Unpacking the GGE's framework on responsible state behaviour: Confidence building measures

GLOBAL PARTNERS DIGITAL
gp-digital.org

At the UN First Committee, two processes—the UN Group of Governmental Experts (GGE) and the Open-ended Working Group—are currently exploring the same question: responsible state behaviour in cyberspace. This term comes from a 2015 report by the previous GGE, which defines it according to a framework of four components: 1) norms, rules and principles; 2) confidence-building measures; 3) capacity building; 4) the application of international law in cyberspace.

Understanding these components is crucial to engaging effectively at the GGE and OEWG. In this series, we'll be looking at each component in turn—looking at what they mean, how they have been defined, and their relevance to human rights. In this entry, we examine confidence building measures. This explainer was authored by Kristine Hovhannisyan and Eneken Tikk of Cyber Policy Institute (CPI) and Sheetal Kumar of Global Partners Digital.

Defining confidence building in cyberspace

The concept of confidence building in international relations emerged during the Cold War. Strong antagonism and adversarial relations between the US and the Soviet Union led to deep distrust and fears of an outbreak of war in the international community. The UN Disarmament Commission characterised this era by: "Common concern about the deterioration of the international situation, the continuous recourse to the threat or use of force and the further escalation of the international arms build-up, with the concomitant rise in instabilities, political tensions and in mistrust, and the heightened perception of the danger of war, both conventional and nuclear."[1]

In anticipation of an armed conflict, the signs of even normal military action could have easily been mistaken for an attack or other doubtful activities. For instance, military exercises, movements of troops in border areas, and uncoordinated movements in seas or skies could have been misinterpreted as acts of aggression, or preparations towards such acts.

Confidence-building measures (CBMs) became a tool for preventing the unintended escalation of such a situation into a conflict. Directed at creating transparency and increasing coordination and cooperation between otherwise estranged governments, CBMs have been used to reduce misperceptions and misunderstandings in situations of tension. One of the earliest CBMs was the establishment of a direct communications link between the United States and the Soviet Union after the Cuban Missile Crisis, which allowed each party to consult the other in case of doubt about each others activities.[2] Another example of a CBM institutionalised within the UN is the UN Register of Conventional Arms, whereby the UN established a distinct mechanism for the verification and assessment of arms transfers, as a means of promoting transparency.

Therefore, CBMs are a classic tool of disarmament, and were an important means of maintaining peaceful relations between the two superpowers. The UN First Committee discussion on "Developments in the field of ICTs" is the main venue that has so far been used to explore issues related to peace and security in cyberspace at the UN. With the US and Russia the two leading states in this process, it is not surprising that CBMs have become part of these discussions.

The GGE has not provided an explicit definition of CBMs. However, experts have noted that "confidence-building measures strengthen international peace and security" and "can increase interstate cooperation, transparency, predictability and stability."[3] The GGE has also made reference to earlier work on CBMs—notably the Guidelines for Confidence-building Measures adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly.[4] According to these Guidelines, states should use CBMs to diminish mistrust and enhance trust, by reducing and eventually eliminating causes for misunderstanding, misinterpretation and miscalculation. They also emphasise that an "appropriate mixture of different types of concrete measures should be determined for each region, depending on the perception of security and of the nature and levels of existing threats."[5]

Defining confidence building in cyberspace (cont'd)

CBMs from the Cold War era are generally understood to fall into three main groups:

1. Transparency measures, such as the sharing of national doctrines and policies;
2. Cooperative measures, such as setting up points of contact;
3. Restraint measures, such as committing to undertaking certain actions and refraining from undertaking others.

The GGE has adopted a gradual approach to CBMs, starting with transparency measures, and expanding to cooperative measures. So far, no restraint measures have been proposed.

The current situation and trends: confidence building in cyberspace

The concept of cyber confidence building first appeared in the 2010 UN GGE report. But it was not until the consensus report of the 2013 GGE that six specific confidence building measures were proposed.

The main types of CBMs suggested in the 2013 UN GGE report are transparency and cooperation measures. These focus on steps to increase the predictability and transparency of behaviour and to demonstrate the good will of participating states. Transparency measures in the report include "voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs"; "exchanges of information and communications between national CERTs"; and "enhanced sharing of information on ICT security incidents, including exchanging information on national points of contact".

In 2015, a more detailed set of four main CBMs were proposed, accompanied by a set of five additional CBMs which suggested further areas where states could undertake measures to promote confidence and trust.[6] These elaborated on the first set of CBMs from the 2013 report—for example, by recommending that states share information on "categories of infrastructure they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure". Other measures mentioned in the report include "cooperat[ing] with requests from other States in investigating ICT-related crime or use of ICTs for terrorist purposes" and "expand[ing] and support[ing] practices between computer emergency response teams".

Since the adoption of the 2015 GGE report, the focus has shifted to the implementation of CBMs. One way to implement the GGE CBMs has been through bilateral CBM agreements. In particular, the US and Russia have adopted a package of three confidence building measures to strengthen their relations in cyberspace, expand shared understanding of threats appearing to emanate from each other's territory, and prevent the unnecessary escalation of ICT security incidents.[7] Agreed measures include the establishment of links between the two countries' computer emergency response teams (CSIRTs), and a direct, secure voice communications line between the U.S. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council, should there be a need to directly manage a crisis situation arising from an ICT security incident.[8]

However, beyond bilateral agreements, the implementation of the GGE CBMs has been a source of some contention. For example, some countries—notably the US and like-minded states—believe that the CBMs in the 2015 framework are sufficient and should be mainly implemented at the regional level, by organisations such as the Organization for Security and Co-operation in Europe, the Organization of American States and the Association of Southeast Asian Nations, with only a secondary role for the UN (e.g. with the OEWG serving as a space for the exchange of experiences and best practice on the implementation of CBMs). Such countries point to the fact that these regional organisations have already adopted CBMs—meaning they have agreed to implement these measures by working together with member states.

However, other countries, including Russia, believe that new CBMs should be developed, and that the UN should play a primary role in both developing them and in driving their implementation.

In either case, there has been little discussion or research on whether these efforts are having an impact. While their general purpose is clear, it remains undefined and unclear whether (and if so, what) particular threats and insecurities are expected to diminish as a result of the implementation of these CBMs.

There are also a number of challenges in implementing CBMs in cyberspace. These include:

- **Difficulty in measuring cyber capabilities.** The implementation of CBMs, particularly those relating to transparency, requires states to share information about their cyber capabilities. Because cyber capabilities are constantly changing and evolving, this is difficult to measure. Moreover, the development and testing of cyber capabilities is easy to hide, making it challenging to monitor their existence and share information about them. However, not all cyber capabilities are invisible to human observation. For example, a number of countries have established military cyber commands and conduct annual cyber exercises.

The current situation and trends: confidence building in cyberspace (cont'd)

- **Difference in capacities between states and understanding of key terms**. In order to implement CBMs, states need to have adequate levels of capacity. For example, to establish a national contact point, they already need to have certain relevant infrastructure in place. In many states, these resources or infrastructure don't currently exist, which makes the practical implementation of CBMs difficult. Furthermore, a lack of agreement on key concepts and definitions of terminology, like "critical infrastructure" or "cyberattack", further complicates the situation.
- **The unclear role of non-governmental stakeholders**. In cyberspace, compared to other areas where disarmament discussions happen, non-government stakeholders play an important role in maintaining the stability of the internet. As such, practical measures to maintain the stability of the internet will require the engagement of non-governmental stakeholders. For example, one of the proposed GGE CBMs relates to the sharing of threat information. Yet, in cyberspace, threat identification, monitoring and addressing threats is performed in large part by the private sector, and even civil society. However, as CBMs are predominantly national instruments, the role of civil society can become more difficult to discern, as is explained in the final section of this brief.

A cross cutting challenge is that, because CBMs rely on the political will of states, and the dedication of resources, in practice actual implementation has been slow.

Confidence building measures and human rights

The need for CBMs is associated with the potential for serious political conflict and even war. The presumption of adversity and, in the case of cyberspace, even perceptions of ongoing conflict, can create a sense of insecurity and tension. In this context of rising tension and a lack of trust between states, the securitisation of cyber policy can justify greater secrecy, as well as restrictions on privacy and freedom of expression in the name of protecting national security from attack by other states. Furthermore, tensions can lead to increased cyber attacks, which impact human rights. Conversely, if these tensions are reduced, a more positive, enabling environment for the exercise of human rights can be created.

So far, discussion of CBMs has been limited to states; and the CBMs developed by the GGEs, by default, only directly implicate states. There hasn't been a clear role for the private sector or other non-state actors in the discussion or implementation of CBMs. Yet, in practice, the effective implementation of some CBMs would require the involvement of non-state actors; for instance, in conducting national threat assessments and supporting some forms of information exchange. The 2015 report makes some reference to non-state actors—for example, referring to the "consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions" in addressing "ICT security incidents".

Accordingly, human rights defenders can find ways to play a role in maximising the implementation of CBMs. For example, the GGE CBMs focus on transparency and cooperation measures, such as facilitating "cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders" and "development of mechanisms and processes for consultations on the protection of ICT-enabled critical infrastructures; development of mechanisms to address ICT related requests". Such processes and mechanisms will require wide stakeholder input—for example, the vast majority of commercial applications today use some open source components, which have been developed by a range of actors. As such, the addressing of threats and vulnerabilities through cross-border coordination will necessitate multistakeholder engagement.

Another CBM included in the 2015 report refers to the setting up of CSIRTs. A number of multistakeholder initiatives, such as the Internet Governance Forum Best Practice Forum and the Global Forum on Cyber Expertise, offer best practice guidance in setting up CSIRTs. The Brazilian CSIRT, CERT.Br, is one example of a CSIRT which operates in a multistakeholder manner.

Further, human rights defenders could—through research and monitoring—determine whether CBMs are being implemented in a way that respects human rights. For example, the CBM which refers to cooperation in investigations related to the use of ICTs for terrorist purposes, requires that states "cooperate with requests from other States in investigating ICT-related crime or use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory". It is essential that such investigations are human rights respecting, and civil society already play an essential role in providing guidance on and monitoring such practices.[9]

Therefore, although discussion of the GGE CBMs has so far made limited reference to non-state actors, these examples show that civil society has a role to play in ensuring that CBMs are implemented in an inclusive and transparent manner, and that their impact on human rights is monitored at the national, regional and global levels.

End notes

1. General Assembly United Nations, "Special Report of the Disarmament Commission to the General Assembly at Its Third Special Session Devoted to Disarmament A/S-15/3*," https://digitallibrary.un.org/record/39665
2. Igor Scherbak, "Confidence-Building Measures and International Security The Political and Military Aspects: A Soviet Approach," https://heinonline.org/HOL/LandingPage?handle=hein.unl/cobuso0001&div=1&src=home; "Milestones: 1961–1968 - Office of the Historian," https://history.state.gov/milestones/1961-1968/cuban-missile-crisis
3. General Assembly United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," (paragraph 16), 2015, https://digitallibrary.un.org/record/799853?ln=en
4. https://research.un.org/en/docs/ga/quick/regular/43
5. "A/RES/43/78. Review of the Implementation of the Recommendations and Decisions Adopted by the General Assembly at Its Tenth Special Session," https://digitallibrary.un.org/record/192726
6. "Cumulative Recommendations in the UN GGE Reports," https://www.thehaguecybernorms.nl/cumulative-recommendations-in-the-un-gge-reports
7. "FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security | Whitehouse.Gov", https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol
8. Ibid.
9. Minimum Safeguards on Intelligence Sharing Required under International Human Rights Law | Privacy International," https://privacyinternational.org/advocacy/3068/minimum-safeguards-intelligence-sharing-required-under-international-human-rights-law