Promoting international peace and stability by building trust between states in cyberspace: The importance of effective confidence-building measures

CYBERSPACE: THE NEW FRONTIER IN GLOBAL CONFLICT

When people speak of conflict, they typically confine the discussion to the conventional dimensions of land, sea, air and space. The images they paint involve planes, tanks and guns: traditional military weapons that can provoke extensive physical damage but the use of which is, at least theoretically, limited by a number of factors, including cost and fear of retribution. The vast majority of efforts to safeguard international peace and stability have therefore focused on preventing an escalation of tensions in those dimensions, by limiting proliferation of physical weapons, establishing clear lines of communication between states, as well as encouraging greater transparency in state behavior.

However, with the advance of information and communication technology (ICT) a new battle front has emerged. Geopolitical tensions have moved into cyberspace, a domain characterized by novel features compared to kinetic domains of conflict: incredible velocity, a relative absence of geographic boundaries, increased difficulty in identifying perpetrators of malevolent actions, and the ubiquity of technology that does not allow for easy distinction of what could constitute a valid military target.

Moreover, experience has shown that conflict in cyberspace differs from kinetic warfare in that much activity does not reach the international legal thresholds for use of force or armed conflict. While we have seen online activity accompanying traditional confrontations, for example around the Russian-Georgian conflict, or during the North Atlantic Treaty Organization's (NATO) military operation against the Federal Republic of Yugoslavia (FRY) during the Kosovo war, the vast majority of activity takes place in, what is supposed to be, peace time.

Attacks such as WannaCry and NotPetya in 2017 demonstrated the broad impact cyber weapons have on an increasingly connected society. These attacks spread around the world, shutting down hospitals, postal services, and shipping companies. The unintended consequences of such actions are difficult to measure and go far beyond the estimates of computers affected, and profits wiped off balance sheets. They are reflected in the individual stories of heart surgeries that needed to be postponed, opportunities lost because meetings did not take place, or transactions that did not occur in time. Cyberspace today is at the core of not just how we communicate and work, but how our essential services get delivered, and how our devices – from cars to welding machines - operate. It is a key contributor to our economic prosperity and continuous growth. It should therefore not be actively undermined.

Despite, and perhaps because of, the critical importance of cyberspace, cyber offensive capabilities are increasingly seen as a necessary part of a state's geopolitical strategic toolbox. Research shows that more than 60 countries are developing or acquiring offensive cyber operational capacities.

This should serve as a warning sign that we have entered an era of cyber weapons proliferation, the scale of which could be difficult to fully measure or understand.

In other words, we are witnessing a cyber arms race.

Against this background, it is clear that cyberspace has become a new dimension of states' and human interaction and that, as such, it requires the same level of commitment to international peace and stability as any other domain whose protection and security are essential for societies to operate and prosper. It is therefore essential for states to work, bilaterally and multilaterally, on measures that can help prevent the emergence or escalation of conflicts.

The Cybersecurity Tech Accord has made contributing to a stable and secure cyberspace its mission and has been advocating the need for enhanced cooperation among state actors, the private sector, and other entities on cybersecurity. With this in mind, we have looked at like-minded organizations that are striving to achieve this same goal. One of these is the Organization of American States (OAS), which, for more than a decade, has been working to build a cybersecurity culture among its members that would prevent misuse of ICTs, make states' interaction in cyberspace more predictable, and encourage trust and mutual assistance.

As part of this commitment, in 2018, the OAS adopted a resolution stressing the need to prepare and agree upon a set of confidence-building measures (CBMs) for cyberspace to enhance interstate cooperation, transparency, and in turn stability online. The Cybersecurity Tech Accord signatories strongly support the OAS in this effort and have to this end put together the following paper to inform its decision-making process. The signatories believe the potential consequences of a full-scale cyber conflict have made the need for action urgent, and the development of effective channels of communications between states essential. We all need to work together to reduce the risks of misperception and unintended escalation that might stem from the lack of trust and confidence that currently characterizes interaction among states, both on-, and offline.

THE ROLE OF CONFIDENCE-BUILDING MEASURES IN INTERNATIONAL DIPLOMACY

CBMs are not a new tool in the international diplomacy toolbox. Over the past century they have directly served to defuse tensions on numerous occasions, as well as successfully modified states' behavior by making relations between different governments more stable and predictable. Indeed, they are not even a new tool in cyberspace, as they have been considered as a possible mechanism to enhance trust online for almost a decade. However, successful implementation of CBMs requires constant revision, as well as recruitment of new actors, as states expand their roles in cyberspace.

CBMs are typically defined as actions and processes designed to reduce or eliminate the causes of mistrust, tensions and hostilities between states that could fuel arms races or lead to actual conflicts. They do so by virtue of enhancing states' understanding of each other's military capabilities, by for example encouraging governments to provide advance notice of military maneuvers and exercises; or by urging greater transparency in military budgets, strategic doctrine, and legal interpretations. Probably the most well-known example of a CBM is the establishment of a "hot line", a direct line of communications, between two heads of state.

As their effectiveness in the military domain became clear, the use of CBMs has expanded to touch on the economic, environmental, and societal spheres: the development of joint infrastructure and community development projects, joint responses to disaster relief and the set-up of working groups to facilitate people-to-people contacts to promote tolerance and mutual understanding are a few examples of these CBMs. On each such occasion CBMs were tailored to the specific context governments were trying to address, but the underlying ambition remained the same: build trust where there was little to be found.

Furthermore, the use of CBMs over time may result in other outcomes: (i) by identifying areas of disagreement in terms of the background norms (or laws) for state behavior, a state may avoid mistaken assumptions that its understanding of the relevant rules are shared by other actors; and (ii) in areas where there is limited agreement on what international legal principles might apply, CBMs can serve as bridges to a common understanding of what acceptable international norms of behavior might be.

As such, the potential relevance of CBMs to cyberspace seems unassailable. This is a new domain of conflict, where institutions of cooperation have only begun to emerge over the past few years. For example, the Cybersecurity Tech Accord signatories have been heartened by the emergence of a new field of foreign policy – cyber diplomacy, but cyber ambassadors are few and hard to find. Moreover, cyber conflict is a particularly murky domain, where capabilities and intentions of governments are difficult to ascertain with only a small number of countries deciding to make their strategic doctrine public. The additional challenges of attribution, resulting from the difficulty in detecting the source and perpetrator of a particular cyber-attack, have further contributed to a sense of mistrust.

Furthermore, calls on states to increase cooperation in this domain have also been driven by concerns over the lack of a clear governance framework to set boundaries on certain practices, and create a more stable and predictable environment. While international law applies to cyberspace, more precise and clear legal provisions on how it does so are, in fact, lacking. So far attempts by the United Nations to clarify debate in this space have failed to forge the necessary consensus among states, and perhaps CBMs can help in this regard as they have in other domains.

BUILDING TRUST IN CYBERSPACE: EXISTING CONFIDENCE-BUILDING MEASURES - EFFORTS AT BILATERAL AND MULTILATERAL LEVELS

Efforts to design effective CBMs for cyberspace have been undertaken at both multilateral and bilateral levels. While they are all relatively recent, and more work will need to be done for them to be translated into structured processes that generate broad adoption, they have already contributed to advancing the dialogue on cyber stability. Not only that, the discussions around CBMs adoption have resulted in the creation of important platforms that enable governments to have a conversation around these important issues.

Multilateral efforts

At the multilateral level, cyber stability has been firmly on the agenda of the United Nations (UN) and its Groups of Governmental Experts (GGEs) since the early 2000s. In their 2010 report, the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security recommended five actions for the development of confidence-building and other measures to reduce the risk of misperception resulting from cyber disruptions. These actions included (i) elaborating common terms and definitions necessary to advance dialogue in the information security field, (ii) identifying measures to support capacity building in less developed countries as well as (iii) exchanging information on national legislation, ICT security strategies, policies and best practices. Further to this, the UN GGE in 2013 and 2015 produced a number of consensus-based norms, and recommendations for adoption of confidence-building measures, highlighted in the callout box below.

Despite these efforts and despite the UN's success in driving the recognition of cybersecurity as a matter of peace and stability, there has been little progress made in that forum since 2015. As a result of that, and in many ways as a direct response to the proposals adopted at the UN, regional organizations have taken up the mantle of building trust amongst their constituents. Organizations as varied as the Organization for Security and Co-operation in Europe (OSCE), the OAS, and the Association of Southeast Asian Nations (ASEAN) have begun to move the discussion forward. Despite facing numerous challenges along the way, due to states' reluctance to agree on definitive common positions on cyber-related issues, these organizations have proven to be a useful platform for discussion especially because of their focus on regional specificities and their involvement of a smaller number of stakeholders with great common interests and concerns.

Confidence-building measures, adopted by the UN GGE

- The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;
- The development of and support for mechanisms and processes for bilateral, regional, sub-regional and multilateral consultations, to enhance inter-State confidence-building;
- Encouraging, on a voluntary basis, transparency at the bilateral, sub-regional, regional and multilateral levels to increase confidence and inform future work.
- The voluntary provision by States of their national views of categories of infrastructure that 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.
- Strengthening cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests;
- Enhancing cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;
- Establishing a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role.
- Expanding and supporting practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;
- Cooperation, in a manner consistent with national and international law and global, industry-lead best practices, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

- Building on its previous success in developing CBMs in the conventional weapons area, the OSCE worked on and adopted sets of cyber-related confidence-building measures in 2013 and 2016. Through the adoption of these practical measures, the OSCE has come to play a pioneering role in reducing the risks of conflict stemming from the use of ICTs. OSCE transparency-related CBMs focus on information sharing, establishing a mutual understanding of how states perceive and interpret threats and risks stemming from the cyber arena, critical infrastructures integrity and the protection of communication channels. The measures focused on cooperation also encourage OSCE's participating states to apply a specific crisis management mechanism in case of cyber incidents or cyber-attacks.
- ASEAN has also taken steps in this domain. Key member countries, for example Singapore, played an important role in making cyberspace central to the cooperation within the ASEAN community. Under Singapore's initiative, the ASEAN Cyber Capacity Program was launched in 2016 to support cyber norms and CBMs in the region. Prior to that, in 2015, the ASEAN Regional Forum (ARF) launched an open-ended Study Group on Confidence-Building Measures to

reduce the risk of conflict stemming from the use of ICTs. The Study Group was tasked with developing processes and procedures for sharing information between ARF contact points on preventing ICT crises, and criminal and terrorist use of ICTs and with the establishment of a contacts database.

- The European Union (EU) has actively supported regional efforts such as the ones led by OSCE and ASEAN to develop confidence-building measures for cyberspace. Although the EU has yet to launch initiatives of its own in this space, it has stressed several times the importance of enhancing states' cooperation in cyberspace and of achieving broader recognition of the applicability of international law to this new domain. It has, in this regard, given its endorsement to the voluntary non-binding norms, rules and principles of responsible State behavior that have been articulated by the UN Group of Governmental Experts. Other EU efforts in this space included calls on member states to: promote and protect human rights and fundamental freedoms in cyberspace; encourage exchanges of good practices to this end with all relevant stakeholders; contribute actively to the achievement of a global common understanding on how to apply existing international law in cyberspace; and make cyber capacity building an integral part of wider global approaches in all cyberspace domains, among others.

Bilateral initiatives

In addition to the multilateral and regional initiatives highlighted above, numerous countries have brokered bilateral cooperation agreements on cybersecurity. Examples include: Singapore's agreement with the United States and Canada; Israel's agreement with Greece and Cyprus; India's agreement with the Seychelles; and France's agreement with Estonia; Russia's agreement with Spain, to name just a few. Many of these have been light on substance, at least publicly, so it is difficult to tell whether this mesh of diverging levels of commitments between different states will ultimately and cumulatively add to a greater common understanding and improved stability.

Of particular note are the agreements brokered by some of the geopolitical heavy weights: Russia, the United States, and China. While their perceived effectiveness has ebbed and flowed depending on the overall state of relations between and among the countries, that does not differ from how CBMs are agreed upon and dealt with in the kinetic world, where effectiveness needs to be evaluated over the long(er)-term. The most prominent agreements included:

- The June 2013 agreement to reduce the risk of conflict in cyberspace between the United States and Russia extended traditional transparency and confidence-building measures to cyberspace. The objective of the agreement was to avoid a misconstrued cyber incident leading to instability between the two nations. Agreed upon steps included regular sharing of threat indicators between their respective computer response teams, as well as the establishment of a White House-Kremlin direct communications line. Both sides also agreed to expand the role of the Nuclear Risk Reduction Centre established in 1987 to exchange information about planned cyber exercises or cyber incidents.
- The 2015 agreement between Russia and China pledged the two countries to work together to address evolving threats to international peace and stability stemming from the malicious

use of ICT. The agreement stressed the importance of establishing a clear framework for cooperation in this space by creating communication channels to identify joint responses to cyber threats, promoting information exchange between the respective law enforcement agencies on cybercrime and terrorism, as well as sharing expertise for the development of national cybersecurity policies and strategies.

- The 2015 United States and China agreement sought to expand and deepen their bilateral cooperation in, among other topics, cybersecurity. The agreement entailed responding to mutual requests to investigate cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from their territory. The two parties also agreed to refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property, trade secrets or other confidential business information. In addition, both states committed to further identifying and promoting appropriate norms of state behavior in cyberspace within the international community. After a steep decline in Chinese attacks against U.S. companies in the first year after the agreement was concluded, cyber espionage by Beijing seems to be up again with the consequence that relationships between the two countries on that front are deteriorating.

Surely, looking at the challenges to making both bilateral and multilateral efforts on cybersecurity bring the desired effect of increased cyber stability, a new, more comprehensive strategy is needed, which can bring predictability to states' behavior in cyberspace, setting clear red lines of what is acceptable and what is clearly not acceptable in this new dimension and enhancing mutual trust between states.

CHALLENGES TO IMPLEMENTATION

Challenges to making CBMs for cyberspace work certainly exist and they need to be taken into account to ensure that expectations of what is achievable are set appropriately and that, in parallel, potential weaknesses pertaining to these processes are tackled.

Building effective mechanisms of state interaction in cyberspace is essential to reducing the likelihood of conflict. If the path to more specific international cybersecurity norms is still arduous, CBMs for cyberspace can certainly play a role in increasing trust and predictability, fostering dialogue around cybersecurity and facilitating mutual assistance and collaboration between states against malicious cyber activities.

Despite the challenges at hand, efforts across the globe to develop CBMs for cyberspace are to be encouraged and promoted as they can pave the way for more formal and binding agreements between states in the future and can help build a consensus around the ways to make cyberspace more stable and secure.

- *CBMs and international norms for cyberspace as two sides of the same coin:* First of all, advancing dialogue around cybersecurity norms, including international law, is extremely important. CBMs are one of the tools to build trust between states and prevent conflicts, but they need to be supported and complemented by legally binding instruments that set out what constitutes acceptable or non-acceptable behavior in cyberspace. In the absence of clear expectations in this sphere and of a strong commitment to banning certain practices, it might be difficult to push the dialogue forward and remove all causes for mistrust between states. The lack of urgency felt by some states with regard to tackling cyber instability as well as different perceptions around the impact of these new threats on international peace and security have so far prevented the debate around legal and non-legal norms from moving forward. These issues will certainly need to be addressed in parallel with any discussion around CBMs.
- Significant disagreement on key issues and concepts: Moreover, one of the key characteristics of CBMs is that they bring adversaries to the table and engage them in conversations about contentious issues. However, if states' interpretations of these issues and related concepts differ significantly, it might be difficult for parties to form a common understanding of the problems to tackle and agree on effective solutions. Developing a common understanding on what constitutes an "attack" in cyberspace or how states can distinguish between cyber offensive and defensive capabilities, among others, will be necessary as a basis for future dialogue and cooperation. Agreeing on concepts such as critical information infrastructure will also be key as currently, depending on the country and jurisdiction, the issue may be perceived either as the private sector's responsibility or as the responsibility of specific governmental agencies.
- *Continuous evolution of technology:* The absence of common terminology is also due to the fact that cybersecurity is a field in the making and that technology is advancing rapidly and in unpredictable ways, making it difficult for experts and decision-makers alike to develop forward-looking strategies and processes that still capture the 'state of the art' a few years after they have been adopted. Therefore, it is important that CBMs for cyberspace are conceived as

processes subject to continuous evolution: taking stock of progress in the cybersecurity domain will need to be part and parcel of states' dialogue to make sure that solutions are always fit for purpose.

- *Cyberspace as a domain where traditional CBMs do not easily apply:* Another element to take into consideration is that, while looking at conventional CBMs might be useful as a starting point, not all dimensions of these traditional CMBs will be transferable to the cybersecurity domain. For instance, disclosing offensive military cyber capacities is much more unlikely in the cyber context than in kinetic domains since such disclosure can impact their future efficacy. Moreover, in practice, it can be quite difficult to distinguish offensive military cyber capabilities from defensive means. Similarly, it is difficult to distinguish between a cyber-attack and cyber espionage since they are both carried out leveraging existing vulnerabilities and they both entail accessing critical information, with the main difference residing in the payload, which is often difficult to identify. In addition, cyber weapons are easy to deny or hide and their designing, developing and testing can be done in a non-verifiable manner. For this reason, efforts in the direction of greater transparency will be difficult to implement without enhancing a sense of trust and mutual reliability between states.

CYBERSECURITY TECH ACCORD APPROACH FOR EFFECTIVE CONFIDENCE-BUILDING MEASURES

While approaches to CBMs vary, depending on the region and diverging set of stakeholders involved, effective CBMs have been demonstrated to share a set of common characteristics. The OSCE has identified eleven characteristics that effective non-military CBMs share, which include reciprocity, predictability, reliability, long-term commitment, and local ownership. This is why the Cybersecurity Tech Accord signatories are encouraged to see the OAS take on the effort for the Americas region, and not only engaging with its own community in building them but leveraging others that have gone down this path before.

The Cybersecurity Tech Accord signatories would like to put forward a series of recommendations for effective CBMs, which leverage proposals made by authoritative organizations such as the UN and OSCE and that, in our view, could help fill existing gaps in states' approaches to cybersecurity. They include:

- Develop shared positions and interpretations of key cybersecurity issues and concepts, which will facilitate effective dialogue and enhance mutual understanding of cyberspace and its characteristics. As technology continues to evolve, this exercise will need to be reviewed regularly to ensure that the latest developments in cybersecurity are captured, as well as new potential cyber tools, threats and solutions.
- Appoint a "cyber ambassador" to serve as a point of contact not only within the various government agencies and departments, but for foreign governments. This cyber ambassador should come from agencies that have an institutionalized human rights oversight mechanism to ensure that multiple equities in capacity building are considered, including the need for human rights to be protected in cyberspace.
- Encourage governments to develop and engage in dialogue around cyber warfare doctrines, to include those practices that fall below the threshold of armed conflict, to enhance understanding of states' "red lines" in cyberspace, as well as the sharing of best practice.
- Continue a dialogue around international law and cybersecurity norms by exploring how States understand the current State of the law and other non-legal norms as well as the readiness of member states to establish and adhere to binding principles related to acceptable and non-acceptable behavior in cyberspace.
- Develop a list of facilities that are off limits for cyber-attacks, such as nuclear power plants, air traffic control systems, banking sectors, and so forth, to include starting with those entities that already enjoy a protected status under traditional war doctrine, such as hospitals and sites of religious worship.
- Establish mechanisms and channels of communication to respond to requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts (organizing i.e. table-top exercises).

- Establish measures to promote cooperation between law enforcement agencies and legal practitioners, as well as between diplomatic and technical personnel.
- Establish cooperation between national Computer Emergency Response Teams to identify dependencies between states and take appropriate measures.
- Exercise cybersecurity scenarios to ensure efficient and effective response.
- Engage with other stakeholders: As the private sector designs, builds and operates most of the digital infrastructure and are today's main cyber defenders, we encourage their inclusion in the dialogue on CBMs for cyberspace.
- Hold regular meetings among the OAS state representatives including cyber experts to advance dialogue on cybersecurity issues and to advance work around CBMs for cyberspace.

The OAS work on developing effective CBMs can help set the standards for future efforts regarding states' cooperation in cyberspace. Of course, cyberspace, by its nature, requires a global approach, but initiatives in one region can help bolster similar efforts in other areas of the world and lead to a broader consensus. We, therefore, encourage the organization and its member states to continue in their commitment to promote peace and stability in the region including improving states' interactions in this new dimension of international relations. The Cybersecurity Tech Accord signatories stand ready to provide advice and support and to further promote the OAS efforts to make cyberspace more stable and secure.