Cybersecurity

Some Critical Insights and Perspectives

Edited by
Damien D. Cheong

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NSCS
NATIONAL SECURITY COORDINATION SECRETARIAT

The Role of Civil Society in Furthering CBMs

The Role of Civil Society in Furthering CBMs

Daniel Stauffacher

We are undoubtedly living through a moment of significant change whereby a series of developments have led to the loss of public trust. 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 information communications technologies (ICTs) to advance political, military and economic objectives. Indeed, states and non-state actors are increasingly using ICTs to ratchet the advantage during armed conflict or situations of tense political contestation.

This situation has emerged at a moment of broad and complex shifts in the post-cold war international order, solutions for which are proving difficult to shape. It has also 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, democratic or not.

Notwithstanding, for several years a number of states have been engaging 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 use of information and communications technologies (ICTs) in the context of international and regional security. In 2013, representing a major breakthrough in what had heretofore been difficult negotiations, a UN Group of Governmental Experts (GGE) and the Organization for Security and Cooperation in Europe (OSCE) reached initial agreement on the nature of some of these norms, confidence and capacity building measures. Substantive discussions on how these should be applied and implemented

remain, however, at an early stage. 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. Yet, most governments acknowledge 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. To this end, governments have acknowledged the need to build trust and deepen their engagement with other groups – including civil society organisations – as they move to further shape and implement new norms and rules in this area.

Civil society engagement on international governance and security matters is not new, and there are scores of examples of areas in which states have accommodated such engagement. Moreover, this engagement has helped produce positive results, with international and international humanitarian law in particular benefitting enormously from the contribution of civil society organisations. The latter has helped build confidence between and within states (often through the organisation of and participation in track 1.5 and track 2 CBM processes and by fostering dialogue between parties), as well as fostering treaties, promoting the creation of new international organisations, and lobbying in national capitals to gain consent to stronger international rules and standards. International 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.

Yet, to date, civil society engagement 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. 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.

In particular, civil society can contribute by developing strategies for their effective engagement in on-going processes, particularly with regard to supporting and monitoring implementation of the 2013 GGE Report and the OSCE's Initial Set of CBMs. The GGE Report in particular highlights a number of areas in which on-going norms and CBM processes would benefit significantly from greater involvement of civil society (as well as the private sector and academia). And while the OSCE has not identified a role for civil society (nor the ARF for that matter) in shaping or implementing CBMs, there is enough precedent in the work of that organisation to demonstrate how civil society involvement is important and can add much more legitimacy to processes, the outcome of which affect all of society. In addition to direct engagement, civil society organisations can also advocate greater transparency and accountability on the part of governments, highlighting for example, where progress has been made and calling to task national leaders when required. They can similarly work with all relevant stakeholders to deepen the technical and normative knowledge base required to inform sound policy decisions.

If approached effectively and coherently, such engagement can improve the qualitative dimension of multilateral norms and CBM processes regarding international security and state uses of ICTs, affording them greater legitimacy and sustainability. 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.

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg