Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

The missing piece in human-centric approaches to cybernorms implementation: the role of civil society

Sheetal Kumar

To cite this article: Sheetal Kumar (2021): The missing piece in human-centric approaches to cybernorms implementation: the role of civil society, Journal of Cyber Policy, DOI: 10.1080/23738871.2021.1909090

To link to this article: https://doi.org/10.1080/23738871.2021.1909090

Published online: 02 Apr 2021.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2021.1909090

Routledge
Taylor & Francis Group

The missing piece in human-centric approaches to cybernorms implementation: the role of civil society

Sheetal Kumar

Global Partners Digital, London, United Kingdom

ABSTRACT

The importance of a human-centric approach to peace and security in cyberspace has been consistently noted in cybernorms discussions, including in the UN First Committee's Open-Ended Working Group on ICTs. However, an analysis of what a human-centric approach to implementing cybernorms means in practice has so far been lacking. Furthermore, literature and discussions about the role of cybernorms in maintaining international peace and security have, to date, dealt mainly with the role of state actors and the private sector, while the role of civil society has not been widely or adequately researched and documented. This article posits that civil society actors, working in collaboration with other stakeholders, have an important role to play in defining and implementing the human-centric approach to cybersecurity through their implementation of cybernorms. It unpacks the human-centric approach through three practical case studies and examples of the implementation of cybernorms grounded in different contexts. In this way, it aims to contribute to the understanding of what it means to implement cybernorms in a human-centric manner, and, by extension, to implement a human-centric approach to cybersecurity.

ARTICLE HISTORY
Received 15 October 2020
Revised 22 January 2021
Accepted 11 February 2021

KEYWORDS
Human-centric; cybernorms; cybersecurity; civil society

Introduction

Policy discussions relating to cybersecurity have proliferated in recent years. In multilateral forums, cybersecurity is discussed in relation to international peace and security, as well as in relation to internet governance and digital technology policy more generally. These discussions often refer to the transnational and multifaceted nature of both the internet and the threats which undermine its security and resilience and that of digital technologies. The discussions which take place in the increasing number of policy forums and processes relating to cybersecurity are shaped by the actors present; multilateral and state-led discussions pertaining to international peace and security will expectedly reflect the national security and geopolitical preoccupations of nation states, for example. Yet the reliance of societies globally on digital technology means that both the understanding of cybersecurity threats, and the responses developed to address them, have ramifications for human rights and for communities around the world and

CONTACT Sheetal Kumar sheetal@gp-digital.org

should therefore involve the engagement of a broad range of stakeholders. This includes those who can contribute to a better understanding of cybersecurity which is sensitive to the direct impact of cybersecurity on people: a human-centric understanding. In this article, the author argues that civil society stakeholders have a distinctive role to play in elucidating a human-centric understanding of cybersecurity within relevant policy forums, and in implementing human-centric approaches to cybersecurity measures, including cybernorms developed and adopted within these forums. Yet, this role is neither well documented nor well understood. In order to address these gaps, this article analyses existing literature on the 'human-centric' approach to cybersecurity and identifies some of its main characteristics. Then, in order to illustrate the ways in which civil society supports the human-centric implementation of cybernorms, it presents three case studies. The three case studies were selected to illustrate both the diversity of civil society and the range of roles that civil society stakeholders play in supporting cybernorms implementation in different geographical contexts. The aim of this article is therefore to make the case that the representation and participation of civil society stakeholders in cybersecurity, including cybernorms discussions, should be expanded.

The human-centric approach to cybersecurity

The concept of the 'human-centric' approach to cybersecurity has received increased attention over the last ten years, in particular within the human rights community, among some scholars working at the intersection of international law and information and communication technologies (ICTs) and in some multilateral and multistakeholder discussions. For human rights defenders, the increasing reliance of communities on digital technologies requires strong and secure networks and technologies to ensure human rights are protected and realised. In this sense, cybersecurity is a positive enabler of human rights. On the other hand, measures taken by both state actors and the private sector can either promote or undermine human rights, for example through policies that introduce disproportionate measures that undermine human rights in the name of addressing cybercrime or in the name of 'collective' or 'national security' (Brown and Esterhuysen 2017, 2019). The behaviour of states in cyberspace, in particular, has been the subject of discussion over the last two decades in multilateral forums, beginning with UNGA's First Committee's first group of governmental experts (GGE) in 2003 and most recently with the sixth GGE and the Open-Ended Working Group (OEWG) on ICTs. Cybernorms, which seek to shape state behaviour in cyberspace, have been discussed and developed in these forums to promote greater stability and security in cyberspace by clarifying roles and setting out expectations for behaviour, as well as identifying the practices and measures which states, and other actors, should either undertake, or refrain from, in cyberspace. In this way, the implementation of cybernorms can be understood as an important element of cybersecurity practices, as well as a means by which to promote international peace and security in the digital age more widely.

The defining element of a human-centric approach to cybersecurity refers to what is positioned or privileged as the object of security in discourse; in other words, the referent object of security (Dunn Cavelty 2014). This approach is related to the 'human security approach' which has been applied in other security-related fields and regimes and which asks: security for whom, from what and through what means? (Brown and

Esterhuysen 2017, 2019; Dunn Cavelty 2014). In the 'human security' approach, it is 'the human being' who is central – and not, for example, the nation-state, regime interests or economic imperatives (Dunn Cavelty 2012; Klein and Hossain 2020). Citing Pawlak, Boulanin (2016) describes cybersecurity as 'ensuring people's ability to enjoy the capabilities and opportunities offered by ICT and thereby their wellbeing in cyberspace … this analysis not only includes risks posed by states and non-state actors to other states and their citizens but also those resulting from a state's negligence or premediated actions against its own citizens'.

Discussions centred on regime interests are more inclined to be affected and shaped by geopolitical relationships – or the 'nation state's security' – at any given time for example, than the interests of citizens and users (Dunn Cavelty 2012). Privileging the nation state and its interests in cyber policy discussions, including through the use of military discourse such as 'war', 'arms' and 'deterrence'; the inclusion of cyber operations in military strategy, doctrines and operations; and the increased investment in cybercapacities to gain strategic advantage have been termed by some as the 'militarisation of cyberspace', challenging a human-centric approach (Liaropoulos 2015; Pytlak 2020), particularly because, and as is shown in more detail below, the security objectives of the state may not coincide with the security of individual citizens (Dunn Cavelty 2012). For example, an emphasis on national security denotes that the strategic and military aspects of cyberspace are increasingly resourced, resulting in the development of military assets, like the establishment of cyber commands. An increasing investment in cyber commands, including in offensive capabilities, leads to the accumulation and exploitation of vulnerabilities in computer systems by states, which has a destabilising effect on the wider communications ecosystem as both Deibert (2020) and Dunn Cavelty (2014) have pointed out. Yet, a number of states that have recognised the applicability of human rights in cyberspace, as well as the links between human rights and cybersecurity, are also expanding cyber commands and investing in offensive cyber capabilities – such as, for example, the UK and the US (Healey 2020; Prince 2020). The impact of these actions, which can contribute to heightened tension, could be seen as counterproductive to the efforts of normative agreements – how they contribute to the undermining of cybernorms arguably requires greater scrutiny from actors, such as civil society stakeholders, who do not have a vested interest in the development of cyber offence capabilities for either national security or economic reasons.

The way threats are defined by some state actors in multilateral cyber discussions reflects this prioritisation of the military and geostrategic aspects of cyberspace: a state-centric approach 'prioritises the territorial sovereignty of networks, where threats such as hacking, espionage, intellectual property control and ownership over information/intelligence are those that undermine regime interests' (Deibert 2018). A state-centric approach can classify humans as threats, leading to the increased use of measures such as filtering technologies, kill switches, restrictions on the use of encryption and mass surveillance in order to protect the stability of the state regime (Brown and Esterhuysen 2019). National security approaches conceptualise the state, infrastructure, and its institutions at the centre of threats, while the private sector may have a different referent – whereby 'humans become reduced to nodes in the network, needed to ensure the wealth and health of networks', because economic imperatives like profit maximisation are decisive (Dunn Cavelty 2012). On the other hand, a human-centric approach

conceptualises the human impact of threats as of central importance; and sees threats emanating from a range of actors, both state and non-state (Brown and Esterhuysen 2017, 2019; Deibert 2018).

Discussions of the human-centric approach to cybersecurity have emphasised the importance of international human rights law as a basis and framework for the human-centric approach to cybersecurity, for a range of reasons. First, it privileges the human being as the main referent. Instead of privileging sovereignty, which itself is particularly difficult to apply in cyberspace due to the lack of territorial boundaries, it conceives of the 'nation state in a supporting role' (Deibert 2018) where ultimate beneficiaries are individuals, regardless of their territorial position. Moreover, international human rights law applies at all times, which is particularly well suited to the nature of cyber incidents, the majority of which are 'non-coercive, non-kinetic' (Kilovaty 2019) and occur in peacetime. A human rights-based approach to a peaceful and secure cyberspace requires states to abide by their human rights obligations when developing and implementing cybersecurity measures, and also to implement their commitments to uphold responsible state behaviour in cyberspace (Freedom Online Coalition 2020). For example, this could be achieved through the promotion of strong encryption which protects privacy and data protection, the support and protection of security researchers, and the protection of secure access to the open internet (Boulanin 2016; Brown, Esterhuysen, and Kumar 2019; Dunn Cavelty 2012). These links between human rights and cybersecurity have been highlighted by a number of civil society organisations at the OEWG on ICTs, for example (see Access Now 2019; Centre for Internet and Society 2020; Global Partners Digital 2020a; ICT4 Peace Foundation 2020a; Women League for Peace and Freedom 2020).

Open and inclusive approaches to governance are another feature of a human-centric approach, and widely cited as an important element in relevant discussions and literature. Inclusive governance can be seen as a foundational element of the human security approach mentioned earlier, which refers to the importance of 'multistakeholder partnerships grounded in local realities, and prevention addressing root causes of vulnerabilities and the promotion of solutions that advance human rights' (UN 2018). Inclusive governance is important to the human-centric approach to cybersecurity because a number of the roles which non-state actors play – such as the provision of oversight, monitoring and critical assessment of policies and their implementation – can only occur where meaningful opportunities for engagement exist. This provides the 'possibility of public oversight and scrutiny, complying with democratic principles of restraints and checks and balances on political power' (Deibert 2018). Although the GGE framework and other cybernorms initiatives have been designed to increase trust and mutual understanding, regulatory and policy gaps – whether perceived or real – can create incentives to develop, acquire and use cyber capabilities to pursue strategic interests (Dunn Cavelty 2014). This undermines trust and can be exacerbated by long-standing geopolitical tensions and relationships, a situation that has already led to cyberoperations that have direct impacts on human rights (Kavanagh and Cornish 2020).

References and commitments to human rights and to the importance of inclusive processes by member states exist in a range of multilateral and multistakeholder forums, including the Freedom Online Coalition (2020), the Organization for Security and Cooperation in Europe (2019), and within the First Committee of the UN General

Assembly (see Pytlak 2020), meetings of the Open-Ended Working Group on ICTs (see Reaching Critical Will 2020), and Arria formula meetings of the UN Security Council (see Brown 2020). In addition, a number of national cybersecurity strategies make reference to the importance of implementing and respecting human rights (Global Partners Digital 2020a). As Pytlak points out, these references can and should build on the long-standing work that has already been done on applying the human rights framework to digital technologies in forums such as the Human Rights Council (2020). In addition, she points out that human rights approaches have been integrated into other security issues that are dealt with within the UN First Committee, such as nuclear weapons, citing the pivotal engagement of civil society in these cases. Yet, implementation of cyber-norms lags behind and states continue to frame threats, act, and implement measures – either in pursuit of their strategic interests or in the name of 'security' – which are not human-centric, and which undermine human rights.

The role of civil society in the implementation of cybernorms

Definitions of civil society are contested and vary. However, most definitions centre on what makes civil society distinctive in comparison to other stakeholder groupings; for example, civil society comprises those stakeholders which are separate from the state and the market, and motivated, not by profit, but by public interest concerns (Kavanagh and Stauffacher 2014). Civil society can therefore include a range of institutions and organisations, including NGOs, media and consumer protection groups, transnational networks, think-tanks, academia, some technical community actors (e.g. not-for-profit technical community actors) and other professional bodies or communities (Kavanagh and Cornish 2019). Within each of these groupings, moreover, there are also differences. Civil society varies in geographic scope (transnational, national, grassroots), and in its cultural context, resource levels, constituencies and tactics. Some scholars have, for example, highlighted the differences between the roles of large INGOs in global civil society, who operate transnationally on 'global governance issues' – ranging from climate change, to financial institutions, to internet governance – and are 'unable to represent or advocate the same way as domestic civil society' but can 'fulfil a bridging role in creating multi-organizational alliances linking grassroots, national and international civil society organizations' (Lewis and Kanji 2009). Kaldor has offered definitions of civil society based on what 'it does', highlighting the different kinds and roles of civil society in relation to the political realm and existing political power structures. For example, definitions of civil society as 'activist' may denote an understanding of civil society as constituting an active citizenship and self-organisation, a disruptive power outside formal political circles, where citizens attempt to influence – and shift – the conditions in which they live through political pressure. Other definitions see civil society, not as restraining state power but as providing a substitute for functions of the state, a 'neoliberal' version sometimes associated with the 'non-profit voluntary third sector'. A postmodern conception sees civil society as occupying a range of political roles, 'an arena of pluralism and contestation', both counter-hegemonic and hegemonic (2011). Considering the contested and heterogenous nature of civil society outlined, this article adopts a broad definition of civil society linked to Scholte's which emphasises 'associations of citizens' who 'seek, from outside political parties, to shape the rules that govern one or the

other aspect of their common life' (2007). Therefore, civil society actors are understood as those that self-organise outside state institutions and the market, not primarily motivated by profit or the retainment of public office but which nonetheless engage in collective and deliberate action to shape the governance 'of aspects of their common life'.

It has been widely acknowledged, including within multilateral discussions that the nature of cyberspace, with its distributed networks that span territorial borders, and multi-faceted range of actors who both use and provide online services, requires a range of stakeholders to develop and maintain it. One of the earliest forums within the UN to discuss the issue of internet governance, the World Summit on the Information Society (WSIS), acknowledged the roles and responsibilities of all stakeholders in the Tunis Agenda (WSIS 2005). As a result of the nature of the internet, therefore, the importance of the 'multistakeholder' approach has, over time, become a norm in and of itself in certain internet governance-related forums, even if challenges relating to overcoming inherent power dynamics continue to be a source of contestation.

This acknowledgement of the role of all actors, and openness to their engagement within discussions, is more contested at UNGA's First Committee and in other multilateral and regional forums where issues related to responsible state behaviour are discussed. Access to these discussions has been limited to ECOSOC-accredited NGOs, that is those NGOs who have applied and received a particular status by the UN allowing them to participate in the work of the UN. Outside these formal avenues for engagement, non-governmental stakeholders tend to be represented by industry actors and some from academia. The engagement and representation of a broader set of stakeholders, including civil society actors, has been less evident. An exploration of the various factors that explain the limited representation of civil society in these discussions is beyond the scope of this paper; instead, in this section, the author on seeks to summarise the work already done to understand the role of civil society in the implementation of cybernorms as a proxy for their role in cybersecurity more generally. In doing so, it sets the basis for the following section which illustrates these roles by applying them to real-life cases, situated in three different regions.

With regard to the role of civil society in implementing cybernorms, there are three main elements which have been studied and discussed by scholars and practitioners thus far: (1) the heterogeneous and diverse make-up of civil society (as noted above); (2) the distinctive stakes which civil society has in being involved in relevant discussions and in a secure and peaceful cyberspace and (3) the varied and distinct roles which civil society plays in supporting a secure and peaceful cyberspace.

With regard to the distinctive stakes which civil society has in cybernorms discussions, the actions of states and private actors in cyberspace can have a direct, immediate and serious effect on the public and on society. Moreover, civil society can be the direct target of cyberattacks, or work with affected communities – such as, for example, human rights defenders, journalists, security researchers and marginalised or vulnerable groups, such as women (Access Now 2019; Brown and Pytlak 2020). Outside of cybersecurity and cybernorms discussions, scholars and practitioners have reflected on the role of civil society in peace and security discussions more broadly, in preventing conflict and mitigating crises in a way that promote peace (Kavanagh and Stauffacher 2014) and as 'makers and managers of meaning', offering 'alternative visions to dominant government discourse' due to their status as 'moral entrepreneurs' (Khagram, Riker, and Sikkink 2005).

Similarly, the increased use of cyberspace and digital technologies for military and strategic purposes and the impact of these actions on individuals and communities establish a 'normative stake' for civil society, with their remit to protect the public interest (Kavanagh and Stauffacher 2014). The intended aim of cybernorms, including the UNGGE cybernorms, is to reduce tensions and support a peaceful and secure cyberspace: civil society consequently also has an interest and stake in the effective, and human-centric, implementation of cybernorms.

With regard to the varied and distinct roles which civil society plays in supporting a secure and peaceful cyberspace, literature on the roles of civil society has, to date, highlighted a wide range, including the building of trust through the convening of different stakeholders, the provision of expertise on technical subject areas and the monitoring of commitments through research and advocacy (EU Cyber Direct 2019; Kavanagh and Cornish 2019; Kavanagh and Stauffacher 2014) as well as the provision of 'information, insights methods and advice into policy processes which can replicate, confirm, reinforce and strengthen existing policy knowledge' (Scholte 2007). For the purpose of this paper, they are summarised around two roles which civil society plays in implementing or in supporting the implementation of cybernorms: direct engagement and participation, and fostering transparency and accountability.

Direct engagement and participation, including in supporting effective diplomacy and capacity building

Civil society engages directly in relevant forums, as well as building capacity and raising awareness among key stakeholders of normative frameworks like the UNGGE norms through the development of tools such as 'explainers' and training (Brown, Esterhuysen, and Kumar 2019; UNODA 2017). It also convenes track 1.5 and track 2 dialogues which bring together a range of stakeholders through forums for discussion and where civil society actors act as 'diplomatic actors' or convenors of different actors (EU Cyber Direct 2019; Kavanagh and Cornish 2019; Kavanagh and Stauffacher 2014). This convenor role is critical in not only raising awareness of norms, but also in developing a mutual understanding of the roles and responsibilities of different actors in the implementation of cybernorms and the wider framework or policy and regulatory environment in which they operate. Capacity building at the national level, which can support the implementation of cybernorms in national-level frameworks, can include the provision of expertise during the development and implementation of cybersecurity strategies and other policy or legal frameworks (Global Partners Digital 2020b). Civil society actors also advise delegations by organising or participating in consultations which inform state delegations prior to, or following, multilateral discussions (Kavanagh and Stauffacher 2014). Aside from this policy-related capacity building, capacity building can also refer to the sharing and building of technical knowledge required to implement cybernorms by responding to cyber incidents, mitigating the harm arising from them and, in the longer term, developing resilient networks.

Fostering transparency and accountability

Likewise, civil society plays a unique role in fostering transparency and accountability of state and private sector actions in cyberspace (Brown and Esterhuysen 2019). The report

of the 2019 Geneva Dialogue on Responsible Behaviour in Cyberspace acknowledged this by asking,

> how can civil society play a greater and more targeted role in promoting civilian oversight of national and international policy and strategy relating to ICT in the context of peace and security? How can this kind of oversight be applied to the growing interest of States in offensive capabilities and operations?. (Kavanagh and Cornish 2019)

While it is not possible in this paper to consider the range of literature sthat has examined the role of civil society in, for example, addressing democratic and legitimacy deficits in global governance mechanisms by demanding and providing greater accountability and transparency, it is acknowledged that there is a wide range of research and perspectives on this issue. Scholte, for example, has examined the roles global civil society actors play in addressing democratic deficits in global governance mechanisms since the spread of globalisation, particularly the role played in highlighting gaps in accountability and transparency in a range of global governance mechanisms, including international trade and finance mechanisms (2011), while Glasius has illustrated the role of civil society in providing accountability at the International Criminal Court (2008). Yet, as they point out, claims of international NGOs to legitimacy based on 'representativeness', require scrutiny and can actually serve to undermine civil society's legitimacy and accountability. Nonetheless, it is not claimed here that civil society should be seen to represent a 'global demos'; but rather that civil society has played, and continues to play, a role in supporting greater transparency and accountability in global governance institutions like the UN.

As mentioned above, civil society has played a key role – in other, more long-standing international peace and security discussions so far – in providing this independent oversight through research, lobbying for the creation of oversight bodies, and the development of international rules and standards (Kavanagh and Stauffacher 2014). Within UNGA's First Committee discussions about responsible state behaviour in cyberspace, some preliminary work has already occurred in the proposal of oversight mechanisms (ICT4 Peace Foundation 2020b), while outside of those discussions, the work of a wide university network in supporting independent and neutral technical attribution, and the work done by civil society networks in identifying threats – including through targeted vulnerability searches – provide examples of the ongoing efforts to promote transparency, accountability and independent oversight in the implementation of cybernorms (Mueller et al. 2019). The inclusion of civil society stakeholders who conduct independent research and oversight within cybersecurity discussions can also provide greater democratic legitimacy (Kavanagh and Stauffacher 2014), both domestically and internationally, by assuring other stakeholders that actions and decisions are not driven solely by political and ideological interests. It has also been recognised elsewhere that civil society has a distinct role to play in supporting independent oversight of the private sector and state obligations to protect and promote human rights (Brown and Esterhuysen 2019; Kavanagh and Stauffacher 2014). For example, civil society brings to light the impact of surveillance technologies sold by cybersecurity firms like NGO Group on human rights (Centre for Internet and Society 2020; Citizen Lab 2019), and the impact of the nexus of relationships between private companies who sell surveillance technologies and the nation states that use them. In this way, civil society stakeholders foster transparency and accountability for

actions in cyberspace – both of which are key incentives for the effective implementation of cybernorms.

It should be noted that these roles interlink and can overlap: for example, research can help in the interpretation of cybernorms and therefore contribute to capacity building and raising awareness; the sharing of research findings through track 1.5 and track 2 dialogues cannot only support greater transparency and accountability, it can be the basis for bringing different stakeholders together and thereby building trust and confidence between stakeholders. Each of the case studies below illustrates these roles and interlinkages.

Implementing the human-centric approach to cybernorms

The case studies below were chosen for regional diversity, as well as to illustrate the diversity in profile of civil society organisations that implement cybernorms, ranging from a technical non-profit organisation to a human rights organisation, and a multistakeholder civil society-led network organisation. The author has experience engaging with the organisations in a professional context and, as a result, approached the organisations to discuss their engagement in cybernorm implementation.

The information for the case studies below was collected through semi-structured interviews with senior staff members of the respective organisations and acknowledged in the acknowledgements section below. The information for the first case study was gathered through four 45-minute to 60 min-long interviews. The information for the second and third case studies was gathered through one longer interview, lasting about 90 min. The author took notes during the interviews and wrote drafts of the case studies on the basis of these notes. Following the completed interviews, drafts of each of the case studies were written and sent, along with the text of the article, to the respective interviewees. The interviewees, therefore, received the article and their case study – they did not receive the drafts of the two other case studies. They provided feedback on the text, which was incorporated into the final case studies published here.

The interviews began with a description of the intended aim of the journal article, that is to elaborate on the understanding of a human-centric approach to cybernorms implementation and to illustrate the role of civil society organisations in implementing a human-centric approach to cybernorms. The author also asked questions aimed at understanding the role of the organisation in the cybersecurity landscape and the context for its work in cybersecurity; their perception of their role in the cybersecurity landscape; relevant actions/activities undertaken; working methods, values and principles. These elements were explored so the author could understand if and how each organisation exemplified the facets of the human-centric approach in the implementation of cybersecurity activities and policy relevant to the agreed UNGGE cybernorms. The interviewees were interested in unpacking the understanding of a 'human-centric' approach, and in varied ways, identified with applying a human-centric approach to their work. In their feedback on the draft case studies, two out of three of the representatives of the organisations interviewed noted that they agreed with the analysis and expressed the view that this article had helped to build their own understanding of human-centric approaches to cybernorms implementation.

APNIC: building human fibres in incident response

APNIC is a regional internet registry that administers IP addresses for the Asia Pacific region. It is a member-based not-for-profit organiation whose primary role is to distribute and manage internet number resources in countries in the Asia Pacific region. The work of APNIC and internet registries more broadly can relate to the ongoing operationalisation of some of the 2015 UNGGE norms (UN General Assembly 2015) – most directly those related to preventing and mitigating cyber incidents, and 'incident response', a term used to describe the process by which an organisation handles a security breach or cyberattack, including the way the organisation attempts to manage the consequences of the attack or breach (Lord 2018). This includes the UNGGE norms on cybercrime (norm 'd'), vulnerability reporting (norm 'j'), attribution (norm 'b'), request for assistance (norm 'h') and computer security incident response team (CSIRT) coordination (norm 'k'). APNIC supports the implementation of these norms mainly by delivering capacity building efforts, which are holistic, long-term and focused on building lasting relationships and networks between relevant stakeholders.

Incident response requires capacity and interaction between different stakeholders who have established strong and trusted relationships. Mature technical capacity, for example the ability to analyse and provide advice on the technical nature of cyberattacks, and respond in a way to prevent them or mitigate their impact, cannot be meaningfully leveraged unless trusted relationships pre-exist between CSIRT communities and other stakeholders (vendors, internet service providers, law enforcement agencies, etc.) who respond to these attacks. This is important, considering there might be sensitive and political issues associated with those cyberattacks, such as state-sponsored attacks, and their possible impact on a range of stakeholders.

In order to support effective incident response, APNIC carries out technical capacity building efforts that include, as a primary part of their goals, the importance of connecting people and the building of trust between them; an essential 'resource' and enabler of incident response. For APNIC, capacity building involves bringing different stakeholders together, to clarify and understand security concepts and each other's roles, as well as the sharing of experiences and best practices with regards to managing a security response team and the tools and platforms that can also enable collaboration. Cyber incident 'role plays' and 'table-top exercises' are a key part of APNIC's capacity building work and help illuminate and address the wide range of challenges which incident responders face in their everyday work.

> In doing simulations, certain things have come up that CSIRTs have to deal with, real issues as to what information is disclosed to whom, so there are lots of human aspects as well as technical aspects. You can actually have a strong CSIRT providing basic services with just two people, because everyone is well connected to a wider trust-based CSIRT support ecosystem.

As this quote from a senior APNIC specialist illustrates, knowing and trusting the relevant actors in advance is key to effective incident response as cyber incidents or attacks can be sensitive in nature and bring up questions relating to process – about what kind of information is shared, with whom, and when.

In the last three years, APNIC has carried out dozens of capacity building training and community building initiatives in support of the development of new national CSIRTs in the Asia-Pacific region. These trainings bring a range of stakeholders together and have

nurtured the next generation of incident responders in different economies. Below, the lead facilitator of the training describes how important convening multistakeholder discussions are to ensure the sustainability and long-term success of CSIRTs.

> We want to make sure that: (a) everyone is on the same page and agrees on clear goals and objectives of a national CSIRT; (b) there is long-term continuity and sustainability after the CSIRT is launched (c) we clarify roles and responsibilities of different stakeholders, such as law enforcement agencies, network operators, civil society groups and the judiciary sector (d) we understand the security needs of the constituents that the CSIRT is serving. Finally, the CSIRT serves a long-term need, so having all stakeholders supporting their work is critical from the outset. The CSIRT can start with a low budget and few people and sustainably grow over-time according to local needs, also considering ongoing support networks.

In order to ensure webs of trust are sustained over time and scaled at the regional level, APNIC also maintains ongoing contact with participants of their capacity building programme through a fellowship programme, to help with which connecting incident responders from underrepresented countries and regions.

The implementation of cybernorms, including the UNGGE norms, depends primarily on the sharing and exchange of information. This in turn relies on trusted relationships which are built over time and sustained through capacity building workshops and the sharing of best practices. The bringing of communities together, to ensure a diversity of voices that understand the mutually dependent roles of different stakeholders, is part of building the 'human fibre' which supports capacity building and effective response capability. It also displays some of the key factors of the human-centric approach discussed in Section 1 of this paper; a centring of 'individuals' and humans as the main referent or benefiting party of cybersecurity, and the emphasis on inclusive governance. Through their workshops, APNIC also plays a range of roles identified in Section 2 of this paper; they build the capacity of key stakeholders and in so doing they act as convenors of multistakeholder dialogues, and they help to foster transparency and accountability by addressing cyber incidents through networks of trusted relationships. APNIC's website states 'fellows typically pass on the knowledge and skills they obtain through the programme to their local colleagues, helping to broaden the development of the Internet in the region'. However, participants of the workshops were not contacted, and it is therefore not possible to comment on how the workshops were perceived by the participants themselves. The purpose of this and the other case studies, however, is to showcase the work being done by civil society to support the implementation of norms; how this work is perceived by other stakeholders admittedly requires further research.

A focus on building 'human fibres' and connecting people lies at the heart of APNIC's capacity-building efforts. Yet, this can be difficult to carry out if there is a government-centric approach to CSIRTs, as governments are only one of a number of stakeholders in the incident response community. There is also the challenge of CSIRTs providing advice or assessment, particularly when it comes to addressing state-sponsored attacks. This can lead to a reluctance to share information with and between national CSIRT entities. It can also make dialogues between different actors impractical, as high-level security clearances and other obligations make it unlikely that certain incident responders will partake in multistakeholder discussions, thereby reducing opportunities for collaborative security approaches and direct and honest communication. Other challenges faced by CSIRTs include the impact of state-imposed sanctions in cyberspace, as they block

incident-response processes (FIRST 2019). Further research into the importance of CSIRT collaboration, the impact of policy instruments such as sanctions, and the role of incentivising cyber industry development and growth, including through human-centric capacity building workshops that focus on building trust between people, could therefore support greater cybersecurity and resilience within countries.

Fundación Karisma: supporting a rights-respecting vulnerabilities disclosure process in Colombia

Fundación Karisma (hitherto referred to as Karisma) is a civil society organisation dedicated to protecting digital rights in Colombia. It supports the human-centric and rights-based use of technologies in Colombia and the region, including through evidence-based research and advocacy.

In 2016, Karisma began to conduct simple audits of government website pages and apps as part of its work on protecting human rights in the digital age. Government websites store large amounts of personal data, which, in the context of recovery from a prolonged civil war, include highly sensitive data. Strong cybersecurity systems are key to protecting this data. However, Karisma's simple audits revealed a range of vulnerabilities that exposed citizens' data to misuse.

In order to raise awareness of, and address this issue, Karisma attended government meetings and solicited some support from the Ministry of ICT to implement principles of coordination, cooperation and distributed responsibility in disclosure of these vulnerabilities in government systems. However, varied levels of understanding, differing priorities, and reserve from other areas of the government revealed a climate of initial resistance and required a tailored approach, which took into account the different perspectives and priorities, in order to build trust and understanding. This included the hosting of round tables with different stakeholders, comparative analyses and a blog series which featured guest posts from the diverse perspectives represented in the government, as well as a series of recommendations on developing a rights-respecting vulnerability disclosure process which fed into consultations on the national cybersecurity strategy (NCSS). Throughout this time, Karisma worked to connect the government with technical security experts, including an independent cryptographer who was experienced in carrying out security audits for data protection authorities.

The NCSS, adopted in 2020, includes a government-wide commitment to developing a coordinated vulnerability disclosure process (Consejo Nacional De Política Económica Y Social República De Colombia 2020). For example, the strategy makes clear that the country's data protection authority, as well as government authorities, are required to have a publicly available form for vulnerability disclosure by third parties. The strategy also stipulates that its governance must be inclusive of other stakeholders. However, challenges remain. For example, ensuring the security of the government's database of vulnerabilities will require ongoing monitoring and independent oversight. Moreover, the author did not interview any of the stakeholders Karisma has engaged with; this may have revealed further challenges to ascertaining the substantive impact of the vulnerability equity process instituted.

Through its strong connections with the technical community, Karisma was able to act as a facilitator between stakeholder groups and bring the perspectives and expertise of

security researchers to the government's discussions. In this sense, they acted as a 'bridge' between the technical community, who, in the past, had lacked trust in reporting vulnerabilities, and the government. Karisma's participation in the NCSS process worked to bring to light vulnerabilities and support the development of a coordinated process and has had a direct impact on the ability of the government to implement the UNGGE norm on vulnerability processes. In parallel, it has worked to support the protection of a range of human rights which are increasingly impacted by cybersecurity practices, including the rights to privacy, to data protection and to health. Karisma is now participating in multilateral processes, including in the OECD, to share its experience of working with stakeholders to support the development of government vulnerability disclosure processes.

Karisma's work has also served as an inspiration to other civil society groups in the region, who, in the context of the COVID-19 pandemic and increased reliance on digital technologies, have started to conduct more security research, by working with technical experts to conduct technical analyses or by publishing reports of the legal aspects and ramifications of digital technology solutions to the pandemic. In this context of increased reliance on digital technology, the prosecution of security researchers and lack of clarity around vulnerability disclosure weaken cybersecurity and can directly impact human rights. Karisma has set up a dedicated technical team, 'K-lab', to support technical research, and it assists the capacity building of other organisations by publishing its auditing methodologies, raising awareness of the intersections between human rights and cybersecurity, and promoting the importance of evidence-based research through presentations at national and regional conferences.

Karisma's work on the Columbian government's vulnerability disclosure process displays the range of roles that civil society plays in cybernorm implementation, as explored in Section 2. In providing technical expertise through the conducting of audits, its research supported greater transparency and accountability. Furthermore, its independence as an NGO allowed it to play a unique role; as an outsider it was also able to see the disconnected nature of discussions among different government authorities and encourage a whole-of-government approach. It was able to advocate for a human-centric approach as its impetus, to ensure the respect of human rights, including the rights to privacy and data protection. This required bringing affected parties, such as security researchers, to the table. Going forward, its independence and expertise will also be imperative for monitoring the commitments in the country's NCSS, and ensuring that transparent processes which involve all stakeholders – so key to effective vulnerability disclosure – are respected.

KICTANet: bringing citizen's voices to critical infrastructure policy

The Kenya ICT Action Network (KICTANet) is a civil society-led multistakeholder platform composed of more than 300 active members, dedicated to ensuring open and inclusive internet governance policy discussions in Kenya. KICTANet was one of the founding members of the country's national internet governance forum, and its members regularly organise civil society-led multistakeholder convenings to input into national policy discussions relating to ICTs.

In 2015, KICTANet received information from the government relating to proposed changes in critical infrastructure protection policy, including the proposal for a law on critical infrastructure. However, the discussions contained no mention of ICT systems, despite the extensive and increased reliance of the population on the internet, particularly through mobile-based applications. KICTANet was invited to participate in a government meeting on critical infrastructure, where they brought to the fore the importance of ICT systems to critical infrastructure, including the need to address gaps in the ICT regulatory framework pertaining to the management of fibre optic cables. The provision and maintenance of fibre optic cables at the time was of increasing concern to local people and affecting local industries. Challenges included the lack of regulatory and policy guidance for the laying of fibre optic cables; this lack of clarity had led to the haphazard digging of trenches and side roads to lay cables for other infrastructure, such as waste management piping. This in turn led to the installation of subterranean infrastructure in a way that was highly disruptive to the provision of the internet to the local populations. The ongoing issues relating to the lack of reliable internet access in Kenya were directly affecting KICTANet members. As expressed by one KICTANet member:

> Internet access is 'in a way' a human right, because we are so dependent on it; there are different uses of it which are fundamental to the exercise of rights. In this sense, a functioning and stable internet is a critical infrastructure in and of itself, without which citizens are left unable to express themselves and access financial services. When people don't have it, it can amount to a denial of rights.

As a result of this direct stake in the discussions, KICTANet members attended government consultations on critical infrastructure and submitted a detailed input into the discussions. This included: recommendations to clearly define critical infrastructure and distinguish between critical ICT infrastructure (registry, content delivery networks) and traditional critical infrastructure; criteria for the identification of critical infrastructure and the importance of distinguishing between critical internet/ICT infrastructures and critical infrastructures connected to the internet; as well as a range of recommendations related to research and development strategies, coordination and risk management frameworks, and incident reporting mechanisms. It recommended the consideration of an overarching strategy or policy, instead of the passing of a law, to ensure a holistic and broad-based approach with the flexibility to adapt to changes in technological trends. It also highlighted the importance of considering the needs of local people, inclusive discussions and consultations, and transparent decision-making processes. KICTANet continued to participate in relevant policy discussions, including in discussions on the country's overarching ICT Policy, where critical infrastructure policy was ultimately subsumed. The ICT Policy, adopted in 2020, recognises the intersection of ICTs and critical infrastructure in Kenya and commits the government to 'address(ing) any gaps in a regulatory capacity, especially in the face of convergence of networks and services' (Ministry of Information, Communications and Technology (ICT) Policy, Kenya 2019). This will support the Kenyan government in implementing cybernorms related to critical infrastructure, including the UNGGE norms.

KICTANet's profile as a multistakeholder platform means that it is able to play a unique role in relevant discussions; bringing together the voices of different stakeholders, highlighting practical concerns (such as those around the unregulated digging of trenches

and the direct impact this has on local industries and the economy), raising awareness of, and translating legal and policy discussions for, affected stakeholder communities through tools and policy briefs. It has thereby played a role in promoting a human-centric approach to cybernorm implementation in Kenya which communicates the direct impact of policy measures on Kenyan citizens and is rooted in accountable and inclusive governance. However, it is important to note that while KICTANet does not purport to represent more than its members, it is not known whether its internal decision-making processes reflect an inclusive approach to representing its members' views. The KICTANet members interviewed described the process for collecting views of members but only senior members of the organisation were interviewed. As with the other case studies, the author did not interview other sources – such as those in government – with whom KICTANet engaged and therefore further research will be required to ascertain whether KICTANet's engagement in discussions relating to critical infrastructure policy continue to reflect the concerns of the citizens involved.

Summary

By positioning humans as the primary referent and benefactor of cybersecurity policies and measures, the human-centric approach to cybersecurity conceptualises threats in cybersecurity as those which undermine human rights and directly impact humans. It also understands security and human rights as mutually reinforcing. Therefore, in understanding cybersecurity as a positive enabler of human rights it follows that measures which undermine cybersecurity also undermine human rights. The international human rights framework acts as a basis or reference for the human-centric approach; its application to the digital environment is the subject of ongoing work done within national, regional and international human rights mechanisms, including the Human Rights Council.

As the case studies above aim to show, civil society comprises a range of stakeholders with expertise and a 'normative' stake in the implementation of cybernorms. As subject experts and facilitators, they support the implementation of cybernorms by convening track 1.5 and track 2 dialogues, conducting legal and technical analyses of cybersecurity policies and measures, and by carrying out tailored and multistakeholder capacity building which builds the 'human fibre' between relevant stakeholders. By conducting independent research, they also support and monitor commitments to cybernorm implementation and can thereby contribute to the building of trust between all stakeholders, which in turn supports democratic legitimacy.

This research and the case studies provided illustrate that civil society stakeholders already support the implementation of cybernorms, including the UNGGE cybernorms in a wide range of contexts. Future research in this area could: (1) further explore the intersection between human rights and cybernorm implementation, providing further guidance on how cybernorms can be implemented in a way which respects human rights in different contexts, and documenting examples of where actions by both state and non-state actors violate or undermine norms; (2) gather examples of cybernorm implementation by civil society stakeholders from a wider range of contexts and (3) expand understanding of the range of roles civil society plays in promoting a secure and stable cyberspace.

In particular, civil society stakeholders should consider the intersections of their work and the commitments made by state and private actors to cybernorms, and the roles they can play in supporting the implementation of cybernorms, for example through national cybersecurity strategies, and/or through technical research, policy recommendations, and work with communities directly affected by poor cybersecurity, or by cybersecurity policies which undermine human rights. In order to highlight the direct impact of cybersecurity on people and their communities.

Policymakers should actively engage civil society in cybersecurity policy discussions and processes at the national and regional levels, as well as those relevant to international peace and security in multilateral forums such as UNGA's First Committee. By holding open, inclusive and transparent consultations with civil society, policymakers can benefit from the range of expertise and knowledge within civil society to implement a human-centric approach to cybernorms, and thereby adhere to protect human rights their commitments to implement cybernorms which are intended to build a peaceful and secure cyberspace.

Acknowledgements

The author is grateful to Adli Wahid (APNIC), Pablo Hinjosa (APNIC), Grace Githaiga (KICTANet), Victor Kapiyo (KICTANet), and Amalia Toledo (Fundación Karisma) for their indispensable contributions to the case studies, as well as Lea Kaspar (GPD) for her review and feedback on the first draft of this article.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Sheetal Kumar is Senior Programme Lead at Global Partners Digital where she provides strategic oversight for a global cybersecurity and human rights programme which supports the facilitation of civil society perspectives into global level cybersecurity policy discussions and supports civil society organisations to protect and promote human rights in cybersecurity policy discussions. She acts as liaison civil society partners and provides practical research, facilitation, and coordination support on a day-to-day basis to enhance their ability and effectiveness to influence cyber-related policies at the national, regional and global levels. She has facilitated the engagement of civil society into a wide range of global policy spaces, including UNGA First Committee discussions and UN WSIS+10 negotiations, in order to promote more open, inclusive and transparent policymaking processes.

References

Scholte, Jan Aart. 2007. "Civil Society and the Legitimation of Global Governance." *Journal of Civil Society* 3 (3): 305–326. https://doi.org/10.1080/17448680701775796.

Scholte, Jan Aart. 2011. "Towards Greater Legitimacy in Global Governance." *Review of International Political Economy* 18 (1): 110–120. https://doi.org/10.1080/09692290.2011.545215.

Access Now. 2019. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-accessnow.pdf.

Boulanin, Vincent. 2016. "Information and Communication Technology, Cybersecurity and Human Development." Sipri. https://www.sipri.org/yearbook/2016/10. Accessed March 5, 2021.

Brown, Deborah. 2020. "It's Time to Treat Cybersecurity as a Human Rights Issue." (blog) *HRW*, May 26. https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue.

Brown, Deborah, and Anriette Esterhuysen. 2017. *A Rights-Based Approach To Cybersecurity: A Pipe Dream Or A Critical Means To A Secure And Stable Internet? Recommendations And Considerations*. Creative Commons Licence: Attribution 4.0 International (CC BY 4.0): Association of Progressive Communications. https://www.apc.org/sites/default/files/IGF17-_A_rights-based_approach_to_cybersecurity_-_recommendations_201807018.df.

Brown, Deborah, and Anriette Esterhuysen. 2019. "Why cybersecurity is a human rights issue, and it is time to start treating it like one." (blog) *APC*, November 28. https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one.

Brown, Deborah, Anriette Esterhuysen, and Sheetal Kumar. 2019. Review of Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms. Global Partners Digital and Association of Progressive Communications. https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/.

Brown, Deborah, and Allison Pytlak. 2020. "Why Gender Matters in Cybersecurity". Women's International League for Peace and Freedom and the Association for Progressive Communication. *Reaching Critical Will*. https://www.reachingcriticalwill.org/resources/publications-and-research/publications/14677-why-gender-matters-in-international-cyber-security.

Centre for Internet and Society. 2020. Comments on the 'Pre-Draft' Report of the United Nations Open-Ended Working Group. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-accessnow.pdf.

Citizen Lab. 2019. "NSO Group/Q Cyber Technologies: Over One Hundred New Abuse Cases." *Citizen Lab*, October 29. https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

Consejo Nacional De Política Económica Y Social República De Colombia, Departamento Nacional De Planeació. 2020. *Política Nacional De Confianza Y Seguridad Digital*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf.

Deibert, Ronald J. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32 (4): 411–424. https://doi.org/10.1017/s0892679418000618.

Deibert, Ronald. 2020. *Reset: Reclaiming the Internet for Civil Society*. Toronto: House Of Anansi Press.

Dunn Cavelty, Myriam. 2012. "The Militarisation of Cyberspace: Why Less May be Better". *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolkowski. NATO CCD COE Publications. https://ccdcoe.org/uploads/2012/01/2_6_Dunn-Cavelty_TheMilitarisationOfCyberspace.pdf

Dunn Cavelty, Myriam. 2014. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20 (3): 701–715. https://doi.org/10.1007/s11948-014-9551-y.

EU Cyber Direct. 2019. "*Strengthening the Multi-stakeholder Approach*". *EU Cyber Direct*, November 25. https://eucyberdirect.eu/content_events/strengthening-the-multi-stakeholder-approach/.

Forum of Incident Response and Security Teams (FIRST). 2019. Position paper by the Forum of Incident Response and Security Teams on cybersecurity developments within the UN context, submitted to Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2–4 December 2019). https://www.un.org/disarmament/wp-content/uploads/2019/12/oewg-position-paper-first-v20191209.pdf.

Freedom Online Coalition. 2020. "Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies". https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf.

Glasius, Marlies. 2008. "Global Justice Meets Local Civil Society: The International Criminal Court's Investigation in the Central African Republic." *Alternatives: Global, Local, Political* 33 (4): 413–433. https://doi.org/10.1177/030437540803300402.

Global Partners Digital. 2020a. "Pre-draft of the OEWG's report on ICTs: Global Partners Digital response". *Reaching Critical Will*, March. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-gpd.pdf.

Global Partners Digital. 2020b. "*Toolkit for Inclusive and Value-based Cybersecurity Policymaking.*" *Global Partners Digital*, August 26. https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/.

Healey, Jason. 2020. "The Cyber Budget Shows What the U.S. Values – And It Isn't Defense." *Lawfare Blog*, June 1. https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense.

ICT4 Peace Foundation. 2020a. "Comments on the Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security." *Reaching Critical Will*, March. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/comment-ict4peace.pdf.

ICT4 Peace Foundation. 2020b. *ICT4Peace Proposed States Cyber Peer Review Mechanism for State-Conducted Foreign Cyber Operations*. https://ict4peace.org/wp-content/uploads/2020/03/ICT4Peace-Proposed-States-Cyber-Peer-Review-3.pdf.

Kavanagh, Camino, and Paul Cornish. 2019. *Geneva Dialogue on Responsible Behaviour in Cyberspace: Phase 1 Report*. https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Final-Report.pdf.

Kavanagh, Camino, and Paul Cornish. 2020. "Cyber Operations and Inter-State Competition and Conflict: The Persisting Value of Preventive Diplomacy." EU Cyber Direct, September 7. https://eucyberdirect.eu/content_research/cyber-operations-and-inter-state-competition-and-conflict-the-persisting-value-of-preventive-diplomacy/.

Kavanagh, Camino, and Daniel Stauffacher. 2014. *A Role for Civil Society? ICTs, Norms and Confidence Building Measures in the Context of International Security*. Geneva: ICT4Peace Foundation. https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2104-A-Role-For-Civil-Society.pdf.

Khagram, Sanjeev, James Riker, and Kathryn Sikkink. 2005. *Restructuring World Politics: Transnational Social Movements, Networks, and Norms*. Minneapolis: University of Minnesota Press.

Kilovaty, Ido. 2019. "An Extraterritorial Human Right to Cybersecurity." *Papers.Ssrn.Com*, July 19. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3422938.

Klein, Joëlle, and Kamrul Hossain. 2020. "Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change." *Arctic Review on Law and Politics* 11: 1–18. https://doi.org/10.23865/arctic.v11.1936.

Lewis, David, and Nazneen Kanji. 2009. *Non-governmental Organizations and Development*. London: Routledge.

Liaropoulos, A. 2015. "A Human-centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia." *Journal of Information Warfare* 14 (4): 15–24. https://www.jstor.org/stable/26487503.

Lord, Nate. 2018. "What is Incident Response?" Digital Guardian, September 7. Accessed October 15, 2020. https://digitalguardian.com/blog/what-incident-response.

Ministry of Information, Communications and Technology (ICT) Policy, Kenya. 2019. National ICT Policy. Ministry of Information, Communications and Technology, Kenya. https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf.

Mueller, Milton, Karl Grindal, Brenden Kuerbis, and Farzaneh Badiei. 2019. "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?" *The Cyber Defense Review* 4 (1): 107–122. https://www.jstor.org/stable/26623070?seq=1.

Organization for Security and Co-operation in Europe. 2019. *Summary Report: A Human Rights-centred Approach to Technology and Security*. Vienna, November 8. https://www.osce.org/files/f/documents/e/b/442384.pdf.

Prince, Conrad. 2020. "On the Offensive: The UK's New Cyber Force". *RUSI*, November 23. https://rusi.org/commentary/offensive-uk-new-cyber-force.

Pytlak, Allison. 2020. "In Search of Human Rights in Multilateral Cybersecurity Dialogues." In *Routledge Handbook of International Cybersecurity*, edited by Eneken Tikk and Mika Kerttunen, 65–78. London: Routledge. https://doi.org/10.4324/9781351038904-7.

Reaching Critical Will. 2020. *"Cyber Peace & Security Monitor, Vol.1, No. 7", Reaching Critical Will*, March 30 2021. https://reachingcriticalwill.org/disarmament-fora/ict/oewg/cyber-monitor/14659-cyber-peace-security-monitor-vol-1-no-7

United Nations General Assembly resolution 70/237. 2015. Report of the First Committee (A/70/455). https://undocs.org/en/A/RES/70/237.

United Nations Office for Disarmament Affairs (UNODA). 2017. *Civil Society and Disarmament: 2017. Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary*. https://www.un.org/disarmament/publications/civilsociety/civil-society-and-disarmament-2017/.

United Nations Trust Fund for Human Security. 2018. "What Is Human Security?" *The Human Security Unit*. https://www.un.org/humansecurity/what-is-human-security/.

Women's International League for Peace and Freedom. 2020. "Responses to the pre-draft of the Final Report of the UN OEWG on developments in the field of information and telecommunications in the context of international security." Reaching Critical Will, April. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/WILPF_OEWG_response_April2020.pdf.

WSIS Executive Secretariat. 2005. *Wo.1rld Summit on the Information Society – Tunis Agenda for the Information Society*. Tunis: ITU. Accessed October 15, 2020. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc.