III. Confidence-building measures for information and communication technologies

IAN ANTHONY

International governance of information and communications technologies (ICTs) is extremely challenging because of the speed, scale and nature of their development. Important issues related to, for example, the use of the Internet in criminal activities and the protection of private and confidential personal data continue to be discussed in various forums.[1] Several sets of guidelines, as well as some international laws, have been agreed in these issue areas.[2]

A recent study published by the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence noted that the perception of cybersecurity, 'formerly viewed as an exclusively technical and organisational challenge' has changed:

> Cyber security has become an inherent part of national security, as evident by the multitude of national cyber security strategies issued since 2008, and thus also a matter of international peace and security.
>
> Some States emphasise the potentially deadly characteristics of cyber tools and the risk of cyberspace transforming into a new global battlefield. Indeed, the armed forces of several States tend to consider cyberspace the fifth domain of warfare.[3]

The economic, political and strategic importance of ICTs, and the fact that diverse actors make common use of certain infrastructure, means that the issue of regulation cannot easily be confined by geographical, military–civilian and public–private boundaries. However, this section limits its scope to a discussion of risks to international peace and security posed by ICTs, focusing in turn on discussion in the United Nations, in the Organization for Security and Co-operation in Europe (OSCE), and between Russia and the United States.

[1] Tikk, E., *Frameworks for International Cyber Security* (NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, May 2010).

[2] E.g. the 2001 Convention on Cybercrime (Budapest Convention), negotiated in the framework of the Council of Europe, is considered to be the most advanced international cyber-related agreement of its kind. The convention requires signatories to establish a range of criminal offences in national law, including the criminal offences of illegal access to computer data and systems, illegal interception of non-public transmissions of computer data and the intentional hindering of the functioning of a computer. Convention on Cybercrime, opened for signature 23 Nov. 2001, entered into force 1 July 2004, <http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp>.

[3] Ziolkowski, K., *Confidence Building Measures for Cyberspace: Legal Implications* (NATO Cooperative Cyber Defence Centre of Excellence: Tallinn 2013), p. 6.

Developments in United Nations forums

The question of information security has been discussed in the United Nations since 1998, but without agreement.[4] In 2011 China, Russia, Tajikistan and Uzbekistan sent the UN Secretary-General a draft Code of Conduct and asked him to distribute it at the next session of the UN General Assembly.[5] No code was adopted, but the draft proposal did stimulate further analysis.

A Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security—which had been authorized by the UN General Assembly in 2011—reported in June 2013. One of its conclusions was that 'voluntary confidence-building measures [CBMs] can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception'.[6] The experts also encouraged discussion of CBMs in bilateral and multilateral settings, including in regional groups.

Developments in the Organization for Security and Co-operation in Europe

In December 2013 the participating states in the OSCE agreed on an initial set of CBMs to reduce the risks of conflict stemming from the use of ICTs.[7] The primary objective of the states making the agreement was to avoid the escalation of a suspected malicious incident into a serious crisis. In the OSCE context, states identified the risk that an unusual cyber event could be misinterpreted as a hostile action, in particular during a period of heightened tension, and in an extreme case this might increase the likelihood of open conflict.[8]

[4] UN General Assembly Resolution 53/70, 4 Dec. 1998.

[5] Chinese Ministry of Foreign Affairs, 'China, Russia and other countries submit the document of International Code of Conduct for Information Security to the United Nations', 13 Sep. 2011, <http://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/t858978.shtml >.

[6] United Nations, General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, para. 26.

[7] OSCE, Permanent Council, 'Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies', Decision no. 1106, PC.DEC/1106, 3 Dec. 2013. For a brief description and list of members of the OSCE see annex B, section II, in this volume.

[8] In recent years a number of what appear to be serious and coordinated cyber attacks against the state authorities in OSCE states have been reported, e.g. in Estonia and Georgia. Terlikowski, M., 'Cyberattacks on Estonia: implications for international and Polish security', *Polish Quarterly of International Affairs*, no. 3, 2007; and US Cyber Consequences Unit, 'Overview by the US-CCU of the cyber campaign against Georgia in August of 2008', Aug. 2009, <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

The OSCE elaborated a list of voluntary CBMs intended to reduce the identified risk. The measures will require participating states to initiate a focused dialogue in order to further develop them operationally.

Under the agreement, OSCE participating states will provide their views on various aspects of threats to, and in the use of, ICTs. They will develop cooperation among the competent national bodies, initiate an exchange of information and conduct consultations in order to reduce the risks of misperception. The information sharing should include an explanation of national organization, strategies, policies and programmes, and participating states promised to nominate contact points and provide contact data in order to facilitate the process.

One specific task that OSCE participating states set for themselves was to put together a list of national terminology used in the field of ICT security, with a view to producing a common OSCE glossary.

As part of the agreement on CBMs, OSCE participating states agreed that the package of information to be shared should include an explanation of the national measures taken to ensure an open, interoperable, secure and reliable Internet. The OSCE Permanent Council adopted the CBMs by consensus, and they are, therefore, supported by all participating states. However, at the time the decision was taken one state—Russia—submitted an interpretative statement noting that, in giving its support, it 'will be guided in its implementation by a firm commitment to the principles of non-interference in the internal affairs of States, their equality in the process of Internet governance and the sovereign right of States to Internet governance in their national information space, to international law and to the observance of fundamental human rights and freedoms'.[9] One analysis has pointed out that the Russian perspective on cybersecurity incorporates the idea of sovereignty in cyberspace:

> Russia, along with a number of like-minded nations (for example members of the CIS [Commonwealth of Independent States], CSTO [Collective Security Treaty Organization] and SCO [Shanghai Cooperation Organisation]), strongly supports the idea of national control of all internet resources that lie within a state's physical borders, and the associated concepts of application of local legislation.[10]

The work carried out by the OSCE participating states is not intended to be seen in isolation, but is one part of the wider and deeper international discourse on ICT security. As made clear in a background paper presented

[9] OSCE, Permanent Council, Delegation of the Russian Federation interpretative statement under Paragraph IV.1(A)6 of the Rules of Procedure of the Organization for Security and Cooperation in Europe, Decision no. 1106, PC.DEC/1106 attachment, 3 Dec. 2013.

[10] Giles, K., 'Russia's public stance on cyberspace issues', eds C. Czosseck, R. Ottis, and K. Ziolkowski, *Proceedings of the 4th International Conference on Cyber Conflict* (NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, 2012), p. 65. For brief descriptions and lists of members of the CIS, CSTO and SCO see annex B, section II, in this volume.

by Germany, the final objective should be cooperation and collaboration in a multilateral framework to create international cyberspace stability by agreeing on what represents responsible behaviour.[11] As noted above, consultations on ICT security continue in the framework of the UN, and other actors have also taken initiatives in this area.

In its Cybersecurity Strategy published in February 2013, the European Union (EU) promised to support the development of ICT-related CBMs.[12] In its presentation to the OSCE Annual Security Review Conference, the EU endorsed and supported the OSCE's activities in this field.[13]

Developments in Russian–US relations

In June 2013 Russia and the USA agreed to establish a working group on cyber issues under the Bilateral Presidential Commission. It met for the first time in November.[14] Building on an exchange of white papers describing national approaches to cybersecurity, in June 2013 Russia and the USA also agreed three bilateral CBMs. First, links were established between the respective Russian and US computer emergency response teams, and these bodies will exchange information on identified malware that appears to originate from the other's territory. Second, existing nuclear risk-reduction centres in Russia and the USA will be used to clarify those incidents that could be interpreted as deliberate malicious acts. Third, a secure voice communications line was added to the existing White House–Kremlin Direct Secure Communication System (the so-called hotline) linking the US Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council. This hotline would be used in case there is a need to manage an ICT-related crisis situation.[15]

[11] 'OSCE participating states agree initial set of confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies', Background paper, 3 Dec. 2013.

[12] European Commission, European External Action Service, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final, Brussels, 7 Feb. 2013, p. 16.

[13] European Union, EU statement on Working Session I: transnational threats and challenges, OSCE 2013 Annual Security Review Conference, PC.DEL/538/13, Vienna, 21 June 2013.

[14] US Department of State, 'U.S.–Russia bilateral presidential commission', <http://www.state.gov/p/eur/ci/rs/usrussiabilat/index.htm>; and White House, 'Joint statement on the inaugural meeting of the U.S.-Russia Bilateral Presidential Commission working group on threats to and in the use of information and communication technologies (ICTs) in the context of international security', 22 Nov 2013, <http://www.whitehouse.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi>.

[15] White House, 'U.S.–Russian cooperation on information and communications security', Fact sheet, 17 June 2013, <http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>.

In 2013 Russia proposed supplementing the Russia–USA bilateral dialogue by incorporating cybersecurity into the NATO–Russia Council work programme, but this proposal was not accepted by NATO.[16]

The ongoing discussions in these forums in 2013 show that international governance of ICTs is still evolving. Norms are developing, but it is too soon to predict their final form and where the balance will fall, for example, between state control and international collaboration in cyberspace.

[16] Russian Ministry of Foreign Affairs, 'Interview by the Russian Foreign Minister Sergey Lavrov to Russia Today TV-channel', Press release no. 2606-24-12-2013, 24 Dec. 2013, <http://www.mid.ru/brp_4.nsf/0/E76E9D275ED12CBF44257C5B001DF024>. For a brief description of the NATO–Russia Council see annex B, section II, in this volume.