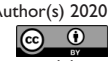
Article

International Relations
2020, Vol. 34(3) 391–412



DOI: 10.1177/0047117820948247
journals.sagepub.com/home/ire


Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance

Madeline Carr and Feja Lesniewska
University College London

Abstract

The implementation of the Internet of Things (IoT) is central to what the World Economic Forum has coined the 'Fourth Industrial Revolution'; a technological revolution built upon cyber-physical systems that will blur the lines between the physical, digital and biological spheres. Novel interconnections will emerge as a result, challenging traditional relations and modes of governance. However, a central feature of the IoT is that the implications of cyber (in)security are *no longer abstract*. The IoT also returns us to the world of kinetic effects in international relations; more familiar territory for IR. The resulting cooperation and coordination challenges are transboundary in nature, occur at multiple levels across sectors, between institutions, and will impact all actors, both public and private, in complex, often highly politicised ways. In this article we argue that advances in global climate governance appear to be offering an early model of a consensual rules-based approach within the existing international order that provides space for advancing agility, flexibility, and polycentrism to meet the demands of 'wicked problems' like the cybersecurity of the IoT. Perhaps one of the most important lessons to be drawn across from climate governance is the role of robust mechanisms for knowledge exchange – specifically between the technical and policy communities.

Keywords

climate change, cybersecurity, digital technology, governance, Internet of Things, wicked-problems

The Internet of Things (IoT) is a prime example of the increasingly dense and complex nature of human and non-human interconnections. Within, between and beyond human and non-human beings, and supported by an ever-expanding planetary wide

Corresponding author:
Madeline Carr, Department of Science, Technology, Engineering and Public Policy, University College London, Gower St, Bloomsbury, London WC1E 6BT, UK.
Email: m.carr@ucl.ac.uk

cyber-physical mega-infrastructure, the IoT (interconnecting physical and virtual things *including* humans) is being implemented to support transformations from healthcare to energy security. Emerging through an increasing dependency on the IoT, these interconnections will be integral to shaping international relations in the twenty-first century also signal a failure to pre-empt and manage the impact of creating such a co-dependent relationships.

Over the past quarter century, the governance of digital technologies has emerged as one of the 'wicked problems' of our time. Questions have arisen (many remain unanswered) about the extent to which cybersecurity impacts on international security and order. At a technical level, global cooperation on cybersecurity has been remarkably effective at mitigating against and responding to threats to interconnected systems – especially considering the lack of precedent for the scale and scope of the challenges involved. The (largely unseen) community of global Computer Security Incident Response Teams (CSIRTs) develop and share solutions, support one another during incident response, run training and capacity building programmes and generally cooperate to manage cybersecurity challenges as they arise – across borders and political chasms.[1]

Yet despite a shared sense of exposure, global policy cooperation has been very slow to come about where differing value systems, competition for resources, and broader geopolitical tensions exist. The past two decades of trying to deal with the politics of global cybersecurity has been carried out through a combination of post WW2 instruments established to ensure a peaceful international order in which all can prosper, coupled with forums established more recently to accommodate the 'multi-stakeholder' model of Internet governance. In general, negotiations have consistently struggled to incorporate the integrated, interconnected and interdependent elements of digital technologies and cybersecurity while accommodating a Westphalian view of the state system. As the need increases, the pace of international political coordination remains stuck in an analogue gear – out of sync with the demands placed upon it through running a global economy on a digital platform.

The implementation of the IoT is central to what the World Economic Forum (WEF) has coined the 'Fourth Industrial Revolution'[2]; a technological revolution built upon cyber-physical systems that will blur the lines between the physical, digital, and biological spheres.[3] The IoT also blurs the boundaries between security and safety, and consequently pushes existing cybersecurity global governance mechanisms and processes even further to – or perhaps beyond – their limits. A central feature of the IoT is that cybersecurity and the implications of it are *no longer abstract*. While vulnerabilities like intellectual property theft, financial fraud, and ransomware remain current challenges, the IoT returns us to the world of kinetic effects in international relations. Counterintuitively then, this stage of technological innovation is in some ways, more familiar territory for IR – but it is also quite different in other ways.

The cooperation and coordination challenges involved in minimising the security risks of the IoT have many similarities to the governance of climate change. Both are 'super-wicked' problems that are transboundary in nature, occur at multiple levels across sectors, between institutions, and will impact all actors, both public and private, in complex, interconnected, and often highly politicised ways. Although climate change has distinguishing characteristics such as its complex interrelationship with planetary ecological systems,

there are lessons to be learned from how the international community has approached navigating the unfamiliar problematic landscape of IoT cybersecurity. Advances in climate policy, especially since the 2015 UN Paris Agreement, appear to be offering (albeit not without some difficulties between states such as the US, Saudi Arabia, China and small island states) an early model of a consensual rules-based approach within the existing international order that provides space for advancing agility, flexibility, and polycentrism to meet the demands that wicked problems present.

In this article we argue that one of the important lessons to be drawn from climate governance into the global governance of the IoT is the role of robust mechanisms for knowledge exchange – specifically in the human interconnections between the technical and policy communities. To make this argument, we draw on four years of empirical research into international initiatives to address the cyber (in)security of the IoT. We frame this global governance challenge as a 'super-wicked problem' and highlight how efforts to 'tame' it through existing forums is hampered by silos of information and expertise.

Concepts and data gathering

In this project, we draw directly on research conducted within the PETRAS Cybersecurity of the Internet of Things research hub (now a National Centre of Excellence) between 2016 and 2019. PETRAS (and specifically the Standards, Governance, and Policy stream within which we worked) was established to provide an evidence-based overview of how we might maximise the significant potential of the IoT while mitigating against the also very significant security issues. Much of our work focused on evaluating and informing national and international policies and measures that are emerging to address the cybersecurity of the IoT.[4]

The observation that there is inadequate integration of technical advice into the global cybersecurity governance discourse emerged through several years of observation of, and direct participation in, multilateral and multi-stakeholder meetings at the global level where cybersecurity was the central topic of discussion. These included international meetings hosted by the United Nations, the Organization for Economic Cooperation and Development (OECD), the World Economic Forum (WEF), the European Union (EU), various state-led bi-lateral meetings including Track 2 and Track 1.5 delegations, numerous government consultations or workshops and participation in the International and Telecommunications Union (ITU) eighteenth Plenipotentiary in 2018. Many of these meetings included representatives of American tech firms like Google, Amazon, Microsoft, Facebook and Apple, private sector cyber security firms, NGOs (particularly those concerned with privacy and human rights) as well as academics. From 2016 to 2019, we carried out unstructured, informal and semi-formal interviews at these events to ask participants from the global cybersecurity policy community ('cyber-ambassadors', diplomats and policy officials responsible for national cybersecurity strategy, the digital economy, etc.) how they envisaged the IoT impacting on their efforts to maintain a peaceful international order in the twenty-first century.

In addition to these engagements, we analysed the (unrestricted) documentation circulated in advance of these meetings and at the conclusion of them to understand how

issues arising from the IoT were dealt with. We also analysed the position on global IoT security from eight international organisations.[5] Here, we looked at what specific issues were raised and how 'problems' were perceived and framed. This type of interpretive work draws on methods from the Social Construction of Technology (SCoT) – a field that focuses on human interaction with technology.

The SCoT provides tools for interpreting actor's or group's perceptions of problems that will or might emerge from technological change. Understanding how an actor or community perceives a 'problem' with technology reveals much about how they expect it to perform or 'be' in a perfect state. And that reveals a lot more about how they hope to shape the world than it does about technology. Debates about the trade-offs inherent in interoperability versus privacy highlight this well. Having IoT devices connect seamlessly to other devices or systems without the need for human interaction makes them easy to use (and perhaps, easier to sell) but also limits the user's oversight of the ways in which their data may be exploited. A 'good' device can be one that is easy to use and easy to profit from or it could be one that promotes human rights. This is not to suggest that these attributes are mutually exclusive or incompatible but rather to highlight that a manufacturer may view the 'problem' with any particular technology in quite a different way to a regulator or to civil society. Tracing the perception of a 'problem' back to its source is also a way of identifying power dynamics in these transactions because it is those problems perceived by powerful actors that tend to be addressed.[6]

Building on this observational and documentary work, we also designed and hosted five workshops to bring together people from the global cybersecurity community and the technical community – especially those who work in Cyber Security Incident Response Teams (CSIRTs). CSIRTs form international practitioner networks that respond to cybersecurity challenges by supporting one another and those who are at risk to mitigate against threats. In these workshops, we again employed SCoT concepts of 'reverse salience' and 'closure' to examine the range of ways in which different actors framed a common problem. 'Reverse salience' refers to the point at which a particular technology is being held back from developing further – the battery life of phones, for example. It is often a point at which we see increased innovation and investment. 'Closure' refers to the perception that a problem is 'solved' and is useful for understanding how different actors or groups conceptualise problems and 'good' outcomes. Four of these workshops were held at United Nations Internet Governance Forums in 2016,[7] 2017,[8] 2018[9] and 2019.[10] The fifth workshop was held as part of the UK's inaugural 'Living in the IoT' conference co-hosted by the Institute of Engineering and Technology and the PETRAS Cybersecurity of the IoT research hub.[11]

We also drew on the literature from Public Policy on 'wicked problems' – specifically Daviter's work on alternative approaches to governing them.[12] This gave us a framework for analysing how actors are approaching the challenges of cybersecurity of the IoT. This was particularly useful because we were able to draw parallels between the governance of cybersecurity and the climate which provided some avenues for comparison with regard to 'coping' or 'taming' the perceived problem – as opposed to attempting to 'solve' problems.

Finally, guided by these concepts from SCoT and Public Policy, we carried out extensive desk-based research. We conducted a comprehensive analysis of other research

projects that sought to address the type of international security and governance problems that we were concerned with. We looked at the research agendas of 58 projects from 26 countries to see where support for addressing this gap might be developed. The review revealed a focus amongst research institutions, both public and private, in Europe, Asia, Latin America and North America, on the technical, economic and social potential of the IoT. Key areas of research were interoperability, innovative business models and data management to ensure consumer trust. Few research projects focused on the security challenges, especially at scale, that the IoT would bring for states and the international community.

This focus on problem framing is important because identifying how problems are perceived, combined with the analysis of relative power dynamics, can be a strong indicator of which 'problems' will be addressed.[13] Overwhelmingly, through our work, two factors emerged as important in the international discussions about the IoT. First, there was considerable emphasis on how to extract maximum economic value from the IoT. Second, there was a focus on ensuring that human rights were not undermined by pervasive surveillance.

These priorities are really a continuation of those that dominated the previous digital age (characterised by the expansion of the Internet and the World Wide Web) and while they remain relevant to international security in the Fourth Industrial Revolution, they do not fully capture the challenges of the IoT. For the past three decades, the international politics of cybersecurity has largely dwelt upon intellectual property theft, financial breaches and attacks on critical infrastructure. This application of existing priorities to new security vulnerabilities holds up only in the absence of critical input from the technical community. Once their voices and perspectives are introduced, the fragility of the foundations upon which the international policy community has thus far discussed the IoT quickly become visible. Improving this interaction between policy and technical communities then, has global security implications that need to be considered. A starting point for this argument requires some background of what exactly the IoT is and why it matters for international relations.

The Internet of Things and International Relations

The IoT is not a new technology itself. Rather, the IoT refers to a set of interoperable, emerging technologies such as machine learning, algorithmic decision-making, 5G infrastructure and robotics. In 2012, the International Telecommunications Union defined the IoT as 'a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.' It is a term that is currently most often used colloquially to refer to household devices like smart kettles or fridges that are connected to the Internet. This usage of the term tends to trivialise cybersecurity concerns and reduce them to the everyday mundane.

In fact, the IoT is short-hand for much broader, complex 'cyber-physical systems' in which we see three important elements. The first is a proliferation of sensors in the natural and built environment (also, increasingly on or within the human body) that collect vast quantities of data (light, motion, temperature, etc.). Second, there are tools that

analyse and make sense of those massive data flows. And finally, there are 'actuators' that, in response to the data analytics, make something happen in the physical world – often without direct human interaction.[14] The IoT will facilitate and hasten a transformation in how humanity sees itself, having implications for all relations (gender, racial, biocultural, sexual) leading to an expansion in posthuman knowledge systems.[15]

The main distinct features of the IoT that have implications for international relations are the following.

The IoT connects the digitial and physical worlds having clear effects on the latter

Unlike past implementations of digital technology, the IoT is not abstract. Its influence and implications go beyond connectivity, communications, online transactions and intellectual property. The IoT is characterised by widespread, automated transactions that generate effects in the physical world. And these effects can be in safety critical systems like transportation system or implantable health devices.

For the last 30 years, there has been a deep divide within International Relations and Strategic Studies literature as to the implications of digital technologies. 'Cyber-sceptics' have maintained that the absence of any potential for violence keeps this particular technological shift in the realm of civil society or law enforcement. (For coverage of these debates about digital technologies and political violence, see Carr's, 'Cyberspace and International Order'[16].) The kinetic effects of the IoT means that those arguments no longer hold true. The IoT results in a blurring of the lines between safety and security which is important for international relations – particularly international law.

The application of the international Laws of Armed Conflict (LoAC) to cyberspace is an example of where existing mechanisms for managing and governing global security have been pushed beyond their original point of usefulness. Although there has been agreement amongst states that existing international law does apply in cyberspace,[17] states have been confounded by the challenge of interpreting exactly *how* it can be applied, particularly LoAC. Key sticking points have been the difficulties associated with defining an 'armed attack' and the 'use of force' in an abstract domain with little or no kinetic effects. The IoT, with its physical, safety critical implications, will reshape these debates that have been stalled trying to apply legal concepts developed for the physical world to intangible, online only practices. The IoT returns us to kinetic effects upon which LoAC was originally devised.

Data as global critical infrastructure

Cybersecurity in national critical infrastructure (transport, energy, communications, etc.) has attracted plenty of attention in IR already because it has long been regarded as a key target in conflict.[18] Indeed, a prohibition against attacking critical infrastructure through digital technologies has been the basis of two of the 11 proposed international cyber norms that have come out of the UN Group of Governmental Experts on Developments in the field of information and telecommunications (UNGGE) in the context of international security.[19]

This focus on the protection of critical infrastructure continues to have relevance, of course, but in the hyper-connected context of the IoT, *data flows themselves become*

critical infrastructure rather than simply forming a mechanism to access or tamper with more conventional critical infrastructure. A key feature of the IoT is the quite dramatic increase in data generated. Predictions are difficult in a rapidly evolving ecosystem but it has been suggested that that the IoT will generate 79.4 ZB of data in 2025 (one zettabyte is equivalent to a trillion gigabytes).[20] Data sets can be globally generated and aggregated in novel ways for different applications. Literally billions of IoT devices will increasingly be embedded within public and private spaces to undertake performative tasks. Weather data may be combined with pedestrian footfall data to help manage busy public transport hubs. Either of those data sets (both of which appear to be benign) could be tampered with thereby 'polluting' the aggregated data and potentially causing an incident or even accident in the public transport hub.[21] The integrity of diverse data flows can be central to safety issues when combined.

In globally interconnected and interdependent safety critical systems such as transport, health, building management, etc., the integrity and security of data flows becomes a global security vulnerability to be protected and/or exploited by state and non-state actors. Given the significant vulnerabilities inherent in the IoT, which is not being implemented with security prioritised, we are effectively building a global dependency upon un-securable data flows.

Un-securable devices

A key element of the IoT is the proliferation of billions of sensors and actuators embedded in our built and natural environment, our homes and workplaces, even our bodies which will enable novel transhumanism to emerge. In many cases, these sensors perform a relatively simple function; measuring temperature, light, movement, etc., and then transmitting that data to an intelligent system. Cheaply produced in response to markets that are struggling to respond to IoT consumer and industrial demand, these sensors can be unobtrusive or invisibly fit within already small devices. (A motion sensor inside a lightbulb allows the light to turn on and off in response to a person entering the space.) As a consequence, these tiny sensors often do not have the capacity to carry the additional functionality required for conventional security mechanisms like software updates, passwords or other access controls. At this current stage of the implementation of the IoT, many devices are *un-securable* from the start; this is much more than a localised technological problem for those devices.

This inbuilt insecurity generates international security concerns through two vectors. First, the global supply chain for IoT devices and components is so complex that the same care given to importing parts for safety critical systems (like automobiles, for example) that we have exercised in the past will not be easily replicated in this context. In many cases, IoT sensors and actuators are embedded in devices and systems managed by those with little understanding of the potential vulnerabilities that could be exploited at the destination implementation. Toy manufacturers, for example, have extensive knowledge about the safe use of plastics, about the size of dangerous ingestible parts in age appropriate toys, etc. But they do not typically understand data protection laws, the risks of recording devices in different settings, and the implications of national surveillance regimes. In 2015, a doll equipped with a speaker, microphone, and Bluetooth transmitter allowed children to ask questions that the doll would answer following an Internet search – just

like using a Siri or Echo. The doll was found to have a security vulnerability that allowed third parties to listen to the children and their families without detection and it was subsequently removed from the market.[22] In this way, both simple consumer devices and complex industrial applications can become conduits through which physical harm can be remotely actuated. Those designing and selling sensors and actuators cannot always know what the eventual applications for their products will be and therefore, what the global security implications might be. At an international relations level, the concern is not that one vehicle loses its steering function but rather, that every black cab on the road in London loses steering capacity at the same time. The scale is important here with predictions of as many as 125 billion IoT devices by 2030.[23]

The second vector through which these devices impact on international relations is the wider (and possibly more concerning) implication of connecting billions of insecure (or un-securable) components and devices to our networks. Every one of these devices represents a gateway to the network to which they are connected. The IoT is often trivialised in common discourse leading to questions like 'why would anyone want to hack my fridge?' Questions like this belie the broader implications of consumer markets rapidly producing, purchasing, and connecting un-securable devices to networks that do have security significance. National and international initiatives of good security practice and cyber hygiene that have been developed over the past two decades are seriously undermined by the IoT – almost to the point that they risk becoming 'security theatre'[24] rather than security practices.

As the IoT becomes a meta-critical infrastructure upon which all other critical infrastructures (energy, water, transport, financial services, etc.) depend, its complexity and scale of interconnections (human and non-human) will increase. Multiple governance regimes such as security, trade, environment, human rights, will be impacted in numerous ways resulting in a multilevel, transnational, interconnected governance landscape.[25] The sub-problems to IoT: responsibility and liability for safety critical impacts, intellectual property, lack of security of consumer devices, global supply chains, interoperability and sustainability, each contribute to the governance conundrums.[26] It is here that the work from Public Policy on understanding and dealing with 'wicked problems' provides a useful basis for thinking through global IoT cybersecurity.

Governing wicked problems

The nature of twenty-first century global challenges such as climate change, pandemics and cybersecurity, has prompted work in the field of Public Policy on 'wicked problems'. Wicked problems refer to those that are complex, interdependent, interconnected and resistant to solutions. That means that rather than 'solve' them, we work instead to 'tame' them by dealing with a discreet aspect of a larger problem, or to 'cope' with them by utilising existing institutions and mechanisms.[27] This literature allows us to take a different view, not only of our *perception* of problems, but critically, of what might be novel or useful approaches to *addressing* those problems.

Wicked problems introduce unprecedented challenges for several reasons. First, wicked problems are inherently destabilising.[28] Typically, they will consist of several sub-problems that have different consequences for both actors and context making any

single policy approach ineffective. We already understand that cybersecurity is perceived differently in different political contexts (notions of privacy, human rights, free speech, etc.) but the IoT's additional layer of insecurity coupled with a complex global supply chain means that it becomes very difficult to imagine any single policy approach proving implementable.

Second, not only are wicked problems difficult to comprehend, they are also difficult to resolve. Ritter observed that a wicked problem is 'one for which each attempt to create a solution changes the understanding of the problem'.[29] It is common for wicked problems to transform and morph into often more complex problems, with governance interventions frequently having unanticipated perverse outcomes that can compound the impacts.[30] For example, the transition to a decarbonised global economy can result in new natural resource wars and ecosystem destruction as countries become locked into supply chains for lithium.[31] And sustaining a thriving data-based economy can undermine individual rights to privacy. The dynamic nature of wicked problems is compounded by an increasing awareness and sensitivity to the interconnections between humans and non-humans and an appreciation of how response measures can exacerbate existing inequities and injustices for marginalised communities.

Third, wicked problems are increasingly transnational making cooperation amongst affected states (and relevant non-state actors) essential to managing the impact. The multilevel, transnational, cross-sectoral interconnected nature of wicked problems means that there are no simple governance or technical solutions.[32] Ultimately, they are problems without an end, and ones that often only become more complex over time as the world becomes more dependent upon the system itself and/or the emergent mechanisms produced to cope with the original wicked problem (such as antibiotic drugs or the Internet).

In an escalation of terminology that recognises gradients of wicked problems, we now see the use of the term 'super-wicked problem'. The term has increasingly been applied to climate change but can also apply to the IoT. Super-wicked problems have four key features: time is running out; the central authority needed to address the problem is weak or non-existent; those who cause the problem also seek to create a solution; and hyperbolic discounting occurs that pushes responses irrationally into the future.[33] Climate change poses an existential crisis to the current global political economic system of a magnitude that far exceeds the IoT. Climate change is resulting in differentiated impacts upon peoples, especially vulnerable and marginalised groups (women, ethnic groups, migrants, indigenous peoples and non-human species) in many countries who did not contribute to the crisis. The IoT is frequently, alongside other parts of the emergent cyber-physical global infrastructure, identified as key to mitigating and adapting to climate change through enabling more sustainable natural resource management. The increased dependency on the IoT to address planetary environmental threats escalates the need to ensure that the challenges the technology presents in and of itself are effectively addressed. By not doing so, multiple interconnections will be open to insecurities previously unknown. To manage 'super-wicked problems' it is necessary to adopt a creative hybrid approach to policy design, one that has emerged from 'thinking outside the box'.

Both climate governance and global cybersecurity governance can be described as 'polycentric' systems – those in which we see diverse actors exercise considerable

independence to make norms and rules within a specific domain like a state or province, a region, a national government or an international regime'.[34] As such, polycentric systems can have multiple governing authorities at different scales. The authorities can take many forms from technical associations to global corporations, non-governmental organisations to governments.[35] We see most benefit where there is effective coordination and collaboration within multilevel, multi-actor models, where they are more fluid and less restrictive than formal state-centric multilateral approaches based on legally binding rule making.[36]

According to Black, a normative framework can help to support the emergence of customary practice between all actors contributing to a more predictable and stable, transnational, multilevel order.[37] The rationale here is that stability and predictability can foster more effective cooperation, resulting in a more resilient dynamic governance environment in which innovation can be perpetually nurtured. In such conditions, as the wicked problem morphs over time, it can continue to be managed. Overarching rules or norms then, are important to effectively cope with global wicked problems.[38]

Establishing norms is a social process that requires agreement about what constitutes acceptable behaviour amongst relevant parties.[39] However, in climate or cybersecurity governance, the sheer number and heterogeneity of relevant stakeholder configurations can intensify questions of who should be involved in consultation and governance processes.[40] It also intensifies the challenges of establishing and maintaining interconnections and communication across all kinds of intellectual and value-based divisions and boundaries. Ostrom argues that in order to avoid the spectre of the Tower of Babel in these settings, a common language framework is needed.[41] Folke observes that for any common language to be resilient in the long-term, all agents engaged in governance processes must contribute to and share it.[42]

Science communication has gained new currency through efforts to deal with the 2020 Covid-19 global pandemic but communicating complex scientific or technical material to a non-specialist audience has long been recognised as key to sound, evidence-based policy making.[43] Although climate governance is far from perfect, one factor that has made a positive contribution to agreed outcomes is the mechanism for reaching some consensus on the science behind climate change and proposed initiatives prior to diplomatic negotiations. Cybersecurity lacks this mechanism in general and that has always been one of the impediments to more coordinated global governance of this issue. But, as discussed above, the IoT exacerbates cybersecurity challenges and makes this all the more urgent to resolve. Looking to other domains like climate governance, where knowledge exchange instruments and processes are more mature, can provide impetus and precedent for implementing similar practices here.

Science advice and communication in climate governance

As noted earlier, the IoT has many similarities to the challenges that have emerged within the climate change context. In both cases, the problems are transboundary in nature, occur at multiple levels across sectors, between institutions, and will impact all actors, both public and private, in complex ways. Issues of accountability, responsibility, liability and rights that the IoT raises for law and policy makers challenge

established governance models. As with climate change, state centric, multilateral governance initiatives on cybersecurity are encumbered by political legacy and are unable to address the security complexities. However, we have seen some progress in the context of climate governance that has yet to be matched in the context of the IoT.

Over the last decade a polycentric governance approach to climate change, in which multiple actors are involved in addressing the problem has emerged.[44] The most significant milestone in this transition is the Paris Agreement to the UN Framework Convention on Climate Change (UNFCCC). The Paris Agreement emerged in 2015 after two decades of multilateral struggle within the UN system where developed and developing states were pitted against each other over debates about what constituted fair and equitable governance approaches to mitigating against and adapting to climate change.[45] A growing frustration with the perceived failure of the UN negotiations to arrive at an agreement fuelled non-state actors' initiatives and activities, including from those who felt excluded from formal processes especially women, ethnic minorities, indigenous peoples, and children. These actors independent and complementary processes had a lasting legacy on the outcome of the formal UN process. In contrast to the top-down structure of the UNFCCC's Kyoto Protocol, adopted in 1997, the Paris Agreement has a bottom up structure that formally recognises opportunities for non-state actors to be involved in processes to reach zero net emissions by 2050.[46] This is seen as an expression of innovation in governing super-wicked problems with all stakeholders, not just states, encouraged to engage more directly to achieving the overall objective.[47] Actors and sectors that are significant greenhouse gas emitters such as aviation,[48] cities,[49] and forestry,[50] set their own targets, standards and ambitions to contribute to the Paris Agreement objective. Critically, through its implementation framework, the Paris Agreement will facilitate monitoring and reporting processes that will help to build reflexive and agile governance models based on data from a wider range of actors.

In the UN climate change governance model, technical advice is continually provided to the climate change negotiations through the International Panel on Climate Change (IPCC), and the Subsidiary Body on Science and Technological Advice (SBSTA). The IPCC's knowledge claims have underpinned the slow but steady push for global policy action since the late 1980s. Key claims from IPCC reports inform the UNFCCC negotiations, especially the annual Conference of the Parties (COP). Advisory bodies, such as the SBSTA, also rely on the IPCC for scientific experts when invited by parties to draft text on specific issues related to mitigation and adaptation policies and measures. The IPCC collates peer-reviewed research in a format that is usable for negotiators, policy makers, business and civil society and it has maintained a solid foundation for knowledge sharing and the emergence of a common language, no matter how disputed the findings may be for policy development.

This means that there is a common scientific language for negotiators to draw on at the COPs and these knowledge sharing mechanisms have been fundamental to enabling greater collaboration across a fragmented institutional and organisational landscape. Indeed, the IPCC reports have an influence well beyond the UNFCCC negotiations. IPCC reports, and the scientific data they draw on, also inform the policies and measures of many other international environmental agreements such as those on biodiversity,

pollution, as well as human rights and indigenous peoples' approach to climate change related issues. Also, numerous organisations focused on specific sectors and aspects of climate change, for instance the World Trade Organisation, the International Civil Aviation Authority, and the International Maritime Organisation use IPCC reports to inform their climate related negotiations.

It is important to acknowledge that having a recognised foundation of best available knowledge like the IPCC source does not prevent disputes over policy priorities and regulatory approaches. Jasanoff has argued that the IPCC has 'projected an impersonal, apolitical and universal imaginary of climate change science that cuts against the grain of common sense' denying other sites of knowledge production such as indigenous peoples.[51] The IPCC's 'performative' power that shapes fields of political possibility – to put certain policy options on the table, while potentially obscuring others – is increasingly becoming a significant source of social, economic and political contestation as the world looks to decarbonise.[52]

These blurred lines between scientific advice and shaping the policy landscape are not new – they have been evident in the context of digital technologies for decades and are central to current work on science diplomacy.[53] Despite the IPCCs flaws and with a full appreciation of the underlying, and ongoing issues that have surfaced during its history, the IPCC can become a reference point for future decision-making, knowledge exchange and learning.[54] It can also become a model for improving the technical support needed by those involved in global security issues that take the form of similarly super-wicked problems.

In the context of the IoT, a foundation for an international framework could yet emerge to facilitate coordinating initiatives, establishing platforms for knowledge exchange and capacity development. Yet the form that any international framework might take will no longer necessarily mirror traditional international governance arrangements such as treaties, conventions and declarations. An emergent polycentric governance model for the IoT and cyber physical technologies for the twenty-first century may well not require the same institutional structures of those adopted by states in the late twentieth century. What emerges from current and future multilevel and multi-stakeholder initiatives may reflect the paradigm shift that Durante argues is taking place in ICT in which the world is 'moving from a State-based form of regulation towards multi-agent and multi-level forms of regulation'.[55]

In the next section we demonstrate how a polycentric governance system is emerging to address security issues in relation to the IoT but that the continued lack of coordination of recognised technical advice (in part indicative of embedded differences between states like the US, China and Russia) is holding back progress.

The IoT and global governance of cybersecurity

States first seriously addressed cybersecurity related issues within a multilateral forum after 1998 when the UN General Assembly passed a Russian-sponsored resolution expressing concern that information and communication technologies (ICTs) could be used for purposes that may 'adversely affect the security of States'[56] and 'divert an enormous amount of resources that are so necessary for peaceful creativity and

development'.[57] In response, the UN Committee for Disarmament and International Security (the First Committee) which deals with disarmament and threats to the international community, established a Group of Governmental Experts on Developments (UNGGE) in the Field of Information and Telecommunications in the Context of International Security in 2004. Subsequently, states regularly meet within the UNGGE – always the five permanent members of the Security Council plus a growing list of increasingly interested states. The primary focus during this time has been on avoiding state sponsored cyber warfare and preventing escalation to a kinetic conflict.

One of the key achievements of the UNGGE has been the development in 2015 of 11 proposed norms of responsible state behaviour in cyberspace. Although the UNGGE failed to reach consensus on how to progress those norms during the 2017 negotiations, both Russia[58] and the United States[59] have subsequently sponsored UN General Assembly resolutions calling for meetings between sovereign states to resume in order to continue to focus on advancing international cooperation on ICT and cybersecurity issues.[60] This has been expanded to include the Russian initiative of the Open Ended Working Group which allows all states to participate.

Within the UNGGE process, several countries have promoted the IoT as a separate discussion point. However, they did so without tabling any concrete views on what it is about the IoT that differs from, or additionally informs, the international cybersecurity discourse.[61] Other countries pointed out that without a clear understanding about whether and how the emergence and proliferation of the IoT affects international peace and security, there is no reason to address the issue in the UNGGE. The IoT has only featured in three written submissions to the UNGGE. One expert specifically mentioned the IoT as a low priority for the purposes of the UNGGE. Another expert emphasised that whatever new technologies will be addressed, it is essential to keep in mind the determination of threats to international peace and security deriving from Article 39 of the UN Charter.[62] The third expert wrote that (developing) countries will need assistance in developing IoT related policies.

Those UNGGE participants that did appear to have more than a superficial understanding of the IoT still regarded it as too complex to discuss. At the fifth UNGGE in 2017 it was suggested that 'new and serious threats are brought about by new technological systems, notably by the IoT, autonomous robotic systems, ICT abuse in the political interests on the cognitive levels etc.' and that experts were expected to discuss 'norms addressing new emerging threats, e.g. IoT'.[63] Importantly, a technologically advanced country pointed out that the development of technologies, such as the IoT, may further blur data jurisdiction in the future. However, the expert of this country concluded that although an interesting academic issue, this was too complex an issue to discuss in the UNGGE at this time. The interim conclusion of the UNGGE was to focus on continued technological development and the growing technological divide rather than singling out or addressing the IoT.

This sense of being overwhelmed by the implications of emerging technologies is understandable – especially for those in domestic or international policy roles who may have a complex portfolio or who may have transitioned into a cybersecurity role from an unrelated previous post (or both). This is exactly where technical advice and support becomes so important but in the UNGGE process, this takes place at a domestic level rather than a joined up, international level. In an effort to inject some much needed

technical literacy into the process, UNIDIR hosted a day-long meeting in August 2019 at which technical experts and policy academics were asked to present high level introductions to some emerging technological systems – including the IoT.[64] Essentially though, this forum remains devoid of any coordinated, agreed technical or science advice.

Recognising the need to incorporate more actors into discussions of global cybersecurity, the UN Secretary General launched a *Strategy on New Technology* and established a *High-level Panel on Digital Cooperation* (HLPDC) that included leading figures from the international technology business community from the global north and the global south.[65] The HLPDC report was published in June 2019 and several governance approaches to foster cooperation and collaboration were proposed.[66] One concrete proposal was for the UN Secretary-General to appoint a Special Envoy on Technology akin to the UN Secretary-General's Special Envoy for the 2019 Climate Change Summit (which has subsequently happened) – a clear indication that the existing lack of technical knowledge exchange that we have identified in our own research is becoming increasingly seen as a limiting factor in global governance of emerging technologies. In May 2020, a Roadmap for Digital Cooperation was agreed to by the UN to implement the HLPDC in which it was agreed the Special Envoy on Technology would be appointed by 2021 to facilitate capacity building, especially in developing countries.

For many, the attraction of the IoT is in capturing the economic value and exploiting the potential of new business models. In 2017, the McKinsey Institute estimated that by using the IoT to link the physical and digital worlds 'up to $11.1 trillion a year in economic value' could be generated by 2025.[67] In an early effort to engage with this issue, the Organisation for Economic Cooperation and Development (OECD) emphasised the necessity of technical security if the economic value was to be fully harnessed in a 2016 report.[68] The OECD's report however placed more focus on individual products rather than the potential economic instability that could result from the IoT being embedded within critical infrastructure such as health, energy, and transport systems. Other forums, such as the G7 and G20 have taken a similar approach to the OECD, focusing on consumer products more so than critical infrastructure and the industrial IoT. However, the coordination and joined up thinking necessary to approach a complex technological shift like the IoT remains missing in these forums.

Some forums do explicitly bring together the policy and technical communities. The UN Internet Governance Forum (IGF) is an annual event at which issues of global internet governance and cybersecurity are discussed in a multi-stakeholder setting. While the IGF does attract a good mix of technical, policy and industry participants, somewhat frustratingly (although also predictably) they tend to cluster in likeminded groups rather than using the opportunity to explore alternate perspectives. While some policy participants will use the opportunity to learn more about technical elements they are engaged with, it is less common to have technical participants join in policy sessions. In effect, the policy and technical communities can quite easily spend a week at the same venue and rarely interact – an indication that proximity alone is not an adequate catalyst for real interconnections.

In recent years, there have been plenty of technical sessions on the IoT and related developments at the IGF. Perhaps one of the most significant policy relevant initiatives emerged at the 2014 IGF, when a Dynamic Coalition on IoT[69] began to develop a 'good

practice' paper to promote the ethical development of IoT. Through a multi-stakeholder process including intersessional regional workshops and online forums the Dynamic Coalition on IoT developed a draft 'IoT Good Practice' paper placing emphasis on procedural norms such as transparency, usability and accountability.[70]

As a forum with no decision-making authority, the IGF sometimes struggles for relevance. To some extent, we see a power shift away from this and other multi-stakeholder Internet forums established in the 1990s by the US under a neo-liberal order. Yet European preference for the IGF as an advocate of a rights-based model for cyber systems governance, including the IoT, remains high. This was evident when the President of France, Emmanuel Macron, proposed that the IGF report directly to the UN General Secretary, receive a budget (currently the IGF relies on donations) and help promote multilateralism.[71] The future of the IGF will depend on developments out of its control. For now, Europe appears to be taking it on to bolster its rights-based approach to cyber stability including the IoT. Meanwhile the HLPDC's Road Map for Digital Cooperation has the IGF as the lead forum to build cooperation globally.

The International Telecommunications Union (ITU), a technical standard setting body, was an early advocate of the need to consider the security of the IoT. The ITU does provide space for the engagement of technical and policy groups, but the processes are deeply politicised for a number of complex reasons – not least being the 'one flag, one vote' principle that promotes lobbying of disinterested countries by major powers or alliances. In addition, the ITU is a hybrid UN organisation which is member based and not as transparent in its processes as other agencies. Access to materials is restricted so important deliberations that will affect the governance landscape of the IoT globally, based on different jurisdictional approaches, receives limited analysis by researchers.

One organisation that has adopted an assertive approach to addressing this governance gap in cybersecurity of the IoT is the World Economic Forum. The WEF has integrated agendas on the environment, economy and technology to invest in research to advance ideas that support a sustainable IoT.[72] As the founding organisation for the concept of a Fourth Industrial Revolution, the WEF is keen, like many state and non-state actors, to promote the potential transformative benefits of the IoT, not just economically, but also socially and environmentally.[73] With a vision of the interconnections between these domains, the WEF also recognises the failure by states to address pressing issues regarding digital technologies, security, and governance which hold back the secure widespread adoption of these technologies.

In May 2019, working alongside major tech companies, multinationals, government representatives, academics and civil society, the WEF established six Global Fourth Industrial Revolution Councils, including one on the IoT, to guide multistakeholder collaboration, research and thought leadership. The initiative is indicative not only of the WEF's belief in cyber physical systems as fundamental to achieving sustainable future economic growth but also that the international governance and legal system is not fit to deliver the coordinating framework any time soon. Signalling its intent to prioritise this, the WEF will intends to host a tier one summit in late 2020 – on the same level as the annual WEF Davos meeting.

Such a circumvention of traditional international institutions at points of deadlock in negotiations is not unusual. Forest certification emerged when international negotiations

over an international treaty became gridlocked.[74] What could be different with this particular private sector governance initiative over emerging technologies globally is the unprecedented scale and potential political, economic, social and environmental implications that such interventions could have. The absence of effective international leadership in assuming responsibility for setting and steering the strategic governance design to cope with the super-wicked problem of IoT security issues is becoming all too evident. Particularly lacking is the necessary engagement with the technical sector which will be essential if any significant progress is to be made to create a more cyber secure environment in the near-future.

Conclusion

Geopolitics remains as integrally linked to technological innovation as it ever did but future collaboration on global 'super-wicked problems' may well be more problematic now as interests are not so clearly aligned. In the first two decades of the twenty-first century, the diverse interconnections between humans and non-humans at multiple scales across time and space are coming to shape international relations responses to global problems. It is clear that governing the IoT will not, indeed arguably cannot, take the same trajectory as the one adopted to address climate change. Climate change governance had its foundational roots firmly set within the state centric exclusive international relations systems. However, those seeking to tame the 'wicked problem' of IoT cybersecurity can draw on the hybrid manoeuvre which the Paris Agreement demonstrated to circumvent gridlock within state-based negotiations to draw upon the potential of other vested interests, business especially, to become part of a more diffused governance approach. Having a shared language such as that provided by the IPCC would contribute to easing collaboration between the technical community, businesses and government policy-makers.[75] The appropriate organisation to fill this role is not immediately apparent though perhaps a UN digital technology advisor as proposed by the UNHLP on Digital Cooperation would be one option as a first step.

What has become increasingly clear is that the mechanisms, forums and instruments developed to address the global security problems of emerging technologies are not able to cope with the demands of the last decade of technological innovation and are in no way equipped to move forward into the next decade. The Paris Agreement broke the mould in which it was cast: that being a state-centric hierarchical rules based top-down treaty. In doing so, Falkner argues, it lay the foundations for a 'the new logic of international climate politics'.[76] The Paris Agreement created spaces for the multiple interconnections that existed globally to be made visible. It modelled a path for those impacted, not only by climate change but also by the response measures, to have their voices heard, to begin to claim power, and to shape policy that addressed their own priorities – especially women in developing countries, indigenous peoples and displaced peoples. Arguably, the same needs to happen in the global governance of technology and it is the capacity for IoT systems to result in physical harm that are most likely to be the catalyst for this transformation.

Governing the global security challenges that emerge from the IoT will call for state level regulation, international coordination and the involvement of a broad array of other public and private actors. Central to and essential to sound decision-making in this sphere, will be much improved mechanisms for providing technical support to the policy

community. We are not without precedent for significant progress in the mitigation of global security problems. But it is clearly past time to stop looking over the same ground within cybersecurity, strategic studies and international relations for inspiration to move forward in the governance of emerging technologies. Multidisciplinary approaches are essential at the academic level, bringing together computer science, engineering, economics, diplomacy and legal scholars is an integral element to strengthening both technical and policy discussions in practice settings. How to do that effectively will be the challenge of our time and achieving it will transform global cyber (in)security more profoundly than any technical innovation alone.

Acknowledgements

Several people have had input into our thinking and research over the past three years. Specifically, we'd like to acknowledge the following: Irina Brass, Lorraine Elliott, Pablo Hinojosa, Duncan Hollis, Saba Mirza, Leonie Tanczer, Eneken Tikk and Fareeha Yahya.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was funded by the EPSRC funded PETRAS Cybersecurity of the Internet of Things Research Hub (EP/N022785/1).

Notes

1. Leonie Maria Tanczer, Irina Brass and Madeline Carr, 'CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy', *Global Policy*, 9(S3), 2018, pp. 60–6.
2. Klaus Schwab, *The Fourth Industrial Revolution: What It Means, How to Respond* (Geneva: World Economic Forum, 2017), p. 8.
3. Schwab, *The Fourth Industrial Revolution*, p. 9.
4. Kruakae Pothong, Irina Brass and Madeline Carr, *Cybersecurity of the Internet of Things: PETRAS Stream Report* (PETRAS IoT Research Hub: London, 2019).
5. Leonie Tanczer, John Blythe, Fareeha Yahya, et al., *Summary Literature Review on IoT Security* (London: Department for Digital, Culture, Media and Sport, 2018), pp. 1–18.
6. Madeline Carr, *US Power and the Internet in International Relations: The Irony of the Information Age* (Basingstoke: Palgrave, 2016).
7. Pablo Hinojosa, Duncan Hollis and Madeline Carr, 'WS132 NetGov, Please Meet Cybernorms. Opening the Debate', UN Internet Governance Forum, 2016, available at: https://www.intgovforum.org/multilingual/content/igf-2016-day-3-room-2-ws132-netgov-please-meet-cybernorms-opening-the-debate (accessed 20 July 2020).
8. Pablo Hinojosa, Duncan Hollis and Madeline Carr, 'WS38 International Cooperation Between CERTS: Technical Diplomacy for Cybersecurity', UN Internet Governance Forum, 2017, available at: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/5902/858 (accessed 20 July 2020).
9. Pablo Hinojosa, Duncan Hollis and Madeline Carr, 'WS50 Who Is Collected, Disclosed and Protected: CERTS: Viewpoint', UN Internet Governance Forum, 2018, available at: https://www.intgovforum.org/multilingual/content/igf-2018-ws-50-whois-collected-disclosed-and-protected-certs-viewpoint (accessed 20 July 2020).
10. Pablo Hinojosa, Duncan Hollis and Madeline Carr, 'IGF 2019 WS #63 Usual Suspects: Questioning the Cybernorm-Making Boundaries', UN Internet Governance Forum, 2019,

available at: https://www.intgovforum.org/multilingual/content/igf-2019-ws-63-usual-suspects-questioning-the-cybernorm-making-boundaries (accessed 20 July 2020).
11. Madeline Carr, Feja Lesniewska, Irina Brass, et al., *Governance and Policy Cooperation on the Cyber Security of the Internet of Things* (London: Institute of Engineering and Technology, 2018), p. 33.
12. Falk Daviter, 'Coping, Taming or Solving: Alternative Approaches to the Governance of Wicked Problems', *Policy Studies*, 38(6), 2017, pp. 571–88.
13. Carr, *US Power and the Internet in International Relations*.
14. Leonie Tanczer, Irina Brass, Madeline Carr, et al., 'The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape', in Ryan Ellis and Vivek Mohan (eds), *Rewired: Cybersecurity Governance* (Hoboken, NJ: Wiley, 2019).
15. Discussed also in Kessler and Lenglet and Grove papers in this special issue.
16. Hidemi Suganami, Madeline Carr and Adam Humphreys (eds), *The Anarchical Society at 40: Contemporary Challenges and Prospects* (Oxford: Oxford University Press, 2017), pp. 168–70.
17. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).
18. Madeline Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', *International Affairs*, 92(1), 2016, pp. 43–62.
19. UN Secretary General, Report by Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, (22 July 2015), p. 8.
20. Carrie MacGillivray and David Reinsel, *Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023* (Framingham, MA: International Data Corporation, 2019), available at: https://www.idc.com/getdoc.jsp?containerId=US45066919 (accessed 20 July 2020).
21. Leonie Tanczer, Ine Steenmans, Irina Brass, et al., 'Networked World: Risks and Opportunities in the Internet of Things', *Emerging Risk Report* (London: Lloyds of London, 2018), pp. 27, available at: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world
22. Jeffery Esposito, 'Forget Books, Time to Burn the Dolls: Connected Dolls Pose a Hacking Risk', *Kaspersky Daily*, 21 February 2017, available at: https://www.kaspersky.com/blog/my-friend-cayla-risks/14087/ (accessed 20 July 2020).
23. IHS Markit, 'The Internet of Things: A Movement, Not a Market', IHS Markit, 2017, pp. 1–9, available at: https://cdn.ihs.com/www/pdf/IoT-ebook.pdf (accessed 20 July 2020).
24. Bruce Schneier, 'Beyond Security Theater', *New Internationalist*, 1 November 2009, available at: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html (accessed 20 July 2020).
25. Richard Lazarus, 'Super Wicked Problems and Climate Change: Restraining the Present to Liberate the Future', *Cornell Law Review*, 94, 2008, p. 1153.
26. Kruakae Pothong, Irina Brass and Madeline Carr (eds), *Cybersecurity of the Internet of Things: PETRAS Stream Report* (London: PETRAS IoT Research Hub, 2019), available at: https://s3-eu-west-1.amazonaws.com/uclpetras/wp-content/uploads/2019/10/28144344/PETRAS-Stream-Report.pdf (accessed 20 July 2020).
27. Daviter, 'Coping, Taming or Solving', pp. 571–88. See also: David Coen and Tom Pegram, *Wanted: A Third Generation of Global Governance Research* (Rochester, NY: Social Science Research Network, 2019), available at: https://papers.ssrn.com/abstract=2765904 (accessed 16 July 2020).
28. Paul S. Berman, 'Global Legal Pluralism as a Normative Project', *UC Irvine Law Review*, 8(2), 2018, pp. 149–82.

29. Horst Rittel and Melvin M. Webber, 'Wicked Problems', *Man-Made Futures*, 26(1), 1974, pp. 272–80.
30. Brian W. Head and John Alford, 'Wicked Problems: Implications for Public Policy and Management', *Administration & Society*, 47(6), 2015, pp. 711–39.
31. Camille Grosjean, Pamela Herrera Miranda, Marion Perrin, et al., 'Assessment of World Lithium Resources and Consequences of Their Geographic Distribution on the Expected Development of the Electric Vehicle Industry', *Renewable and Sustainable Energy Reviews*, 16(3), 2012, pp. 1735–44.
32. Edward P. Weber and Anne M. Khademian, 'Wicked Problems, Knowledge Challenges, and Collaborative Capacity Builders in Network Settings', *Public Administration Review*, 68(2), 2008, pp. 334–49.
33. Kelly Levin, Benjamin Cashore, Steven Bernstein, et al., *Playing it Forward: Path Dependency, Progressive Incrementalism, and the 'Super Wicked' Problem of Global Climate Change* (Chicago: International Studies Association 48th Annual Convention, 2010).
34. Elinor Ostrom, 'Polycentric Systems for Coping With Collective Action and Global Environmental Change', *Global Environmental Change*, 20(4), 2010, pp. 550–7.
35. Peter M. Haas, 'Introduction: Epistemic Communities and International Policy Coordination', *International Organization*, 46(1), 1992, pp. 1–35.
36. Roger Cotterrell and Maksymilian Del Mar, *Authority in Transnational Legal Theory: Theorising Across Disciplines* (Cheltenham: Edward Elgar Publishing, 2016).
37. Julia Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes', *Regulation and Governance*, 2(2), 2008, pp. 137–64.
38. Marcel J. Dorsch, Andrew Jordan, Dave Huitema, et al. (eds), 'Governing Climate Change. Polycentricity in Action?', *Politische Vierteljahresschrift*, 60(1), 2019, pp. 187–90.
39. Toni Erskine and Madeline Carr, 'Beyond "Quasi-Norms": The Challenges and Potential of Engaging with Norms in Cyberspace', in Anna-Maria Osula and Henry Roigas (eds), *International Cyber Norms Legal, Policy & Industry Perspectives* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), p. 23.
40. Mark Raymond and Laura DeNardis, 'Multistakeholderism: Anatomy of an Inchoate Global Institution', *International Theory*, 7(3), 2015, pp. 572–616.
41. Elinor Ostrom, *Understanding Institutional Diversity* (Princeton, NJ: Princeton University Press, 2009).
42. Carl Folke, 'Resilience: The Emergence of a Perspective for Social–Ecological Systems Analyses', *Global Environmental Change*, 16(3), 2006, pp. 253–67.
43. Alex Stevens, 'Telling Policy Stories: An Ethnographic Study of the Use of Evidence in Policy-Making in the UK', *Journal of Social Policy*, 40(2), 2011, pp. 237–55.
44. Oscar Widerberg and Johannes Stripple, 'The Expanding Field of Cooperative Initiatives for Decarbonization: A Review of Five Databases', *WIREs Climate Change*, 7(4), 2016, pp. 486–500.
45. Karin Bäckstrand, Jonathan W. Kuyper, Björn-Ola Linnér, et al. 'Non-State Actors in Global Climate Governance: From Copenhagen to Paris and Beyond', *Environmental Politics*, 26(4), 2017, pp. 561–79.
46. Sander Chan, Harro van Asselt, Thomas van, et al., 'Reinvigorating International Climate Policy: A Comprehensive Framework for Effective Nonstate Action', *Global Policy*, 6(4), 2015, pp. 466–73.
47. The Paris Agreement objective is stated in Article 2.1(a) 'Holding the increase in the global average temperature to well below 2°C above pre-industrial levels and pursuing efforts to limit the temperature increase to 1.5°C above pre-industrial levels, recognizing that this would significantly reduce the risks and impacts of climate change.'

48. See the International Civil Aviation Organisation (ICAO) Carbon Offsetting and Reduction Scheme for International Aviation (CORSIA) which drew on IPCC scientific reports for emission calculations – https://www.icao.int/environmental-protection/CORSIA/Pages/CORSIA-background-information.aspx (accessed 20 July 2020).
49. The C40 Cities Climate Leadership Group is a group of 94 cities around the world that represents one-twelfth of the world's population and one-quarter of the global economy – the C40 group draw on IPCC reports to inform policy – see https://www.c40.org/about (accessed 20 July 2020).
50. The New York Declaration on Forests is a partnership of governments, multinational companies, civil society and indigenous peoples who strive to halve deforestation by 2020 and to end it by 2030 – text available https://nydfglobalplatform.org
51. Sheila Jasanoff, 'A New Climate for Society', *Theory, Culture & Society*, 27(2–3), 2010, pp. 233–53.
52. Silke Beck and Martin Mahony, 'The IPCC and the New Map of Science and Politics', *Wiley Interdisciplinary Reviews: Climate Change*, 9(6), 2018, p. 547.
53. Ben Koppelman, Natalie Day, Neil Davison, et al., *New Frontiers in Science Diplomacy: Navigating the Changing Balance of Power* (London: The Royal Society, 2010).
54. Warren Pearce and Martin Mahony, 'The Intergovernmental Panel on Climate Change: Transferable Model or Cautionary Tale?', International Network for Government Science Advice, 2018.
55. Massimo Durante, 'An Informational Approach to the Law', in Massimo Durante (ed.), *Ethics, Law and the Politics of Information : A Guide to the Philosophy of Luciano Floridi*, (Dordrecht: Springer Netherlands, 2017), pp. 185–214.
56. UN General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/RES/53/70, 4 January 1999, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf (accessed 20 July 2020).
57. Igor Ivanov, 'Russian Foreign Minister in a Letter to the UN Secretary General', in Eneken Tikk-Ringas (ed.), *Evolution of the Cyber Domain: The Implications for National and Global Security* (London: The International Institute for Strategic Studies, 2015).
58. UN General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/RES/73/L.27/Rev.1, 29 October 2018, available at: http://undocs.org/A/C.1/73/L.27/Rev.1 (accessed 20 July 2020).
59. UN General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security', A/RES/73/L.37, 18 October 2018, http://undocs.org/A/C.1/73/L.37 (accessed 20 July 2020).
60. The previous multilateral discussions at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security had last met in 2017 but states failed to reach a consensus on the report containing recommendations on how international law applies in cyberspace.
61. Note that the UNGGE is a closed process and therefore positions cannot be attributed.
62. Charter of the UN – Article 39 – 'The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security', (14th August 1941).
63. Note that the UNGGE is a closed process and therefore positions cannot be attributed.
64. Madeline Carr, 'Why the IoT is Not About the Fridge', Presentation to the UNIDIR Innovations Dialogue: Digital Technologies and International Security, United Nations, Geneva, 19

August 2019, available at: http://unidir.org/programmes/security-and-technology/2019-innovations-dialogue-digital-technologies-and-international-security (accessed 20 July 2020).

65. Secretary-General's High-level Panel on Digital Cooperation, 12 July 2018, available at: http://www.un.org/en/digital-cooperation-panel/ (accessed 20 July 2020).
66. UN High Level Panel on Digital Cooperation, 'The Age of Digital Interdependence', June 2019, available at: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf (accessed 20 July 2020).
67. James Manyika, Michael Chui, Peter Bisson, et al., 'The Internet of Things: Mapping the Value Beyond the Hype', McKinsey Global Institute, 2017, available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (accessed 20 July 2020).
68. OECD, 'The Internet of Things: Seizing the Benefits and Addressing the Challenges', 4 May 2016, DSTI/ICCP/CISP(2015)3/FINAL, available at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En (accessed 20 July 2020).
69. Since its third meeting in Hydrabad in 2008, the IoT has been on the agenda for the IGF annual meetings.
70. Article 3, DC IoT, Draft IoT Good Practice Paper for IGF review, September 2018, available at: https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6186/1407 (accessed 20 July 2020).
71. Khaled Fattal, 'Has President Macron Thrown Multistakeholderism Under the Bus at UN IGF 2018 Paris?' *CircleID*, 13 November 2018, available at: http://www.circleid.com/posts/20181113_has_president_macron_thrown_multistakeholderism_under_the_bus/ (accessed 20 July 2020).
72. See World Economic Forum, 'Realizing the Internet of Things: A Framework for Collective Action', World Economic Forum, February 2019, available at: https://www.weforum.org/whitepapers/realizing-the-internet-of-things-a-framework-for-collective-action (accessed 20 July 2020).
73. World Economic Forum, 'Accelerating the Impact of IoT Technologies Initiative', World Economic Forum, 2016, available at: https://www.weforum.org/projects/accelerating-the-impact-of-iot-technologies (accessed 20 July 2020).
74. David Humphreys, *Logjam: Deforestation and the Crisis of Global Governance* (Abingdon: Routledge, 2012).
75. Glen Peters, 'The Best Available Science to Inform 1.5 C Policy Choices', *Nature Climate Change*, 6, 2016, p. 646; Mike Hulme, '1.5 C and Climate Research After the Paris Agreement', *Nature Climate Change*, 6, 2016, p. 222.
76. Robert Falkner, 'The Paris Agreement and the New Logic of International Climate Politics', *International Affairs*, 92(5), 2016, pp. 1107–25.

Author biographies

Madeline Carr is a Professor of Global Politics and Cybersecurity at UCL. Her research focuses on the implications of emerging technology for national and global security, international order and global governance. She has published on cyber norms, multi-stakeholder Internet governance, the future of the insurance sector in the IoT, cybersecurity and international law and the public/private partnership in national cyber security strategies. She is the Director of the UK Research Institute on Sociotechnical Cyber Security (RISCS).

Feja Lesniewska is a environmental law and policy scholar specialising in climate change and ecosystems, especially forest and land use. She has published widely on forest related law and governance. Feja has undertaken fieldwork in China, Central and West Africa, Europe and Russia. Her current research explores the interface between cyber-physical systems and environmental law and governance.