Regulating Digital Security by Design?: Implications of The Perspectives From DSbD Programme Stakeholders

Journal:	*Information and Computer Security*
Manuscript ID	ICS-01-2023-0010.R1
Manuscript Type:	Original Article
Keywords:	Computer Hardware, Innovation, Regulation, Security, Social responsibility

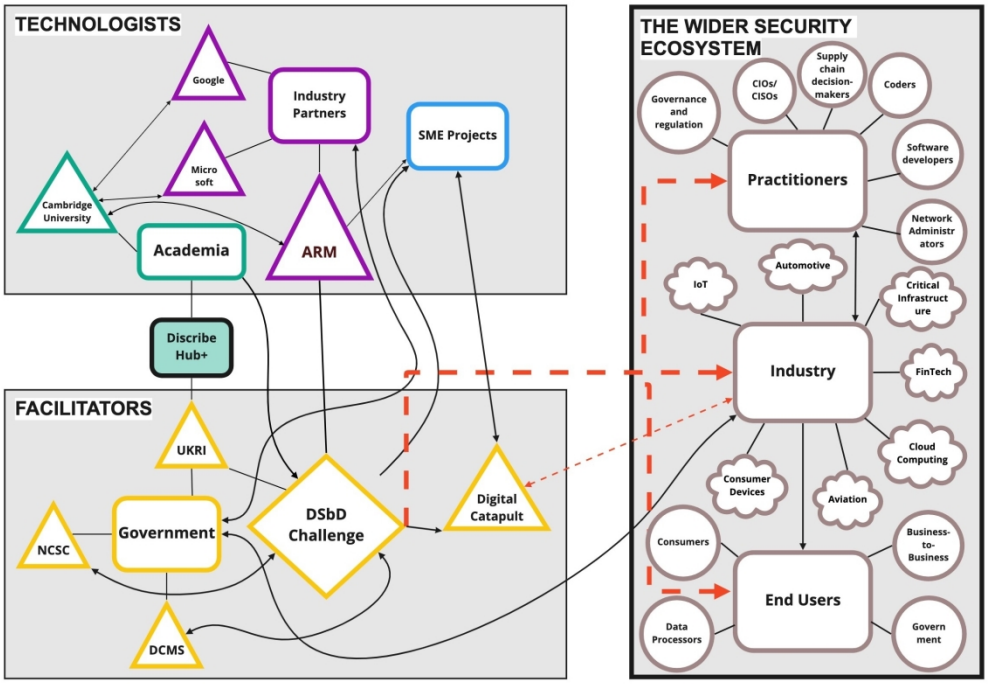

Figure 1. DSbD stakeholder map (Adapted from Slesinger, I., Coles-Kemp, L., Panteli, N. and Hansen, R.R. (2022), "Designing Through the Stack: The Case for a Participatory Digital Security by Design", Proceedings of the 2022 New Security Paradigms Workshop, p. 5.)

819x564mm (72 x 72 DPI)

Baseline Interviews	- Participant's relationship to DSbD project - Define/compare/contrast DSbD, CHERI and Morello - Evaluate participants views on the use and value of CHERI technology - Ask participants to identify stakeholders in the project, and who the users of CHERI technology will be - Ask participant to hypothesise the first likely application for CHERI, and who would be sufficiently motivated to bring the technology to market
Additional Prompts for SME Interviews	- Description of organisation and position in organisation - Description of participant's DSbD De Minimis project - Reasons/motivations for getting involved in DSbD - Benefits of participation - Challenges faced in project - Participant's expectations of CHERI technology, and the extent to which these expectations were met - Whether participant hopes or expected to continue involvement with DSbD programme research, and the resources needed to facilitate this. - What responsibilities – if any – does the participant believe their organisation has in implementing and using DSbD technologies - Whether any factors of responsibility, failure or risk were integrated in the participant's *De Minimis* project design - How the participant thinks DSbD technology should be regulated and whether they would like for their organisation to be involved in the regulatory process

Figure 2. Table of semi-structured interview topic prompts

Regulating Digital Security by Design?: Implications of The Perspectives From DSbD Programme Stakeholders

Abstract

Purpose – As part of the growing necessity for inter-organisational and multi-disciplinary interaction to facilitate complex innovation in digital security, there needs to be greater engagement with regulation in the innovation process. This is particularly true in the case of security technologies that are embedded within wider systems and that are largely invisible to most of the users of that system. This paper describes stakeholders' perspectives on regulation in the digital security innovation process and evaluates the implications of these perspectives on anticipatory regulation in digital security.

Design/methodology/approach – Using a qualitative methodology based on semi-structured expert interviews and ethnographic participant-observation, the study draws on the authors' involvement in a formally organised programme of academia-industry-government collaboration called Digital Security by Design (DSbD).

Findings – The study highlights a relational dimension to establishing regulatory responsibilities that is enabled through interdisciplinary dialogue. The study contributes to understanding the multifaceted roles of regulation in digital security innovation across organisations and areas of expertise. It does so by identifying four themes in how regulation is perceived in the DSbD programme: ethical imperative, adding value, adoption lever and passive compliance.

Practical implications – Incorporating regulatory responsibilities through dialogue early in the innovation process, rather than only once a security technology's deleterious effects are noticeable, could make digital innovation and transformation safer and better regulated. It can also make regulation successfully adopted, rather than an exercise in damage control or an adversarial process between regulators and organisations.

Originality/value – This paper presents original empirical research on how regulation is considered by stakeholders in a novel multi-disciplinary digital security innovation process. It then uses these findings as a basis to evaluate the implications for establishing regulatory responsibilities for a class of security technologies that are embedded within wider systems and that are largely invisible to most of the users of those wider systems.

Keywords: *digital security, regulation, hardware security, innovation, responsible design*

Paper type: Research paper

Introduction

A specific area of multidisciplinary concern that will both shape and be affected by the social, economic and political implications of digital security innovation is regulation and policymaking. Technology regulation can be a complex, contested and fraught process (Black, 2007; Hicks, 2022; Woods and Ceross, 2021), and an area in which regulators often struggle to keep pace and assert appropriate scrutiny over novel and game-changing innovations (Zuboff, 2015). Compounding the already challenging regulatory landscape for existing technologies, front-loading an anticipatory regulation paradigm earlier in the innovation process for technologies that do not yet fully exist (in both technical and social terms) likely requires an imagining of the future in detailed and granular terms that is difficult to achieve. Nevertheless, for digital security technologies such detailed and granular understanding of future use is essential. The consequences for not getting regulation right within the security context, creates risks of catastrophic data breaches, making consumers vulnerable to invasions of privacy and predatory business practices, implications for health and safety in terms of critical infrastructures and unsafe devices, detrimental impacts on people's livelihoods and threats to democratic institutions.

Alongside the changing paradigm for regulation of digital security is an increasing and widespread recognition of the importance of responsibility in research and innovation, which aligns research and innovation to the values, needs and expectations of society (Owen *et al.*, 2021). To achieve this, there is a need for partnerships that promote industry-academia collaborations as well as research and technological development projects that draw upon interdisciplinary knowledge and expertise. Such partnerships create opportunities for engaging with the multifaceted nature, complexity and epistemological depth of socio-technical system (STS) approach. These partnerships are particularly significant in the area of information and computer security, where responsible research and innovation must integrate within an already existing large and complex ecosystem, and incorporate specialised technical knowledges with social, legal, regulatory and business knowledges and modes of practice. (Guest *et al.*, 2022).

In the present study, we draw on our own engagement with an interdisciplinary and cross-sectoral research project to evaluate the implications of a specific innovation in digital security for regulation and policy across sectors and use scenarios. This engagement derives from our work as part of the UKRI-funded Discribe Hub+, a multi-institutional and cross-disciplinary social scientific research programme dedicated to understanding the societal, economic and political implications of innovation in digital security technology. The Discribe Hub+ is a subsidiary of a wider programme of innovation between the UK government, academia and the private sector called Digital Security by Design (DSbD). The primary objective of DSbD is to facilitate the adoption of an 'on chip' hardware security model for memory protection and compartmentalisation developed by computer science researchers at Cambridge University called CHERI (Watson et al 2015). A central aspect of DSbD is an experimental project launched by Arm, called Morello, that has created a prototype board containing a CHERI-enabled ARM processor for SME and business demonstrators to experiment with in a range of applications and test cases. CHERI capabilities offer memory protection and compartmentalisation implemented at the base of the software stack. This technological innovation offers the potential to robustly control access to data by compartmentalising malware and thereby stopping its spread and by implementing granular data protection profiles. Because of these factors, the UK government has identified digital

security by design as a key area for focussed development in the recently published UK National Cyber Strategy (2022, pp. 83–84).

CHERI is representative of a particular class of security technology that provides security functionality within the design of the chip embedded within a larger digital system and whose regulatory impacts are both shaped by its design and by the systems into which such technology is embedded. Our unique perspective of the innovation process of this type of digital security gives us a particular vantage point from which to consider how contributing approaches derived from the social sciences can better integrate responsible and anticipatory regulation in the design process of DSbD. Based on this, the driving research question of this study is: *How is regulation understood by diverse stakeholders in the DSbD initiative and what are the implications for including regulatory compliance as part of DSbD product development?* We have specifically centred our approach to examine how stakeholders' knowledge can be productively exchanged across organisational and disciplinary boundaries at the design phase of DSbD technologies to establish regulatory responsibilities as part of technology design and implementation processes.

The next section will review literature on regulation and then responsible research and innovation to set the background for examining regulatory responsibilities within DSbD. Following from this the specific programme of our study is identified and the methods adopted for the data collection presented.

Regulation within the Digital Security Context

Traditionally security management has long relied on regulation in the form of standardisation, legal compliance, and good practice to establish how to assess the security worthiness of an individual, organisation or technology. Regulation is also used in information security as a means to resolve contentions around which security controls to deploy (Johnson and Goetz, 2007) and when regulatory compliance is regarded as part of the wider compliance programme that information security is subject to, which often creates a resource overhead for the organisation that has little security return (Beauement *et al.*, 2008). Larger organisations have regulatory roles in order to support decisions about which controls to deploy and there is little consensus around how these roles should be enacted. This contention in part happens because regulation can be seen as a means of dumping liability for the security of data, technology and services as well as a means of taking responsibility (Anderson, 1994; Burdon and Coles-Kemp, 2019). Stajano and Isozaki (2002) suggest that addressing security at the design stage can provide a corrective to 'liability dumping' by putting responsibility on manufacturers to mitigate in design the maximum damage that a device can cause.

Coglianese and Lazer (2003, p. 693) argue that regulation seeks to address an imbalance between the profits and societal benefits private business actors accrue, and the "potential positive and negative externalities (social goods and bads)" they produce "that affect society." They identify three approaches to regulation that may occur in the planning, acting or output stages of an organisation's activities. The first approach is technology-based regulation that occurs in the acting stage, and which specify particular technical solutions or

procedures that must be implemented. The second approach is performance-based regulation that prescribes what social outcomes must be realised or avoided at the output stage. The third strategy is a more self-regulating management-based approach in which a regulated organisation focuses more on their own management structures and internal policies at the planning stage to improve accountability and "increase the achievement of public goals" (Coglianese and Lazer, 2003, p. 694). Gilad (2010) suggests that the latter can provide a more ideal form of regulation by incorporating a concept of "meta-regulation" that introduces a learning-oriented approach to evaluating and modifying organisational governance to ensure better regulation. However, Gilad (2010, p. 485) also warns that "realizing these advantages requires a rare combination of high regulatory capacity, a stable regulatory agenda, and a supportive political environment."

Bonnìn Roca et. al. (2017) highlight the challenges of designing regulation in scenarios of technological innovation because of the high degrees of contingency and uncertainty endemic to such contexts. They argue that regulatory design must account for the heterogeneity of both specific technologies and the organisations and industries that produce these technologies, as well as the temporal dimension in which uncertainty technologies' societal impacts and the implications of their use shift relationally to the societal and business context in which they exist and act. They recommend that these ambiguous dimensions make "technology-based regulation, which has traditionally been reviled as an innovation-constraining approach, … a useful tool both to control risks and to enhance the gathering of knowledge." Such knowledge gathering "is essential in technologies where certain aspects of performance can only be discovered through use" and thus necessitate a "learning by using" component in regimes of technology regulation (Bonnín Roca *et al.*, 2017, p. 1229). In the case of DSbD, the question of regulation is further complicated by the DSbD technologies being both embedded within other technologies and as a result being largely invisible to users of digital technology; yet fundamentally affecting how data is both accessed and protected.

Responsible Research and Innovation

Regulatory compliance forms part of the wider picture of responsible research and innovation. Attending to growing societal concerns regarding the governance and regulation of emerging technologies and innovation, the last decade or so has witnessed the growing relevance of Responsible Research and Innovation (RRI) and the wider social, economic, political and environmental impact of scientific research and innovation. Largely anchored to the policies and values of the European Union's Horizon 2020 programme, RRI is an approach that "anticipates and assesses the potential implications and societal expectations with regard to research and innovation, with the aim to foster the design of inclusive and sustainable research and innovation" ("What is RRI?", n.d.). In a shift beyond a moralistic form of responsibility that places the onus for responsible action on the individual, RRI instead brings into focus the idea of responsibility as more of a social/collective endeavour – one that is ascribed to a plethora of stakeholders (including researchers, designers, businesses, policymakers and even citizens). This approach seeks to align the values, goals and outcomes of each stakeholder throughout the entire process of research and innovation. Stilgoe et al. (2013, p. 1570) define "Responsible innovation" in such terms as "taking care of the future through collective stewardship of science and innovation in the present."

In doing so, Stilgoe et al. (2013) suggest that a move towards responsible research and innovation should include a broad range of considerations, including how certain risks and benefits will be distributed across society (and how these should be defined and measured); the anticipation and potential mitigation of any impacts (including any potential unknowns); who should take responsibility if things go wrong; and what are the motivations of both the research and researcher(s). To tackle these broad considerations, they set out a framework which proposes four dimensions for responsible innovation:

- Anticipation - an attempt to improve foresight and increase resilience by prompting the 'what if' questions in relation to innovation.
- Inclusion - an attempt to improve the legitimacy of research and innovation practices, by including new voices and stakeholder interests in discussions of the ends AND means of innovation.
- Reflexivity - the practice of holding up a mirror to one's own activities, beliefs and judgements, questioning the taken-for-granted assumptions we might have, and considering how the responsibilities of individual stakeholders may blur with wider, moral responsibilities.
- Responsiveness - the notion of responsible research and innovation must be engaged in "responding to new knowledge as this emerges and to emerging perspectives, views and norms" (Stilgoe *et al.*, 2013, p. 1572).

Offering a direct critique of this RRI agenda, van de Poel and Sand (2018) note how responsible innovation, in effect, ascribes a range of new responsibilities upon individual agents (such as scientists, engineers, developers, or CEOs), arguing whether it is reasonable or fair to expect innovators to bear the burden of such responsibilities - raising difficult questions about where collective responsibility might lie. They go on to argue that accountability and responsibility-as-virtue are important in relation to responsible innovation. For accountability, this confirms the moral ownership of innovators, but also shared moral rules and community around forms of innovation. Responsibility-as-virtue also explicates a willingness and desire from different stakeholders to take on more specific responsibilities, whilst also stressing the “open-ended character of responsibility in innovation” (van de Poel and Sand, 2018). Building on Stilgoe’s four analytical dimensions of responsible innovation, their work discusses some of the complexities and challenges in achieving responsible design.

There has also been work looking at how different views on where the locus of responsibility lies might be bridged. Grimpe et al. (2014) explored how a responsible innovation research agenda can be brought into conversation with HCI research and design. In doing so, they argued that there is a need for "an ongoing distributed effort of many parties at many levels i.e. a continuous strive for shared responsibility" (Grimpe *et al.*, 2014, p. 2972).

The DSbD Context

As has been stated in the introduction, this study examines the work of the UK government’s Digital Security by Design (DSbD) programme to better understand how regulation and regulatory compliance is considered in the development of security technologies that are

designed to be embedded into a wide range of larger digital technologies and systems. In order to understand how regulation and regulatory responsibilities are understood, we need to first examine the motivation for the technology and how stakeholders are able to engage with its initial design. We set this out for the CHERI technology in the following subsections.

Market Faliure(s) in Security Innovation

The stated objective of DSbD is to "radically update the foundation of the insecure digital computing infrastructure by creating a new, more secure hardware and software ecosystem" to "underpin future digital products and services" (Papadakis, 2020). This is intended to correct what has been termed as a "market failure," or alternatively "broken market," by the architects of DSbD. However, the nature and meaning of this market failure is multiple and varied between DSbD's architects and key participants, and in the course of our research we have identified four distinct explanations of the nature of the perceived market in digital security hardware innovation. The first explanation is that industry is reluctant to innovate hardware without an existing software infrastructure to support the new hardware, and conversely there is a lack of appetite to develop the new software required to support hardware innovation without an existing hardware platform to develop upon. The second is that there is a mismatch between the longer timescale required for significant hardware innovation and the shorter software and device product design and launch cycle. The third explanation of the market failure that forms the underlying rationale for DSbD is that security is perceived by businesses as a negative externality for which the seek to pay the bare minimum to mitigate and insure against as it is not seen as a growth driver. Lastly, the fourth explanation is that the way liability for security failure is distributed within the digital technology market disproportionately places responsibility onto the end user for the consequences of failure, in contrast to the manufacturer of a product or intermediate suppliers within the supply chain. In practice, the reasons for perceived market failure are often a combination of all four positions.

CHERI and Morello

DSbD is in fact solely focused on the adoption of a particular technological approach called CHERI (Capability Hardware Enhanced RISC Instructions), a theoretical model for instantiating more precise control of how memory is accessed by computer processors that was developed jointly by computer scientists at Cambridge University and SRI international, initially with funding from the US government's Defence Advanced Research Projects Agency (DARPA). The developers of CHERI claim that the technology has the potential to prevent 70% of current cyber-attacks (Gardner, 2022), which are caused by memory vulnerabilities. Arm has developed an experimental hardware prototype called the Morello board, which instantiates the CHERI model in a hardware platform, and which is the medium through which the stakeholder ecosystem can engage with CHERI and influence its initial development and design.

The Morello boards are being distributed to both Small to Medium Enterprise (SME) demonstrators and several larger business demonstrators, including the Hut Group, who are tasked with developing some of the software implementation and use cases for CHERI. ARM

have emphasised that Morello is not a commercial prototype in order to make clear that CHERI is not part of its current roadmap for product development. This has implications in terms of Arm's business model which is to license its proprietary intellectual property for processor architecture to chip and device manufacturers. Instead, the proponents of CHERI want the technology to be interoperable, and thus universal, between all processor architectures, including RISC-V, Intel and Arm.

The present research is part of the Discribe Hub+, which is a UK Economics and Social Research Council-funded programme within the broader aegis of DSbD. It is an interdisciplinary project comprised of four work packages focusing on adoption, readiness, regulation and policy and across contexts. Across these work packages multiple disciplinary approaches and methodologies are applied and combined including qualitative science and technology studies, business and management, social psychology, narrative studies, economics and game theory, computer science and automated machine learning techniques. These diverse knowledges and approaches encapsulated even within a more specific social science focussed sub-set of DSbD are a microcosm of the deep hybridity of the programme at large, and thus our research is embedded within the complex network rather than being passive outside observers of it. This highlights the multiple and heterogenous disciplinary purviews and roles of academia within DSbD. The next section will map out the socio-technical network of the DSbD programme in greater detail in order to identify viable pathways for encouraging stakeholder engagement around regulation within the programme.

Mapping the DSbD ecosystem

[INSERT **FIGURE 1** HERE]

The DSbD programme entails a diverse network of stakeholders from across the UK government, academia, industry and SME (diagrammed in Figure 1). Key nodes include Arm, who are running the Morello project and several individuals in the Computer Science department at Cambridge University who developed the CHERI model.

Methodology

Our research used a qualitative approach to gathering and evaluating data, which combined semi-structured elite interviews with participant-observation as members of the DSbD community. Whilst these methods are well-established in the social sciences, we were applying them in a unique situation and context. We conducted two sets of semi-structured interviews. The first was a set of eight baseline interviews with key individuals within DSbD and the wider hardware security community (e.g. program director, industry and academic partners). These interviews sought to ascertain how participants understand some of the key concepts related to CHERI and DSbD, as well as key stakeholders in the DSbD programme and its wider ecosystem. As a final provocation, we asked participants to consider what the likely first application of CHERI might be, and what actors would be sufficiently motivated to bring the technology to market. These interviews were conducted on a "Chatham House" rule basis

to encourage our participants to be more open in their discussion than would be possible in an on-the-record basis. A second researcher took notes to ensure a more accurate record of the discussion. These notes were then collated and sent back to the participant for additional input and approval. This ensured the informed participation of our research participants and mitigated against any potential inaccuracies or missed information in our notes prior to analysis.

[INSERT **FIGURE 2** HERE]

The second set of interviews was conducted with five SMEs who had received *de minimis* funding from DSbD to carry out projects that tested and applied a virtual platform environment (VPE) prototype of the CHERI stack in a range of sectors. In addition to discussing some of the same themes as the baseline interviews, these interviews also examined the experiences of the SME organisations in conducting their projects, including the successes and challenges they faced in integrating the technology with their businesses' objectives and the extent to which the technology was effective in addressing their business needs. We also asked these interview participants to reflect on how they perceived their regulatory responsibilities and how they anticipated their responsibilities might apply in relation to the commercialisation of the CHERI technology (see figure 2 for interview topic guide). In contrast to the baseline interviews, these were audio recorded by the research team with the participants' consent and professionally transcribed for analysis. This is because we deemed these interviews to be less sensitive than the baseline interviews since the participants are less centrally involved in the DSbD ecosystem and we believed this approach would provide greater ease and nuance for our analysis.

The collected data was then analysed using a thematic coding methodology, which was carried out using NVIVO qualitative data analysis software. This coding process was informed by the research question of the study and its topical focus on stakeholder attitudes to regulation and responsibility. We sought to understand what regulation means for our study participants and to identify and distil generalisable approaches to regulation that would have analytical value for scholars and regulation and policy practitioners. Initially, all discussions of regulation across the interview data were identified using key word searches for the terms 'regulation' and 'responsibility.' Then summative codes were created in accordance with four unifying themes we identified in participants' perspectives to regulation. The researchers then carried out another pass through the collated data to assign codes and cross-reference their accuracy in accordance with the interview data.

Whilst the number of participants might seem small, the sample is in fact representative of the DSbD stakeholder community at the time of researching and writing. The small number of study participants was a result of the insular nature of the DSbD programme's organisation and the novelty of both the CHERI technology and the remit of the programme. With our data we were able to produce analysis that shows the position of DSbD stakeholders on regulation and regulatory responsibility in the DSbD context. Our analysis stabilised and were able to demonstrate that we had saturated the findings from our data analysis and were able to reach generalised conclusions. Likewise, much of the front-facing research conducted with commercial organisations focussed on the experiences of SMEs due to the fact that SMEs are the current adopters of the DSbD technology, and not larger organisations. Because of their

comparatively small size and fewer resources, SMEs tend to have more agile organisational structures that are characterised by employees multi-tasking in a number of roles, including those relating to digital security and data privacy. In contrast, larger organisations such as corporate entities tend to have more distinctly differentiated and hierarchically organised roles. However, the focus of our study is to look at how regulation and regulatory compliance are considered at the start of the development journey and the generalised findings shine a light on how we might both surface and establish regulatory responsibilities for security technologies that are embedded in larger systems, and which are built into the lower part of the software stack away from human computer interaction. As DSbD reflects, such a development journey often begins with specialised technical teams within university departments, specialised SMEs, or within dedicated organisational units within larger technology companies. Whilst the use of such technologies will evolve in larger organisations, the core technology is already developed and positions on inclusion and regulation will already be baked into the design.

Findings

Two core findings from the study are i) the diversity of views that exists among key DSbD stakeholders on regulation for this type of digital security technology and ii) the importance of dialogue and relationship building to establish and implement regulatory responsibility into the technology. We explore this below and present the different perspectives on regulation that emerged.

Stakeholders' diverse views on regulation

There are two significant vectors for implications of regulation in DSbD. One is the role of the UK government in the innovation process, which puts government in an influential position to determine how the CHERI technology will be positioned within the existing regulatory landscape, and in shaping the future regulatory landscape for CHERI. Another vector for both the significance of discussion around regulation and the complexity of elucidating and developing the regulatory landscape around CHERI is the broad diversity of sectors and use cases in which the technology is likely to be applied. This includes (but is not limited to) financial services technology, critical national infrastructure, cloud services, healthcare data management and consumer devices.

The findings of our research demonstrate that regulation is a complex and multifaceted issue affecting a range of DSbD stakeholders, and that stakeholders held heterogenous and widely diverse views on regulation. These perspectives seem to be influenced by multiple considerations including individual stakeholders' attitudes to regulation, sector, organisation size and positioning, and goal orientation. We also noted a motivation from certain stakeholders, particularly those who felt outside the core of the DSbD network, to have input in contributing to shaping the regulatory landscape around DSbD.

Perspective 1: Regulation as an ethical imperative

For some stakeholders across sectors and institutions regulation was seen ultimately as an ethical responsibility. This came from SMEs, innovators from 'big tech' and government stakeholders. In some situations this was due to participants' work in relation to areas in which existential or financial risk was acute and consequential such as critical national infrastructure, aviation and healthcare. One stakeholder related an anecdote about their experience working with a US robotics company working on unmanned aerial vehicle in which an executive from that company expressed a view that they had no responsibility for ensuring compliance with the DO-178 aerospace software safety regulation. The participant continued:

> "Wind forward to last year and he was on a forum we've got writing standards for unmanned aerial systems and he came on telling us, urging us to allow all this open-source crap software into an aerospace environment. So the question really … is do you want to have software and … functionality in the air that could potentially go straight through the windscreen of your airliner?"

Others saw an ethical responsibility in how they pitched the technology to other business users, government and the public. In one notable instance a participant from a big tech company describes the CHERI technology as "necessary but not sufficient". This perspective suggests that CHERI can provide an extra degree of data protection but needs to be understood relationally as one part of a wider security ecosystem rather than as a singular security panacea. This understanding highlights the need for a robust regulatory structure alongside other changes in the digital ecosystem including CHERI. This requires a more holistic digital security by design that engages stakeholders in planning for security in a way that exceeds technological solutionism and includes consideration of the roles of regulation, standardisation, socio-technical interactions, economic and political factors (Slesinger *et al.*, 2022).

Perspective 2: Regulation as adding value

Another approach to regulation that appeared in the course of our research is a proactive attempt to include regulation in the business model as a source of added value for a product or service. This was most noticeable in the SME interview package and manifested in two ways. The first is incorporating verification and regulatory compliance into the organisations business model. The second is encouraging regulatory oversight as a mark of quality for the company's standard of service provision. According to a founder of a healthcare technology SME that we interviewed:

> Regulations were the key driving factor for us. I mean, we understand GDPR applies in the UK and the EU, HIPAA applies in the US and there are a whole raft of other privacy and medical regulations that we have to be aware of… But what all these regulations mean is [that] we have to have a system of both technological and from a process standpoint that maintains the sanctity and the privacy of the data we hold. They were our driving factors, we know that we cannot participate in markets unless we are complying with the regulations that I've mentioned… So, for us it's a huge motivator.

This response shows that there are multiple motivations and contexts in how stakeholders approach regulation. One is an ethical and moral regulation to maintain "sanctity" and "privacy." Another motivation for some business stakeholders is to leverage a comparative advantage by applying regulatory expertise at the intersections of sector-specific contexts and

international regulatory regimes across territorial borders. The implications of the commercial significance of expertise here are complex and ambivalent. It could either encourage a participatory approach to regulation as shared learning allows for knowledge and product development in respectively specific niche areas that do not overlap. Conversely though, the commercial role of expertise could be a barrier to participatory engagement as stakeholders would feel disincentivised to share knowledge due to the risk of losing their comparative advantage in a specific or adjacent area to their business model, or for advancing a regulatory model that contravenes their organisation's interests.

Perspective 3: Regulation as an adoption lever

Key proponents of the CHERI technology, particularly in academia and certain branches of government see regulation in an instrumental way as a possible lever to encourage adoption. One senior civil servant responsible for innovation policy made clear in an interview that they would be willing to pull any levers possible in order to ensure that CHERI is used, including government policy on technology procurement or regulatory mechanisms.

In this view, regulations can be put in place that will subsequently encourage or necessitate adoption of CHERI to fulfil the new requirements, or as stronger evidence of compliance with existing regulations. However, regulations are typically established as a set of broad guidelines and criteria that must be met, but do not necessarily prescribe the means by which these criteria ought to be met. This requires the parties being regulated to establish procedures and equip their organisation in a way that meets the regulatory standards in line with the structure and strategic trajectory of that organisation, and to evidence the steps taken to comply to satisfy the relevant regulators. Based on the way regulation works in practice, it is unlikely that regulation can actually provide a certain and clear pathway to leverage the adoption of CHERI writ large. Another factor influencing this question is the extent of interoperability between the technology's capacities and national and intergovernmental regulatory structures, as well as the extent to which international standards bodies will cooperate with such an attempt.

Perspective 4: Passive Compliance

In contrast to the engaged attitudes to regulation demonstrated above, a small group of SME stakeholders were either indifferent or ambivalent to having a role in shaping the regulatory landscape of DSbD. These tended to come from a view that it is not their responsibility to establish regulation, merely to follow what the regulators set out. One SME stakeholder

> I don't see the stick approach in making DSbD prevalent and successful, I see the carrot approach as making DSbD prevalent and successful. Because if you said to me [that] we're going to regulate, you're going to have to move to DSbD… [the] first thing you would do as a, especially if you had a very large company, is just migrate to the jurisdiction where you don't have to do it. And what you're left [with] is tiny little players that can't move to another jurisdiction and then you're hampering their innovation to be able to challenge the bigger players.

This suggests those with such a viewpoint distance themselves from the attitude of regulation as a form of responsibility, and that they see personal and organisational responsibility as

lying elsewhere. This contrasts with others who take a more activist position in advocating anticipatory regulation, who see regulation as both an organisational and social responsibility.

Discussion

This study makes contributions at the nexus between the three related areas of regulation, digital security and responsible innovation. The analysis of the different positions on regulation surfaces how security technologies, embedded into larger systems engage issues of regulatory responsibility at the start of the development journey. It does so by applying concepts from STS and innovation studies to provide a sociology of innovation in computer security, particularly in relation to hardware security. Specifically, the evaluation of DSbD that this paper contributes is in itself noteworthy due to DSbD's novel process for enrolling substantial resources and stakeholders to shape and accelerate the innovation process. Its temporal positioning early in the innovation process, as well as its emphasis on the experiences of SMEs with regulation in innovation are also significant additions to the literature.

Relational Dimension of Regulation

DSbD is an intrinsically interdisciplinary and inter-organisational endeavour. It relies on the engagement between academia, industry and government as a catalyst for success. As a result, it has brought together academics in collaboration with key industry players. For example, researchers from the Cambridge University Computer Science Department were responsible for creating the manuals for CHERI compatible coding as well as the FREE BSD virtual platform environment (VPE) for Morello that was used in the SME *De Minimis* projects. Likewise, the SME projects would liaise with the Morello project team at ARM in order to obtain assistance in troubleshooting problems with the Morello VPE as they arose. Twice yearly DSbD 'all-hands' events provided an opportunity for cross-disciplinary interaction through presentations from project leaders across academia, government, and industry, as well as poster sessions in which other participants could engage with academic researchers and break-out groups that addressed a number of technical, social and business aspects of CHERI adoption including regulation. The findings presented in this paper reflect a diversity of views on both the relevance of regulatory compliance for the technologies such as DSbD and the different approaches to ensuring regulatory compliance. The findings of our study highlight the relational dimensions of establishing regulatory responsibility through interdisciplinary multistakeholder engagement and discussion. The success of such discussions are based are firmly anchored in the ability of each stakeholder to understand the position of the others and to co-create a joint understanding of regulatory responsibilities. This is particularly important when the security technology is embedded within a wider system and shapes data and technology protection whilst remaining largely of sight. With such technologies it is important to establish the regulatory positioning and responsibilities of the technology and make such positioning explicit from the outset. In this way the regulatory responsibilities can be interrogated once the security technology has been deployed.

Hierarchical vs. Lateral Approaches to Regulatory Development

In the study, we have sought to examine responsible research and innovation within the context of an interdisciplinary project on the regulatory framework of digital security. We found that the DSbD programme was effective in bringing together a broad spectrum of stakeholders towards a common goal. However, interdisciplinary collaboration was not necessarily natural or inevitable in the DSbD programme due to the vertical hierarchal structure through which the programme was established and organised. That said, we observed a strong motivation and desire for a more lateral form of working to problem solve technical challenges and barriers to adoption in order to actualise and promote CHERI as a viable project. A significant aspect of this work is to establish both what CHERI-based hardware can and should do in terms of security provision, and as such how standards and regulation ought to govern the technology's use. We identified a diverse set of views across disciplines, organisations and individuals about what regulatory responsibility might mean in relation to CHERI-based hardware, and the extent of stakeholders' ownership over responsibility in the innovation process. This indicates that regulatory compliance is not decided at an initial stage in the design process of DSbD technologies but needs to be included at the initial stage and then continue as different contexts of use are discussed. This has a further consequence in that responsibilities in affected areas such as data assurance needs to be discussed as the use of DSbD technologies evolve. It thus places an emphasis on regulatory dialogue throughout the design and implementation processes.

Broadening Stakeholder Engagement

Our findings highlight a need for more organic stakeholder engagement in DSbD, both *tout court*, and particularly in the area of anticipatory regulation. In their interviews several stakeholders pointed to a dynamic in which those 'inside the [CHERI] tent' are separated from those 'outside the tent' and there is a failure to bring those would-be collaborators inside the tent and properly engage with their needs and perspectives. Compounding this problem in terms of regulation is a lack of engagement with regulators who would likely be involved in the regulatory process. In order to better address the challenge of anticipatory regulation in the complex information security eco-system it is best to engage all of these parties together both in conversation, and more deeply in terms of understanding security practices, techniques and things to create a regulation that shares responsibility in a positive and proactive way, rather than as an adversarial system.

The institutional constraints introduced by the bureaucratic structures in which DSbD is situated present a challenge to the successful inculcation of productive engagement in the DSbD innovation process. This includes the temporal constraints to the duration of the project that could adversely affect the subsequent continuity of participation in designing regulation, as well limitations imposed by funding constraints. Our findings show that the regulatory significance of the DSbD technologies is both inherent in the design of the technology and the security capabilities that it enables as it is deployed. Understanding the implications of this significance requires on-going multi stakeholder dialogue.

Conclusion and Implications

This paper examined stakeholder attitudes to regulation in a novel multi-scalar and multi-disciplinary innovation process sponsored by the UK Government in coordination with several major technology corporations called Digital Security by Design. Our research team conducted eight semi-structured interviews with key figures in the leadership of DSbD and the wider digital technology industry, and another five interviews with SMEs working on an initial VPE simulation of the CHERI environment. By analysing these interviews, using qualitative data coding, we identified four distinct key themes in how various participants perceived the role of regulation in the digital security innovation process. These can be summarised as follows: 1) regulation as an ethical imperative; 2) regulation as adding value to a product or service; 3) regulation as an adoption lever; 4) passive acceptance of regulation as a compliance regime.

Based on these findings, as well as by drawing from the wider set of interview data we gathered, our work highlights the relational dimension of regulatory compliance and the importance of dialogue to share views and build relationships between stakeholders. We have suggested that there is a drive for a more participatory and organic stakeholder engagement both in general within the context of digital security, and specifically towards collaboratively establishing the regulatory environment and requirements around CHERI with consideration of sector-specific obligations and requirements. Such a collaborative approach might involve building participatory stakeholder engagement around CHERI, including developing knowledge about how it fits into both currently existing and anticipated regulatory landscapes, and how the technology can be used to problem-solve emergent regulatory challenges. However, in order for such an approach to be successful, the vertically hierarchal elements of DSbD's structure and organisation must be supplemented with more lateral and non-prescriptive forms of engagement between stakeholders towards developing the shared goals and features that would make the technology viable and desirable in the marketplace.

Our study identifies areas for further research that can be developed by research teams in the future. Chief amongst these would be a longitudinal study on the mechanisms that help to understand how the regulation issues of such embedded security technologies evolve as they are adopted into larger systems. Another avenue for further research is on how and to what extent interactions between different stakeholders influence the acceptance of responsible regulation in digital security, and what the resulting regulation would look like.

Finally, in addition to contributing to the scholarship of the relationship between digital security innovation and regulation, the study has implications for practitioners and policymakers. This includes how to develop processes for creating and implementing regulatory frameworks, and what criteria should influence the contents of such regulation. It also invites practitioners to create opportunities for diverse stakeholders' voices to be heard as well as to better understand and actively engage with the role of government and other policymakers in ensuring responsible regulation. There are opportunities for the security industry to take an active role and drive an industry-led regulatory framework in digital security.

References

Anderson, R.J. (1994), "Liability and computer security: Nine principles", in Gollmann, D. (Ed.), *Computer Security — ESORICS 94*, Vol. 875, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 231–245, doi: 10.1007/3-540-58618-0_67.

Beauement, A., Sasse, M.A. and Wonham, M. (2008), "The compliance budget: Managing security behaviour in organisations", Association for Computing Machinery.

Black, J. (2007), "Principles Based Regulation: Risks, Challenges and Opportunities", University of Sydney, 27 March.

Bonnín Roca, J., Vaishnav, P., Morgan, M.G., Mendonça, J. and Fuchs, E. (2017), "When risks cannot be seen: Regulating uncertainty in emerging technologies", *Research Policy*, Vol. 46 No. 7, pp. 1215–1233, doi: 10.1016/j.respol.2017.05.010.

Burdon, M. and Coles-Kemp, L. (2019), "The significance of securing as a critical component of information security: An Australian narrative", *Computers & Security*, Vol. 87, p. 101601, doi: 10.1016/j.cose.2019.101601.

Coglianese, C. and Lazer, D. (2003), "Management-Based Regulation: Prescribing Private Management to Achieve Public Goals: Management-Based Regulation", *Law & Society Review*, Vol. 37 No. 4, pp. 691–730, doi: 10.1046/j.0023-9216.2003.03703001.x.

Gardner, R. (2022), "Research into developing a software ecosystem for a more secure digital future", *Cambridge University Department of Computer Science and Technology*, 24 February, available at: https://www.cst.cam.ac.uk/news/research-developing-software-ecosystem-more-secure-digital-future (accessed 24 August 2022).

Gilad, S. (2010), "It runs in the family: Meta-regulation and its siblings", *Regulation & Governance*, Vol. 4 No. 4, pp. 485–506, doi: 10.1111/j.1748-5991.2010.01090.x.

Grimpe, B., Hartswood, M. and Jirotka, M. (2014), "Towards a closer dialogue between policy and practice: responsible design in HCI", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, NY, USA, pp. 2965–2974, doi: 10.1145/2556288.2557364.

Guest, D., Knox, A. and Warhurst, C. (2022), "Humanizing work in the digital age: Lessons from socio-technical systems and quality of working life initiatives", *Human Relations*, SAGE Publications Ltd, Vol. 75 No. 8, pp. 1461–1482, doi: 10.1177/00187267221092674.

Hicks, A. (2022), "Transparency, Compliance, And Contestability When Code Is(n't) Law", p. 11.

HM Government. (2022), *National Cyber Strategy*, p. 130.

Johnson, M.E. and Goetz, E. (2007), "Embedding Information Security into the Organization", *IEEE Security & Privacy Magazine*, Vol. 5 No. 3, pp. 16–24, doi: 10.1109/MSP.2007.59.

Owen, R., Pansera, M., Macnaghten, P. and Randles, S. (2021), "Organisational institutionalisation of responsible innovation", *Research Policy*, Vol. 50 No. 1, p. 104132, doi: 10.1016/j.respol.2020.104132.

Papadakis, G. (2020), "Unleash of the release – Enabling the Digital Security by Design (DSbD) ecosystem", *Www.Dsbd.Tech*, available at: https://www.dsbd.tech/blogs/unleash-of-the-release-enabling-the-digital-security-by-design-dsbd-ecosystem/ (accessed 3 May 2022).

van de Poel, I. and Sand, M. (2018), "Varieties of responsibility: two problems of responsible innovation", *Synthese*, Springer Netherlands, doi: 10.1007/s11229-018-01951-7.

"Research". (n.d.). *Discribe DSbD*, available at: https://www.discribehub.org/research (accessed 30 August 2022).

Slesinger, I., Coles-Kemp, L., Panteli, N. and Hansen, R.R. (2022), "Designing Through The Stack: The Case for a Participatory Digital Security By Design", p. 15.

Stajano, F. and Isozaki, H. (2002), "Security issues for Internet appliances", *Proceedings 2002 Symposium on Applications and the Internet (SAINT) Workshops*, presented at the Proceedings 2002 Symposium on Applications and the Internet (SAINT) Workshops, pp. 18–24, doi: 10.1109/SAINTW.2002.994548.

Stilgoe, J., Owen, R. and Macnaghten, P. (2013), "Developing a framework for responsible innovation", *Research Policy*, Vol. 42 No. 9, pp. 1568–1580, doi: 10.1016/j.respol.2013.05.008.

Watson, R. N., Woodruff, J., Neumann, P. G., Moore, S. W., Anderson, J., Chisnall, D., ... & Vadera, M. (2015, May). CHERI: A hybrid capability-system architecture for scalable software compartmentalization. In *2015 IEEE Symposium on Security and Privacy* (pp. 20-37). IEEE.

"What is RRI?" (n.d.). , available at: https://www.rri-practice.eu/about-rri-practice/what-is-rri/ (accessed 20 September 2022).

Woods, D.W. and Ceross, A. (2021), "Blessed Are The Lawyers, For They Shall Inherit Cybersecurity", Association for Computing Machinery (ACM), pp. 1–12, doi: 10.1145/3498891.3501257.

Zuboff, S. (2015), "Big other: Surveillance Capitalism and the Prospects of an Information Civilization", *Journal of Information Technology*, Vol. 30 No. 1, pp. 75–89, doi: 10.1057/jit.2015.5.