Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015

This contribution is submitted by the United Kingdom's Multi-stakeholder Advisory Group on Cyber issues and should not be considered to represent the views of Her Majesty's Government.

Executive Summary

The UN Group of Governmental Experts (GGE) agreed norms of responsible state behaviour in cyberspace by consensus in 2010, 2013, and 2015. Those consensus norms are an important contribution to establishing how international law applies in cyberspace. The United Kingdom (UK) recognises cyberspace as a fundamental element of securing critical infrastructure and an essential foundation for economic and social activity online[1]. The UK reaffirms its commitment to a free, open, peaceful and secure cyberspace. The UK acknowledges that implementing the agreed, voluntary, and non-binding norms cannot be achieved by states alone, but requires cooperation with and the expertise of many stakeholders including the private sector, academia, civil society, and other experts.

In an effort to encourage transparency, the sharing of best practices, and increase mutual understanding, the United Kingdom's informal and ad hoc Multi-stakeholder Advisory Group on Cyber issues, formed of non-governmental stakeholders and sponsored by the UK Government, is submitting this written contribution to the Open-Ended Working Group (OEWG) Intersessional meeting with Industry Partners and NGOs (2-4 December 2019). The contribution presents the work and practical steps taken by diverse stakeholders to operationalise on a voluntary basis the norms developed by the UN GGE. This includes ongoing efforts, case studies, cooperation and coordination with government entities, and lessons learned. The paper first sets out general efforts being undertaken by stakeholders, followed by efforts related to specific norms.

Ongoing efforts by stakeholders to promote agreed UN GGE norms

Alongside supporting the implementation of individual norms as detailed below, stakeholders in the UK – often in cooperation with international counterparts - have been crucial in promoting the norms. This work is an important element of the wider international cyber stability framework which underpins UN GGE and OEWG discussions.

Implementing norms to promote cybersecurity and stability in cyber space requires action and commitment by all stakeholders, and is an ongoing process which will need to be evaluated, adapted, and readdressed as technology and risks evolve. It needs to be an agile and iterative process. The examples given in this paper are non-exhaustive. Many non-governmental stakeholders in the UK are working with international partners to implement existing norms. Initiatives like those set out in this paper show the importance of ongoing dialogue and information sharing to work together to take practical steps to implement the

[1] https://www.un.org/disarmament/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.p

voluntary, non-binding norms recommended by the UN GGE reports in 2010, 2013, and 2015.

A key, positive aspect of the initiatives is multistakeholder engagement. Industry, academia, civil society, the technical community and all experts must avoid silos and work together to develop, adopt and implement norms. This cooperative approach is illustrated with examples of work by Chatham House, Global Partners Digital, Vodafone, Queen's University Belfast, and the IoT Security Foundation – not only in their coordination with the UK government and other governments, but also with non-governmental and private sector stakeholders. This is particularly important for capacity building and coordinated efforts to address cybersecurity and Internet issues.

For example, Chatham House, the Royal Institute for International Affairs, currently has a call for papers for a special issue of its peer-reviewed Journal of Cyber Policy with the hashtag #Cyberspace4All. The issue is being implemented in tandem with the OEWG and UN GGE processes and is aimed at creating a 'body of knowledge on global cyber governance to help inform policy development in this area'[2]. The project will bring together authors from diverse stakeholder groups, disciplines and geographic regions. It will be supplemented with a series of multimedia products including bespoke videos, explainers and podcast series to provide a clear narrative on global cyber governance, communicated clearly and succinctly to a general audience. Through audio-visual mediums, the multimedia outputs will help to build capacity in the general public's understanding of the importance of cyber governance and the key issues.

In 2019 Chatham House held three workshops and roundtables as part of the project 'Implementing the Commonwealth Cybersecurity Agenda', funded by the UK Foreign and Commonwealth Office. Focusing on both a global and Commonwealth perspective, the multistakeholder meetings took place in Ethiopia, Barbados, and London. In Addis Ababa, five UNGGE representatives took part in the meeting in addition to representatives to the UN OEWG, academia, civil society, and industry. The Addis Ababa meeting in October 2019 focused on pillars of the Commonwealth Cyber Declaration related to agreed norms in areas such as applicability of international law, responsible state behaviour and confidence-building measures – both in promoting frameworks and furthering discussions[3]. These efforts together increase transparency, enable the development of mutual understanding, and facilitate the promotion of best practices among stakeholders.

Other capacity building activities undertaken by Chatham House include a global cyber conference in Jordan, to be held in May 2020. This conference will bring together regional stakeholders including governments, civil society, academia and industry, to discuss the issue of global cyber governance from a Middle East and North African perspective. In addition, a research paper on 'The application of international law to states' cyber operations below the use of force: sovereignty and non-intervention' will be published in December 2019. The

[2] https://think.taylorandfrancis.com/cyber-policy-cyberspace-governance/?utm_source=TFO&utm_medium=cms&utm_campaign=JOK12208

[3] https://www.chathamhouse.org/event/cyber-governance-commonwealth-towards-stability-and-responsible-state-behaviour-cyberspace

paper aims to provide some food for thought in addressing some of the questions and ambiguities in this area, and to offer interpretative possibilities at a time when a number of states are starting to form and publicize their views on how these principles might apply in relation to states' actions in cyberspace.

Global Partners Digital (GPD)[4], a UK-based civil society organisation, contends that cyber norms play an important role in advancing understanding of both state and non-state obligations in cyberspace, and thus in promoting a peaceful and secure cyberspace. They consider it is imperative that the development of new norms and the implementation of existing norms happens in an open, inclusive and transparent manner. With regard to the norms adopted as part of the UN GGE's responsible state behaviour framework (2015), GPD suggests that civil society has important roles to play in implementing current frameworks of cyber norms. This includes through the collection and provision of data and research, understanding and documenting the contributions of relevant stakeholders, and raising awareness of cyber norms among all relevant stakeholders. For example, UK stakeholders including GPD and academics from the London School of Economics co-organised a workshop at the 2019 Internet Governance Forum in Berlin on the role of the technical community in promoting cyber norms[5].

Industry's expertise and role in innovating and enabling technologies also has a significant role to play in implementing norms. As the example of Vodafone illustrates in this paper, industry can incorporate best practices into their everyday business processes and engage with stakeholders to promote and implement norms. Examples provided here include transparency programmes and reporting, engaging with industry bodies and multistakeholder initiatives, and formalising governance processes, controls, and policies.

In their own way, each of these examples from the UK supports transparency, sharing of best practices, and increased mutual understanding of how international law applies in cyberspace, and voluntary, non-binding implementation of the norms agreed in the UN GGE reports of 2010, 2013 and 2015. Developing and supporting these and other initiatives will bring us closer to creating a free, open, peaceful and secure cyberspace.

Stakeholder Efforts to promote particular agreed UN GGE norms

Norm 1 (UNGGE 2015 report, paragraph 13a) – Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are agreed to be harmful or that may pose threats to international peace and security.

Technical standards development where standards are industry-led, consensus driven, interoperable and global enables the stability and the security in the use of ICTs. Standards

[4] The text and examples provided by Global Partners Digital also appear in a forthcoming publication "Unpacking the GGE's framework on responsible state behaviour: norms", authored by Deborah Brown and Anriette Esterhuysen (Association of Progressive Communications) and Sheetal Kumar (Global Partners Digital).

create the basis for technology to develop in a consistent and global manner. This stability provides the basis upon which norms and measures can be applied consistently and universally.

The development of 5G has been driven by the needs of global industry in the 3rd Generation Partnership Project (3GPP), an alliance of standards developing organisations from across the globe. Industry from all over the world participate and cooperate across geographical and geopolitical divides in order to reach a consensus agreement for the technical standards used for deployment of the next generation of mobile networks. Practically, this means that a consumer can use their 5G enabled mobile phone in almost any country around the world.

UK industry and other stakeholders participate actively in 3GPP to discuss, debate and development standards for global 5G deployment. Though industry is the lead, all stakeholders take part.

Norm (1) calls on states to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security. Some technologies and practices could pose risks to human rights if not used in a manner consistent with applicable international human rights law, e.g., any unlawful or arbitrary use of facial recognition or other biometric technologies to conduct surveillance, ordering of network shutdowns, any unlawful or arbitrary surveillance by states and any disproportionate restrictions of content, that violate international law. These practices have been widely documented in research carried out by civil society organisations, with recommendations, with recommendations provided on how to address these practices[6].

Norm 2 (UNGGE 2015 report, paragraph 13b) – In case of ICT incidents, States should consider all relevant information, including, inter alia, the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences

To overcome the challenges of attribution in the ICT environment, highlighted in Norm 2, it is important to work with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of human rights. A lack of attribution, or misattribution can lead to the escalation of tensions between states which may harm human rights by increasing the potential for attacks which compromise access to essential services and the integrity of data. Civil society organisations can bring the perspectives and voices of otherwise underrepresented and vulnerable communities who are disproportionately affected by cyberattacks, as well as provide information on the impact of cyberattacks on the enjoyment of human rights.

[6] See for example, "Freedom on the Net", Freedom House, https://freedomhouse.org/report-types/freedom-net; Association for Progressive Communications, https://www.apc.org/en/publications; Access Now, https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/; Open Observatory of Network Interference, https://ooni.org/

Private sector sources, including cybersecurity companies, developers and communications service providers (CSPs) provide much of the technical information required for accurate attribution. The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative which allows stakeholders to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact of cyber threats on UK business[7].

Norm 3 (UNGGE 2015 report, paragraph 13c) – States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

The implementation of Norm 3 is dependent on capacity building and technical assistance. The digital divide means that some states, especially developing and least developed countries. currently lack the capacity to recognise or act upon the use of their territory for internationally wrongful acts. Capacity building is crucial, first for some states to understand that the norm exists, and then to start to build the capabilities required for the successful implementation of the norm. Currently, much of the required expertise sits within the private sector and technical communities. UK stakeholders are actively involved in the Global Forum on Cyber Expertise, as members (Vodafone)[8] and as part of the advisory committee (Chatham House, co-chair cybercrime working group[9]). Academics from the University of Cardiff have been active in promoting capacity building, for example by hosting a dedicated conference involving international stakeholders on capacity building in Internet governance and cybersecurity[10]. The Centre for Secure Information Technologies (CSIT)[11] at Queen's University Belfast have been actively promoting capacity building through their annual World Cyber Security Summit[12], now approaching its 10th year. CSIT played a key role in establishing the Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity[13] (Global EPIC) alongside the Hague Security Delta (Netherlands), Global Cyber Resource at Carleton University (Canada) and Cyberspark (Israel) and it now connects 28 such ecosystems around the world with the aim of facilitating knowledge exchange as well as building research, innovation and technical collaborations and capability in host regions.

According to international human rights law, states must protect against human rights abuses within their territory and/or jurisdiction by third parties, including business enterprises. Human rights defenders play a role in supporting the state's obligations by monitoring and reporting these abuses where they involve the use of ICTs and thereby help support state actors to hold private actors to account[14].

[7] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
[8] https://www.thegfce.com/organization/members
[9] https://www.thegfce.com/organization/advisory-board
[10] https://www.cardiff.ac.uk/news/view/1009969-gigarts2018
[11] https://www.qub.ac.uk/ecit/CSIT/
[12] https://www.qub.ac.uk/ecit/Events/
[13] https://globalepic.org/
[14] For example, see Amnesty International, https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/; Citizen Lab, https://citizenlab.org/2017/06/reckless-exploit-mexico-nso/

Norm 4 (UNGGE 2015 report, paragraph 13d) – States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

For Norm 4 to be implemented effectively, the measures adopted by states to address terrorist and criminal use of ICTs need to be human-rights respecting. Yet, as documented by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, the restriction of rights and closing of civic space as part of measures to address criminal and terrorist use of ICTs represent an increasing trend. Civil society groups in the UK, and cooperating with international partners, are playing an important role in documenting these practices, as well as in providing concrete guidance on how states can cooperate to address criminal and terrorist use of ICTs while protecting human rights[15].

Norm 5 (UNGGE 2015 report, paragraph 13e) – States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions A/HRC/RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age), to guarantee full respect for human rights, including the right to freedom of expression;

Vodafone is a leading example of how industry contributes to implementing Norm 5, through its sustainable business strategy[16], including commitments to operate responsibly and ethically, and its corporate transparency programme. Vodafone's transparency disclosures on matters related to digital human rights include its policies, approach and principles regarding government access to customer data, and its approach to managing issues such as freedom of expression, censorship and the digital rights of the child[17]. Vodafone was a founding member of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy, which was created in order to advance freedom of expression and privacy rights in the telecoms industry. Vodafone's policies and process align with the Telecommunications Industry Dialogue Guiding Principles on Freedom of Expression and Privacy. In March 2017, Vodafone became a member of the multi-stakeholder Global Network Initiative[18].

[15] See for example, "UPR reports", Front Line: International Foundation for the Protection of Human Rights Defenders, https://www.frontlinedefenders.org/en/upr-reports; "Global Statement on the 20th Anniversary of the UN Declaration on Human Rights Defenders" by CIVICUS: World Alliance for Citizen Participation, https://www.civicus.org/index.php/media-resources/news/3717-global-statement-on-the-20th-anniversary-of-the-un-declaration-on-human-rights-defenders-2; "Terrorism/Counterterrorism", Human Rights Watch, https://www.hrw.org/topic/terrorism-counterterrorism; Amnesty International, https://www.amnesty.eu/news/category/statements-and-reports/human-rights-and-counter-terrorism-statements-and-reports/

[16] https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/sustainablebusiness2019.pdf

[17] See https://www.vodafone.com/content/index/about/sustainability/operating-responsibly/human-rights/digital-rights-and-freedoms.html

[18] https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone_drf_alignment_telecom_industry_dialogue_principles.pdf

Civil society human rights defenders also play a role in implementing Norm 5, by documenting state practices at the national level, conducting research and litigation, and using mechanisms at the regional and global level, in particular the UN Human Rights Council, the Special Procedure system, the Treaty Body system, the Universal Periodic Review (UPR) and the Office of the High Commissioner for Human Rights (OHCHR), to highlight both good practice and violations of human rights. The research and advocacy work conducted by civil society in this regard is crucial in providing the evidence base that promotes compliance with the human rights commitments referred to in this norm.

Due to the dependence of individuals and societies on ICTs in the digital age, measures which increase stability and security in the use of ICTs can be an enabler for the enjoyment of human rights. Therefore, measures which weaken cybersecurity, such as measures which introduce vulnerabilities or backdoors into software and hardware, both undermine human rights and weaken the security and stability of cyberspace. The importance of technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity and human rights have been widely researched and documented by civil society[19].

Norm 6 (UNGGE 2015 report, paragraph 13f) - A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

The protection of critical infrastructure - which may include transport, water and wastewater systems, food and agriculture, electricity, financial services and telecommunications - is essential for the enjoyment of a wide range of human rights, including the rights to health, work and education. Resolution 58/199 refers to eleven measures that can be taken to protect critical infrastructure, including the promotion of "partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information" and the training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities." Civil society groups currently carry out simulation exercises and training, as well as promote national and international research, and the application of security technologies that meet international standards[20].

Norm 7 (UNGGE 2015 report, paragraph 13g) – States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account, inter alia,

[19] APC's Internet Rights programme and the Universal Periodic Review, https://www.apc.org/en/project/universal-periodic-review ; "Travel Guide to the Digital World: Encryption policy for human rights defenders"; Global Partners Digital, https://www.gp-digital.org/publication/travel-guide-to-the-digital-world-4-encryption-policy-for-human-rights-defenders/; "Defending the right to privacy globally: 8 key recommendations for the digital age"; Access Now; https://www.accessnow.org/defending-the-right-to-privacy-globally-8-key-recommendations-for-the-digital-age/; "Encryption", Internet Society, https://www.internetsociety.org/issues/encryption/

[20] See, for example, Chatham House, https://www.chathamhouse.org/publication/annual-review-2017-18; DiploFoundation, https://www.diplomacy.edu/cybersecurity; Internet Society, https://www.internetsociety.org/resources/

General Assembly resolution 58/199 (2003) "Creation of a global culture of cybersecurity and the protection of critical information infrastructure", and other relevant resolutions;

Cooperation between stakeholders is necessary to create a global culture of cybersecurity and meet the challenges of protecting critical infrastructure from ICT threats. UK stakeholders have played leading roles in multistakeholder commissions, such as the Global Commission on Internet Governance and the Global Commission on the Stability of Cyberspace, both of which have advocated for improvements in basic cyber hygiene.

Much critical infrastructure, whilst subject to regulation, is owned and managed by the private sector. Where higher standards and processes are adhered to, the more resources are available to focus on real threats. Any approaches which strengthen general cyber resilience will help create more robust critical infrastructure, whether the threat arises from bad actors or from failures in basic cyber hygiene. For instance, Vodafone has strict governance processes and controls in place to protect customer personal data, respect their privacy and proactively manage the cyber security risks[21]. Vodafone is committed to continuing to make significant investments in the network infrastructure, coverage and quality that will be required for a competitive economy and to deliver a high-quality service[22].

Norm 8 (UNGGE 2015 report, paragraph 13h) - States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty;

UK non-governmental stakeholders have long experience in voluntary coordination and cooperation through Computer Emergency Response Teams (CERTs). Computer incident response teams represent a wide range of organisations, including non-government actors. The network "FIRST" for example, includes as part of its membership, civil society organisations who provide incident response support for vulnerable populations[23]. The network "Computer Incident Response Center for Civil Society", or CiviCERT[24], is a network of CERTs, Rapid Response teams, and independent Internet Content and Service Providers focused on supporting civil society to prevent and address digital security issues.

Norm 9 (UNGGE 2015 report, paragraph 13i) – States should take reasonable steps to ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

The IoT Security Foundation (IoTSF) is a UK based, collaborative, vendor-neutral, non-profit organisation. Work is member-driven and members include industry and topic experts from around the world. IoTSF's mission is to help secure the IoT. As expressed by the UK, the IoTSF recognises a

[21] See https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/sustainablebusiness2019.pdf, at pages 53-55.
[22] https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/sdgs.pdf
[23] FIRST membership, https://www.first.org/members/map
[24] CiviCERT, https://www.civicert.org/

need to adopt IoT security best practices, such as a 'secure by design' approach to products and take the burden of security away from consumers.

To realise this aim, the IoTSF has developed a series of documents for IoT stakeholders such as product developers, original equipment manufacturers (OEM) managers, and vendors to foster the adoption of IoT security best practices[25]. IoTSF has also developed materials aimed at policymakers, regulators and IoT providers and vendors. For example, one report explored regulatory structures in 5 different jurisdictions to better understand how existing legislation may be applicable to the IoT[26].

The development of national guidance, globally applicable technical standards and internationally recognised industry-led guidance highlights the benefits of stakeholders working together toward transparency, sharing of best practices, and increasing mutual understanding in order to create a shared body of knowledge and operationalise agreed norms. For example, a study by the UK Department of Digital, Culture, Media and Sport found the IoTSF's publications to be the most closely mapped guidance to the UK Consumer IoT Security Code of Practice - which was the basis of the ETSI TS 103 645 standard.

The Centre for Secure Information Technologies (CSIT) at Queen's University Belfast leads the UK Research Institute in Secure Hardware and Embedded Systems (RISE)[27] which seeks to identify and address key issues that underpin our understanding of hardware security. Supported by the UK National Cyber Security Centre (NCSC) and Engineering and Physical Sciences Research Council (EPSRC), RISE was established to address a number of research challenges in hardware security and develop cutting edge solutions to these challenges:

- Understanding the technologies that underpin hardware security, the vulnerabilities in these technologies and development of countermeasures.
- Maintaining confidence in security throughout the development process and the product lifecycle.
- Hardware security use cases and consideration of value propositions.
- Security development.

Vodafone Group is taking a lead in trialling innovative new technology in Europe that promises to greatly increase the number of companies that can supply mobile network equipment to telecom operators. The global supply of telecom network equipment has become concentrated in a small handful of companies over the past few years, creating 'too big to fail' supply chain risks. More choice of suppliers will safeguard the delivery of services to all mobile customers, increase flexibility

[25] See, for example Secure Design Best Practice Guides (Release 2, 2019): https://www.iotsecurityfoundation.org/wp-content/uploads/2019/11/Best-Practice-Guides-Release-2.pdf; IoT Security Compliance Framework: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

[26] IoT Cybersecurity: Regulation Ready (2018) https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Cybersecurity-Regulation-Ready-White-Paper-Full-Version.pdf

[27] https://www.ukrise.org/

and innovation and help address some of the cost challenges that are holding back the delivery of internet services to rural communities and remote places across the world[28].

Confidence in the security of ICT products is critical for the exercise of a range of human rights including the rights to freedom of expression, the right to privacy and other civil and political rights, and a range of economic, cultural and social rights, including the right to work, to health. Ensuring the integrity of the supply chain requires that cybersecurity-related laws, policies and practices uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services.

Human rights organisations have already played a role by highlighting the proliferation of malicious ICTs and techniques, in defending human rights in supply chains by developing tools such as 'human rights impact assessments' and in monitoring compliance with human rights standards. They have also recently developed a tool for assessing human rights impact of internet registries[29].

Norm 10 (UNGGE 2015 report, paragraph 13j) – States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

Good practices relating to vulnerability disclosure include protecting security researchers and clearly outlining the roles and responsibilities of all stakeholders, including vendors, in reporting processes. Vulnerability disclosure is widely recognised as a security best practice, particularly as more 'things' are added to networks with varied security capabilities. In addition to norms, efforts to increase responsible vulnerability reporting include government guidance (e.g. the UK Consumer IoT Security Code of Practice), internationally recognised technical standards (e.g. ETSI TS 103 645), and specialised agencies (e.g. ENISA Good Practice Guide on Vulnerability Disclosure).

However, a recent study by the IoTSF found that fewer than 10% of IoT product companies had a vulnerability disclosure scheme available to researchers. To facilitate the uptake of vulnerability disclosure and make the practice more accessible to a wider range of IoT providers, the IoTSF has developed best practice guidance based on member (industry and subject-matter expert) contributions[30]. The IoTSF will continue to work to increase awareness and accessibility of vulnerability disclosure, particularly as related to the IoT.

Civil society organisations have a role to play in ensuring that processes for responsible state disclosure exist, that they do not criminalise security researchers, and that they are aligned with best practice[31].

---

[28] See, for example https://www.vodafone.com/news-and-media/vodafone-group-releases/news/vodafone-pioneers-innovative-network-tech-to-increase-suppliers-and-extend-rural-internet-access

[29] See, for examples Reckless VI, Citizen Lab, https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/; Business and Human Rights Resource centre, https://www.business-humanrights.org/; "Assessing the human rights impacts of Internet registries", Article 19, https://www.article19.org/resources/assessing-human-rights-impacts-internet-registries/.

[30] Vulnerability Disclosure: Best Practices Guidelines (Release 1.1 2017): https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf

[31] See, for example Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges**,** CEPS**,***https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/*

Norm 11 (UNGGE 2015 report, paragraph 13k) – States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity;

Civil society organisations have a role to play in ensuring the establishment and operation of computer incident response teams in a manner that is independent and transparent[32]. This is important from a rights perspective to ensure that a computer incident response team carries out its work without impinging on freedom of expression or privacy.

[32] See, for example National CSIRTs and Their Role in Computer Security Incident Response, New America Foundation, https://www.newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/