharing System (CTSS) in 1961, the focus of computer systems security has been the protection of data (Shapiro 2023). Hence, SbD has traditionally sought to safeguard data confidentiality, integrity, and availability (Del-Real, De Busser, and van den Berg 2023). However, the complexity of security within cyberspace is escalating. Modern cyber incidents encompass technological, human, political, and organisational dimensions (Dunn Cavelty and Wenger 2020), blurring the lines between discrete components and deliberate or inadvertent actions (van den Berg, Hutten, and Prins 2021). This complexity necessitates a re-evaluation of security definitions, including SbD, to extend its relevance and scope.

(2) Influence of human factors

Digital technologies are not standalone entities; user behaviour significantly influences and shapes their performance. In turn, the way we design technology and virtual spaces can sway users towards either secure or malicious behaviour (van Steen and De Busser 2021; Bawazir et al. 2016; Moneva and Caneppele 2020; CNIL 2019). The impact of human behaviour on the use of digital technology is becoming increasingly significant with the proliferation of cyber-physical systems, virtual reality, and augmented reality. As digital technologies become more embedded in people's lives, it becomes progressively more challenging to comprehend one without the other. Therefore, the design of technology must consider its interaction with humans.

(3) Evolution of cyber rights

Gone are the days when the security of information systems and networks was safeguarded solely to guarantee the functioning of the European Union Single Market. With the burgeoning domain of cybersecurity and the subsequent recognition of the individual as its nexus, scholarly discourse is evolving to advocate for the development of digital rights (Papakonstantinou 2022). These rights aim to shield individuals—and the things they hold dear—within the digital realm. While the maturation of digital rights is an ongoing journey, noteworthy strides have been made, exemplified by initiatives such as the Cyber Resilience Act, which mandates the creation of secure digital technologies; the NIS2 Directive, which seeks to bolster the cybersecurity of services; and the European Declaration on Digital Rights and Principles for the Digital Decade. Additionally, national movements, such as Spain's establishment of the "right to cybersecurity,"[1] underscore this progression. Thus, the fortification of digital technology's security must now embrace a paradigm shift towards humanistic digitisation, anchoring its focus on the protection of digital life.



[1] Included in the Charter of Digital Rights, Section I "Rights to Freedom," Article 6, "Right to cybersecurity," according to which "*1. Pursuant to law, every person has the right for the digital information systems they use for their personal, professional or social activities, or which process their data or provide services to them, to have the appropriate security measures to guarantee the integrity, confidentiality, availability, resilience and authenticity of the information processed and the availability of the services provided. 2. The public authorities, pursuant to European and national regulations, shall ensure compliance with the guarantees expressed in the above number by all information systems, whether publicly- or privately-owned, in proportion to the risks to which they are exposed. To this end, they may seek the collaboration of civil society. 3. The public authorities shall promote awareness and training in cybersecurity for society as a whole, and shall foster certification mechanisms.*"

Taking these dimensions into consideration, the Dutch Research Council (*Nederlandse Organisatie voor Wetenschappelijk Onderzoek*, NWO) funded the project "Cyber Security by Integrated Design" (C-SIDE) as part of the Dutch "Research Agenda 2018: Cyber security – towards a secure and reliable digital domain" to explore the integration of technical and non-technical views in secure software system design.

Our interdisciplinary approach: the C-SIDE project

The C-SIDE project aims to build a comprehensive tool to help software developers integrate all relevant angles related to legal, policy, governance, organisational, behavioural and technical views in software system security design. To this aim, we are currently working on five pillars:

1. **Expanding the concept of security by design**: The first pillar of C-SIDE involves expanding the concept of SbD to incorporate relevant aspects of both public and private governance, as well as human factors, into the design of secure software systems. Beyond the notions of 'usable security' and 'compliance,' the project aims to promote an approach to SbD that considers human behaviour and aligns with organizational practices and public policy trends.
2. **Improving code scanning and analysis techniques**: The second pillar aims to investigate and further improve state-of-the-art code analysis tools and techniques, with a focus on studying the integration of DevSecOps and code scanning techniques in open-source projects, investigating methodologies to reduce the number of reported false positives in scans of large source code repositories and researching advanced code scanning techniques for black box environments in which the source code is not(fully) available.
3. **Enhancing security metrics**: The third pillar aims to introduce a comprehensive framework to measure the security of software systems. The goal is to enhance the existing measurement approaches, which tend to focus solely on security metrics, by integrating critical human insights – i.e., the mental models of secure software development experts. By intertwining metrics and human perception, the third pillar strives to overcome the hurdles of software security measurement that have long been considered a very hard, unsolvable problem.

4. **Developing an ethical cybersecurity strategy:** The fourth pillar of C-SIDE involves the development of an ethical cybersecurity strategy for private organizations. Such ethical cybersecurity must include a holistic perspective on SbD which includes the social and organizational aspects of technology. The pillar aims to combine stakeholder theory with the ethics of care to provide companies with the tools they need for an ethical cybersecurity strategy that includes SbD.
5. **Assessing the Dutch central cybersecurity governance structure:** The fifth pillar zooms in on the institutional architecture of the Dutch central government to find out how cybersecurity governance is organised within the central government, and whether it is fragmented. It focuses on the organisations that are concerned with the creation, implementation and oversight of cybersecurity policies vis à vis Dutch society, and looks into the possible implications of fragmentation on the creation, implementation and oversight of cybersecurity policies in the Netherlands.

The glue binding all the pillars together is an interdisciplinary view of the SbD concept. As part of our validation, the C-SIDE project foreseen to hold several stakeholder meetings to receive feedback and validate the conceptual revision of SbD. This report discusses the definition of *security by design* (SbD) from the perspective of stakeholders.

Revisiting *security by design*

This report presents the results of a workshop held in Leiden (the Netherlands) in November 2023 with 10 experts in software development discussing the concept of SbD. The experts were members of public and private organizations working in the Netherlands. The workshop was held under the Chatham House Rule. The workshop was organised in three exercises: (1) critical analysis of the current definition of SbD, (2) assessment of statements to foster a revision of the SbD concept, and (3) proposal of an updated definition of SbD.

In the initial exercise, we engaged stakeholders with a definition derived from our systematic literature review (Del-Real, De Busser, and van den Berg 2023):

Security by design

...is an engineering approach that aims to protect software systems, privacy, and identity from vulnerabilities, attacks, breaches, and threats. It involves considering security, defined as the confidentiality, integrity, and availability of information and information systems, in the early stages of the lifecycle and embedding it into software, architecture design, systems, and products by developers.

We prompted stakeholders to evaluate the definition's accuracy regarding actual SbD practices and identify any deficiencies or inaccuracies. The stakeholders suggested four minor amendments: (1) the initial segment should encompass data protection, deemed critical in SbD, (2) SbD should address the broader spectrum of digital technologies and infrastructure, not just software, (3) the sequence "architecture design, software, systems, and products" is preferred over the original order, and (4) the inclusion of the wider stakeholder community in SbD, not solely developers.

Furthermore, stakeholders expressed a significant reservation: they contested the characterisation of SbD as solely an engineering approach. They argued that SbD transcends an engineering approach or procedure, representing instead a paradigm shift. It ought to be perceived as a holistic ecosystem encompassing diverse stakeholders, organisational practices, supportive leadership, and policies, thereby necessitating the adoption of a security culture throughout the entire system producing digital technologies.

A significant point of contention among the stakeholders was the scope of 'security' within the SbD definition. In principle, they agree with the definition of security being defined as the confidentiality, integrity and availability of information. While there was consensus on the traditional definition of security—encompassing the confidentiality, integrity, and availability (CIA) of information—the discussion took a turn when presented with reports of sexual assault in the metaverse (see Diaz 2022).

This prompted a debate on whether SbD should extend beyond the protection of technology to include safeguarding individuals. Views were split: some advocated for an expanded remit of SbD to cover personal safety, arguing that while the focus has been on technological safeguards, the purview should also encompass user protection. Others maintained that SbD should remain focused on the CIA triad, positing that end-user protection falls under 'physical safety' rather than 'security', and that software developers should not bear this responsibility. Furthermore, they contended that an overly broad definition of security could muddle developers' understanding of their design objectives.

Assessing SbD propositions

Following the discussion on the prevailing definition of SbD, we presented the stakeholders with 34 propositions that might characterise SbD. The stakeholders were asked to identify which statements authentically reflected SbD practice, and which, while not currently representative, were deemed desirable. Figure 1 charts the stakeholders' responses.

It is apparent that there was a consensus among stakeholders that SbD pertains to security measures in software system design. Its objective is to reduce vulnerabilities, safeguard corporate assets, uphold the confidentiality, integrity, and availability of information systems, protect personal data and computer systems, embed security into the foundational architectural design of software, and involve a suite of engineering practices—indicated by the endorsement of more than eight stakeholders.

Other propositions receiving moderate support suggested that SbD involves designing security controls, falls within the purview of software developers, starts prior to the software development lifecycle, and seeks to mitigate data breaches, incidents, defects, flaws, and misconfigurations, as well as to shield privacy.

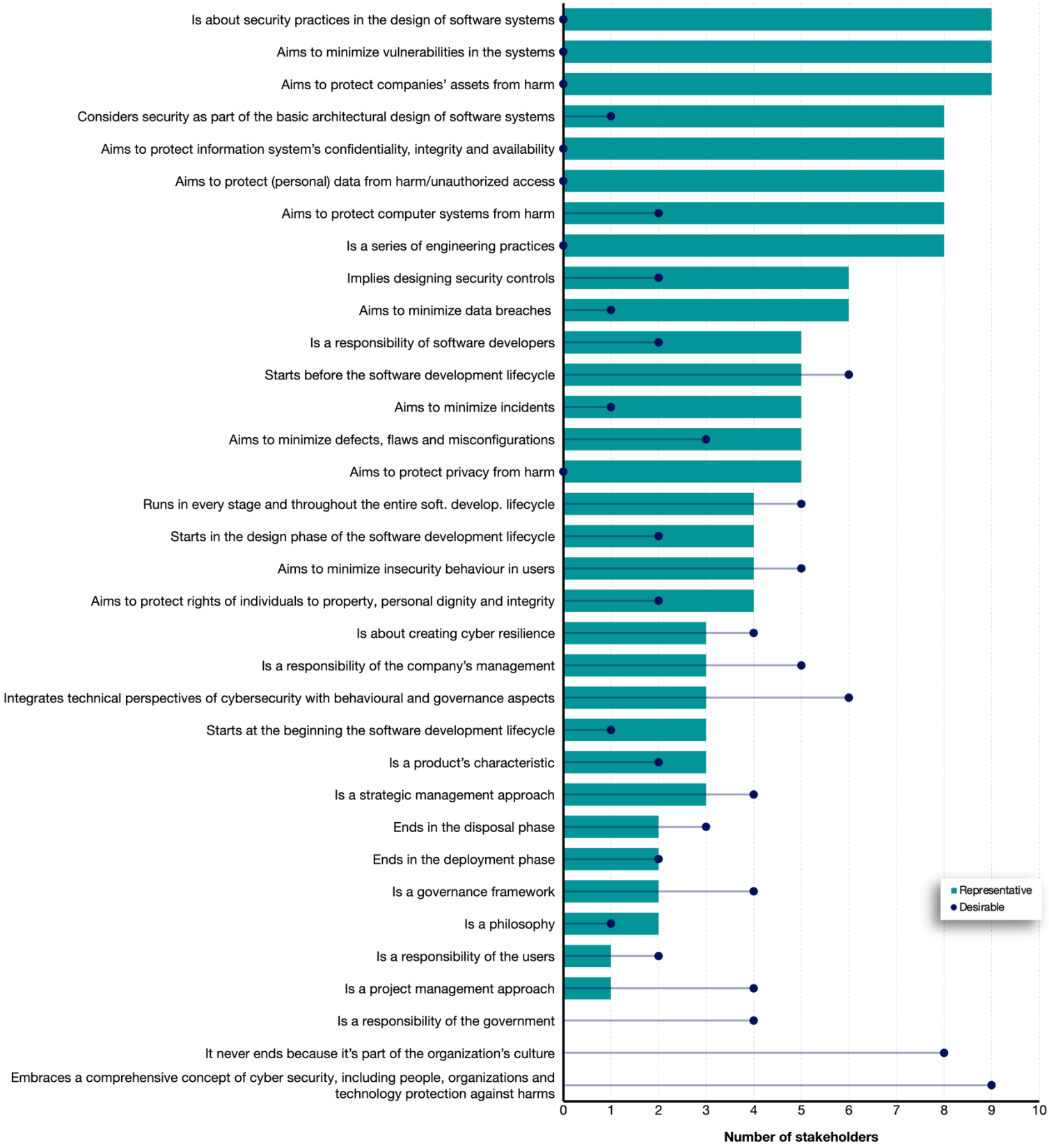


Figure 1. List of propositions and the corresponding number of stakeholders who deemed each to be indicative of current SbD practices (bars) or not indicative but nevertheless desirable (dots). Note: some stakeholders marked some propositions as both representative and desirable. One stakeholder did not facilitate their response (N = 9).

Conversely, certain statements did not resonate with the stakeholders' understanding of current SbD practices. These included the notion that SbD encloses an all-encompassing approach to cybersecurity, covering protection for people, organizations, and technology; that SbD is perpetual as it is ingrained in organizational culture; or that it concludes at the deployment and disposal stages. Additionally, stakeholders did not concur that SbD is a responsibility of governments and users, a project management methodology, a philosophy, a governance framework, a strategic management approach, a product attribute, or that it integrates the technical, behavioural, and governance dimensions of cybersecurity. Lastly, there was no consensus that SbD is about cultivating cyber resilience.

Concerning the propositions that, while not representative of current SbD practices, are nonetheless regarded as desirable by stakeholders, four received the backing of over half of the participants. The most favoured proposition was that SbD should encompass a holistic approach to cybersecurity, prioritising the safeguarding of individuals, organisations, and technology from harm. This was closely followed by the view that SbD should be an intrinsic part of an organisation's culture. The other two supported propositions relate to the belief that SbD should start prior to the software development lifecycle and that it should integrate technical, behavioural, and governance perspectives within cybersecurity.

A revealing part of this exercise was where the perceived desirability of a proposition exceeded the representative nature of it in the current SbD practices, indicating a gap between the normative view of SbD and the positive or descriptive view of SbD. This gap surfaced in four areas:

1. **The phase of the lifecycle or precise timing of SbD in the development process**: the largest gap emerged for the proposition that SbD never ends because it is part of an organization's culture. According to the participants, this is how SbD should be practiced but that is not yet the case.
2. **The purpose of SbD**: calling SbD a project management approach resulted in a relatively wide discrepancy between the current practice and the desired practice.
3. **Who bears the responsibility for SbD**: the participants' opinions slightly diverged on whether SbD is the responsibility of the company or the user. The clearest gap was shown in the proposition that SbD is a responsibility of the government. None of the participants indicated this as a current practice whereas 4 referred to it as a desirable practice.
4. **The content of SbD**: the clearest result showing the widest gap between descriptive and normative view was on the proposition for SbD embracing a comprehensive concept of cybersecurity, including people, organizations and technology protection against harm.

The gaps described here demonstrate a need for SbD practices to catch up with what its normative meaning should be. This is a further indication of the aforementioned paradigm shift towards a wider understanding of SbD than is currently used.

During the dialogue with stakeholders, they articulated three further insights:

1. Security is ideally integrated at the onset of development; however, it frequently becomes a subsidiary consideration. Companies often over-rely on penetration testing, which comes too late to revise core aspects of the design.
2. It was also highlighted that the design process should not be perceived as linear, but rather as cyclical and iterative. Consequently, setting definitive start and end points for SbD is less crucial than consistently embedding security considerations from the outset.
3. Lastly, the stakeholders expressed concerns about the employee's ability to keep pace with rapid technological advances, which poses challenges to enhancing security within software design.

Redefining SbD

In the final exercise, stakeholders were invited to articulate their own definitions of SbD. The ensuing definitions reveal a spectrum of perspectives.

When analysing the definitions, a preference emerges to expand the definition of SbD on two levels: the focal point of SbD as an approach and the phase(s) in the development lifecycle.

First, even though participants disagreed on the precise focal point, it became clear that framing SbD as a purely engineering approach is no longer sufficient. Opinions ranged from a management approach and development approach to a systems approach. Others wished to include attention to people or the culture of an organization. A minority of participants maintained a traditional stance, framing security as the safeguarding of confidentiality, integrity, and availability of information and systems.

Second, a recurring theme across the definitions was the sustained integration of security throughout the product and service development lifecycle. Rather than pointing towards a specific spot for security at a particular stage in the lifecycle, participants prefer to embed the concept of security throughout the whole process. This view corresponds with the notion that SbD is an integrated and continuous practice in the development of technology.

Conclusion

Security by design is a multifaceted and evolving concept. Through our discussions with stakeholders, this report revised and expanded the traditional definition of SbD, advocating for a more holistic approach that transcends technical dimensions to include human, organizational, and cultural factors. This approach to SbD aligns with the broader recognition that cybersecurity is no longer a technical issue, but a complex ecosystem that involves a variety of stakeholders and influences.

This report suggests that SbD should be proactive and integrated, considering security at every stage of development and design, rather than as an afterthought. The iterative and non-linear nature of design, the ongoing challenge of aligning employee skills with the pace of technological development, and the imperative to integrate security as a default in all processes were highlighted as critical considerations for the future of SbD.

SbD should embrace not only the protection of data and systems but also the safeguarding of individuals and organizations, recognizing the human element as central to cybersecurity. This human-centric shift is reflective of the broader societal move towards recognizing the importance of digital rights and the protection of civil liberties within cyberspace. The insights from this workshop will significantly contribute to the ongoing development of the C-SIDE project, as it will contribute to redefining SbD to make it adaptable and inclusive of the rapidly changing digital landscape.

References

- Bawazir, Mohammed Abdullah, Murni Mahmud, Nurul Nuha Abdul Molok, and Jamaludin Ibrahim. 2016. 'Persuasive Technology for Improving Information Security Awareness and Behavior: Literature Review'. In *2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, 228–33. Jakarta, Indonesia: IEEE.
- Berg, Bibi van den, Pauline Hutten, and Ruth Prins. 2021. 'Security and Safety: An Integrative Perspective'. In *International Security Management: New Solutions to Complexity*, edited by Gabriele Jacobs, Iliona Suojanen, Kate E. Horton, and Petra Saskia Bayerl, 13–27. Advanced Sciences and Technologies for Security Applications. Cham, Switzerland: Springer.
- CNIL. 2019. 'Commission Nationale de L'Informatique et Des Libertés. Protéger Les Données Personnelles, Accompagner l'innovation, Préserver Les Libertés Individuelles'. Rapport d'activité. Paris: Commission Nationale de l'Informatique et des Libertés.
- Del-Real, Cristina, Els De Busser, and Bibi van den Berg. 2023. 'Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review'. The Hague: SSRN.
- Diaz, Adriana. 2022. 'Disturbing Reports of Sexual Assaults in the Metaverse: "It's a Free Show"'. *New York Post*, 27 May 2022.
- Dunn Cavelty, Myriam, and Andreas Wenger. 2020. 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science'. *Contemporary Security Policy 41* (1): 5–32.
- Moneva, Asier, and Stefano Caneppele. 2020. '100% Sure Bets? Exploring the Precipitation-Control Strategies of Fixed-Match Informing Websites and the Environmental Features of Their Networks'. *Crime, Law and Social Change 74* (1): 115–33.
- Papakonstantinou, Vagelis. 2022. 'Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?' *Computer Law & Security Review 44* (April): 105653.
- Shapiro, Scott J. 2023. *Fancy Bear Goes Fishing: The Dark History of Information Age, in Five Extraordinary Hacks*. New York: Farrar, Straus and Giroux.
- Steen, Dr Tommy van, and Els De Busser. 2021. 'Security by Behavioural Design: A Rapid Review'. Final report for NCSC-NL. Institute of Security and Global Affairs, Leiden University.

Authors

Cristina Del-Real is an Assistant Professor of cyber crisis governance at the Institute of Security and Global Affairs at Leiden University, and part of the project C-SIDE team. Cristina currently works on the conceptual framework of the project.

Els De Busser is an Assistant Professor of cybersecurity governance at the Institute of Security and Global Affairs at Leiden University. She is the principal investigator of the project C-SIDE.

Acknowledgements
The authors would like to thank Parto Mirzaei, Jasmijn Boeken, and Arina Kudriavtseva for their help in organizing and running the second stakeholders meeting that was held in Leiden in November 2023.

Contact information

Email: info@projectcside.nl
Website: https://www.projectcside.nl/

Address
Project C-SIDE
Faculty of Governance and Global Affairs
Leiden University
Campus Den Haag
Turfmarkt 99
2511 DP The Hague

Published December 2023

Project C-SIDE
Cyber Security by
Integrated Design

Universiteit
Leiden