



Adaptive governance for the Internet of Things: Coping with emerging security risks

Irina Brass

Department of Science, Technology, Engineering and Public Policy, University College London (UCL), London, UK

Jesse H. Sowell

Department of International Affairs, Bush School of Government and Public Service, Texas A&M University, College Station, TX, USA

Abstract

The Internet of Things (IoT) is a disruptive innovation known for its socio-economic potential, but also for generating unprecedented vulnerabilities and threats. As a dynamic sociotechnical system, the IoT comprises well-known cybersecurity risks and endemic uncertainties that arise as IoT adoption increases and the system evolves. We highlight the impact of these challenges by analyzing how insecure IoT devices pose threats to both consumer protection and the Internet's infrastructure. While recent regulatory responses are starting to target IoT security risks, crucial deficiencies – especially related to the feedback necessary to keep pace with emerging risks and uncertainties – must be addressed. We propose a model of adaptive regulatory governance that integrates the benefits of centralized risk regulatory frameworks with the operational knowledge and mitigation mechanisms developed by epistemic communities that manage day-to-day Internet security. Rather than focusing on the choice of regulatory instruments, this model builds on the “planned adaptive regulation” literature to highlight the need to systematically plan for a knowledge-sharing interface in regulatory governance design for disruptive technologies, facilitating the feedback necessary to address evolving IoT security risks.

Keywords: cybersecurity, disruptive technology, internet of things, planned adaptive risk regulation, regulatory governance.

1. Introduction

The Internet of Things (IoT) is projected to have significant positive impacts on contemporary public policy objectives, from remote public service provision in healthcare to more efficient resource management of energy systems. However, many of the IoT devices currently on the market exhibit gross vulnerabilities that are well-known to cybersecurity experts (such as default passwords) and easily exploitable by malicious actors (Makhdoom *et al.* 2019; Boddy *et al.* 2019). Coupled with these vulnerabilities, increasing adoption and deployment of the IoT undermines consumers' security, safety, and privacy, while also facilitating “cybercrime at scale” and lowering the barriers to powerful Distributed Denial of Service (DDoS) attacks that threaten the integrity of the Internet's infrastructure (Maple 2017; Yang *et al.* 2017; Blythe *et al.* 2019). Like other evolving sociotechnical systems, causality, and impacts in the IoT are not always straightforward (Galaz *et al.* 2017). Understanding unanticipated interactions and illicit behaviors requires pre-existing knowledge of IoT device design as well as in situ knowledge of how these devices are deployed and behave within the Internet infrastructure, upon which they fundamentally rely for connectivity and “smart” functionality.

To address these risks, policymakers around the world are re-evaluating the kinds of instruments, knowledge, and evaluative capabilities necessary to balance the positive potential of the IoT while identifying and managing rapidly evolving technological risks (Brass *et al.* 2018; Tanczer *et al.* 2019). To ensure baseline cybersecurity specifications are adopted by key entities in the global IoT supply chain (such as device manufacturers), policy debates

Correspondence: Irina Brass, Department of Science, Technology, Engineering and Public Policy, University College London (UCL), Shropshire House (4th Floor), 11-20 Capper Street, London WC1E 6JA, UK. Email: i.brass@ucl.ac.uk

[Correction added on 30 July 2020, after first online publication: General copyediting errors have been corrected throughout the article.]

Accepted for publication 14 June 2020.

© 2020 The Authors. Regulation & Governance Published by John Wiley & Sons Australia, Ltd

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

have thus far focused on balancing self-regulation and mandatory requirements. While these approaches build on the knowledge of pre-existing cybersecurity risks, they rarely incorporate timely information about emerging risks derived from indicators of Internet security and stability. These indicators of evolving threats and vulnerabilities are continuously developed and refined within communities of operational actors who manage the security of the Internet's infrastructure on a day-to-day basis.

Balancing the trade-offs intrinsic in fostering innovation and managing technological risk demands more timely characterizations of rapidly emerging sociotechnical risks, renewing discussions on the role and scope of technology regulation (Brownsword & Yeung 2008; Raab & De Hert 2008; Bennett Moses 2013; Butenko & Larouche 2015; Kołacz *et al.* 2019). In particular, debates on the practice of risk regulation and regulatory policy highlight the interplay between the design of comprehensive regulatory mixes (Heldeweg & Kica 2011; Stokes & Bowman 2012) and the kinds of expertise necessary for these regulatory mixes to keep pace. Building on notions of reflexive governance, where responding to continuous sociotechnical change requires iterative feedback from regulated entities at each stage of the regulatory policy cycle (Sabel *et al.* 2018; Scott 2018), this article proposes a model that expands the scope of regulatory governance to (i) integrate more timely feedback from actors managing risks and uncertainties in complex sociotechnical systems on a day-to-day basis (Sowell 2019) and (ii) develop strong, explicit commitments to adapting rules in order to address new threats and vulnerabilities as they are identified.

To map the critical path from current regulatory responses to our model of adaptive regulatory governance design, this article identifies three types of emerging responses to IoT security risks – self-regulation, light-touch regulation, and centralized risk regulation – and evaluates them in terms of how effectively they plan for adaptations necessary to secure the IoT. We motivate our analysis by illustrating how poor IoT security poses new threats to consumers and the Internet's infrastructure, and how these threats expose regulatory gaps and misalignments that demand a more adaptive regulatory governance design. The model proposed here ensures timely updates of regulatory requirements by drawing on knowledge from operational epistemic communities' adaptive practices and mitigation mechanisms for managing security uncertainties endemic in a fundamentally transnational Internet. To explain and evaluate our model, we situate our proposal in the regulatory governance literature, in particular the emerging field of “planned adaptation in risk regulation” (McCray *et al.* 2010; Petersen & Bloemen 2015; Sowell 2019). We highlight why IoT security risk requires closer attention to adaptation in risk regulation, and, in particular, the importance of governance mechanisms that facilitate timely rule revisions as knowledge of new risks and vulnerabilities emerges.

The article proceeds in five parts. Section 2 introduces the key features of the “planned adaptive regulation” analytic framework used to evaluate whether emerging regulatory responses integrate the capabilities necessary to keep pace with emerging IoT security risk. To contextualize the impact and implications of an insecure IoT, Section 3 characterizes the IoT as a sociotechnical system that facilitates new threats to consumer protection and the Internet's infrastructure. Section 4 evaluates emerging regulatory responses, highlighting that each has some, but not all of the regulatory governance design features necessary to effectively plan for adaptation to new IoT security risks. We find that each lacks strong commitments to adapting rules based on a broader set of evaluative capabilities. In Section 5, we recommend a regulatory governance model that combines the benefits of a centralized risk regulatory regime – akin to the one emerging in the European Union – with the evaluative capabilities of operational epistemic communities whose monitoring and mitigation practices generate new knowledge of cybersecurity threats and vulnerabilities, as they emerge. One of the key challenges addressed by our model is developing knowledge sharing interfaces that tighten the feedback loops between centralized risk regulatory frameworks and operational epistemic communities, reducing regulatory lag by updating standards and requirements more dynamically, as new IoT security threats and vulnerabilities emerge.

2. Methods and evidence

In 2016, the Mirai attack became the largest Distributed Denial of Service attack on record at the time (Imperva 2016; Krebs 2016a). Powered by compromised IoT devices, this incident raised global awareness of the unprecedented impact of IoT security vulnerabilities. Since 2016, compromised Internet-connected toys, smart home locks, and smart meters have facilitated several data breaches (CisoMag 2020), ransomware exploits

(Oltermann 2017), and attacks on firms and critical infrastructures (Krebs 2016b), moving the challenge of IoT security from discussions amongst technologists to the top of governments' agenda.

2.1. Analytic framework: Planned adaptive regulation

Emerging technologies, such as the IoT, present decision-makers with a familiar yet wicked challenge: how to harness the socio-economic benefits of rapid technological innovation while mitigating the risks and unintended consequences associated with their adoption and use. This dilemma is especially acute when rapid technological advancements make it difficult to project all possible risks based on existing knowledge, giving rise to considerable uncertainty about how new technologies will be implemented, used and potentially misused. Consequently, we sometimes witness a lag between unexpected threats, as they manifest, and existing regulatory frameworks, which predominantly address known risks. This begs a question, which has been at the center of practitioner and scholarly inquiry in science and technology policy, risk regulation, and technology regulation: how do we adapt policies and regulatory requirements as new scientific and technical knowledge about emerging risks becomes available (McCray *et al.* 2010; Stokes & Bowman 2012; Petersen & Bloemen 2015; Bennett Moses 2016; Sabel *et al.* 2018)?

This question has motivated a number of interdisciplinary scholars and practitioners to investigate instances of "planned adaptation in risk regulation" (McCray *et al.* 2010; Petersen & Bloemen 2015; Sowell 2019). These comparative analyses evaluate how organizations plan for and adapt their policy decisions about emerging risks such that "underlying uncertainties are successively reduced – or at least better characterized – over time" (McCray *et al.* 2010, p. 952). Notably, the planned adaptive regulation literature goes beyond investigations into how organizations evaluate the benefits and limitations of alternative regulatory instruments, which has been a fruitful preoccupation of impact assessment practitioners and scholarly studies (Dunlop *et al.* 2012; Scott 2018; Dunlop & Radaelli 2019).

Instead, the planned adaptive regulation literature focuses on how "to further characterize and/or reduce the uncertainties in the assumptions made in past decisions" (McCray *et al.* 2010, p. 958) based on new knowledge about how threats and new risks manifest in the system itself. For instance, planned, periodic reviews of pollution levels are used to update established thresholds for particulate matter in the US and EU regulations (McCray *et al.* 2010). Similarly, the Dutch water defense regulations provide for continuous monitoring of water levels, tide, and storm surge in order to periodically review and adjust safety standards in the dykes system (Petersen & Bloemen 2015). By explicitly planning to incorporate new knowledge about emerging risk as it becomes available, these critical underlying assumptions or standards can be reviewed and adjusted without assessing entire regulatory instruments or mechanisms, reducing the lag between new scientific and technical knowledge and updates of salient elements in regulatory requirements.

The planned adaptive regulation framework aligns with the regulatory governance literature on responsive and reflexive governance models, which move beyond the assessment of different regulatory options toward understanding the variety of feedback mechanisms and sources of knowledge that allow for standards and norms revision in a more dynamic and participatory manner (Brownword & Somsen 2009; Black & Baldwin 2010; Scott 2018). Moreover, as illustrated above, the planned adaptive regulation framework focuses on identifying *ex post* evaluation mechanisms that do not rely solely on feedback about the regulated entities' behavior modification (Scott 2018, pp. 21–22), but on input from a broader set of actors with the capabilities to generate specialist knowledge about emerging risks which can inform timely regulatory adjustments (Sabel *et al.* 2018; Sowell 2019).

2.2. Method of analysis

Analytically, our study employs the "planned adaptive regulation" framework to comparatively evaluate the most notable regulatory responses that have emerged since the 2016 Mirai attack in order to tackle IoT security risks. The evaluation criteria build on comparative analyses of planned adaptive regulation established by McCray *et al.* (2010) and Sowell (2019). In their work, McCray *et al.* (2010, p. 952) identify two features that broadly characterize cases of planned adaptation in risk regulation:

1. "there is a priori commitment to subject an existing policy to *de novo* re-evaluation [emphasis in the original text] and

2. a systematic effort is made to *mobilize new factual information* for use when the re-evaluation takes place” [our emphasis].

Sowell (2019, p. 291) identifies an additional feature that facilitates systematic adaptations, especially in instances when emerging technologies create sociotechnical dependencies that are difficult to predict, generating uncertainties which require constant knowledge generation and rule assessment:

3. “the *evaluative capabilities* necessary to transform new information about the system into prescriptive knowledge about the (mis)alignment of primary rules with the system function” [our emphasis].

Translated to the IoT, our analysis below will address whether emerging regulatory responses (Section 4) consider these three features of planned adaptive regulation so that new knowledge about emerging IoT security threats (Section 3) is captured and translated into revisions of standards and regulatory requirements, in order to keep pace with emerging risks. Table 1 provides a summary of these features and explanatory questions, which informed our analysis.

2.3. Sources of evidence

The empirical findings presented below come from two projects funded in the United Kingdom and the United States which investigated, respectively: (i) the emerging standards, governance and policy responses to IoT cybersecurity risks¹; and (ii) the combined capabilities of operational communities, law enforcement, and policymakers to mitigate cybersecurity threats and systemic vulnerabilities.² Between 2016 and 2019, we actively engaged with key stakeholders shaping the policy and broader governance of IoT security risk. Table 2 summarizes the main policy-making, standards-setting, and operational fora that we took part in at the domestic and international levels.

Employing the “embedded researcher” and “action research” method of inquiry (Avison *et al.* 1999; Vindrola-Padros *et al.* 2017), we worked closely with these stakeholders to understand and define policy, standards, and technology governance problems pertaining to IoT security. To understand existing and ongoing responses, we conducted systematic reviews of emerging standards, regulatory, and operational responses to

Table 1 Operationalization of core features of planned adaptive regulation

Features	Key questions
Formal commitment to re-evaluation based on new knowledge	Do regulatory responses include re-evaluation commitments such as periodic reviews or threshold revisions in security standards or certification schemes, as new risk information becomes available?
Mobilization of knowledge about emerging risk	Is knowledge about emerging risk mobilized to meet the formal commitment to re-evaluate critical criteria (e.g. thresholds, baseline security standards)?
Evaluative capabilities to generate and transform new knowledge	What knowledge is mobilized for critical criteria evaluation? Is it pre-existing (known risks) or new knowledge about emerging security threats? Is it used to adapt critical criteria requirements?

Table 2 Sources of evidence

Policy stakeholder group	Description
Central government (UK)	Participation in the Expert Advisory Group for developing the <i>IoT Secure by Design Code of Practice</i> by the Department of Digital, Culture, Media, and Sport (DCMS).
National standards body (UK)	Participation in the <i>IoT/1 Technical Committee</i> of the British Standards Institution (BSI).
Operational community (transnational)	Participation in the <i>IoT Special Interest Group</i> within the Messaging, Malware and Mobile Anti-Abuse Working Group (M ³ AAWG)
Operational community (transnational)	Participation in <i>Anti-Phishing Working Group's</i> (APWG) works on combined capabilities to mitigate IoT risks.

increased IoT security threats and vulnerabilities, which we provided as evidence in stakeholders' decision-making processes. This review is summarized in Section 4 below. In addition, we became active members of standards-making and operational communities in order to better understand their decision-making and governance structures, how they manage cybersecurity risk in general and how they generate new knowledge and best practices about emerging IoT risks. This "action research" approach is a recognized form of knowledge co-production and has informed the adaptive regulatory governance model we propose in Section 5.

3. The IoT as a complex sociotechnical system

The Internet of Things is a disruptive technology that is expected to "reshape production, consumption, transportation and delivery systems," triggering a profound socio-economic shift further into the Fourth Industrial Revolution (Schwab 2017, p. 4). At a basic level, "the IoT embeds physical objects in information flows and thereby makes them 'smarter'" (OECD 2017, p. 88). Many of them are familiar products – toys, washing machines, and automotive vehicles – enhanced with Internet connectivity that potentially adds compelling new features and efficiencies.

However, these "smart objects" are only the endpoint of a larger sociotechnical infrastructure. The IoT is "an infrastructure of interconnected entities, people, systems and information resources together with services which process and react to information from the physical world and from the virtual world" (ISO-IEC 2018). This definition, adopted in an international standard, provides a clearer description of the IoT as a dynamic sociotechnical system which instruments our physical environment (Nurse *et al.* 2017, p. 22), creating tightly coupled human-cyber-physical interactions (Maple 2017) and, through its reliance on the Internet's infrastructure for connectivity, facilitating globally networked opportunities and risks. In addition, a core difference from traditional information communications technologies (ICTs) is the ease of deployment, persistence, and pervasiveness that characterizes the IoT (Tanczer *et al.* 2018b).

Embedding insecure IoT devices into this tightly coupled and highly dynamic sociotechnical system raises several concerns. At present, most IoT devices do not have sufficient storage and compute power to process, learn, and perform complex tasks on their own. They rely on Internet connectivity and remote computing resources to behave intelligently, integrating local data with larger datasets via cloud storage and by shifting complex analyses to cloud compute. Most IoT products available on the market have poor security controls, which make them both targets of and vectors for attacks on other services and infrastructures (Maple 2017; Yang *et al.* 2017). IoT devices are not just insecure, but relatively easy to compromise, even by low skilled actors (Boddy *et al.* 2019). Thus, insecure Internet-connected devices bring "new vulnerabilities that can extend to other systems," such as healthcare, transportation or the Internet's infrastructure (IRGC 2016, p. 3), facilitating globally networked risk, whereby causality and impacts are not always straightforward, generating unanticipated interactions between system components (Galaz *et al.* 2017).

In complex systems, innovation, and emerging risk are two sides of the same coin. Ideally, when a complex system adapts to user demands and inputs, those changes serve a constructive goal. In the IoT, this could mean more efficacious healthcare or convenient home management tools. We generally frame adaptations with positive effects as innovation. When adaptations created by malicious actors exploiting insecure devices give rise to emergent behaviors that increase risk – such as illicit access to personal health information or consumer devices that serve as launching points for attacks on the Internet's infrastructure – the IoT facilitates unanticipated threats. At the heart of this trade-off space is the general-purpose character of Internet connectivity and technologies that have been integrated into the IoT. Emerging risks are especially pernicious when, as with other Internet technologies, security is an afterthought (Anderson & Moore 2006). Below, we explore two instances of malicious adaptations of an insecure IoT's capabilities, focusing on threats to consumers and to the Internet's infrastructure.

3.1. Threats to consumers

Consumer protection laws are increasingly challenged by tightly coupled human-cyber-physical interactions. Taking the example of a smart burglar alarm, we show how poor IoT security can pose new threats to both safety and privacy. A smart burglar alarm is a product innovation designed to enhance functionality, physical security,

and safety by remotely alerting the owner if an unauthorized person attempts to gain access to a property. However, if compromised by malicious actors, it can be used to disable the intended safety functionality and to surveil the very consumers it is intended to protect, serving as a jumping-off point into the wider home management system, facilitating the compromise of other devices or systems (e.g. energy management) and causing a breach of privacy and data protection (e.g. accessing financial information). Thus, a single compromised IoT device acts as a gateway into the home management ecosystem, posing coupled risks to physical safety, personal security, and privacy.

In this example, the ability to connect to and repurpose (adapt) the device is the critical issue which alters its primary function, introducing new risks that are not compatible with the product's intended use and are inconsistent with the level of consumer protection that most product safety laws currently require (EC 2001, Art 2(b)). A large number of smart consumer goods are reported to have poor security controls and policies, such as default passwords, inadequate vulnerability disclosure policies, or insufficient software coverage over the product's lifespan (DCMS 2018a; Blythe *et al.* 2019). In the EU, several consumer groups conducted tests on smart products and found that a majority – including children's toys – allowed the installation of malicious applications that could take remote control of devices, monitoring activity without the owners' awareness (BEUC 2018). While cybersecurity is increasingly seen as contributing to greater consumer and business protection, low margins in global electronics markets incentivize manufacturers to develop smart products without investing in costly IoT security features and policies (Nicolescu *et al.* 2018).

Because cybersecurity risk is not a consideration in existing product safety legislation, insecure IoT devices pose new challenges to consumer protection, which we categorized as: misalignment between risk-based regulations for product safety and security; and growing information asymmetries between consumers, IoT manufacturers, and digital service providers. We explore these below.

In most jurisdictions, consumer protection laws are based on a risk regulatory approach: regulators set standards and requirements for products and services based on an evaluation of known risks or risk-risk trade-offs (Black 2005, 2010). For the majority of consumer goods, manufacturers have the responsibility to showcase compliance with baseline standards and best practices through certification and labeling schemes (Blythe & Johnson 2018). This regulatory approach has worked well in the past, especially for product safety, as it emphasized "certainty and knowability over uncertainty" (Black 2005, p. 511) – that is known risks versus uncertainty.

The example of the smart burglar alarm above illustrates how insecure IoT can cause harm not directly associated with its physical properties. As noted by consumer protection organizations, current product safety legislation "neither accounts for harm caused by deficient services nor vulnerabilities that occur by strangers accessing and misusing a connected product" (BEUC 2018, p. 1). Thus, an insecure IoT generates opportunities for new adaptations that create harms and vulnerabilities affecting the protection of personal data, the security and the physical safety of consumers (FTC 2018). These new types of harm highlight the misalignment between current regulatory frameworks which address digital and physical risk separately: electronic privacy and data protection on the one hand (digital risk), and safety on the other hand (physical risk) (Brass *et al.* 2017).

An insecure IoT also confounds consumers' ability to make informed decisions about connected products. Consumer International noted that "[a]s products and devices carry out different functions and link to more systems, they will become more complicated and it may become difficult for consumers to have full clarity on how they work" (2016, p. 28). Reduced consumer awareness about the implications of cybersecurity risks is particularly endemic in the IoT consumer goods market populated by products with poor security controls and policies (Blythe *et al.* 2019). Absent formal recognition of cybersecurity risk in current product safety legislation, the IoT generates new information asymmetries between consumers, smart product manufacturers, and providers of IoT services.

Moreover, without awareness about the risk implications of connected devices, consumers might translate the same level of trust in conventional consumer products to their IoT counterparts (Blythe *et al.* 2019). This is exemplified by "set and forget" consumer practices, whereby users of smart products set them up, enjoy their benefits, and forget their digital maintenance. Consumers are largely unaware that the lifespan associated with IoT software is substantively different, and typically much shorter, than the lifespan of the physical viability of that product. In addition, consumers are unaware of how the degree of autonomy and interaction of IoT devices

with other connected systems facilitate adaptations to the “out-of-the-box” behavior of products without the users’ knowledge (Noto La Diega 2016; Manwaring 2017).

Following our characterization of innovation and emerging risks, IoT cybersecurity – or the lack thereof – is a fundamental characteristic that can generate substantive externalities for consumers. Implemented responsibly, the IoT facilitates innovations that enhance functionality. Implemented poorly, it facilitates emerging risks to physical security, safety, and privacy that are not captured in current regulatory frameworks.

3.2. Threats to Internet infrastructure

Many of the factors that contribute to IoT-based consumer threats – poor security, affordability, pervasiveness – also contribute to unprecedented threats to the Internet’s infrastructure. Unlike threats to consumer protection, which can be addressed by regulatory changes in a particular jurisdiction, attacks against the Internet’s infrastructure are often facilitated by compromised devices deployed across many jurisdictions. Attacks focus on a target’s infrastructure, such as the Mirai attacks on Dyn and Deutsche Telekom (described below), and their geographic distribution makes for resilient, transnational cybercrime-as-a-service platforms that can attack targets around the globe, limiting the efficacy of individual jurisdictional responses. These threats have direct socio-economic effects on the resilience of the global Internet infrastructure, raising questions about the effectiveness of domestic regulatory frameworks when dealing with IoT risk.

Threats to the Internet’s infrastructure are compounded by three factors: the aggregate effect of IoT compromises at scale; the geographic distribution of vulnerable devices; and the dynamic character of IoT malware. When IoT vulnerabilities are systematically leveraged by cybercriminals as the building blocks for crimeware-as-a-service, the threat scales, creating markets for illicit operations such as phishing campaigns, exfiltration of private consumer information, and most notably DDoS attacks of unprecedented magnitude. Diverse geographic distribution creates globally networked risks: compromised devices in one jurisdiction are used to attack targets in other jurisdictions, requiring transnational coordination to mitigate and remediate. We explore these below.

Mirai surfaced as a known IoT malware in August 2016, becoming one of the most impactful malware families, attacking prominent web services and infrastructure providers in its first three months (Antonakakis *et al.* 2017). The September 2016 Mirai attack on OVH was, at the time, the largest DDoS in the history of the Internet. Mirai’s most well-known attack on domain name system infrastructure provider Dyn in October 2016 took down high profile web services such as the New York Times, Twitter, and Spotify (Krebs 2016b). In November 2016, a Mirai variant attacked Deutsche Telekom (Goodin 2016). Mirai not only scaled in terms of the number of infections, but it also scaled geographically. Targets were “distributed across 906 [networks] and 85 countries, [...] heavily concentrated in the U.S. (50.3%), France (6.6%), and U.K. (6.1%),” (Antonakakis *et al.* 2017, p. 1104). Mirai’s spread highlights that malware, like licit Internet applications, defies jurisdictional boundaries, garnering much of its utility from the global reach of a fundamentally transnational Internet.

An underestimated yet a distinctive feature of IoT malware is the impact of seemingly innocuous, “low-power” devices. Conventional malware infects “high powered” devices such as desktop computers and laptops. Mirai botnets comprise substantively lower-powered consumer devices. Despite this difference, the scale of infection yielded the second largest DDoS on record and continues to evolve to compromise new devices (Nigam 2019).

The media frequently refers to Mirai in the singular. Like conventional malware, Mirai is a family of malware variants, continuously adapted by cybercriminals to leverage new IoT vulnerabilities. With the October 2016 Mirai source code release, cybercriminals commodified Mirai. Variants were deployed by diverse cybercrime operational networks, some of which attacked each other. In Mirai’s first seven months, at least 33 independent cybercrime operational networks launched 15,194 DDoS attacks (Antonakakis *et al.* 2017, p. 1104).

Mirai also illustrates how conventional analyses miss the systemic risks to the Internet’s infrastructure. Many IoT devices – like the connected video cameras and home routes compromised by Mirai – are always on and always connected to the Internet. Even when reset, they are quickly re-infected. Taking these factors together, insecure IoT devices become the ideal commodity building blocks for cybercrime operational networks, facilitating markets for illicit resources that are easily accessed, leveraged, and adapted, creating a globally networked threat.

The cross-jurisdictional character of IoT threats is one of the biggest challenges for conventional risk regulation. This does not mean risk regulatory approaches should not be pursued or ignored. Rather, the dynamic, systemic character of IoT threats highlights the need to supplement jurisdictional regulatory interventions with regulatory governance arrangements that incorporate more efficient feedback mechanisms necessary to keep pace with the evolving IoT threat landscape.

4. Regulatory responses to IoT threats

In the previous section, we showed how IoT device security vulnerabilities can generate spillover risks to individual safety, privacy, and data protection, and can be exploited en masse to attack part of the Internet's critical infrastructure. These examples show how the IoT behaves as a disruptive sociotechnical system, whereby it is difficult to predict all possible risks resulting from its adoption, creating uncertainties for users, developers, and policymakers.

In Subsections 4.1–4.3 below, we provide a review of the most notable regulatory responses to date aimed at addressing IoT security vulnerabilities as a source of emerging risk. Using the “planned adaptive regulation” framework (Section 2), we explore three emerging regulatory trends, which we broadly classify as self-regulation, light-touch regulation, and centralized risk regulation, noting that each of these responses is at an early development stage, much like the IoT itself. We reflect on the benefits and limitations of these regulatory responses in addressing the three features that allow for planned regulatory adaptations when new knowledge about IoT security risks emerges:

1. formal commitment to rules re-evaluation based on knowledge of emerging risks;
2. new knowledge mobilization;
3. evaluative capabilities to generate new knowledge and transform it into revised critical criteria and regulatory thresholds.

Our analysis highlights that while many of the responses analyzed below have some of the features of a planned adaptive regulatory framework, none of them have all of the three necessary features. In particular, the analysis highlights limited formal commitment to rules re-evaluation (1) and, crucially, deficits of evaluative capabilities (3), setting the stage for understanding the role that external evaluators can play to provide the knowledge necessary for regulatory interventions to keep pace with emerging IoT threats, as they evolve.

4.1. Self-regulation

Rising IoT adoption rates and their attendant security vulnerabilities have accelerated the development of market-driven standards. The number of industry consortia and standards-making bodies developing technical guidelines and codes of practice for IoT security is rising, as reported by the EU Agency for Cybersecurity (ENISA 2017) and the U.S. National Institute of Standards and Technology (NIST 2018). Most of these standards established baseline requirements that directly address critical IoT security challenges, such as stronger authentication requirements in response to weak passwords or system segregation architectures to isolate compromised IoT elements in case of attacks. Moreover, industry consortia and some standards-making bodies have established their own testing, verification, and certification schemes for IoT products and systems (Brass *et al.* 2018, p. 5).

These voluntary initiatives have the advantage of providing timely baseline requirements (standards) for IoT security which draw on expert knowledge about reported device vulnerabilities, extensive use case analyses, threat and asset mapping, or risk management requirements, to name but a few. Because voluntary standards set technical or procedural norms through a consensus-driven process, they are generally understood and referred to as “consensus knowledge” derived from industry and other experts’ input (Steedman 2017). Thus, these self-regulatory initiatives meet two of the three features of planned adaptive regulatory models: they mobilize new knowledge about reported IoT security risks (2) and draw on the evaluative capabilities of experts to transform this knowledge into critical criteria or standards (3).

However, by virtue of their voluntary nature, self-regulatory initiatives exhibit a crucial limitation. They rarely make formal commitments to when critical criteria re-evaluations will occur and whether these are triggered by

new risk knowledge or other considerations such as members' priorities or interests (1). Consequently, most technical or procedural standards capture known risks – i.e. the risk information available at the time of the production of the standard. And, while most formal or informal standards-development organizations have review processes in place, these are rarely based on automatic triggers for critical criteria re-evaluation as new risk information becomes available.

The early development of voluntary IoT security standards exhibits this limitation. As more industry consortia and technical alliances produced IoT security standards, checklists, and testing and certification schemes, the standards landscape became more fragmented (Brass *et al.* 2018). This fragmentation translates into considerable knowledge coordination challenges, given that the critical criteria specified in the standards vary considerably in scope and risk assessment method. For instance, some standards focus on IoT security from a design perspective, others from a networking perspective, while others from an organizational management perspective. This knowledge coordination challenge is recognized in standards-making processes for emerging technologies. In a recent study conducted for the British Standards Institution (BSI) – the UK's national standards body – IoT SMEs reported challenges selecting the most relevant IoT security standards for their business and understanding how to implement these alongside existing standards and regulatory requirements for product safety or data protection (Brass *et al.* 2019, pp. 5–10). In addition, they reported the need to supplement technical specifications or procedural standards for risk management with new mechanisms that would allow them to tap into the latest information about IoT security vulnerabilities. As a top priority, they proposed that national standards bodies or regulatory agencies establish or coordinate “live repositories of IoT vulnerabilities and best practices” in order to capture the latest information about emerging IoT risks (Brass *et al.* 2019, pp. 12–13).

In conclusion, emerging self-regulatory responses benefit from expert knowledge mobilization and the evaluative capabilities provided by standards-makers, who are generally representatives from industry, consumer associations, or academia. They also facilitate the establishment of baseline requirements in the absence of other regulatory interventions, helping set technical or procedural norms for managing the risks of disruptive technologies. However, the IoT security standards landscape also reveals that self-regulatory responses tend to address known risks and have review processes that do not capture the dynamic nature of IoT vulnerabilities. Besides this risk assessment lag, they create knowledge coordination challenges because their scope, assessment, and re-evaluation methods differ considerably.

4.2. Light touch regulation

In response to the increasingly fragmented standards landscape for IoT security, some governments are developing their own initiatives for establishing baseline requirements for IoT security. Below, we present two of the most notable proposals that we categorize as “light touch regulation” in the United States and the United Kingdom. Both responses started from a common approach to promote voluntary codes of practice for IoT security, which incorporated critical requirements from existing standards while trying to eliminate the duplication and landscape navigation challenges presented in Section 4.1 (DHS 2016; DCMS 2018b). Beyond this common starting point, their respective regulatory proposals diverge. Light touch regulatory approaches do not follow a single template. In general, they are associated with a preference against regulatory prohibitions and restrictions, taking the form of principles-based or outcomes-based regulation, allowing regulated entities to set their own means of attaining regulatory objectives (Etienne *et al.* 2018).

In the US, a legislative proposal – *The IoT Cybersecurity Improvement Act* – was first introduced in 2017 and is currently due its first reading in the Senate (S.734 – 116th Congress). The Bill went through several amendments but maintains its core structure. The objective is to ensure that IoT government procurement follows the latest security standards established by the National Institute of Standards and Technology (NIST). The Bill asks for “Contractor and vendor compliance with policies and procedures – the procedures [...] shall include a limitation that prohibits an agency from acquiring or using any Internet of Things device from a contractor or vendor if [they] fail to comply with the guidelines published under section 5(a) [by NIST]” (Art 6c, S734). Section 5 stipulates NIST set “guidelines on coordinated disclosure of security vulnerabilities relating to information systems, including IoT devices” (Sec 5, S734). Thus, this proposal does not specify technical requirements for IoT security. Instead, it requires vendor compliance with guidelines established by the national standards body. At present,

NIST has produced several standards, the most notable being the *Recommendation for IoT Device Manufacturers*, a procedural standard currently in its second draft, which advises manufacturers how to conduct a risk assessment for their IoT devices (Fagan *et al.* 2020).

In the UK, the approach was different. In 2019, the government consulted on a proposal for a legislative framework that would mandate conformity with the top three principles of the *Code of Practice for Consumer IoT Security* (DCMS 2018b). The regulation would be implemented via a labeling scheme which “[m]andates retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self-assess [against the three guidelines] and implement a security label on their consumer products” (DCMS 2019, p. 14). The three guidelines are:

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated

However, the government proposed a binary labeling scheme, whereby manufacturers self-declare if they do or do not conform to these specifications. For instance, a positive IoT security label would state, “essential security features included,” referring to the three guidelines above. A negative label would state, “essential security features NOT included” (DCMS 2019, p. 13). Consequently, as long as IoT consumer products have one of these labels, they will continue to be sold on the UK market, making this a light-touch intervention which does not eliminate poor security products from the market – or them connecting to the Internet’s infrastructure – it just labels them as either having met or not the three requirements.

Addressing the three features of planned adaptive regulation, the light touch approaches presented above carry some clear benefits, but also some limitations. With regard to feature (1), neither proposal makes a clear commitment to re-evaluate critical requirements based on new IoT security knowledge. With regard to features (2) and (3), there is a considerable difference between the two proposals. The US proposal emphasizes the importance of establishing coordinated disclosure of IoT security vulnerabilities (Sec 5 S734), and tasks the national standards body with setting these guidelines. The UK proposal relies on a labeling scheme based on known IoT security risks, such as default passwords, but does not specify whether these will be re-evaluated based on new risk knowledge and who is charged with their adaptation. Thus, the US proposal appears to integrate the flexibility necessary to respond to the dynamic nature of IoT security risks more proactively than the UK approach, drawing on the evaluative capabilities of the national standards body to publish guidance on the procedures for reporting, coordinating, publishing, and receiving information about future vulnerabilities (Sec 5(a) S734).

4.3. Centralized risk regulation

In contrast to the light-touch regulatory approaches which are emerging in the US and the UK, a different model is developing in the European Union (EU). We categorize this response as an emerging centralized risk regulation regime because it relies on the establishment of a cybersecurity agency and the adoption of regulations which specifically tackle cybersecurity risks.

In 2019, the European Parliament and Council adopted Regulation (EU) 2018/881, known as *The Cybersecurity Act*. Broadly, the Act has two pillars. First, it establishes ENISA – the former European Union Agency for Network and Information Security – as the EU Agency for Cybersecurity, tasked primarily to ensure harmonized implementation of cybersecurity policy across the Member States and to support with capacity-building and cyber resilience (Art 4 and 5). Second, it stipulates the establishment of a European cybersecurity certification framework (Art 46), and tasks ENISA to maintain a database of existing and obsolete certification schemes, including statements of conformity by manufacturers or providers of ICT products, services, and processes (Art 46–52). In addition, it sets the assurance levels for the European cybersecurity certification scheme (Art 52) and specifies that statements of conformity are based on self-assessment and are initially voluntary, but this requirement can be reviewed at a latter point (Art 53–54). While declaring conformity is currently voluntary, the overall structure of this emerging cybersecurity regime resembles existing risk regulatory regimes in the EU, such as product safety, which are based on the establishment of a specialized agency with oversight responsibilities, clear safety baselines, self-assessment, and conformity reporting.

This centralized risk regulatory approach has a number of features, which resemble the planned adaptive regulation framework presented in this paper. First, the Regulation identifies the IoT as an emerging digital technology that contributes to increasing cybersecurity risk, but brings it into a broader regulatory framework, without focusing too closely on its existing vulnerabilities. Importantly, it gives ENISA new powers to “develop its own resources, including technical and human capabilities and skills” (Art 3(4)) necessary to perform its duties as a Cybersecurity Agency charged with building and reviewing the cybersecurity certification framework (Art 8), ensuring operational cooperation at the Union level (Art 7), and “performing long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents” (Art 9). Thus, the Regulation makes a formal commitment to re-evaluate cybersecurity practices, standards, and emerging risks and tasks ENISA to keep this information up to date. This corresponds to feature (1) of the planned adaptive regulation framework.

Before becoming the EU Cybersecurity Agency, ENISA was a quasi-formal European coordination mechanism that facilitated information-sharing and best practice about managing cybersecurity threats. At its core, ENISA acted as a coordination platform for Computer Emergency Response Teams (CERTs) in Europe, not just the EU. The CERTs perform a critical function: they identify and sometimes respond to cybersecurity incidents, and share this knowledge with other stakeholders, including other CERTs and government agencies, to prepare for future responses (Tanczer *et al.* 2018a). Regulation (EU) 2019/881 maintains this commitment for ENISA to provide a “knowledge and information” platform (Art 9), by tapping into and mobilizing operational knowledge. This corresponds to feature (2) of the planned adaptive regulation model.

However, while Regulation (EU) 2019/881 provides these two features of planned regulatory adaptation, it does not indicate connections between ENISA’s information convening role and the cybersecurity certification framework. Requirements for manufacturers, developers or CERTs to provide and share knowledge once a cybersecurity incident occurs are a very promising first step. However, it is not clear whether pre-incident knowledge resulting from constantly monitoring network traffic and emerging vulnerabilities is captured within ENISA’s responsibilities. For instance, ENISA recently published a review of software security practices to inform the certification framework, which identifies the development of a “common repository for shared security measures” as a priority, though most of this information would be generated by manufacturers of Internet-connected products and other ICT providers (ENISA 2019, p. 12).

Consequently, this centralized risk regulatory response addresses the main knowledge coordination challenges exhibited in self-regulatory alternatives and the main knowledge mobilization challenges identified in light-touch regulatory responses. However, for this centralized risk regulatory model to stay responsive to emerging cybersecurity risk, it requires constant monitoring of vulnerabilities as they develop, not only at the point of or after impact, which is feature (3) of a planned adaptive regulatory framework. Considering a broader pool of evaluative capabilities is crucial in order to ensure that emerging risks, at the monitoring rather than at impact stage, are captured and translated into new regulatory requirements.

In conclusion, each of the regulatory responses described in this section have some, but not all, of the features of a planned adaptive regulatory regime. The two that are closest to this model are: the US light-touch regulatory proposal and the centralized risk regulatory approach emerging in the EU, which tasks ENISA to act as a coordinator of emerging cybersecurity risk, including IoT security risk. The procedural requirements in the US approach identify NIST as the authoritative source of guidelines for coordinating vulnerability disclosure (mobilizing knowledge of risks) and corresponding risk analyses (guidelines for evaluating risks). That said, it does not provide the necessary systematic commitments to re-evaluation. In the EU, ENISA does incorporate a number of commitments to re-evaluate and collaborate with external evaluators that lend themselves to a planned adaptive framework. However, it remains unclear how systematically these commitments will be acted upon. Further, and most importantly, it is not clear whether knowledge used for re-evaluation is post-incident (such as data from CERTs or manufacturers) or whether it includes pre-incident indicators that require monitoring within the Internet infrastructure. To fill these gaps, the next section argues for a planned adaptive regulatory model that builds on the centralized risk regulation approach, supplementing it with governance mechanisms that mobilize knowledge created by actors that constantly monitor cybersecurity vulnerabilities at play in the Internet’s infrastructure.

5. Adaptive governance of emerging sociotechnical risks

Ensuring governance mechanisms keep pace with dynamic, evolving IoT threats requires iterative feedback mechanisms for integrating new information about cybersecurity risk back into the design and codification of existing standards and regulatory requirements. As Mandel argued, “designing a flexible governance system that can respond to changing knowledge and information is necessary to optimally handle the benefits and risks of emerging technologies” (2009, p. 78). Such adaptive regulatory governance mechanisms must effectively mobilize new factual knowledge critical to creating and maintaining security standards that keep pace with a constantly evolving IoT. In this section, we first describe operational epistemic communities as actors that already have the evaluative capabilities necessary to monitor and mitigate emerging (pre-incident) cybersecurity threats as a potential source of knowledge about emerging IoT risks. In the second half of this section (Section 5.2), we draw on the broader “technology regulation” literature to describe and evaluate the kinds of governance mechanisms – in particular the notion of a knowledge-sharing interface – necessary for these operational epistemic communities to supplement a centralized risk regulatory framework in a way that meets the criteria of all three features of a planned adaptive regulatory regime.

5.1. The role of operational knowledge from transnational epistemic communities

Network operations and cybersecurity communities – engineers, technicians, and analysts that manage and coordinate the day-to-day security and operations of the individual networks that make up the global Internet – have long recognized that no single actor has sufficient purview into the Internet’s decentralized, yet interdependent infrastructure to mitigate and remediate cybersecurity threats alone (The Rendon Group 2011; Sowell 2018). For these transnational communities, the continuous co-production of knowledge to understand, mitigate, and remediate emerging cybersecurity risks is a critical necessity, not an option. These actors recognize that best practices must necessarily change to keep pace with innovations by cybercriminals. Adaptive governance of operational practices is the norm within these communities, not the exception. Information and knowledge about these distributed, decentralized threats does not necessarily become obsolete, but it does quickly become incomplete. Mobilizing collaborative practices among these communities to iteratively create, update, and distribute knowledge about emerging threats is critical to developing a responsive, adaptive regulatory model for IoT security.

Like conventional threats from compromised personal computers and smart mobile phones, understanding emerging transnational threats like Mirai requires integrating local insights to understand, then collaboratively mitigate, these transnational network externalities. Unraveling how to mitigate and defend against IoT threats requires expertise in software development, operating systems, networking, and Internet communications protocols. To protect both their own networks, and the Internet more broadly, network operators have developed collaborative practices for sharing information about: how malware spreads from device to device, how it infects and/or damages systems, and the technical and operational strategies for how to stop it. These actors share information such as how to identify vulnerable systems, quick fixes to mitigate these vulnerabilities, tools and methods for identifying indicators of infection in network traffic, and how to filter this traffic to mitigate attacks and further infection. They not only share this information, but also share experiences applying these strategies, reasoning about these strategies’ efficiency and efficacy, and iteratively transforming this information into experience-based cybersecurity knowledge and best practice (Fig. 1).

Generalizing these pragmatic steps, three interdependent, yet conceptually distinct classes of collaborative practices can be identified, creating feedback loops that enhance these actors’ understanding of the threats, improve monitoring and threat identification, ultimately facilitating rapid, iterative threat mitigation (Fig. 1). First, as novel threats emerge, information sharing focuses on understanding a new threat. Second, as these understandings are developed, they are iteratively applied to develop and update immediate mitigation tactics to limit damages and to improve the coordination strategies intended to identify sources of attack and infection. Third, as mitigation reduces the immediate threat, the knowledge generated about how to mitigate, and in many cases how to remediate, is codified and distributed more broadly through organizations such as M³AAWG (M³AAWG 2020), the Anti-Phishing Working Group (APWG 2019a), Information Sharing and Analysis Centers (ISACs) (National Council of ISACs 2020), and Computer Emergency Response Teams (CERTs) (Tanczer *et al.* 2018a).

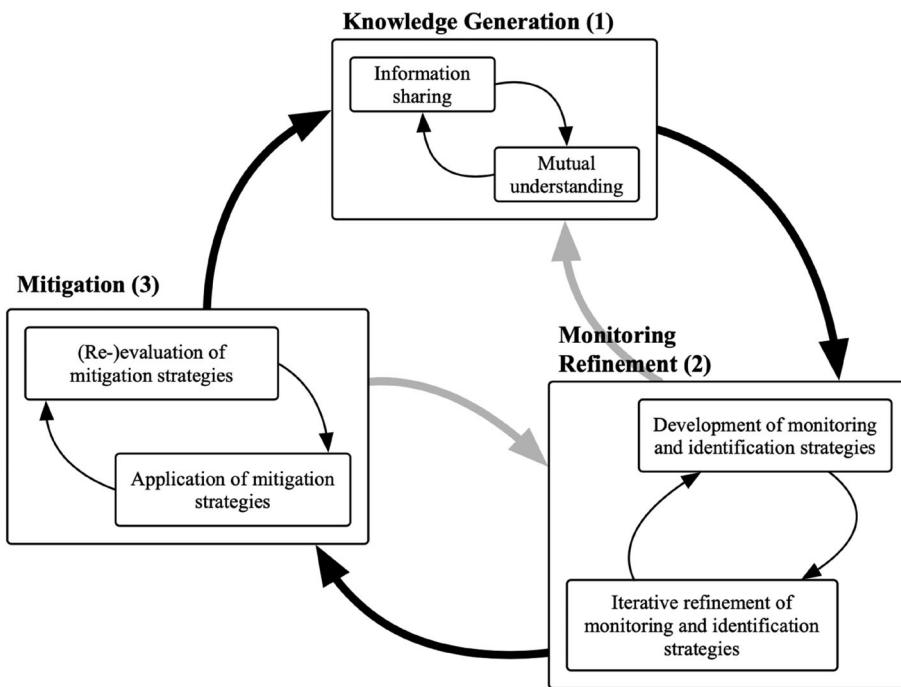


Figure 1 Iterative feedback processes within cybersecurity operational communities.

While these pragmatic steps are described linearly to convey the key concepts, the power of these communities lies in the nested, iterative feedback loops depicted in Figure 1, continuously refining monitoring information into risk indicators applied to mitigate new threats as they emerge and evolve. These knowledge generation processes create what was categorized as pre-incident knowledge in Section 4. It is important to stress that these processes generate knowledge of emerging threats and potential risks as they are evolving. Some of the participants in the organizations listed above do engage in and support these feedback loops, serving as convening fora and knowledge dissemination organizations that help coordinate incident response with external actors (such as regulatory agencies and law enforcement) and the dissemination of knowledge, often codifying the mitigation strategies developed in step three as best practices.

These cybersecurity communities are decentralized, yet form a transnational, interdependent network capable of quickly mobilizing new information and knowledge about cybersecurity threats among its members. Albeit nonhierarchical, these actors form close-knit groups where “informal power is broadly distributed among group members and the information pertinent to informal control circulates easily among them” (Ellickson 1991, pp. 177–178). These norms and the attendant governance mechanisms are familiar to the literature on adaptive and collaborative regulatory regimes. Sabel *et al.* “call such systems of regulation under uncertainty recursive, or, drawing on American Pragmatism, experimentalist, because they continuously revise initial and inevitably incomplete understandings of hazards in light of shortcomings revealed by efforts to address them,” (Sabel *et al.* 2018, p. 372). Iterations of the feedback loops above represent pragmatic experiments in which norms, best practices, and strategies are evaluated based on their efficacy when coping with emerging threats such as IoT insecurity.

Moreover, these adaptations are proactive, mobilizing evaluative capabilities when needed to address threats as they are identified and develop (Sowell 2018). Thus, a responsive governance regime for managing IoT threats demands all three features of a planned adaptive regulatory model: evaluative capabilities that generate and update knowledge of emerging threats apace with innovations in cybercrime (feature 3); a regulatory governance design focused on mobilizing these actors’ knowledge into standards and regulatory requirements (feature 2), and formal mechanisms that ensure commitment to rule re-evaluation as knowledge about emerging risks becomes available (feature 1).

5.2. An adaptive regulatory governance model for emerging IoT risks

In this section, we recommend strategies for integrating the knowledge generated by operational epistemic communities into emerging risk regulatory frameworks for cybersecurity. In order to tackle the dynamic nature of IoT risk, we propose supplementing the strengths of centralized risk regulatory frameworks with iterative feedback from operational epistemic communities. The planned adaptive security governance model proposed here combines formal commitments to re-evaluation possible in centralized risk regulatory frameworks with procedural requirements for updating standards and critical risk criteria based on knowledge generated by operational epistemic communities. Under this model, IoT security baselines are not static, based solely on known risks recognized at the initial development of a standard/regulatory requirement. Rather, they facilitate updating IoT security specifications and critical criteria, such as thresholds for evaluating the impact of emerging IoT threats, as knowledge of “live” security vulnerabilities become available.

A way of achieving this adaptive regulatory governance design is developing a knowledge sharing interface between centralized risk regulatory frameworks and operational epistemic communities. This knowledge sharing interface facilitates the joint problem-solving and mutual understandings necessary to effectively trigger commitments to re-evaluation based on knowledge generated by the distributed evaluative capabilities of operational epistemic communities. For instance, one element of such an interface may be a vulnerabilities repository (such as described in Section 4.1), provisioned or coordinated by a national standards body (as described in Section 4.2) or a cybersecurity agency such as ENISA (as described in Section 4.3), and populated with “live” risk knowledge from operational epistemic communities. These repositories would allow regulatory agencies to access the latest information about IoT security vulnerabilities, to jointly evaluate its impact with the operational and technical communities, and establish whether critical criteria in standards, certification schemes, or other regulatory instruments need to be revised. In effect, this model would facilitate “building options into final rules” and “instituting a somewhat standardized process for modification [which] allows such change to become part of the expected governance system” (Mandel 2009, p. 89), as increasingly recommended in the literature on the regulation of emerging technologies.

Moreover, this model would mitigate some of the knowledge deficits that we encounter when devising risk regulatory regimes based on known risks, at the time of rule development. Even when regulatory regimes have the first two features of planned adaptation, they often lack the necessary interface with actors that have the evaluative capabilities to identify new classes of disruptive dynamics. In the case of the IoT, these disruptive dynamics are the vulnerabilities exploited by cybercriminals “in the wild,” which can only be observed in a timely manner from within the system, rather than, for instance, being reported by product manufacturers after an incident occurred. As noted by Sabel *et al.*, the deficiencies faced by conventional risk regimes are often a consequence of “technological constraints: complex, continuous process operations with interdependent subsystems that transmit disruptions rapidly, often in unforeseen and self re-enforcing ways [...]” (Sabel *et al.* 2018, p. 373).

These deficiencies are not universal, though. McCray *et al.* (2010) highlight that, although rare, select regulatory agencies have explicitly planned the development of knowledge sharing interfaces to overcome them. While this balance is currently the exception in risk regulatory regimes (McCray *et al.* 2010; Sabel *et al.* 2018), it is not unprecedented. For instance, the National Transportation Safety Board (NTSB) in the US has invested in “go-teams” that leverage deep technical and operational knowledge to credibly assess civil aviation accidents in terms of whether safety rules need to be updated, then works with the Federal Aviation Administration (FAA) to implement these updates (McCray *et al.* 2010, p. 955). This relationship, like the relationship we propose between operational epistemic communities and a cybersecurity agency, illustrates that planned adaptive regulation is rare, but possible. However, as the case of the NTSB and the FAA shows, the regulatory governance design must ensure effective mechanisms for mobilizing new knowledge necessary for re-evaluation, but also ensure the independence and credibility of the evaluator.

In these cases, planning for adaptation requires the explicit design of governance mechanisms that establish a formally codified interface between a regulatory body committed to systematically re-evaluate regulatory requirements and standards as new knowledge becomes available (features (1) and (2) of planned adaptive regulation) and organizations with the evaluative capabilities necessary to generate the knowledge needed to inform rules re-evaluation (feature (3) of planned adaptive regulation). In cybersecurity, the features of a planned adaptive regulatory regime are often distributed across multiple organizations (Sowell 2019), requiring collaboration and the

co-production of knowledge to effectively cope with the dynamics of disruptive technologies. Thus, for planned adaptive regulation of IoT risks, the challenge is not just specifying what a knowledge-sharing interface should look like, but identifying the respective organizational capacity necessary to implement it to commit the regulatory body and operational epistemic communities to effectively engaging across that interface. While the discussion about the required administrative capacity goes beyond the scope of this article, we offer some suggestions below.

Transnational organizations such as M³AAWG and APWG are convening fora for operational epistemic communities that may also serve as potential links to characteristically distributed operational epistemic communities. As noted earlier, some, but certainly not all, of these organizations' participants are actors in these operational epistemic communities. Organizations such as M³AAWG and APWG have increasingly invested in elements of the knowledge-sharing interface, in particular, engagement with policy and regulatory actors. M³AAWG's Public Policy Committee regularly provides public feedback on policy and regulatory issues affecting cybersecurity (M³AAWG 2019), as well as collocating meetings with UCEnet, an organization that brings together regulators and law enforcement from around the globe to share information and knowledge on fighting unsolicited communications (UCENet 2020). The APWG has worked with the Council of Europe and the EU Commission on online user safety initiatives (APWG 2019b) and the implications of regulations such as the GDPR on information sharing practices necessary to mitigate cybercrime (APWG). While this selection of initiatives illustrates a progressive, regular, informal commitment to transmitting new knowledge to government actors, it does fall short of the formally codified commitments necessary for a planned adaptive regulatory regime.

An adaptive regulatory governance model for the IoT will require complementary changes in evaluative capabilities, and the supporting organizational capacity, necessary for information sharing and the co-production of knowledge by both conventional regulatory regimes and operational epistemic communities. Despite the structural differences (vertical hierarchy and nonhierarchical close-knit communities), Mandel highlights the incentives at play that can lay the foundations for these changes: "mutual concerns about [technological and regulatory] uncertainty not only provide normally opposed stakeholders incentives to work together, but also could be exploited to produce agreement on a particular governance system" (Mandel 2009, p. 81). Both are concerned with mitigating and remediating IoT security threats. This approach resonates with the epistemic communities literature, identifying a "common policy enterprise...to which [epistemic communities'] competence is directed" (Haas 1992, p. 4). To take advantage of the incentives to engage in a common policy enterprise, participants on both sides must actively engage in joint problem solving, distinguishing "reflexivity from traditional bargaining" (Scott 2018, p. 18).

The model of planned adaptive regulation presented here is one of many possible organizational arrangements that can facilitate planning for the adaption necessary to manage the uncertainty endemic in disruptive technologies. Applied to the IoT, this initial model integrates the strengths of centralized regulatory frameworks with the dynamic, responsive capabilities of operational epistemic communities. For both the IoT and disruptive technologies more broadly, regulatory models will need to look beyond the cyclical evaluation of risk regulatory instruments. Regulatory governance design must consider the governance mechanisms and administrative capacities necessary to create a knowledge-sharing interface that can update instruments apace with changes in continuously evolving sociotechnical systems such as the IoT.

6. Conclusions and implications

The IoT illustrates important considerations for the regulation and governance of disruptive technologies. IoT technologies are continuously being adapted to new constructive innovations – such as smart home management, healthcare, and transportation – as well as to new illicit purposes that threaten both consumers and the Internet's infrastructure. The IoT is celebrated for generating positive externalities but demands a regulatory model that can keep pace with emergent negative, often globally networked, externalities that are difficult to manage. Such a model requires commitments to establishing feedback mechanisms that identify and adapt the standards and regulatory requirements of an evolving IoT. Analytically, these feedback mechanisms require "changing the frame from 'regulating technology' or 'regulating new technology' to 'adjusting law and regulation for sociotechnical

change' [that] enables a better understanding of the relationship between law, regulation and technology" (Bennett Moses 2016, p. 2). For IoT security, like Internet security in general, this adjustment means recognizing that it is not a question of whether rules will need to be adapted, but when, how often, and to what extent.

Changes in the framing and scope of new regulatory interventions need to increasingly recognize that the expertise necessary to characterize emerging sociotechnical risks is rooted not only in those who design or regulate these technologies, but in the day-to-day operational expertise developed among those who deploy, operate, and manage them on the ground. The strength of the three regulatory responses evaluated here, in particular, the centralized risk regulatory framework being developed in the EU, is the capability to explicitly incorporate commitments to adapting rules as knowledge of new threats and vulnerabilities becomes available. The weakness of these models is that they do not always have the capabilities to generate this new knowledge themselves. To keep pace, regulatory governance regimes must integrate a broader pool of evaluative capabilities. The strengths of operational epistemic communities – their capabilities to both recognize and mitigate new threats and vulnerabilities in situ – can fill this knowledge gap. The challenge, however, is developing and investing in the knowledge sharing interfaces that effectively integrate these very different sets of rule-making and risk evaluation mechanisms into a common, timely feedback mechanism. It is important to stress that planning for adaptation does not mean anticipating the disruption itself. Rather, the model proposed in this article recognizes the need for dynamic regulatory governance mechanisms that can be invoked as needed to create knowledge-sharing interfaces necessary to fill knowledge gaps as new threats and vulnerabilities emerge.

In contrast to models that stress designing and reviewing regulatory instruments comparatively, the regulatory governance model proposed here does not require a complete revision of regulatory interventions every time new risk knowledge becomes available. Rather, we recommend a regulatory governance design in which strong commitments to adaptation ensure the interorganizational planning and evaluative capabilities necessary to distinguish between adaptations that update regulatory standards with new information versus more intensive adaptations, such as changing or replacing the regulatory instruments themselves. The ability to distinguish between these is, in and of itself, a distinct evaluative capability born of combining regulators' deep knowledge of instrument design with operational epistemic communities' deep knowledge of threats and vulnerabilities that may warrant regulatory attention. As such, our model of regulatory governance for IoT security focuses on planning for adaptation as a means to efficiently and effectively fulfill commitments to adapt rules as new risk knowledge becomes available.

While this article focuses on a particular set of operational epistemic communities – those dealing with the uncertainties endemic in managing a "live" Internet and IoT – the broader notion of operational epistemic communities speaks to a pool of evaluative capabilities rooted in experience-based knowledge that comes only from managing global complex engineering systems in the wild (Sowell 2019). The knowledge generated by these expert communities is a necessary input into the kinds of reflexive (Scott 2018) and recursive (Sabel *et al.* 2018) regulatory governance mechanisms that facilitate the dynamic, responsive management of emerging and disruptive technologies.

Acknowledgments

The authors would like to thank the PETRAS Internet of Things Research Hub (Engineering and Physical Sciences Research Council, UK), the Stanford Cyber Initiative, and the Freeman Spogli Institute's International Policy Implementation Lab for funding the primary research underpinning this work.

Endnotes

¹ This research was conducted as part of the *Standards, Governance, and Policy Stream* of the *PETRAS IoT Research Hub: Cybersecurity of the Internet of Things*, sponsored by EPSRC in the UK, between October 2016 to August 2019. The PETRAS IoT Research Hub became the *PETRAS National Centre of Excellence for IoT Systems Cybersecurity* in 2019.

² This research was conducted as part of two projects at Stanford's Center for International Security and Cooperation (CISAC) from 2017 to 2018: *Documenting Combined Capabilities for Internet Security*, funded by the William and Flora

Hewlett Foundation through the Stanford Cyber Initiative, and *Developing a Reliable Capacity to Deploy Combined Capabilities in Internet Security*, funded by Stanford's Freeman Spogli Institute's International Policy Implementation Lab.

References

- Anderson R, Moore T (2006) The Economics of Information Security. *Science* 314, 610–613.
- Antonakakis M, April T, Bailey M et al. (2017) *Understanding the Mirai Botnet*. In: Proceedings of the 26th USENIX Security Symposium, pp. 1093–1110, Vancouver, BC, Canada: USENIX Association.
- APWG (2019a) *Unifying the Global Response to Cybercrime*. In: Anti-Phishing Working Group. [Last accessed 14 Apr 2019]. Available from URL: <https://apwg.org/>.
- APWG (2019b) *Bucharest Symposium on Global Cybersecurity Awareness*. Anti-Phishing Working Group. [Last accessed 29 June 2020]. Available from URL: <https://apwg.eu/bucharest-global-cybersecurity-awareness-2019/>.
- Avison D, Lau F, Myers M, Nielsen PA (1999) Action Research. *Communications of the ACM* 42, 94–98.
- Bennett Moses L (2013) How to Think about Law, Regulation and Technology: Problems with “Technology” as a Regulatory Target. *Law, Innovation and Technology* 5, 1–20.
- Bennett Moses L (2016) Regulating in the Face of Sociotechnical Change. In: Brownsword R, Scotford E, Yeung K (eds) *The Oxford Handbook of Law, Regulation and Technology*. Oxford, UK: Oxford University Press.
- BEUC (2018) *Factsheet: How the EU Can Make Smart Products Consumer-Proof*. BEUC The European Consumer Organisation. [Last accessed 4 Apr 2019]. Available from URL: https://www.beuc.eu/publications/beuc-x-2018-103_safety_of_connected_products.pdf.
- Black J (2005) The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom. *Public Law (Autumn)*, 510–546.
- Black J (2010) Risk-Based Regulation. *Risk and Regulatory Policy: Improving the Governance of Risk*, pp. 185–224. Paris: OECD Publishing.
- Black J, Baldwin R (2010) Really Responsive Risk-Based Regulation: Really Responsive Risk. *Law & Policy* 32, 181–213.
- Blythe JM, Johnson SD (2018) *Rapid Evidence Assessment on Labelling Schemes and Implications for Consumer IoT Security*. HMG Government Department of Digital, Culture, Media and Sport. Available from URL: <https://www.gov.uk/government/publications/rapid-evidence-assessment-on-labelling-schemes-for-iot-security>.
- Blythe JM, Sombatruang N, Johnson SD (2019) What Security Features and Crime Prevention Advice Is Communicated in Consumer IoT Device Manuals and Support Pages. *Journal of Cybersecurity* 5(1), 1–10.
- Boddy S, Pompon R, Cohen R (2019) The Hunt for IoT: So Easy to Compromise, Children are Doing It. In: *F5 Labs*. [Last accessed 24 Aug 2019]. Available from URL: <https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot-so-easy-to-compromise-children-are-doing-it.html>.
- Brass I, Tanczer L, Carr M, Blackstock J (2017) Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things? *CARR Risk and Regulation Magazine* 33, 12–15.
- Brass I, Tanczer L, Carr M, Elsden M, Blackstock J (2018) Standardising a Moving Target: The Development and Evolution of IoT Security Standards. *Living in the IoT: PETRAS IoT-IET Conference Proceedings IEEE Xplore*, 1–9.
- Brass I, Pothong K, Haitham M (2019) *Navigating and Informing the IoT Standards Landscape: A Guide for SMEs and Start-Ups*. BSI, PETRAS IoT.
- Brownsword R, Somsen H (2009) Law, Innovation and Technology: Before We Fast Forward—A Forum for Debate. *Law, Innovation and Technology* 1, 1–74.
- Brownsword R, Yeung K (2008) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*. Hart, Oxford, UK.
- Butenko A, Larouche P (2015) Regulation for Innovativeness or Regulation of Innovation? *Law, Innovation and Technology* 7, 52–82.
- CisoMag (2020) *10 IoT Security Incidents that Make you Feel Less Secure*. Cyber Security Magazine. [Last accessed 28 Apr 2020]. Available from URL: <https://www.cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/>.
- Consumer International (2016) *The Internet of Things and Challenges for Consumer Protection*. Last accessed 3 Apr 2019]. Available from URL: <https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>.
- DCMS (2018a) *Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report*. HMG Department for Digital, Culture, Media and Sport, London, UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf.
- DCMS (2018b) *Code of Practice for Consumer IoT Security*. HMG Department for Digital, Culture, Media and Sport, London, UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf.
- DCMS (2019) *Consultation on the Government's Regulatory Proposals Regarding Consumer Internet of Things (IoT) Security*. HMG Department for Digital, Culture, Media and Sport, London, UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/862953/Government_response_to_consultation_Regulatory_proposals_for_consumer_IoT_security.pdf.
- DHS (2016) *Strategic Principles for Securing the Internet of Things*. US Department of Homeland Security.
- Dunlop CA, Radella CM (2019) Policy Instruments, Policy Learning and Politics: Impact Assessment in the European Union. *Making Policies Work: First- and Second-Order Mechanisms in Policy Design*, pp. 115–136. Edward Elgar Publishing.

- Dunlop CA, Maggetti M, Radaelli CM, Russel D (2012) The Many Uses of Regulatory Impact Assessment: A Meta-Analysis of EU and UK Cases. *Regulation & Governance* 6, 23–45.
- Ellickson RC (1991) *Order without Law: How Neighbors Settle Disputes*. Harvard University Press, Cambridge, MA.
- ENISA (2017) *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructure*. European Union Agency for Cybersecurity, Heraklion, Greece.
- ENISA (2019) *Advancing Software Security in the EU: The Role of the EU Cybersecurity Certification Framework*. European Union Agency for Cybersecurity.
- Etienne J, McEntaggart K, Chirico S, Schnyder G (2018) *Comparative Analysis of Regulatory Regimes in Global Economies*. HMG Department of Business, Energy and Industrial Strategy, London, UK.
- Fagan M, Megas KN, Scarfone K, Smith M (2020) *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (Draft 2)*. NIST.
- FTC (2018) *Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection*. US Federal Trade Commission.
- Galaz V, Tallberg J, Boin A et al. (2017) Global Governance Dimensions of Globally Networked Risks: The State of the Art in Social Science Research. *Risk, Hazards & Crisis in Public Policy* 8, 4–27.
- Goodin D (2016) Newly Discovered Router Flaw Being Hammered by in-the-Wild Attacks. In: *Ars Technica*. [Last accessed 23 Mar 2019]. Available from URL: <https://arstechnica.com/information-technology/2016/11/notorious-iot-botnets-weaponize-new-flaw-found-in-millions-of-home-routers/>.
- Haas PM (1992) Introduction: Epistemic Communities and International Policy Coordination. *International Organization* 46 (1), 1–35.
- Heldeweg MA, Kica E (eds) (2011) *Regulating Technological Innovation—A Multidisciplinary Approach*. Hampshire: Palgrave Macmillan.
- Imperva (2016) *Breaking Down Mirai: An IoT DDoS Botnet Analysis*. Blog. . [Last accessed 24 Aug 2019]. Available from URL: <https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/>.
- IRGC (2016) *Governing Cyber Security Risks and Benefits of the Internet of Things Application to Connected Vehicles and Medical Devices*. Lausanne, Switzerland: International Risk Governance Council.
- ISO-IEC (2018) *ISO/IEC 20924:2018 Internet of Things Vocabulary*. International Organization for Standardization. Available from URL: <https://www.iso.org/standard/69470.html>.
- Kołacz MK, Quintavalla A, Yalnazov O (2019) Who Should Regulate Disruptive Technology? *European Journal of Risk Regulation* 10, 4–22.
- Krebs B (2016a) KrebsOnSecurity Hit with Record DDoS. In: *Krebs on Security*. [Last accessed 20 Mar 2019]. Available from URL: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>.
- Krebs B (2016b) *DDoS on Dyn Impacts Twitter, Spotify, Reddit*. In: *Krebs on Security*. [Last accessed 20 Mar 2019]. Available from URL: <https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/>.
- M³AAWG (2019) *Public Policy Comments*. Messaging, Malware, Mobile Anti-Abuse Working Group. [Last accessed 15 Apr 2019]. Available from URL: <https://www.m3aawg.org/for-the-industry/published-comments>.
- M³AAWG (2020) *Messaging, Malware, Mobile Anti-Abuse Working Group (M³AAWG)*. [Last accessed 6 May 2020]. Available from URL: <https://www.m3aawg.org/>.
- Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W (2019) Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys Tutorials* 21, 1636–1675.
- Mandel GN (2009) Regulating Emerging Technologies. *Law, Innovation and Technology* 1, 75–92.
- Manwaring K (2017) Emerging Information Technologies: Challenges for Consumers. *Oxford University Commonwealth Law Journal* 17, 265–289.
- Maple C (2017) Security and Privacy in the Internet of Things. *Journal of Cyber Policy* 2, 155–184.
- McCray LE, Oye KA, Petersen AC (2010) Planned Adaptation in Risk Regulation: An Initial Survey of US Environmental, Health, and Safety Regulation. *Technological Forecasting and Social Change* 77, 951–959.
- National Council of ISACs (2020) National Council of ISACs. In: *Natlouncilofisacs*. [Last accessed 6 May 2020]. Available from URL: <https://www.nationalisacs.org>.
- Nicolescu R, Huth M, Radanliev P, De Roure D (2018) Mapping the Values of IoT. *Journal of Information Technology* 33, 345–360.
- Nigam R (2019) New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems. In: Unit42. [Last accessed 24 Mar 2019]. Available from URL: <https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/>.
- NIST (2018) *Interagency Report on Status of International Cybersecurity Standardisation for IoT*. US National Institute of Standards and Technology, Gaithersburg, MD.
- Noto La Diega G (2016) Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom. *Journal of Law and Economic Regulation* 9(1), 69–93.
- Nurse JRC, Creece S, Roure DD (2017) Security Risk Assessment in Internet of Things Systems. *IT Professional* 19, 20–26.
- OECD (2017) *The Next Production Revolution: Implications for Governments and Business*. Paris: OECD Publishing.
- Oltermann P (2017) German Parents Told to Destroy Doll that Can Spy on Children. In: *The Guardian*. [Last accessed 21 Aug 2019]. Available from URL: <https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children>.
- Petersen AC, Bloemen P (2015) *Planned Adaptation in Design and Testing of Critical Infrastructure: The Case of Flood Safety in The Netherlands*

- Raab C, De Hert P (2008) Tools for Technology Regulation: Seeking Analytical Approaches beyond Lessig and Hood. In: Brownsword R, Yeung K (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, pp. 263–286. Hart Publishing, London, UK.
- Sabel C, Herrigel G, Kristensen PH (2018) Regulation under Uncertainty: The Coevolution of Industry and Regulation. *Regulation & Governance* 12, 371–394.
- Schwab K (2017) *The Fourth Industrial Revolution*. Penguin Random House LLC, New York, NY, USA.
- Scott C (2018) Integrating Regulatory Governance and Better Regulation as Reflexive Governance. In: Garben S, Govaere I (eds), *The EU Better Regulation Agenda: A Critical Assessment*pp. 13–25, Hart Publishing, Oxford, UK.
- Sowell JH (2018) *Combining Capabilities in Cybersecurity Incident Response*. Center for International Security and Cooperation, Freeman Spogli Institute for International Studies, Stanford University, Stanford, CA.
- Sowell J (2019) A Conceptual Model of Planned Adaptation. In: Marchau V, Walker W, Bloemen P, Popper S (eds) *Decision Making under Deep Uncertainty: From Theory to Practice*, pp. 289–320. Springer, Cham, Switzerland.
- Steedman S (2017) *Standards—Enabling Innovation and Change in the Digital Economy*. The IET, London.
- Stokes E, Bowman DM (2012) Looking Back to the Future of Regulating New Technologies: The Cases of Nanotechnologies and Synthetic Biology. *European Journal of Risk Regulation* 3, 235–241.
- Tanczer L, Brass I, Carr M (2018a) CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy* 9, 60–66.
- Tanczer L, Steenmans I, Brass I, Carr M (2018b) *Networked World: Risks and Opportunities in the Internet of Things*. Lloyds of London and UCL, London, UK.
- Tanczer L, Brass I, Elsden M, Carr M, Blackstock J (2019) The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In: Ellis R, Mohan V (eds) *Rewired: Cybersecurity Governance*, pp. 37–56, Wiley, Hoboken, NJ, USA. Wiley.
- The Rendon Group (2011) *Conficker Working Group: Lessons Learned*. [Last accessed 18 Dec 2019]. Available from URL: <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/LessonsLearned>.
- UCENet (2020) *Unsolicited Communications Enforcement Network*. [Last accessed 5 May 2020]. Available from URL: <https://www.ucenet.org/>.
- Vindrola-Padros C, Pape T, Utley M, Fulop NJ (2017) The Role of Embedded Research in Quality Improvement: A Narrative Review. *BMJ Quality & Safety* 26, 70–80.
- Yang Y, Wu L, Yin G, Li L, Zhao H (2017) A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal* 4, 1250–1258.

Laws cited

- EC (2001) *Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety*. European Union, Brussels.
- EU Regulation 2019/881 (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- S.734 - Internet of Things Cybersecurity Improvement Act of (2019) 116th Congress (2019–2020).

[Correction added on 30 July 2020, after first online publication: the laws cited 'EC (2001)', 'EU Regulation 2019/881 (2019)' and 'S.734' have been extracted from the References section and placed under 'Laws Cited' section.]