CYBER SECURITY POLICY PROCESS
BRIEF

A ROLE FOR CIVIL SOCIETY?

ICTs, NORMS AND CONFIDENCE BUILDING MEASURES IN THE CONTEXT OF INTERNATIONAL SECURITY

Camino Kavanagh and Daniel Stauffacher

GENEVA 2014
ICT4Peace Foundation

ICT4Peace Publishing, Geneva.

Copies available from www.ict4peace.org

A ROLE FOR CIVIL SOCIETY?

ICTs, NORMS AND CONFIDENCE BUILDING MEASURES IN THE CONTEXT OF INTERNATIONAL SECURITY

Camino Kavanagh and Daniel Stauffacher

ICT for peace
FOUNDATION

ACKNOWLEDGEMENTS

The authors wish to thank Ben Basley-Walker (UNIDIR), Gustavo Diniz (Instituto Igarrape), Dr. Roger Hurwitz (CSAIL-MIT), So Jeong KIM (National Security Research Institute of ETRI), Mihoko Matusbara (Hitachi Systems SSRC/ Pacific Forum CSIS), Sanjana Hattotuwa (ICT4Peace), Ben Hiller (OSCE), Prof. Duncan Hollis (Temple University), Tim Maurer (New America Foundation), Amb. (ret'd) Paul Meyer (Simon Fraser University), Chris Parsons (Citizen Lab, University of Toronto), Robert Parker and An Vranckx (SaferWorld), Dr. Tim Stevens (King's College London), Dr. Eneken Tikk-Ringas (IISS) and a number of other colleagues for the insightful comments and suggestions that helped shape this paper.

INTRODUCTION

As noted in earlier ICT4Peace publications, over the past five years states have become increasingly engaged in a series of policy discussions over norms, confidence and capacity building measures aimed at lowering risk and building trust among states with regard to the uses of information and communications technologies (ICTs). In 2013, initial agreement was reached by a UN Group of Governmental Experts (GGE) and the Organisation for Security and Cooperation in Europe (OSCE) on the nature of some of these norms, confidence (CBMs) and capacity building measures. Nonetheless, substantive discussions remain at an early stage. Governments have acknowledged the need to build trust and deepen their engagement with other groups - including civil society organisations - as they move to shape new norms and rules in this area. As we discuss, civil society engagement on international governance and security matters is not new and there are scores of examples of areas in which states have accomodated such engagement. Cyber security should not be an exception. Moreover, it is an area that by its very nature and the broad range of normative concerns involved, calls for much deeper civil society engagement than experienced in other areas. If approached effectively and coherently, such engagement we argue, can afford greater legitimacy and sustainability to on-going multi-lateral norms and CBM processes concerning international security and state uses of ICTs. It can also help ensure that broader normative concerns are attended to, and that the right technical expertise is leveraged when solutions are being sought. Combined, the latter can help build trust between states, and between states and society.

We have divided the paper into three sections: the first provides a short overview of the current context; the second discusses why civil society is important to furthering norms and confidence building measures regarding the use of ICTs in the context of international and regional security; and the third tables some suggestions for civil society engagement under three headings: i) engaging effectively; ii) fostering transparency and accountability; and iii) deepening knowledge.[1]

The paper is aimed at civil society organisations, national governments, international and regional organisations and other key actors concerned with ICTs and their impact on international and regional security. For the purpose of the paper we define civil society as a social sphere separate from both the state and the market and made up of non-state, not-for-profit, voluntary organizations. Civil society organizations can unite people at different levels (local, national, regional and international) to advance shared goals and interests, working across a range of thematic areas. They perform a wide range of functions, including policy-oriented research, advocacy, networking. They can perform

[1] This paper builds on a presentation made by Amb. (ret.) Daniel Stauffacher on Confidence Building Measures and Norms for Cyber Security and the Future of Internet Governance hosted by the Centre of Excellence for National Security (CENS) of the S. Rajaratnam School of International Studies (RSIS), Singapore, 3-4 July 2014.

watchdog/ monitoring functions and often coordinate or represent other groups and organisations. In the Internet/ cyber security world, civil society organisations often work in specific issues areas, many technical or functional in nature and tied to the maintenance of the Internet. Others advocate certain civic interests such as privacy. Often, the area of work is proscribed by the domestic context. Civil society does not include the private sector. Nevertheless, natural alliances are emerging between certain of the more tech-oriented civil society organisations (for example, the Internet Society or the IEEE) and some Tier 1 carriers (i.e. those carriers that have a direct connection to the Internet and the networks it uses to deliver voice and data services), and major transnational vendors and Internet Service Providers (ISPs).

1. THE CONTEXT

Undoubtedly we are living through a moment of significant change whereby a series of developments have led to the loss of public trust, to a confidence gap between those who govern and those who are governed. The links between states on the one hand; and between state and citizens on the other are being increasingly challenged by a range of state practices, including the negative uses of ICTs to advance political, military and economic objectives. This situation has emerged at a time when citizen trust in the behaviour of state actors (and politicians) has decreased considerably. Evidence of this mistrust became manifest in the calls for more enhanced democratic representation and more effective government across regions as the first decade of the 2000s drew to a close; and has been somewhat aggravated by the recent revelations of the unchecked monitoring and surveillance practices of a number of governments.

Despite the mushrooming of Cassandresque statements by numerous government officials over the past five years, an all out ‘cyber war’ or Armageddon-like incident has thankfully not happened, nor is it likely to happen in the near future, not only from a strategic theory perspective[2], but also because of the asymmetries that continue to exist between states and between states and non-state actors in this area. ICTs are, however, increasingly used by states and their adversaries to ratchet the advantage during armed conflict or situations of tense political contestation. Indeed, ICTs and cyber capabilities have been used either as a means to attack or as a target of attack, for example:

- Within the context of broader conflicts (Georgia, 2008; and Syria since the beginning of the civil war).

[2] See for example, Libicki, Martin, (2014), Why Cyber War Will Not and Should Not Have Its Grand Strategist. *Strategic Studies Quarterly* (Spring 2014); Rid, Thomas (2013), *Cyber War Will Not Take Place*. Oxford University Press; Betz, David (2013), Cyber Power in Strategic Affairs: Neither Unthinkable nor Blessed | Kings of War, *Journal of Strategic Studies*, 35:5, 689-711, DOI: 10.1080/01402390.2012.706970

- Outside the context of an overt armed conflict, the direct use or manipulation of ICTs has been used to attain political and strategic objectives (for example in Estonia 2007; Iran in 2010, Republic of Korea in 2013), purportedly demonstrating, particularly in the case of Iran (via Stuxnet in Operation Olympic Games)[3] that the manipulation of ICTs (or rather, ICT-driven sabotage) can have an important impact on a country's critical infrastructure.[4]

These developments - particularly the growing interest of states in developing what are frequently referred to as defensive and offensive cyber capabilities - have taken place against a background of important shifts in the broader global strategic environment: the rise of China as a global economic and a regional military power coupled with an increased assertiveness in international and regional politics on the part of many rising middle-income states and the perception of a gradual diffusion of power away from the West;[5] a recrudescence of extremism and organised crime across regions; the global financial crisis, the effects of which are still resonating at the domestic level, particularly amongst unemployed (and increasingly tech-savvy) youth in the world's mega-cities; and faultlines in the post-cold war international order, including an overt rejection on the part of some leaders of democratic norms and principles, in tandem with a growing citizen disillusion with the liberal welfare state and its perceived failure to deliver. The uncertainty in the international environment provoked by these shifts has added to the sense of complexity and mistrust surrounding discussions on 'cyberspace' and the uses of information and communications technologies (ICTs) for attaining political, military or economic goals.

The interest for greater state involvement was initially stoked by the events in Estonia in 2007. These events inadvertently coincided with a period of intense turf fighting in the United States over the entity responsible for cyber defence. Then, between 2009 and 2012, an increasing number of governments moved to develop and publish national cyber security strategies.[6] Governments – particularly those of an authoritarian ilk – focused on the potentially destabilizing role of ICTs and social media as citizens embraced the new opportunties they promised for organization and for voicing dissent.[7] The Shanghai Cooperation Organisation (SCO) cemented these concerns in a regional agreement in 2009.[8] This attention increased and spread across regions as ICTS were perceived (perhaps

[3] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Broadway Books. (2012). The real impact of Stuxnet has been increasingly contested, however.

[4] It is important to note in this regard that states continue to define critical infrastructure differently.

[5] See *inter alia*, Carothers, T. et al, in 'Is the World Falling Apart?' 14 August, 2014. Carnegie Endowment for International Peace. Available at: http://carnegieendowment.org/2014/08/14/is-world-falling-apart/hkuw

[6] Cyber Index: International Security Trends and Analysis (2013), CSIS, IPRSP, UNIDIR. Available at: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

[7] Kavanagh, C (2012), 'The Limits of Dissent in Cyberspace.' Policy Brief prepared for CyberDialogue 2012: What is Stewardship in Cyberspace. March 18-19, 2012, Toronto, Canada. http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012briefs/brief-2.pdf

[8] SCO Agreement on Cooperation in the Field of Information Security.

exaggeratedly) to have played a central role in the political upheavals in North Africa and the more recent conflicts in the Middle East, with some governments moving to shut-down, block access, or filter network traffic at the height of the crises. Governments of many ilks also began to use social platforms as propaganda tools against citizens in arms, to maintain loyalty among regime supporters and propagate an alternative narrative on the conflict both at home and abroad.[9]

These developments were in turn followed by revelations that states used sophisticated malware such as Stuxnet to achieve foreign policy goals; and the disclosures of extensive and largely unchecked monitoring and surveillance practices of intelligence bodies in both democratic and authoritarian states alike. As has emerged, many of these practices were warranted for national security purposes. Many others were not. Meanwhile, certain private corporations are perceived to be playing an increasingly contentious role in defending against (through the practice of 'active defence,' or 'hacking back') different uses of ICTs by state and non-state actors.[10] While real data surrounding these practices is elusive, they have nonetheless provoked strong reactions by state and non-state actors, some of which have rushed to emulate rather than help frame norms and rules for their use them.[11] In addition, many less technologically sophisticated states are taking advantage of the growing market – facilitated mainly by Western private companies - in intrusion detection software (for example, FinFisher Spyware).[12]

Taking advantage of existing policy and regulatory gaps (and the technological advances that have removed many financial and practical obstacles), some states have rushed to develop or acquire these and other tools and capabilities, using them against other states as a means to advance their interests, and at home for political control and the suppression of the media and civil society. This reality – manifest across a range of political regimes – has the potential of further undermining confidence and trust between states, and

[9] Clark, M. and Abas A., 'The Hard Realities of Soft Power: Keeping Syrians Safe in a Wired War,' Background Paper, SecDev, 12 June 2013. Available at: http://gallery.mailchimp.com/eb7c0bde6ff78e88f9b0c8662/files/SecDev_wiredconflict_25June2013.pdf?utm_source=Syria+report+distribution+list&utm_campaign=1ae1bd351d-MIGS-1&utm_medium=email&utm_term=0_8b953783f7-1ae1bd351d-52609969

[10] The lack of domestic regulatory frameworks or international norms and standards regarding the latter echoes similar issues that emerged with the mushrooming of private military companies in the early 1990s, whereby the outsourcing of military needs lead to a loss of democratic control over the army, posing challenges to questions of sovereignty including through the erosion of the state's monopoly over the use of force.

[11] For a discussion on the legal dimensions of the Hack-Back debate, see Alexei Alexis, 'Debate Brewing Over Whether Companies Should Strike Back at Their Cyber Attackers,' *Bloomberg*, April 19, 2013. The American Bar Association's Standing Committee on Law and National Security has also developed a work stream in this area. See for example: http://www.abajournal.com/news/article/how_far_should_companies_be_allowed_to_go_to_hunt_cyberattackers/ or http://www.americanbar.org/news/abanews/aba-news-archives/2013/08/_active_cyber_defens.html

[12] Email communication with Duncan Hollis, Associate Dean for Academic Affairs and James A. Beasley Professor of Law, Temple University, 15 August, 2014.

between states and citizens.[13] In response to these developments, a range of domestic and international efforts has been initiated to manage the use of ICTs and shape state behavior in cyberspace. However, different societal values and interests, problems of attribution, constantly evolving technology, the behavior of some states, and the roles played by certain private companies in this field have posed barriers to reaching consensus.[14] For example, despite agreeing on the applicability of existing international law to cyberspace,[15] states have not yet been able to define what constitutes a 'cyber attack' or a 'cyber weapon' in the context of international humanitarian law (particularly the means vs. effects debate) or in broader international law and policy.[16]

Moreover, many of the on-going efforts to reach consensus have run into difficulty not least because it is hard (yet not entirely impossible) to fit ICTs into traditional security paradigms. For example, attempts have been made to fit ICTs into traditional arms control frameworks. This approach has been complex, due in large part to the number of different actors involved in the security supply chain, which would likely pose difficulties in terms of reaching agreement on guarantees and certification.[17] Notwithstanding, in December 2013, the member states of the Wassenaar Arrangement announced new controls relating to 'intrusion software' and 'IP network surveillance systems' which will lead to changes in members states' national export control regimes in the coming years.[18] This was a significant step, although it will be important to monitor how the new controls are translated into practice.

Beyond the traditional strategic landscape, the risk of a growing 'digital divide', whereby ICTs could reinforce rather than reduce inequalities internationally and at the national

[13] OHCHR's recent report on the Right to Privacy in the Digital Age notes how "[t]he State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before," suggesting that these newly expanded capabilities have led to infringement of the right to privacy and other fundamental rights. The Report was a result of the UN General Assembly Resolution on the "The right to privacy in the digital age" adopted without a vote, in the Third (Human Rights) Committee and then by the General Assembly as a whole in 2013, and will be discussed in this year's sessions of the Human General Council and the General Assembly. See: Right to Privacy in the Digital Age: Report of the Office of the UN High Commissioner for Human Rights (A/HRC/27/37) of 30 June 2014. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[14] Hathaway, M. E. (forthcoming), Connected Choices: How the Internet is Challenging Sovereign Decisions, *American Foreign Policy Interests*.

[15] Report of the UN Group of Governmental Experts On Developments in the Field of Information and Telecommunications In the Context of International Security, June 2013.

[16] Communication with UNIDIR, 25 August, 2014.

[17] There are nonetheless examples of mixed state, private sector and civil society regimes in other areas, for example civil aviation, which might be considered part of traditional international security mechanisms, and the lessons of which might be worth studying further. Email communication with Roger Hurwitz, Research Scientist, MIT-CSAIL, 10 August, 2014.

[18] As noted by Maurer *et al*, it is important to note that intrusion software itself was not controlled. Instead, the wording of the controls is very explicit in that only components for the generation, operation, delivery and communication with the malware are subject to the control. In other words, 'the control list targets those who purchase intrusion software and seek to target others, not those who are infected by it.'

level, was acknowledged as early as 1990 in an expert report on New Technologies and International Security submitted to the General Assembly. The report presciently noted: '[f]or the developing countries without the means to acquire information, the increasing real cost of information makes it more difficult to catch up. Some of them are deeply concerned that the information technology revolution should not bypass them as the industrial revolution has done. Security lies in access to information.'[19] Some thirteen years later, the WSIS Geneva Declaration of Principles and the accompanying Plan of Action (2003)[20] stressed the central role of ICTs in many areas of economic and social development, recommending that ICTs be harnessed to transform the digital divide into a digital opportunity for all. However, as also acknowledged, economic development and prosperity can only be achieved if the domestic and regional context is stable and peaceful.[21] Throughout the world, many regions experiencing conflict continue to miss out on development opportunities. The return on investing in conflict prevention, mitigating violence and in building lasting peace is significantly larger than the investments that are required to reconstruct countries and build peace after conflict and violence.[22] And as increasingly acknowledged, ICTs can play an important role in this regard, yet unless progress is sustained in international and regional negotiations, their negative use may overshadow that potential.[23]

2. NORMS, CBMS AND CIVIL SOCIETY: WHY?

Over the past decades, most governments have accepted the role norms and CBMs can play in strengthening trust between states and within states. In addition, core governance principles such as participation, transparency, and accountability can help build and deepen trust between states, and between states and citizens.[24] These processes and principles often overlap and may conflict (for example trade-offs between openness and privacy; rights and security); they generally play out in practice according to the actual social context; and their application is complex, not least because their implementation depends on how political power is exercised.

[19] Report of the Secretary-General, Scientific and Technological Developments and their Impact on International Security. A/45/568 of 17 October, 1990.

[20] WSIS Declaration of Principles and Plan of Action, Geneva 2003 (Document WSIS-03/GENEVA/DOC/5-E). Available at: Document WSIS-03/GENEVA/DOC/5-E

[21] See Report of the High-Level Panel on the Post-2015 Development Agenda; see also the Center on International Cooperation (CIC) blog piece, 'The Role of Peace and Security in the Post-2015 Development Agenda: the Perspective of African States and LDCs,' availabe at: http://cic.nyu.edu/blog/global-development/role-peace-and-security-post-2015-agenda-perspective-african-states-and-ldcs

[22] See: World Bank. 2011. *World Development Report 2011: Conflict, Security, and Development*. World Bank. © World Bank. https://openknowledge.worldbank.org/handle/10986/4389 License: CC BY 3.0 IGO."

[23] https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

[24] UNDP's1997 Governance and Sustainable Human Development Report lays out a set of principles that, with slight variations, appear in much of the literature.

Finnemore notes how civil society organizations have long lobbied for a ‘seat at the table’ of state-centric multilateral institutions on numerous issues; and how the United Nations has opened up extensive ‘consultative arrangements’ with civil society organizations on certain topics.[25] In 2004, the Chair of the Eminent Panel on United Nations-Civil Society Relations established to study the relationship of NGOs with the UN system, characterized civil society’s increasingly important role as one of ‘the landmark events of our times.’[26] Civil society organizations now directly engage on a range of international governance and security issues, either through direct engagement with the UN or in relation to specific isues area such as the WTO, environmental treaty bodies, land mines, cluster munitions and outer-space activity.[27] Moreover, this engagement has helped produce positive results, with international and international humanitarian law in particular benefitting enormously from the contribution of civil society organizations. The latter have helped build confidence among and within states (often through the organization of and participation in track 1.5 and track 2 CBM processes and by fostering dialogue between parties)[28], as well as ‘fostering treaties, promoting the creation of new international organizations, and lobbying in national capitals to gain consent to stronger international rules and standards.’[29] Moreover, as noted by Finnemore, greater engagement of additional actors with multi-lateral processes can increase ‘the “qualitative” dimension that legitimates and undergirds multilateralism as a form of political action.’[30] Sometimes this engagement is welcomed by states; often it is not. And where states and national governments have fail to deliver or reach consensus on certain global ssues – for example, climate change – the opportunities for civil society actors to suggest alternatives are increasing.[31]

[25] Finnemore, M. (2014), “New Faces, New Forms for 21st Century Multilateralism.” A conference paper prepared for the Nobel Institute Symposium on “Does the rise and fall of great powers lead to conflict and war?” Oslo, Norway, June 18-22, 2014.

[26] Former President of Brazil Fernando Henrique Cardoso, ‘Transmittal Letter from the Chair’ in We the peoples: civil society, the United Nations and global governance. Report of the Panel of Eminent Persons on United Nations–Civil Society Relations, UN Doc A/58/817 (11 June 2004). https://www.globalpolicy.org/empire/32340-panel-of-eminent-persons-on-united-nations-civil-society-relations-cardoso-panel.html

[27] Email communication with Duncan Hollis, 15 August, 2014.

[28] Organizations such as HD Centre, CMI and similar have a lengthy track record in this area as do many European and US-based think-tanks.

[29] Charnovitz, S. (2006). ‘Nongovernmental organisations and International Law.’ *American Journal of International Law*, *100*(2), 348–372 (p. 348). Retrieved from http://www.jstor.org/stable/3651151. See also: K Raustiala, 'NGOs in International Treaty-Making' in D Hollis (ed), *The Oxford Guide to Treaties* (OUP, 2012).

[30] Finnemore, M. (2014). See also Vedder, A. (ed) *NGO Involvement in International Governance and Policy: Sources of Legitimacy*.

[31] Ibid. Finnemore discusses two core examples: The Global Fund to Fight Aids, Malaria and Tyberculosis, which is a public-private partnership that uses money from private philanthropic foundations to provide financing for implementation carried out by both government entities and NGOs; and the C40 Cities Climate Leadership Group, a network of the world’s largest megacities focused on responding to the challenges posed by climate change.

In the field of cyber security, consultative and participative arrangements are still somethat limited. Indeed, to date, engagement (whether direct or indirect) of civil society in the shaping of national cyber security strategies or in regional and international norms and CBM processes has been minimal, despite the fact that civil society organisations represent, along with the private sector, academia and policy think-tanks, core links in the ICT value chain and have 'normative concerns' with regard to how ICT-driven international and regional security concerns are resolved.[32] Indeed, the expertise, knowledge and reach of these groups is fundamental to resolving or responding to many of the core technical problems inherent in the ICT environment and many of the insecurities and mistrust that has emerged between and within states regarding the uses of ICTs.

Undoubtedly, there are lessons to distill from how civil society organizations have supported government efforts to leverage ICTs in responding to *intra-state* conflict and humanitarian disasters. This engagement stemmed from the the World Summit on Information Society (WSIS) Declaration of Principles and accompanying Geneva Plan of Action which included emphasis on 'building confidence and security in the use of ICTs.'[33] In 2005, under the WSIS Tunis Commitment, governments also committed to using ICTs to promote peace and prevent conflict. Paragraph 36 of the accompanying Tunis Commitment specifically emphasised the role ICTs can play in 'identifying conflict situations through early-warning systems, preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction' between peoples, communities and stakeholders involved in crisis management, humanitarian aid and peacebuilding.[34] Despite the dangers involved, civil society organizations, particularly those working on the ground, continue to play a critical role translating these commitments into reality, through ICT-supported efforts to disseminate information about kinetic conflicts and support recovery, either alone, with private tech companies, or in tandem with government or

[32] Ibid. As noted by Finnemore, "expanding participation with new types of actors today is driven not only by effectiveness concerns (i.e. who needs to be involved to construct a solution to the problem) but also by normative concerns (i.e. who is affected by the problem, and has a stake in the way it gets resolved).

[33] See 'Building the Information Society: A Global Challenge in the New Millennium.' Specifically para. B5 - Building Confidence and Security in the Use of ICTs, specifically paragraphs 35-37 relating to building a trust framework; preventing the use of ICTs for purposes inconsistent with the objectives of maintaining international stability and security; and dealing with spam at the appropriate national and international levels. http://www.itu.int/wsis/docs/geneva/official/dop.html

[34] Para. 36, Tunis Commitment: 'We value the potential of ICTs to promote peace and to prevent conflict which, *inter alia,* negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction.' http://www.itu.int/wsis/docs2/tunis/off/7.html Para. 36 was introduced to the diplomatic negotiations in 2004 by the Swiss and Tunisian Governments for its adoption as part of the WSIS Tunis Commitment in 2005. The ICT4Peace Foundation (www.ict4peace.org) was subsequently established in spring 2006 to raise awareness about the Tunis Commitment and promote its practical realization in all stages of crisis management.

international security and humanitarian organisations.[35] The UN Secretariat also envisaged the participation of non-governmental entities in implementing its 2008 Information Communications Technology Strategy at the global level.[36] As evidenced in the report 'Information and Communication Technologies for Peace: The Role of ICTs in Preventing, Responding to and Recovering from Conflict,' civil society organisations have played an active role in this regard, particularly in the area of crisis management.[37]

In contrast, ICT-related norms and CBM processes in the context of international and regional security have not fully benefitted from the engagement of civil society and other non-governmental actors. In 2011 ICT4Peace made a call for expanded engagement and the pooling of resources of different stakeholders.[38] Yet even international conferences such as the series launched in London in 2011[39] - aimed specifically at broadening the cyber security dialogue beyond government participants - has stalled, leaving many civil society organisations knocking at the door. Indeed, the Seoul Conference on Cyberspace sought to respond to a perception of over-participation in previous years by putting a ceiling on the number of non-governmental groups attending. It did however invite non-governmental groups such as ICT4Peace and the Atlantic Council to host side meetings and present their statements in plenary session.[40] It remains unclear how the government of The Netherlands will engage civil society and other non-governmental actors when they host the next international conference on cyberspace in 2015.

At the same time, it is important to acknowledge that non-governmental organisations joined the discussion rather late, only recently realizing the links that exist between the international security dimensions of ICTs on the one hand, and technical, human rights, development and governance issues on the other.[41] Civil society organizations – including those working on Internet-related technical issues, but also those with experience in shaping international law or development and trade policy – can rally together to help

[35] To hear how ICTs are being leveraged for conflict prevention and peacebuilding, gp to: http://www.unicef.org/education/bege_73728.html

[36] See the United Nations Secretariat's 2008 Information and Communications Technology Strategy (A/62/793 and Corr.1 and A/62/793/Add.1) and the 2010 update report (A/65/491) available at: http://daccess-ods.un.org/TMP/5780049.56245422.html and http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/567/93/PDF/N1056793.pdf?OpenElement respectively.

[37] ICT4Peace/UN ICT Task Force. Available at: http://bit.ly/1bR0yPI

[38] ICT4Peace (2011), Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyberspace. Available at: http://ict4peace.org/%EF%BF%BCgetting-down-to-business-realistic-goals-for-the-promotion-of-peace-in-cyber-space/

[39] https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement

[40] See for example: http://ict4peace.org/wp-content/uploads/2013/10/ICT4Peace-Statement-Seoul-Conference-on-Cyberspace-2013-1.pdf

[41] At the domestic level, the linkages have been greater however, as evidenced in the reports of UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the manner in which human rights organizations and privacy advocates have engaged with the executive and legislative branches on different aspects of national cybersecurity policy.

break down barriers to engagement and ensure more qualitative and inclusive multilateral processes.

In 2013, windows of opportunity opened up in this regard. Indeed, the 2013 Report of the UN Group of Governmental Experts[42] acknowledged the role of civil society and private sector in implementing norms, CBMs and capacity building measures.[43] More specifically, paragraph 12 of the report acknowledges that 'while States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society.'[44] (While we can read what we may into what the term 'appropriate' means and who gauges what is appropriate in this context, civil society and the private sector should interpret it as an important opportunity to engage).

The report's detailed section on norms, rules and principles of responsible behaviour by States[45] take this further by noting specifically that:

> States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. (paragraph 24)

and that

> Member States should consider how best to cooperate in implementing the above norms and principles of responsible behaviour, including the role that may be played by private sector and civil society organizations. These norms and principles complement the work of the United Nations and regional groups and are the basis for further work to build confidence and trust. (paragraph 25)

In reference to CBMs and Exchange of Information,[46] the report specifically notes in paragraph 28 that '[w]hile States must lead in the development of confidence building measures, their work would benefit from the appropriate involvement of the private sector

[42] For background on the ICT-related Group of Governmental Experts (GGE) see Kavanagh *et a*l, Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security. ICT4Peace (2014). Available at: http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security/; Maurer, T. (2012), Cyber Norm Emergence at the UN: An Analysis of the Activities at the UN Regarding Cyber Security. Belfer Centre for Science and International Affairs. Available at: http://belfercenter.ksg.harvard.edu/publication/21445/cyber_norm_emergence_at_the_united_nationsan_analysis_of_the_uns_activities_regarding_cybersecurity.html; and Tikk-Ringas, E. (2012), Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012. ICT4Peace. Available at: http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

[43] See UN Secretary-General Report 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,' (A/68/98*) of June 2013 (pp.7-9)

[44] Ibid. (p.7)

[45] Ibid. (p. 4)

[46] Ibid. Section IV (p.9)

and civil society.'[47] Combined, these recommendations for greater direct and indirect engagement are of significance.

In comparison to the GGE report, the OSCE Permanent Council (PC) Decision 1106 on an 'Initial Set of CBMs to Reduce the Risks of Conflict Stemming from the Use of ICTs' adopted by the regional body's Permanent Council in December 2013 does not mention civil society.[48] However, this does not necessarily mean that civil society and other core actors should not play a role in implementing the initial set of CBMs. First, the OSCE's Guide on non-Military CBMs prepared by the OSCE Secretariat stresses how CBMs should ideally involve both government structures and civil society, with the latter also playing a role in reaching out to broader society in the implementation phase of CBMs.[49] It stresses that a CBM requires 'buy-in' from society at large (i.e. the qualitative, legitimizing aspect of the multi-lateral process) if it is to succeed. While realistic about civil society's limitations, the Guide stresses the important role of civil society in securing that buy-in. Second, OSCE holds that platforms can be established to ensure consultation with civil society on a range of issues, including CBMs. In this vein, the OSCE aims to oganise a meeting with nongovernmental stakeholders to discuss their needs and expectations in relation to the OSCE CBM process. The meeting is set to take place in November 2014.[50]

Regarding Internet-specific processes, in April this year, the government of Brazil hosted a multistakeholder conference on the future of Internet governance in which civil society played a robust role (at all stages of the meeting). Moreover, the Conference closing statement tabled a set of core Internet governance process principles emphasizing the importance of the multi-stakeholder approach in contributing to an inclusive, effective, legitimate, and evolving Internet governance framework. Moreover, it noted that 'effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.' The statement also emphasized the principles of open, participative and consensus-driven governance; transparency; accountability; inclusivity and equity; the distributed and collaborative character of the Internet; and participation.[51] Undoubtedly these principles are just as applicable to ICT-related processes in the context of international and regional security.

[47] Ibid. Section IV, para. 27 (p.9)

[48] For an overview of the OSCE PC Decision 1106 see: Kavanagh *et al*, Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security. ICT4Peace 2014. Available at: http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security/

[49] OSCE Guide on Non-Military Confidence Building Measures (2013). Available at: http://www.osce.org/cpc/91082

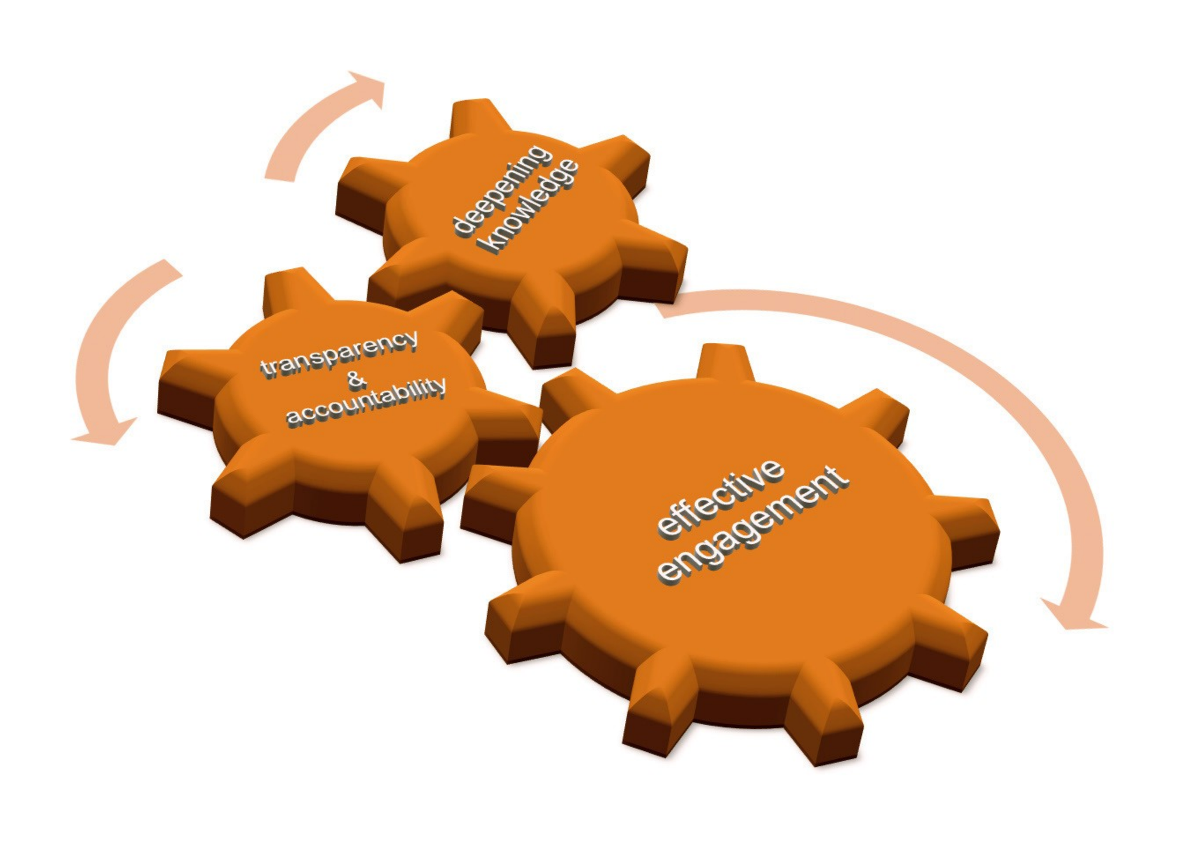
[50] Communication with OSCE, 11 August, 2014.

[51] NETmundial Multistakeholder Statement, 24 April, 2014. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

In short, there are many precedents in the United Nations, regional organizations and other international fora for a more welcoming, equitable and effective approach to engaging actors beyond government – i.e. civil society, as well as academia and the private sector - in a range of norms and CBM processes. As is becoming increasingly evident, cybersecurity should certainly not be the exception.

3. WHAT ROLE, THEREFORE, FOR CIVIL SOCIETY IN FURTHERING NORMS AND CBMS IN THIS FIELD

Civil society can help further change to: ICT-related norms and CBMs in three separate, yet over-lapping areas: i) Engaging Effectively; ii) Fostering Transparency and Accountability; and iii) Deepening Knowledge. Combined, these measures can strengthen the legitimacy and sustainability of on-going processes; ensure that broader normative concerns are attended to, and that the right technical expertise is leveraged when solutions are being sought; and ultimately help build trust between states and between state and society.



EFFECTIVE ENGAGEMENT

As noted above, there are many precedents in the UN and regional organizations for a more welcoming, equitable and effective approach to engaging civil society on issues pertaining to global governance and international security. Given the nature of the eco-system, cyber security should not be an exception. Certainly, the range of legitimacy and normative concerns as well as the technical issues involved call for much deeper engagement of civil society than other areas. One of the chief objectives of civil society should be therefore to lobby for the right to influence directly or indirectly in the multilateral discussions that purport to reach agreement on norms and CBMs in this area. While legitimate national security concerns have been raised concerning some of the non-public aspects of processes in the cybersecurity field (particularly confidence-building exercises between militaries), there are sufficient examples of how civil society can engage. For example:

- Civil society organisations can request or organise hearings before and after government participation in CBMs, norms and other cyber-security-related processes, with government and parliament. This is done in other areas pertaining to international peace and security, and there is no reason it cannot be done with regard to cybersecurity.

- They can also lobby for their direct of indirect participation in CBMs and norms processes as per the outcome of the 2013 GGE report. For instance, civil society representation can be included in government delegations to CBM and norm discussions. The United States included strong civil society representation in its delegation to the WCIT meeting in Dubai 2012; the government of Estonia has included a representative from an international think-tank in its delegation to the last GGE and will do the same in the current one (although the academic representative who had participated in the past two GGEs has since been replaced by a government lawyer); the government of the Republic of Korea included a member of one of the country’s leading think-tanks, ETRI and a professor of law at Korea University’s Cyber Law Center as advisors in its delegation to the 2014 GGE; ICT4Peace supported the government of Switzerland ahead of OSCE discussions on CBMs; and civil society and academia have formed part of the on-going EU-China CBM discussions.

- Civil society can request the establishment of structures such an advisory board or panel to accompany the work of the new GGE that commenced work in June 2014. Such an advisory board can be composed of individuals representing civil society, industry and academia invited by the UN Secretary-General to provide expert advice to the GGE and national governments when requested (for instance, with regard to paragraphs 24 and 25 (section on Norms, Rules and Principles of Responsible Behavior by States) of the 2013 UN GGE Report, which specifically references a role for civil society and the private sector in supporting implementation of the package of norms and principles recommended in the report).

- The section on Confidence Building Measures and Exchanges of Information in the 2013 GGE report calls for 'Exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERTcommunities, and in other fora, to support dialogue at political and policy levels.' It also calls for '[i]ncreased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems,' noting that '[t]his could include guidelines and best practices among States against disruptions perpetrated by non-state actors.'[52] Certainly non-government CERTs are perhaps an example of one of the most direct forms of civil society involvement in responding to threats and vulnerabilities across networked systems. They have deep understanding of the technical issues at hand, are well positioned to develop guidelines and record good practices, and have extensive experience in building trust across communities. Needless to say, on-going norms and CBM processes would benefit significantly from deeper engagement with such CERTs.

- Civil society organizations can participate in/support capacity building efforts or indeed organize events in tandem with national authorities that are designed to implement exisiting CBMs. For example, the OSCE Initial Set of CBMs, encourages States to *inter alia* 'share information on measures that have been taken to ensure an open, interoperable, secure and reliable Internet.'[53] Such a measure in particular would benefit significantly from strong civil society and private sector engagement.

- The The 2013 GGE report also includes a section on capacity building, highlighting the importance of involving other stakeholders in capacity building efforts. Already civil society groups and academia are working with governments and international organizations to translate these commninttments and recommendations into reality. For example, ICT4Peace is commencing a new capacity building project with different regional organisations aimed at levelling the playing field, ensuring that all regions are substantively and technically equipped to participate in international and regional ICT-related CBMs and norms processes. Other non-governmental groups involved in capacity building efforts include Oxford University's Cyber Security Capacity Centre.[54] Some civil society groups might take another tack, for example, monitoring the actual effectiveness of capacity building efforts in this area in contributing to international and regional security as well as longer-term development.

[52] 2013 GGE Report, para. 27(iv) and v)

[53] OSCE 'Initial Set of OSCE Confidence Building Measures to Reduce the Risk of Conflicts Stemming from the Use of Information Communications Technologies.' PC.DEC/1106 of 3 December 2013 (para.4) Available at: http://www.osce.org/pc/109168?download=true

[54] See: http://www.oxfordmartin.ox.ac.uk/institutes/cybersecurity

- Finally, not all civil society engagement is effective, nor is it always productive. If civil society is to engage in this area, it must also develop mechanisms with other stakeholders to monitor and assess its own contributions.

FOSTERING TRANSPARENCY & ACCOUNTABILITY

Monitoring government policy and action and promoting domestic and international standards

Examples abound of how civil society organisations can monitor government actions and use the data it collects to influence a change in policy, set rules and standards etc. For instance, civil society engagement in the development of standards governing weapons transfers[55] or the use of specific weapons has been quite effective, despite the difficulties inherent in working in this area. The process leading to the Ottawa Mine Treaty (the Anti-Personal Mine Ban Convention) also stemmed from strong civil society engagement,[56] as did the process to develop the treaty banning cluster munitions.[57] In the field of ICTs and international security, civil society engagement is still limited, although growing. For example:

- Civil society groups have made repeated calls for governments to regulate the export of surveillance technology to end users with questionable human rights records.[58] Their justification is that effective export controls for such dual-use technologies will ensure that they could be used to facilitate human rights abuses. Some argue that regulation in this area is pointless.[59] At the same time, there is still insufficient analysis of the policy dimension of this problem and the degree to which existing export control regulations cover this technology. Civil society organizations can play an important role by continuing to monitor and document government and industry

[55] For example, the UK-based NGO SaferWorld has played an active role in informing EU parliaments on the issue of traditional arms transfers and in influencing relevant policy decisions. This was done through the development of two blackbooks on arms transfers from European countries aimed at contributing to the review of the EU common Position on arms exports. The two blackbooks are: *Rhetoric or Restraint? Trade in military equipment under the EU transfer control system,'* published in 2010 and '*Lessons from MENA: Appraising EU transfer of military and security equipment to the Middle East and North Africa,'* published November 2011. The latter covered armoured vehicle construction in Sudan under licensed production with German and French companies and was responded to rather swiftly with the closing down of that construction facility. Communication with Saferworld, December 2012 and July 2014.

[56] Both the role of civil society and some of the challenges regarding its involvement in this process are discussed in: Short, N. (2009). The Role of NGOs in the Ottawa Process to Ban Landmines. *International Negotiation* 4: 481–500, 1999. http://faculty.maxwell.syr.edu/rdenever/IntlSecurity2008_docs/Short_NGOsOttawa.pdf

[57] For a discussion on the role of civil society in this process, see Bolton, M. and Nash,T. (2010), The Role of Middle Power-NGO Coalitions in Global Policy: The Case of the Cluster Munitions Ban.' *Global Policy*, Vol. 1, Issue 2, May 2010.

[58] Maurer *et al* (2014).

[59] See for example, Lewis, J.A. (2010), 'Multilateral Agreements to Constrain Cyberconflict,' *Arms Control Association*. https://www.armscontrol.org/print/4261

practices, identifiying further gaps, and providing deeper policy and technological analysis to inform policy.

- Regarding broader issues relating to the military uses of ICTs (or cyber warfare), steps toward standard setting can include working with governments and other actors on framing, redefining and communicating the associated normative concerns and issues.[60] (See IHL examples in the next section on Deepening Knowledge)

- Civil society action can also involve campaining *against* government policies and actions it believes are of normative concern to specific groups or society at large. For instance, many civil society organizations have played a significant role responding to data rights concerns at the domestic level and shaping state behaviour on this topic.[61] Similarly, civil society groups and other non-state actors such as academia and think-tanks concerned with privacy issues can work together to lobby for and monitor implementation of the recommendations tabled in the recent Report of the Office of the High Commissioner for Human Rights on the Right to Privacy in the Digital Age.[62] [63]

Until very recently, very little information regarding international, regional and bi-lateral processes on cyber security was in the public domain. To a large degree, many of these discussions have received limited scrutiny from traditional sources of checks and balances, including civil society. As a means to overcome this challenge, civil society groups can:

- Develop tools to monitor their own government's role in international, regional and bi-lateral norms and CBM discussions and make knowledge regarding progress or setbacks in international and regional norms and CBM processes readily available to the public, working with media and other groups to organise public discussions around them. For example, in May this year, ICT4Peace published its first annual review of ICT-related events and processes that have implications for international and regional security.[64] Other civil society organizations have embarked on similar endeavours. For example, Global Partners Digital recently published an extensive

[60] For examples of civil society engagement in some of these areas see Rappert *et al* (2012), 'The roles of civil society in the development of standards around new weapons and other technologies of warfare.' *International Review of the Red Cross.* http://www.icrc.org/eng/assets/files/review/2012/irrc-886-rappert-moyes-crowe-nash.pdf

[61] For example, civil society's campaign to reject U.S. proposals to regulate copyright infringement/on-line piracy via the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) led to a wide array of company-driven and civil society organized protests, including the darkening of Wikipedia for a day.

[62] Meyer, P. "Surveillance: A Potential 'Chilling Effect' on Human Rights? Report on 'Right to privacy' calls for independent civilian oversight agency." Canadian International Council, 15 August, 2014. Available here: http://opencanada.org/features/the-think-tank/comments/surveillance-a-potential-chilling-effect-on-human-rights/

[63] Right to Privacy in the Digital Age, Report of the Office of the High Commissioner for Human Rights, (A/HRC/27/37) of 30 June 2014.

[64] Cf footnote 42 above.

report on Internet governance-related processes highlighting some of the major areas of tension and discord in this area.[65]

- At another level, civil society organizations can help develop and promote common, ideally internationally recognised standards for transparency reporting on domestic and international cyber security issues. The main challenge is to determine what such transparency reports should focus on: For example, if the focus is on promoting greater transparency in government monitoring and surveillance practices, should reporting focus on the more narrow aspects of SIGINT access to data or broader issues such as data retention periods, takedowns etc.? At any rate, civil society organisations, working with the relevant government institutions and/or private enterprise and academia is well placed to advance both narrow and broader forms of transparency reporting.[66]

Monitoring government expenditure

As it is, the majority of public funds channelled into responding to cyber-related risks and vulnerabilities that pose a threat to international security are being invested in the military areas of defence and offence, or in the field of intelligence, often without sufficient justification. While rendering information on expenditure in this area public might be difficult given i) the difficulties in breaking down expenditure in this field into specific and coherent budget lines; and ii) the fact that much of the relevant information is classified for national security purposes, some form of transparency and accountability is necessary to reassure domestic constituencies (vis-a-vis civil liberties as well as institutional efficacy concerns) on the one hand, and build confidence between states on the other.

- First, despite the classified nature of military expenditure in this area, civil society can still play an important advocacy role, including with specialized parliamentary committees, to ensure minimal transparency and accountability in government expenditure. In this regard, civil society organizations can push for the publication of high-level budgetary details, for example, the budget allocated to the ‘sections’ tasked with defensive operations (this level of budgetary detail need not be classified, even if more specific line items might be). Similarly, civil society organizations can push for or monitor high-level accountability. Studying reports such as the UK Interception of Communications Commissioner reports,[67] which annually indicate accountability within the intelligence organizations, might be an important crutch to lean on in this regard.

[65] Internet Governance: Mapping the Battleground, Global Partners & Associates (2013). http://www.gp-digital.org/wp-content/uploads/pubs/Internet-Governance-Mapping-the-Battleground.final_1.pdf

[66] Email communication with Chrisopher Parsons, Post-Doctoral Fellow, Citizen Lab, University of Toronto. 13 August, 2014.

[67] See for example: 2013 Annual Report of the Interception of Communications Commissioner. http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

- Second, civil society organisations can advocate for an adequate balance of investment between the different, yet overlapping policy areas (security/ defence, governance, development and protection and promotion of human rights).

Each of these areas would require the prior existence of a working disclosure of information regime (including freedom of information/ access to information legislation). Hence, in those countries where the latter is absent or lacks effective implementation, such efforts should be linked to broader state building and/or democracy building efforts. Such advocacy efforts should be combined with strategies aimed at influencing public attention, pressing alternate legal avenues, advocating for space for whistle blowing and so forth.[68]

DEEPENING KNOWLEDGE

Enhancing knowledge and sharing information is core to building a secure and resilient ICT environment, and for strengthening trust and confidence between states. To this end, civil society can:

- Work more closely with academia and the private sector to ensure that evidence-based research is made available to government representatives engaged in norms and CBMS discussions on the one hand; and made accessible to the broader public on the other. Examples of these kinds of initiatives already exist:
    - In June 2014, government, civil society and industry experts attended a meeting organized by the Centre on International and Strategic Studies (CSIS) ahead of the commencement of the work of the new UN GGE. The aim of the meeting was to address key topics relating to international [cyber] security and provide an in-depth discussion between government and non-governmental experts on these issues as a means to develop common understandings and consider the range of possible cooperative measures proposed in previous GGEs.
    - Since 2011, a consortium involving MIT, Harvard and the University of Toronto's Citizen Lab has brought together different stakeholders from government, academia, civil society and the private sector to discuss norms and CBMs for cyberspace. The outcome of these meetings has served as useful input to international and regional discussions, while the meetings themselves have served as an important platform for networking and deepening knowledge across sectors and regions on specific cyber security-related issues.[69]

[68] Email communication with Chrisopher Parsons, 13 August, 2014.

[69] See Hurwitz, Roger (2012), An Augmented Summary of the Harvard, MIT and University of Toronto Cyber Norms Workshop. Available at: http://ecir.mit.edu/images/stories/augmented-summary-4%201.pdf

- In June 2013, ICT4Peace organised a workshop on CBMs and options for international and regional cybersecurity. The workshop's combination of civil society, government, academia and the private sector from different regions was important, not least because each brought valuable perspectives from their own institutional experience within their own regional and domestic realities. The workshop participants drew up an exhaustive list of potential CBMs across core areas: transparency measures; cooperative measures; communication and collaborative mechanisms; restraint measures; and compliance and monitoring measures for dealing with today's ICT-related challenges. They also highlighted where progress has been made, identified key bottle-necks (both political and technical) and noted which of the on-going processes, such as the UNGGE, the OSCE or the ASEAN Regional Forum (ARF) already include civil society, the private sector or academia in some form or other in their CBM-related processes.[70] The Atlantic Council organized a similar meeting on CBMs with NATO country experts in 2014.

- Also in 2013, a group of private international law scholars finished their work on the 'Tallinn Manual on the International Law Applicable to Cyber Warfare.'[71] The Manual explores the applicability of international humanitarian law and the doctrines of *jus ad bellum* to cyber conflicts. While there are legal and political arguments against some of the applications of international law proposed by the group, the Tallinn Manual has, however, made an important contribution to the discussion of how international law might apply in and to cyberspace. Through its work on New Technologies and International Law[72] the International Committee of the Red Cross (ICRC) is also helping break important ground in this area.

In addition, civil society organizations can:

- Develop stronger ties with the private sector, academia and policy think tanks to identify knowledge gaps or deepen the knowledge base in specific technical or policy areas, and feed core findings into norms and CBM discussions and processes. For example, a number of policy think tanks and civil society organisations are supporting Track 1.5 and Track 2 work in this field. It would be useful for these organisations

[70] See ICT4Peace Report: International Dialogue on Confidence Building Measures (CBMs) and International Cyber Security – ETH Zurich, 20 to 21 June 2013. Available at: http://ict4peace.org/ict4peace-global-dialogue-on-confidence-building-measures-and-international-cyber-security/

[71] The Manual was prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence General. Schmitt, Michael M. (ed.), The Tallinn Manual on the International Law Applicable to Cyber Warfare. Available at: http://www.ccdcoe.org/tallinn-manual.html

[72] See: http://www.icrc.org/eng/war-and-law/contemporary-challenges-for-ihl/ihl-new-technologies/index.jsp

to share their experiences, as a means to more effectively identify and disseminate good practices as well as progress in the field.

- Work with government, parliament, academia and industry to ensure the inter-linkages between different policy areas, namely security, governance, development and human rights. As noted above, the ICT4Peace Review of ICT-Related Processes and Events made an important step forward in this regard.

- Finally, civil society can help deepen understanding of cultural dynamics and differences as a means to build trust in cyberspace and different cyber security challenges. Indeed, significant misunderstandings (many of them cultural) still remain in the area of cybersecurity, which can lead to heightening of tensions between states, and between states and citizens if left unresolved.

CONCLUDING REMARKS

Civil society has an important role to play in furthering norms and CBMs for the uses of ICTs in the context of international and regional security. There is sufficient precedent of civil society engagement on other matters of international and regional security to justify its engagement in this area. Moreover, the very nature of the ICT/cyberspace ecosystem renders its engagement (as well as that of academia and the private sector) necessary, not only to ensure more qualitative multi-lateral processes, but also to ensure that certain normative concerns are attended to, and that the right technical expertise is leveraged when solutions are being sought. Combined, the latter can help foster trust between states and between state and society. In some respects, civil society is already engaging, but more effort is needed on the part of governments and civil society. The 2013 GGE Report and the OSCE PC Decision's provide an important opportunity to deepen that engagement.

ABOUT THE AUTHORS

Camino Kavanagh is currently finalising a Ph.D. at the Department of War Studies, King's College London, where her focus is on information technology and transformation in strategic affairs. She serves as advisor to several organizations including ICT4Peace Foundation and the New York-based National Committee on American Foreign Policy (NCAFP) for who she has developed an annual round table series on Cyber Security and U.S. Foreign Policy. Her professional experience includes some fifteen years working in conflict and post-conflict settings as a practioner and from a policy perspective. She consults regularly for international and government agencies, working between New York, Bamako and London.

Dr. Daniel Stauffacher, a former Ambassador of Switzerland, has a Master's degree in International Economic Affairs from Columbia University, New York and a PhD incopyright and broadcasting media law from the University of Zürich. He worked for the district court of Zurich and was Managing Director of a publishing company before joining the United Nations in New York, Laos and China (1982 – 1990) and the Swiss Government (1990 – 2006). For the latter he was, inter alia, responsible for the hosting and preparation of the UN World Summit on the Information Society (WSIS) held in Geneva in 2003 and Tunis in 2005. He was a member of former UN Secretary-General Kofi Annan's UN Information and Communications Technologies (ICT) Task Force and is also the Founder and President of the ICT4Peace Foundation (www.ict4peace.org) and founding Director of the World Wide Web Foundation Board (www.webfoundation.org). Since 2007 he has served as advisor to several governments and the UN on improving Crisis Information Management Systems (CiMS) and helped develop the UN's Crisis Information Management Strategy. Since 2006 he and his ICT4Peace colleagues have called for and participated in international and regional processes to maintain an open, free and secure cyberspace and have published a number of publications in support of such processes (seebelow).

ABOUT ICT4Peace FOUNDATION

ICT4Peace Foundation www.ict4peace.org was launched as a result of the UN World Summit on the Information Society (WSIS) in Geneva in 2003 and aims to facilitate improved, effective and sustained communication between governments, peoples, communities and stakeholders involved in conflict prevention, mediation and peace building through better understanding of and enhanced application of ICTs. The ICT4Peace Program on Rights and Security in the Cyberspace was started in 2011. ICT4Peace is interested in following, supporting and leading bilateral and multilateral diplomatic, legal and policy efforts to achieve a secure, prosperous and open cyberspace. Sample ICT4Peace publications can be found at: http://ict4peace.org/?p=1076 and include:

- Baseline Review ICT-Related Processes & Events: Implications for International and Regional Security (2014)
- What Next? Building Confidence Measures for Cyberspace (2013)
- The Reach of Soft Power in Responding to International Cybersecurity Challenges (2013)
- An overview of global and regional processes, agendas and instruments (2013)
- ICT4Peace brief on Groups of Governmental Expert (GGE) consultations on Cyber-security at the UN in New York (2012)
- Getting down to business: Realistic goals for the promotion of peace in cyber-space (2011)

ICT for peace
FOUNDATION