Global Policy Volume 9 . Supplement 3 . November 2018

CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy

Leonie Maria Tanczer, Irina Brass and Madeline Carr

University College London, Department of Science, Technology, Engineering and Public Policy

Special Issue Article

Abstract

Ongoing efforts by state actors to collaborate on addressing the challenges of global cybersecurity have been slow to yield results. Technical expert communities such as Computer Security and Incident Response Teams (CSIRTs) have played a fundamental role in maintaining the Internet's functional structure through transnational collaboration. Responsible for security incident management and located in diverse constituencies, these coordination centres engage in joint responses and solve day-to-day cybersecurity problems through diverse national, regional and international networks. This article argues that CSIRTs form an epistemic community that engages in science diplomacy, at times navigating geopolitical tensions in a way that political actors are not able to. Through interviews with CSIRT representatives, we explain how their collaborative actions, rooted in shared technical knowledge, norms and best practices, contribute to the advancement of international cooperation on cybersecurity.

Despite almost three decades of diplomatic efforts, cross-sector collaboration and academic attention, international cooperation on the global governance of cybersecurity has been slow and uncertain (Carr, 2016a; Petratos, 2014). Successful state-driven diplomatic endeavours continue to be limited, and many existing efforts are overshadowed or undermined by conflicting national interests, reciprocal distrust, and/or geopolitical disputes that spill over from other issue areas. Perhaps the single exception is the Council of Europe Convention on Cybercrime (also known as the Budapest Convention[1]). However, the Convention focuses specifically on harmonising national legal frameworks in order to facilitate law enforcement cooperation rather than broader, systemic factors such as the challenge of attribution (Carr, 2017). In short, governments have struggled to gain traction on substantive cooperative efforts to address global cyber(in)security.

While we see conventional geopolitics largely reconstituted in the political arena of international cybersecurity negotiations, there is a community of non-state actors that provide essential security services and do so largely free of such constraints. In this article, we focus on those who work on cybersecurity incident response, known as Computer Emergency Response Teams (CERTs) or Cyber Security Incident Response Teams (CSIRTs). Specifically, we emphasise their role as epistemic communities that, through shared technical expertise, norms and best practices, have established knowledge-based networks that support international coordination in cybersecurity (Haas, 1992; Kaltofen and Acuto, 2018a; in this issue). This allows CSIRTs to maintain the integrity of the Internet's infrastructure at the domestic and transnational level. Through an investigation of the history and practices of CSIRTs, we argue that these networks engage in science diplomacy, which describes how scientific research and technical activities can play a part in fostering positive international relations and cooperation (The Royal Society, 2010).

In addition to desk-based research that brings together literature on international cybersecurity, epistemic communities, and science diplomacy, we actively engaged with the incident response team community. We interviewed a self-selected sample of nine CSIRT and Product Security Incident Response Team (PSIRT) members and also attended an international technical incident response colloquium where we were able to engage in informal, unstructured discussions. The interview sample comprises participants from North and Latin America, Europe and Asia-Pacific. Participants were enlisted through recruitment emails and snowball sampling. The semi-structured interviews were conducted in March and April 2017, either in German or English as well as face-to-face or digitally using Voice over Internet Protocol services. In the course of the interviews, participants were asked to discuss their viewpoints on the role of CSIRTs in the international cybersecurity context, their collaboration and information sharing practices and potential barriers for cooperation. This work informed our understanding of CSIRTs' role in supporting and advancing science diplomacy in cybersecurity and enabled us to illustrate the real-life application of the diplomatic effects of their actions.[2]

It should be noted that the term CSIRT complements the registered trademark 'CERT', which requires teams to be authorised by Carnegie Mellon to adopt it (CERT/CC, 2017). Both CERT and CSIRT are used interchangeably to describe incident response teams, but in this article, we use the term CSIRT to represent the full range of formations (which includes PSIRTs) currently available.

Technical expert communities and the Internet

Technical expert communities have played a lead role in the Internet's functional structure and coordination from the inception of the Internet. Indeed, ARPANET, the predecessor of the current Internet, was largely developed within universities and its architectural foundations and protocols were established and agreed by the researchers and developers working in those higher education and private sector institutions (Leiner et al., 2009).

Since then, much of the Internet's coordination and especially the actions taken to ensure its security, continue to be coordinated from within specialised expert groups. These range from the Internet Engineering Task Force (IETF) to standards-development organisations such as the Institute of Electrical and Electronic Engineers (IEEE). This 'broad community of Internauts' (Leiner et al., 2009, p. 23) comprised of computer scientists, physicists and many other technicians, was not only essential to the original design of the Internet, but also continues to play a central role in many of the processes and practices that constitute the Internet's governance (Raymond and DeNardis, 2015). This observation speaks to the overarching objective of this special issue: to showcase that science diplomacy can be achieved by a diverse set of actors who engage in collaborative practices rooted in technical and scientific expertise that are ultimately 'diplomatic in their quality and/or effect (unanticipated and unintended as well as intended)' (Kaltofen and Acuto, 2018b, in this issue).

Internet security is a global concern with deep and wide-ranging social, political and economic implications. Due to the inherent technical nature, it is ill-suited for governance through solely political or diplomatic channels (Dean and McDermott, 2017). CSIRTs provide, therefore, a useful case for the analysis of science diplomacy in global cybersecurity governance. These response centres and the networks that they build are responsible for global security incident management and are essentially a backbone of today's digital infrastructure.

Background to CSIRTs

CSIRTs were introduced to respond to security shortfalls in the original design of the Internet (Lipson, 2002). The Morris Worm, the first large-scale computer incident of its kind, incentivised authorities in the US to establish a central organisation which could coordinate and react to such insecurities. Launched from an MIT computer by graduate student Robert Tappan Morris, the worm affected machines and networks all over the world (Kelty, 2011). Internet hosts struggled to coordinate its containment. While the existing information exchange between network operators was good, they faced the problem that their communication was itself entirely dependent on the Internet and email. When those systems were out of action, individuals and organisations had no alternative way to contact one another to coordinate a response.

Recognising this fundamental vulnerability, a meeting was convened to discuss ways to improve future incident management. The recommendations arising from that gathering included a call for a single point of contact to be established for Internet security problems. This organisation would act as a trusted clearinghouse for security information. It would hold a list of alternative contact points, such as phone numbers, to communicate between different stakeholders and would facilitate the incident response through quick and effective communication channels and awareness programmes (West-Brown et al., 2003). This resulted in the establishment of the first CERT, CERT/CC (Coordination Centre), at the Carnegie Mellon Software Engineering Institute. It was commissioned by the Defense Advanced Research Projects Agency (DARPA) – a branch of the US Department of Defense – and operated under a US government contract (Maurer et al., 2015a).

The concept of incident response teams gradually expanded and led to a growth of this expert culture (Lipson, 2002). CSIRTs have since moved beyond their initial academic realm and can be found in a range of sectors where they provide services for a particular constituency (West-Brown et al., 2003). These constituencies range from public and private organisations (e.g. universities, financial service providers), governments to those known as PSIRTs that manage security vulnerabilities related to particular products and services. While PSIRTs 'look at all security vulnerabilities in products and services' (P1, interview 31 March) that can affect customers, CSIRTs in an organisation generally 'handle the infrastructure' (P1, interview 31 March) inside a network. Thus, an organisation might have both an internal CSIRT as well as a PSIRT, which mutually focus on security vulnerabilities within a constituency, but do so from different angles.

In addition to these localised formations and as a consequence of the Internet's elevation to a global infrastructure, CSIRTs developed regional and international networks. These range from the Task Force on Computer Security Incident Response Teams (TF-CSIRT) which encourages collaboration and coordination between CSIRTs in Europe, to the Asia Pacific Computer Emergency Response Team (APCERT). In addition to regional networks, there is also a global network called Forum of Incident Response and Security Teams (FIRST). The establishment of these cross-border structures speaks to the inherent transnational nature of cybersecurity threats. Incidents are not confined to state boundaries rather they demand highly internationalised responses. Security incidents on one side of the world affect teams on the other which explains CSIRTs intrinsic interdependence. One interviewee commented that 'we are simply damned to work together' (P2, interview 7 March).

Increasingly, CSIRTs' expertise and competence has been recognised by and incorporated into diplomatic endeavours. The United Nations Group of Governmental Experts on Developments in Information and Telecommunications in the Context of International Security (UN GGE) released a consensus report containing 11 proposed 'cyber norms' for responsible state behaviour in cyberspace. One of these proposed norms

explicitly refers to the CSIRT community, suggesting that '[s]tates should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as CERTs or cybersecurity incident response teams) of another [s]tate' (UN GGE, 2015, p. 8). Furthermore, 'a [s]tate should not use authorized emergency response teams to engage in malicious international activity' (UN GGE, 2015, p. 8). The role of CSIRTs is now also formalised in supranational legislation, such as the EU NIS Directive (European Commission, 2018) where teams help ensure the security of network and information systems for essential services within the Union.

It is important to note that CSIRTs' actions, which are outlined in more depth below, also allow them to respond to a gap in international policy cooperation in cybersecurity, a realm of quintessential diplomatic relevance. Their practices, shared set of norms and actions resemble Haas's (1992) thesis about epistemic communities in that CSIRTs work on a particular issue-area and have agency to develop normative ideas and processes which shape as well as influence outcomes, which are in this case of technical nature.

CSIRTs – epistemic communities in international cybersecurity

CSIRTs are distinct from many other similar expert networks in that they provide security directly. Rather than lobbying for a global 'culture of security' as we see in the domains of nuclear and human security, CSIRTs coordinate joint responses and solve day-to-day cybersecurity problems through diverse national, regional and international networks without relying on states to act. Although CSIRTs do not participate in high-level interstate negotiation, they do engage in technical knowledge exchange with their actions contributing to a diplomatic understanding of collaboration that moves beyond political disputes. Thus, the following section illustrates how, in the absence of a global legally binding treaty on cybersecurity, CSIRTs provide a framework for international cooperation.

In spite of their wide radius of operations, stretching from national infrastructure protection to product security incident response (Huber et al., 2016), CSIRTs' maintain a universal goal to promote cybersecurity through collaborative action (Finnemore and Hollis, 2016). This unifying objective is a key indicator that these geographically and sectorial diverse teams, indeed, form an epistemic community. CSIRTs communicate and collaborate with one another and they collectively respond to incidents like new malware, discovered vulnerabilities or targeted attacks. Incident response teams can be established both within state infrastructures (including law enforcement or the intelligence communities) as well as in private organisations (Bronk et al., 2006). CSIRTs consequently not only speak to the public-private partnership that underpins the Internet (Carr, 2016b; Christou and Simpson, 2006), but embody the idea of science diplomacy through a self-organised professional culture with established information-sharing and monitoring practices, and recognised rules of engagement.

For CSIRTs, their cross-border, needs-derived formation characterises their actions (Bada et al., 2014). CSIRTs are not only active when incidents such as network disruptions occur, but also they continuously work on preventing, monitoring and recovering from incidents. Bada et al. (2014) identified four categories of CSIRTs' services: (1) *reactive*, based on incident handling,[3] support and coordination; (2) *proactive*, based on technology watch and maintenance of security; (3) *artefact handling*, based on digital forensics; and (4) *security quality management*, based on training for risk analysis, business continuity and disaster recovery.[4]

As a result of these incident management capabilities, some equate CSIRTs to a fire brigade, equipped and ready to mobilise in case of emergencies (Caldwell, 2014; ENISA, 2008; West-Brown et al., 2003). Klimburg and Zylberberg (2015, p. 27) consider this description as perhaps too modest. In their view, CSIRTs are more 'akin to insurance, building-code supervisors and law enforcement investigators'. Whether fire fighters or insurers, the consolidated nature of these communities of practice is foundational for their actions in international coordination on cybersecurity. CSIRTs mobilise technical expertise to cooperate on cybersecurity and consequently establish channels of communication to tackle transboundary security threats.

While we acknowledge the view of some who stress that the CSIRT 'model cannot be over-idealised or over-differentiated from the political side' (P4, interview 12 April), CSIRTs' role in the international governance of cybersecurity does deserve recognition. Their function and operation raise questions about where diplomacy happens and what constitutes a diplomatic actor in this context. Teams have been working across geographic, cultural and political borders to collaborate on highly sensitive issues for the last 30 years. In many instances, their establishment is based on a 'model that is community-based, bottom-up, inclusive' (P4, interview 12 April); although this is – due to the rise of interactions with law enforcement and security agencies–currently transforming (Maurer et al., 2015b).

CSIRTs' efficacy in responding to incidents has been linked to their 'quasi diplomatic capability' (Sam Maccherola, cited in: Caldwell, 2014, p. 7). This capacity is largely based on the individuals' formal and informal professional relationships and it is central to the development of mechanisms for information sharing. In particular, the regional and international networks are helpful when CSIRTs 'are not able to reach out to certain people in certain places' (P5, interview 12 April) which further illustrates the cooperative element that characterises these communities. Regional and international CSIRT networks assist the liaison between teams and external bodies. They also facilitate 'capacity building' (P4, interview 12 April) through conferences, trainings, events and coordinated exercises. Through these public developmental practices, where CSIRTs engage with other teams beyond national boundaries, CSIRTs are not simply sharing technical knowledge and exchanging information. They are furthering their global expert culture and carry out important community building processes. They provide support to other units in less developed regions but also have to

manage, just as political actors do, 'cultural and political differences' (P7, interview 28 April). For instance, one participant said that the establishment of a particular regional CSIRT turned out to be quite difficult, because it would have been hard 'to get them [other CSIRTs] into a room. It took years and years to negotiate on a regional level for the establishment of [X]' (P4, interview 12 April). CSIRTs consequently try to identify 'overlaps' (P8, interview 28 April) between teams and their objectives, and use a range of mediation strategies, allowing them to achieve effective incident response.

The extent to which CSIRTs have to navigate political divides while pursuing the goals of collective action in transnational cybersecurity further illustrates their value as an example of science diplomacy. Their extensive networks are a model for a decentralised, self-organised community that reinforces the complex relationship linking diplomacy with scientific and technical endeavours. Their authority and status in the international system lies not in traditional forms and notions of power, but expert knowledge and experience.

CSIRTs also move beyond incident response by agreeing on shared best practices and baseline communication protocols. This ensures that Internet security is embedded in their educational exercises that set a framework for international cooperation between different actors. For example, the regional CSIRT representation body APCERT conducts an annual drill to test the response and cooperation mechanisms of CSIRTs within the Asia Pacific region (APCERT, 2014). During such exercises, CSIRTs need to interact between both local and international partners and coordinate across different boundaries. The latter reflects the strong collaborative element of CSIRTs work and validates the enhanced communication protocols, technical capabilities and quality of incident responses that CSIRTs foster. In order for such exercises to work, the communication exchange through 'mailing lists' (P9, interview 29 April) or 'encrypted email' (P1, interview 31 March) must be well established and in line with pre-agreed 'standard formats' (P9, interview 29 April).

In addition to these horizontal communication channels between CSIRTs, vertical cooperation with various cybersecurity stakeholders at the national and transnational level are also critical for their activities. CSIRTs practices reflect Haas's (1992, p. 3) premise that epistemic communities support a 'common policy enterprise' while maintaining a 'shared set of normative and principled beliefs'. Interviewees mentioned that their 'work is very international' (P2, interview 7 March), that they 'collaborate with other companies – even competitors' (P1, interview 31 March), and engage with external bodies such as 'ISPs' (P2, interview 7 March), the 'ITU' (P8, interview 28 April; P9, interview 29 April) or the 'OAS [Organisation of American States]' (P9, interview 29 April). In fact, participants argue that due to the global architecture of the Internet, one does 'not really have an option not to engage with other parties outside of your organisation, such as . . . the network operators, another CERT or a law enforcement agency' (P5, interview 12 April).

This cooperation also occurs with actors that political players generally struggle to cooperate with. Interviewees emphasised the value of collaborating with teams who may be affiliated with or operating in countries or organisations considered hostile by some policy makers including, 'Iranians or Russians' (P2, interview 7 March) or 'China' (P8, interview 28 April). Because cybersecurity incidents are so interconnected and will ultimately spread across the network, CSIRT community accepts that it is better to collaborate rather than operate in isolation. CSIRTs consequently prefer to have actors of all national and organisational backgrounds 'on board' (P7, interview 28 April) and to have those networks readily available whenever needed. However, interviewees also accept that this cooperation has its limitations. For instance, there would be 'certain things you simply do not ask' (P7, interview 28 April) particular CSIRTs due to the delicate nature of cultural differences or larger political disputes. These sensitivities do not prevent them from working with these particular CSIRTs on issues of mutual interest and illustrates their diplomatic qualities (Sam Maccherola, cited in Caldwell, 2014).

This viewpoint and CSIRTs' mediated engagement with both public and private parties highlight the diplomatic nature of their actions. Essentially, not only they work collaboratively to achieve a particular goal through an awareness of differences, but also through the safety of acting upon a particular 'needs basis' (P5, interview 12 April). This focus on common needs may ultimately be the reason for CSIRTs' cooperative capacity and an explanation for science diplomacy's success in matters of cybersecurity. While political actors have to take into consideration factors such as equity, ethics, legislation, economy, the balance of power, political conflict and political distrust, CSIRTs profit from precisely this ability to ignore or at least partially suppress the political dimensions of their actions. This is not to say that CSIRTs are negligent in disregarding the political nature of their work. Instead, CSIRTs cooperation efforts profit from these technical actors' ability to draw on and work within a framework of shared technical objectives.

The collaboration of CSIRTs is, thus, based on a 'common understanding between individuals and organisations in this community' (P5, interview 12 April). There is a collective cognition evident, with the value of their action contributing to a greater public good and security for society. One participant highlighted this communal element, emphasising that CSIRTs share 'information about our procedures, our tools, our methods and experiences' (P6, interview 21 April) to jointly, and through best practices, contribute to the security of the Internet which is an expression of how a non-governmental actor can foster both state and non-state objectives and strengthen partnerships based on agreed norms. This can be seen in CSIRTs' standardised information exchange format. The Traffic Light Protocol (TLP) (FIRST, 2016a) is a colour coding system to ensure that sensitive information is distributed in accordance with agreed expectations (US-CERT, 2017). While TLP white information may be forwarded without restrictions, TLP red implies that information is not for disclosure and may not be shared with any parties

outside of the specific realm in which it was originally disclosed. The TLP was created in order to facilitate greater sharing of information between teams and although not mandatory, most teams adhere to it.

The usage of such measures illustrates how informal norms and trust are fundamental factors in successful CSIRT operations. They frequently compensate for a lack of formal links or structures. In particular, trust is a factor that has been identified (Huber et al., 2016; Maurer et al., 2015a) as an element that characterises not only CSIRTs but also other technical expert groups including the original founding parties of the Internet (Leiner et al., 2009; Meier-Hahn, 2015). It is a feature that derives from the Internet and the 'Internauts' (Leiner et al., 2009, p. 23) scientific ethos and expert nature, and can, together with the actions of CSIRTs regional and international networks support other, more formal processes of cooperation and behaviours in global cybersecurity.

Conclusions

This analysis highlighted how the evolution of collective action in transnational cybersecurity was founded on the actions of expert communities which established collaborative governance mechanisms independently of state-driven international agreements. In line with the conceptual framework of this special issue, we have demonstrated how CSIRTs are a powerful example of the extent to which technical epistemic communities support and contribute to the achievement of international cooperation in cybersecurity. Their diplomacy is 'about technical people trying to solve technical problems to the best of their capacities and through trusted networks' (P3, interview 12 April). This distinct focus helps them to respond to incidents and develop best practices in a way that political actors struggle with. Thus, CSIRTs are filling a gap in international cooperation on cybersecurity, mobilising their expertise and overcoming disparities.

CSIRTs form an epistemic community that contributes to international coordination in cybersecurity through their characteristic trusted partnerships. It is perhaps unreasonable to expect that the same trusted communities and communication channels could be found in the political realm. However, the enduring success and efficacy of CSIRTs provides some valuable lessons on what might help to shape cyber norms at the international level. A key point here is the benefits of emphasising common ground over differences when addressing global cybersecurity (Erskine and Carr, 2017). Also important is the recognition that there is complementarity between these communities. Collaborating around a clearly defined technical need, CSIRTs' issue-based actions can feed into and support other non-state and state actors' endeavours to solve global collective action on cybersecurity. Their practices neither replace nor overshadow other diplomatic mechanisms – including those carried out by state actors – but they help us to identify and understand the subtle instances of science diplomacy that might otherwise be overlooked.

The continued growth of connected devices and economies means that society and businesses are increasingly dependent on the maintenance of a stable and secure Internet infrastructure. Governance strategies that are therefore adaptive and flexible and allow both state as well as non-state actors to engage in this domain are needed (Tanczer et al., forthcoming). Analysing the importance of this technical community and the support it provides is a helpful lens through which to examine how international cooperation can move forward. States clearly have an ongoing and deeply important role to play in global cybersecurity. However, if policy actors are able to shift their perspectives and modes of thinking by fostering collaboration on topics where interest's overlap, they will have a better chance of meeting the demands of collaborative cybersecurity *governance*, rather than governments.

Notes

This research was supported by the UK Engineering and Physical Sciences Research Council and partner contributions under grant EP/N02334X/1. The authors would like to thank thank Jesse Sowell for his assistance in the data collection process, various FIRST representatives for their helpful feedback and support, and are grateful for all participants who agreed to be interviewed for this article.

1. As of September 2018, 61 states have implemented the Budapest Convention. Yet, it remains quite contentious among some others, often for processual reasons (Brodowski, 2016).
2. The following analysis features extracts from these interviews, with German passages translated into English. Participants are referred to as 'P' and identifying number (i.e., P1). The symbol '[X]' is used to hide words or phrases which could enable participant identification.
3. Incident response describes all of the technical components required to analyse and contain an incident. Incident handling describes the logistics, communications, coordination and planning functions needed in order to resolve an incident in a calm and efficient manner (de Beaupré, 2009). The latter includes preparation measures, the identification and detection of an attack, the containment of an attack, as well as post-incident activities such as recovery and analysis (Cichonski et al., 2012).
4. FIRST's (2016b) Service Framework and the CSIRT Handbook by CERT/CC (2003) would account artifact handling as part of their reactive services.

References

APCERT. (2014) 'APCERT Embarks on Global Coordination to Mitigate Large Scale Denial of Service Attacks' , February 19 [online]. Asia Pacific Computer Emergency Response Team. Available from: https://www.apcert.org/documents/pdf/APCERTDrill2013PressRelease_AP.pdf [Accessed 28 October 2018].

Bada, M., Creese, S., Goldsmith, M., Mitchell, C. and Phillips, E. (2014) *'Computer Security Incident Response Teams (CSIRTs): An Overview' [online]*. Oxford: Global Cyber Security Capacity Centre, pp. 1–23. Available from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CSIRTs.pdf [Accessed 28 October 2018].

Brodowski, D. (2016) 'Transnational Organised Crime and Cybercrime', in P. Hauck and S. Peterke (eds.), *International Law and Transnational Organised Crime*. Oxford: Oxford University Press, pp. 334–357.

Bronk, H., Thorbruegge, M. and Hakkaja, M. (2006) *'A Step-by-step Approach on how to set up a CSIRT'*. Heraklion: European Union

Agency for Network and Information Security [online]. Available from: https://www.enisa.europa.eu/publications/csirt-setting-up-guide [Accessed 28 October 2018].
Caldwell, T. (2014) 'Call the Digital Fire Brigade', *Network Security*, 2014 (3), pp. 5–8.
Carr, M. (2016a) 'Crossed Wires: International Cooperation on Cyber Security', *Interstate – Journal of International Affairs*, 2015/2016 (2), pp. 2–10..
Carr, M. (2016b) 'Public–private Partnerships in National Cyber-Security Strategies', *International Affairs*, 92 (1), pp. 43–62. .
Carr, M. (2017) 'Cyberspace and International Order', in H. Suganami, M. Carr, and A. Humphreys (eds.), *The Anarchical Society at 40: Contemporary Challenges and Prospects*. Oxford: Oxford University Press, pp. 162–178.
CERT/CC. (2017). 'Authorized Users of "CERT"', [online]. Available from: https://www.cert.org/incident-management/csirt-development/cert-authorized.cfm? [Accessed 2 May 2017]
Christou, G. and Simpson, S. (2006) 'The Internet and Public–Private Governance in the European Union', *Journal of Public Policy*, 26 (1), pp. 43–61.
Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012) *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (No. NIST SP 800-61r2). Gaithersburg, MD: National Institute of Standards and Technology.
de Beaupré, A. (2009). 'Incident Response vs. Incident Handling' [online]. Available from: https://isc.sans.edu/forums/diary/6205/ [Accessed 31August 2018]
Dean, B. and McDermott, R. (2017) 'A Research Agenda to Improve Decision Making in Cyber Security Policy', *Penn State Journal of Law & International Affairs*, 5 (1), pp. 29.
ENISA (2008) *Emergency Response to Security Breaches*. Heraklion: European Union Agency for Network and Information Security.
Erskine, T. and Carr, M. (2017) 'Beyond "Quasi-norms": The Challenges and Potential of Engaging with Norms in Cyberspace', in A.-M., O. and H., R. (Eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*. Tallinn: NATO CCD COE Publications, pp. 87–109.Available from: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf [Accessed 28 October 2018].
European Commission. (2018) *'SWD(2018) 157 Final: Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products' [online]*. Brussels: European Commission. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0157&from=en [Accessed 28 October 2018].
Finnemore, M. and Hollis, D. B. (2016) 'Constructing Norms for Global Cybersecurity', *American Journal of International Law*, 110 (3), pp. 425–479.
FIRST. (2016a) 'Traffic Light Protocol (TLP). FIRST Standards Definitions and Usage Guidance — Version 1.0' [online]. Available from: https://first.org/tlp [Accessed 13 May 2017]
FIRST. (2016b). 'Education Program: Service Framework' [online]. Available from: https://first.org/education/service-framework [Accessed 13 May 2017]
Haas, P. M. (1992) 'Introduction: Epistemic Communities and International Policy Coordination', *International Organization*, 46 (1), pp. 1–35.
Huber, E., Hellwig, O. and Quirchmayr, G. (2016) 'Wissensaustausch und Vertrauen unter Computer Emergency Response Teams – eine europäische Herausforderung', *Datenschutz und Datensicherheit - DuD*, 40 (3), pp. 162–166. .
Kaltofen, C. and Acuto, M. (2018a) 'Rebalancing the Encounter Between Science, Diplomacy and International Relations Theory', *Global Policy*, 9 (S3), pp. 15–22.
Kaltofen, C. and Acuto, M. (2018b) 'Science Diplomacy: Introduction to a Boundary Problem', *Global Policy*, 9 (S3), pp. 8–14.
Kelty, C. M. (2011) *The Morris Worm. Limn*, 1, pp. 17–19. Available from: https://limn.it/articles/the-morris-worm/ [Accessed 9 November 2018].
Klimburg, A. and Zylberberg, H. (2015) *'Cyber Security Capacity Building: Developing Access* (No. 6)' [online]. Oslo: Norwegian Institute of International Affairs. Available from: https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf [Accessed 28 October 2018].
Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., et al. (2009) 'A Brief History of the Internet', *ACM SIGCOMM Computer Communication Review*, 39 (5), pp. 22–31.
Lipson, H. F. (2002) *'Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (No. CMU/SEI-2002-SR-009)' [online]. Pittsburgh. PA: Software Engineering Institute. Available from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5831 [Accessed 28 October 2018].
Maurer, T., Hohmann, M., Skierka, I. and Morgus, R. (2015a) *'CSIRT Basics for Policy-makers. The History, Types & Culture of Computer Security Incident Response Teams' [online]*. Washington DC: New America, Global Public Policy Institute. Available from: https://www.gppi.net/fileadmin/user_upload/media/pub/2015/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf [Accessed 28 October 2018].
Maurer, T., Hohmann, M., Skierka, I. and Morgus, R. (2015b) *'National CSIRTs and Their Role in Computer Security Incident Response' [online]*. Washington, DC: New America, Global Public Policy Institute. Available from: https://www.newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/ [Accessed 28 October 2018].
Meier-Hahn, U. (2015) Creating Connectivity: Trust, Distrust and Social Microstructures at the Core of the Internet. Presented at the TPRC 43: The 43rd Research Conference on Communication, Information and Internet Policy 2015, George Mason University School of Law, Arlington, VA: Social Science Research Network [online]. Available from: https://papers.ssrn.com/abstract=2587843 [Accessed 28 October 2018].
Petratos, P. (2014) 'Cybersecurity in Europe: Cooperation and Investment', In E. G. Carayannis, D. F. J. Campbell, and M. P. Efthymiopoulos (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense*. Berlin, Germany: Springer, pp. 279–301. Available from: https://www.springer.com/gb/book/9781493910274 [Accessed 9 November 2018].
Raymond, M. and DeNardis, L. (2015) 'Multistakeholderism: Anatomy of an Inchoate Global Institution', *International Theory*, 7 (3), pp. 572–616. .
Tanczer, L., Brass, I., Elsden, M., Carr, M. and Blackstock, J. (forthcoming) 'The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape', in R. Ellis and V. Mohan (eds.), *Rewired: Cybersecurity Governance*. Hoboken, NJ: Wiley.
The Royal Society. (2010) *'New Frontiers in Science Diplomacy. Navigating the Changing Balance of Power'*. London, UK: The Royal Society [online]. Available from: https://royalsociety.org/~/media/Royal_Society_Content/policy/publications/2010/4294969468.pdf [Accessed 28 October 2018].
UN GGE. (2015) *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (No. A/70/174). New York: United Nations General Assembly, pp. 1–17
US-CERT. (2017) 'Traffic Light Protocol (TLP) Definitions and Usage | US-CERT'[online]. Available from: https://www.us-cert.gov/tlp [Accessed 7 May 2017]
West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R. and Zajicek, M. (2003) *Handbook for Computer Security Incident Response Teams (CSIRTs)* (No. CMU/SEI-2003-HB-002). Pittsburgh, PA: Carnegie Mellon Software Engineering Institute [online]. Available from: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf [Accessed 28 October 2018].

Author Information

Leonie Maria Tanczer is Lecturer in International Security and Emerging Technologies at UCL STEaPP and former Fellow at the Alexander von Humboldt Institute for Internet and Society. Her research focuses on Internet security and centres on the intersection points of technology, security, and gender.

Irina Brass is Lecturer in Regulation, Innovation and Public Policy at UCL STEaPP. Her research focuses on the regulation and adaptive governance of disruptive technologies. Brass is working closely with policy makers and the standards development community on governance frameworks for managing cybersecurity and data protection in the IoT.

Madeline Carr is Associate Professor of International Relations and Cyber Security at UCL STEaPP and Director of its Digital Policy Lab. She has a strong interest in the international policy challenges posed by cybersecurity and is Co-Investigator for Standards, Policy and Governance Stream of the PETRAS IoT Research Hub.