Transparency and confidence-building measures in cyberspace: towards norms of behaviour

Ben Baseley-Walker

In 2012 the world's pulse beats in cyberspace. From commerce to development to fighting wars, cyberspace usage is a defining characteristic of our age. Since 2000, with the dramatic increase in the use of cyber technologies in civil, military and commercial sectors, a new, highly dynamic security stage has arisen. Governments are struggling to contend with the security implications of this emerging arena of potential conflict. Today, as an understanding of global dependence on cyber resources has begun to emerge, governments are now taking strong stances on building predictability, stability and security in cyberspace. As can be seen from Stuxnet to attacks on the New York Stock Exchange, cyberspace is now a domain, like sea, air and outer space before it, where fundamental state interests are starting to be expressed. This is a world where terrestrial borders can no longer be said to be the boundaries they once were. Cyberspace has become a new conduit for governmental, as well as non-governmental, power projection.[1]

Following the cyber attacks in Estonia and Georgia in 2007 and 2008 respectively and the attack on Iranian nuclear facilities in 2010, it is becoming increasingly clear that the potential for cyberwarfare has become an "unavoidable element in any discussion of international security".[2] So far at least 33 states now include cyberwarfare in their military planning and organization.[3] There is a growing realization, however, seen in simulations and through political and military analyses, that currently there is little to no ability to effectively control the escalation of cyberconflict. Nor is there any common understanding of how the existing norms of international humanitarian law would apply—if at all.

This article examines a key step on the road to changing that state of affairs—the creation of norms of behaviour and transparency and confidence-building measures (TCBMs). It first examines the nature of TCBMs for cyberspace, their application and then continues with a look at some of the initiatives already proposed.

For the purposes of definition a clear line should be drawn between cybercrime and cyberwarfare. However, the realities of defining the boundaries between different negative activities in cyberspace are complex. Cybercrime can be defined as non-state sponsored actions which are illegal at either the national or international level. This can range from credit card fraud to child pornography. This article, however, deals specifically with cyberwarfare, which is defined as state-sponsored, offensive cyber activities directed towards another state, its infrastructure or population. It is important to note that a common understanding of the

---

Ben Baseley-Walker is Programme Lead of the Emerging Security Threats Programme at the United Nations Institute for Disarmament Research (UNIDIR). He was previously Advisor on Security Policy and International Law for the Secure World Foundation (SWF). The opinions expressed in this article are the author's own and do not necessarily represent the views of UNIDIR or the United Nations.

parameters of the grey area between espionage—illegal data collection—and cyberwarfare has not yet been developed by the international community.

TCBMs: the concept

TCBMs can be broadly defined as elements of international policy that reduce threats, build trust, and make relationships between states more predictable. TCBMs have a long history as a useful tool for the international community and have been used in a variety of international security issues, most notably dealing with nuclear weapons.[4] TCBMs have traditionally been viewed as instruments with a politically binding effect. Although they are usually seen as a bridge to future legally binding international security instruments, the possibility is not precluded that they could themselves become legally binding.

The concept of TCBMs and norms of behaviour has been the subject of much political debate. The terms confidence, security and transparency have been used in various ways, with each concept invariably generating a negative reaction from one state or another. However, the international community has consistently agreed that cyberspace measures of some sort must be taken and taken soon.

The United Nations has long promoted TCBMs as a mechanism to promote security among Member States. In the early 1980s the UN Disarmament Commission developed a set of guidelines for confidence-building measures, which it presented at a special session of the General Assembly devoted to disarmament:

> 2.2.5 A major objective is to reduce or even eliminate the causes of mistrust, fear, misunderstanding and miscalculation with regard to relevant military activities and intentions of other States, factors which may generate the perception of an impaired security and provide justification for the continuation of the global and regional arms build-up.
>
> 2.2.6 A centrally important task of confidence-building measures is to reduce the dangers of misunderstanding or miscalculation of military activities, to help to prevent military confrontation as well as covert preparations for the commencement of a war, to reduce the risk of surprise attacks and of the outbreak of war by accident; and thereby, finally, to give effect and concrete expression to the solemn pledge of all nations to refrain from the threat or use of force in all its forms and to enhance security and stability.[5]

For the purposes of this article TCBMs are measures designed to lessen the likelihood of conflict escalating through a lack of understanding and trust in the cyber activities of both allies and adversaries. While there are many advantages to why a TCBM should be a legally binding measure, given the general state of uncertainty and mistrust between states on cybersecurity issues, it seems likely that TCBMs in cyberspace will be at most only politically binding.

TCBMs generally come in two types: those dealing with capacity and those dealing with intentions. Some states have framed the first in terms of a "duty of care obligation"—a demonstration of best security practices at the state level. The second focuses on international norms and building a better understanding of state-to-state interaction on cyber-related international security issues.[6] Historically, TCBMs have either been constructed to supplement legally binding instruments or have contributed to laying down the foundations for future progress. This can take the form as either progression towards a legally binding instrument or simply an improved climate for building understanding while continuing, for example, to conduct activities in cyberspace or develop cyber defences, and ensuring doctrine on such developments is made widely available.

It is important to emphasize that TCBMs do not necessarily have to be of a particular form or structure. Activities carried out by completely commercial entities, such as the sharing of data on cyber attacks, can amount to a TCBM that clearly fulfils the role of decreasing political and military tensions at the state level. There is a variety of such profit-driven cooperation in other sectors—in the space sector, for example, the sharing of orbital positioning data among commercial satellite operators through the Space Data Association has had a positive impact on the sharing of data and information among government entities.

What do we want to achieve?

It is clear that the goal is to develop a safe, stable and—above all—predictable environment in cyberspace. A state's incentive to inflame tensions or damage the overall cyber environment is inversely proportional to its national engagement in cyberspace. As a state increases its investment in cyber resources—civilian, commercial and military—and derives ever-increasing economic benefit from the Internet, the asymmetrical advantage of attacking an adversary with a heavy reliance on cyber resources risks engendering significant consequences for the perpetrator.

One of the greatest challenges in cyberspace is attribution of an attack. Even if the perpetrator is identified in a timely fashion with a high degree of confidence, proving an act was state-sponsored is extremely challenging and often impossible. This leaves states with few options—either do nothing or risk a crisis situation which might quickly escalate, given that neither side has a clear idea of the "red lines" of their adversary nor a clear understanding of what the escalatory steps might be. This reality means that building established mechanisms of state interaction in cyberspace is essential if we hope to slow escalation and reduce the likelihood of conflict. TCBMs play a central role in reducing misperceptions and communicating the long-term intentions of states.

Understanding the position of allies and adversaries: a first step

One of the first steps to building an effective TCBM regime is to develop a clear understanding of the parameters within which other actors in cyberspace operate. In the political–military realm the development and sharing of military doctrine, an appreciation of the exact aims of a national declaratory policy on cyberspace and creating crisis management links, such as hotlines, are all essential. Certain political issues are shaping up to be highly contentious. The most current of these is the question of whether information can be viewed as a weapon. Some states view certain mechanisms of dissemination of information as conduits for news and propaganda and potential threats to the state. Consequently, the Internet—and with it cyberspace—is a key mechanism for such dissemination. Other states view the freedom of information as the bedrock of cyberspace interaction. This split in views is not going to be easily overcome. TCBMs do, however, offer a route for progress even on such highly political issues. By building an understanding of both perspectives, approaches and possible "red lines", states can identify and navigate towards areas of common ground. This approach works to avoid slipping into a state of attrition involving entrenched political positions, such as on freedom of information. It allows the foundations to be laid to tackle the key questions such as: what are the military rules of engagement for a conflict in cyberspace?

In addition, there are many questions as to where boundaries and red lines are to be found in the cyber environment. Would a state interpret a state-sponsored attack on its largest commercial bank as an armed attack within the meaning of Article 51 of the United Nations Charter?[7] What is included in a state's critical infrastructure and what is a proportional reaction if attacked? Establishing where these lines lie will result in much clearer recognition by policymakers and military actors of the future realities of state-to-state engagement in cyberspace. The United States has been clear that it considers that the existing international legal structure, including the law of armed conflict, is applicable to cyberspace, but has also stated that it sees a need for further work to be carried out in establishing the principles for reaching "a definitive legal conclusion as to whether a particular disruptive activity in cyberspace constitutes an armed attack triggering the right to self-defense".[8]

Regarding the specifics of self-defence, a clearer understanding needs to be developed on what are considered to be the obligations of states to prevent their territory being used for cyber attacks. Obviously, there is once again a clear difference here between cybercrime and cyberwarfare. The position has been put forward that non-belligerents in a conflict are not obliged to prevent the use of their networks as conduits for offensive purposes under the law of neutrality.[9] Such issues require clarification if effective norms of behaviour for all states—not only those with offensive capabilities—are to be developed.

Current initiatives

The London Conference on Cyberspace

The London Conference on Cyberspace, which took place in September 2011, was instrumental in raising the profile of the steps required to build confidence among international partners. It is clear from the discussions at the London Conference that there is still a range of opinion on the exact nature and definition of cybersecurity. The actual question of defining the term was not directly tackled but a clear split emerged between those who view Internet freedom as a fundamental human rights issue and those who have grave concerns regarding national security risks, information security threats and the use of information as a weapon.[10]

This debate underlines the need to divorce the expression of political ideas in cyberspace from the practical steps needed to develop cybersecurity TCBMs and secure cyberspace in the long term. With regards to the discussion on international security at the London Conference:

> All delegates underlined the importance of the principle that governments act proportionately in cyberspace and that states should continue to comply with existing rules of international law and the traditional norms of behaviour that govern interstate relations, the use of force and armed conflict, including the settlement by states of their international disputes by peaceful means in such a manner that international peace, security and justice are not endangered.[11]

It is important to note that the participants did not consider it timely for legally binding measures to be discussed. The true success of events such as the London Conference is in providing a structured non-formal forum in which such common understandings on the next steps for action and discussion can be agreed. It is hoped that the 2012 and 2013 conferences—hosted by Hungary and the Republic of Korea respectively—will play a similar role.

International code of conduct for information security

A proposal made by China, the Russian Federation, Tajikistan and Uzbekistan for an international code of conduct for information security was first circulated in 2011 in a letter to the Secretary-General of the United Nations.[12] While many disagree over its content, the proposal has been an effective tool for spurring debate.

The proposed code, however, does not detail any recommendations on the creation of norms, TCBMs and definitions but instead is confined to broader statements on the nature of information security and the potential use of information as a weapon.

> Each State voluntarily subscribing to the code pledges:
>
> [...]
>
> (b) Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to

> international peace and security or proliferate information weapons or related technologies.[13]

Such a position of limited freedom of information has been consistently opposed by various states, notably the United Kingdom and the United States. At the current stage of norms development in cybersecurity, it would seem that the international community is not yet ready to start work on such a document. However, it once again underlines the need for cross-cutting foundational work on terminology and establishing where both disagreement and common ground are to be found before there can be any hope of progress on more elaborate and politically sensitive topics.

Regional organizations

Regional organizations have a long history of working with TCBMs in conventional security areas. Housing such initiatives in a regional organization framework has many positive aspects. First, such an initiative builds on models and lines of communication already familiar to participating states. Therefore, methodologies that have been successful in other areas have the potential to be transferred over to cyberspace. Furthermore, regional organizations may be better able to respond to regional concerns or requirements—especially if the cyber capacities of their member states are at a similar stage of development. As an example, Organization for Security Co-operation in Europe (OSCE) member states, with support of key actors such as the United Kingdom,[14] are investigating the possibility of establishing a working group focused on developing confidence-building measures for cyberspace. The working group would be established by a decision of the Permanent Council of the OSCE. If successful, it may become a model that can be applied by other regional organizations.

A further example is the agreement between the member states of the Shanghai Cooperation Organization on international information security.[15] This agreement, signed by China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan in 2009, takes important steps forward on building common political positions on information security. One of its most significant contributions is the inclusion of a list of definitions of basic terms. This will help future discussions between states to progress, as all parties will have a clearer idea of the conceptual parameters within which others are operating.

UN Groups of Governmental Experts on Information Security

The UN General Assembly occasionally convenes Groups of Governmental Experts (GGEs) to explore areas of particular concern and make recommendations. Membership in GGEs is usually limited to no more than 15 experts, nominated to be geographically representative. GGEs meet in several closed sessions, attempting to reach consensus. If the group is successful in reaching agreement, the resulting report is submitted to the Secretary-General for consideration.

At the suggestion of the Russian Federation, a GGE on the topic of information security was convened in 2004. The group failed to reach agreement.[16] In 2009 a second GGE was convened, with the mandate:

> to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as concepts aimed at strengthening the security of global information and telecommunications systems.[17]

This group reached consensus. Their 2010 report made the following recommendations:

> (i) Further dialogue among States to discuss norms pertaining to State use of ICTs [information and communications technologies], to reduce collective risk and protect critical national and international infrastructure;
>
> (ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;
>
> (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;
>
> (iv) Identification of measures to support capacity-building in less developed countries;
>
> (v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.[18]

The General Assembly has agreed to convene a new GGE in 2012, with the mandate to take "into account the assessments and recommendations contained in the [2010] report, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them" as well as "relevant international concepts aimed at strengthening the security of global information and telecommunications systems".[19] Based on the structure of the 2010 recommendations, it would seem that the next step would be to develop some specifics on what the implementation of the recommendations might look like and—equally importantly—designate a forum for future discussion of TCBMs in cyberspace.

Forum of Incident Response and Security Teams

As mentioned above, TCBMs on international security and cyberwarfare do not necessarily need to be constructed at the state level. Given the extensive involvement of the private sector in the development of cyberspace, it can also play a major role.

The Forum of Incident Response and Security Teams (FIRST) network is an example of such an undertaking. FIRST is an international confederation of computer emergency response teams

(CERTs), formed in 1990, with the aim of counteracting challenges arising from, for example, differences in language, time zones and international standards. FIRST aims to coordinate CERTs and cooperatively handle computer security incidents and promote incident prevention programmes. Bringing together the educational, government, military and commercial sectors, it provides a mechanism for the coordination of cyber incident response and provides access to best practices and tools, and to trusted communication with member teams.

Such initiatives, while originating from a very specific need, contribute greatly to the internationalization of best practices in cybersecurity. This is of special relevance for states with less capacity in cybersecurity. It is imperative that the international security community looks to mechanisms such as these and ensures that governmental action at the multilateral level is harmonized with the activities of operators and other stakeholders, such as private businesses relying on cyberspace infrastructure.

International Telecommunication Union

With its Global Cybersecurity Agenda, the International Telecommunication Union (ITU) has continued to build a role in cybersecurity and has generally taken a holistic view on the issues of cyberconflict and cybercrime. Hamadoun Touré, the ITU Secretary-General, has outlined five key principles for "cyberpeace":

1. Every government should commit itself to giving its people access to communications.
2. Every government will commit itself to protecting its people in cyberspace.
3. Every country should commit itself not to harbor terrorists/criminals in its own territories.
4. Every country should commit itself not to be the first to launch a cyber attack on other countries.
5. Every country must commit itself to collaborate with each other within an international framework of co-operation to ensure that there is peace in cyberspace.[20]

While these principles are Touré's personal views, they do seem to reflect the general direction of ITU involvement in cyberspace. The ITU should be commended on its continued efforts to set standards, provide capacity-building and build linkages from cybercrime to cyberconflict. Understanding how such procedural and technical work can contribute to the larger, highly political, international cybersecurity debate demands further examination and an understanding of how this best relates to other ongoing initiatives.

Conclusion

The international community is currently at a turning point in cybersecurity diplomacy. States have become aware of the threats and challenges they now face in an environment that is constantly evolving. Given that the initiatives discussed here are still at the early stages of development, the point has not yet been reached when states are politically chained to a particular initiative and thus are not prepared to consider alternatives. This should be taken advantage of. Currently, there is a window of opportunity to make real progress on definitions and operational TCBMs. While no state's concerns should be disregarded, it is imperative to disassociate those measures that are beneficial to all parties at a foundational level from more conceptual questions regarding the balance between information warfare and freedom of expression.

Clarifying military and political doctrine on issues such as the protection of critical infrastructure and national positions on thresholds for a state to take offensive or defensive action in cyberspace provides plenty of substance for working towards near-term progress.

In terms of specific mechanisms for TCBMs, every option should be considered given that the goal is a cyber environment that is more stable, more predictable and less likely to result in miscommunication leading to conflict escalation. Bilateral understandings between advanced Cyber Powers, a multilateral accord or an international private–public agreement all are possible avenues for progress and deserve further investigation into their feasibility.

2012 through 2014 will be crucial years for setting the future direction of the interaction of states on and in cyberspace. TCBMs developed during this period, it is hoped, will work to ensure that the interaction is as peaceful as possible.

Notes

1. For more information on the Stuxnet attacks see R. Langner, "Cracking Stuxnet: A 21st-Century Cyber Weapon", <www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html>.
2. J. Lewis and K. Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization", UNIDIR, 2011.
3. Ibid., p. 3.
4. See J. Robinson, "The Role of Transparency and Confidence-Building Measures in Advancing Space Security", *European Space Policy Institute Report 28*, 2010, pp. 14–26.
5. General Assembly, *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament*, UN document A/S-15/3, 28 May 1988, pp. 28–33.
6. The comments made by M. Markoff at the conference International Engagement on Cyber, Georgetown University, 29 March 2011, can be found at <www.acus.org/event/international-engagement-cyber-establishing-international-norms-improved-cyber-security/panel-4-transcript>.
7. Article 51 opens with: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security".

8. US Department of State, *Cyber security keynote address by Dr. Deborah Schneider, US Department of State*, document FSC-PC.DEL/30/10, 9 June 2010, p. iv.
9. See N. Melzer, "Cyberwarfare and International Law", UNIDIR, 2011, § IV.
10. For further information on the Internet and human rights see The White House, "VP's Remarks to the London Cyberspace Conference", speech by US Vice-President Joe Biden, 1 November 2011.
11. Foreign and Commonwealth Office, *London Conference on Cyberspace: Chair's Statement*, 2 November 2011.
12. General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN document A/66/359, 14 September 2011.
13. Ibid, p. 4.
14. "Meanwhile the UK will work actively in the UN and with organisations such as the Organisation for Security and Cooperation in Europe (OSCE) to develop practical confidence-building measures to reduce the risk of escalation and avoid misunderstandings between states arising from unexpected incidents in cyberspace"; Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, 2011, p. 26.
15. Shanghai Cooperation Organization, *Annex I to the agreement between the governments of the member states of the Shanghai Cooperation Organization on cooperation in the field of international information security*, 16 June 2009, based on an unofficial translation.
16. In addition to the Permanent Five on the Security Council—China, France, the Russian Federation, the United Kingdom and the United States—Belarus, Brazil, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea and South Africa were also represented. For further information see T. Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security", *Explorations in Cyber International Relations Discussion Paper 2011–11*, 2011.
17. General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010, p. 5.
18. Ibid., p. 8. The GGE was composed of the Permanent Five, Belarus, Brazil, Estonia, Germany, India, Israel, Italy, Qatar, the Republic of Korea and South Africa.
19. General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN document A/C.1/66/L.30, 14 October 2011.
20. ITU, *The Quest for Cyber Peace*, 2011, p. 103.