International Co-operation to Ensure Secure Cyberspace Is The Main Diplomatic Tools

Tawhidur Rahman, MCiiSM
CFIP, CCTA, CHFI, Lead Auditor, CCIP, CCII, Team Leader, BGD e-GOV, CIRT

Today the malicious use of information and communications technology (ICTs) has become one of the greatest transnational threats. Cyber threats are not restricted to a country's geographical boundaries: it is possible to launch an attack in one country, but route it through another. Diplomacy is a critical tool for responding to these threats as it can foster cooperation and can help avoid misunderstandings between states.

Today's Internet – the backbone of the modern digitalized world– works more or less in the same way as it did when it was developed in the 1960s. It was originally designed for use by a closed circle mainly of academics.

Communication was open and security was not a concern. Vulnerabilities existed – and still exist – on many levels, but they were not explored or exploited before the Internet's expansion beyond the circle of Internet pioneers.

With the increasing use of the Internet in everyday life and especially in global business, traditional crimes such as fraud, identity theft, and buying illegal goods are now being conducted through the Internet as well. On an organized level, black markets hidden within the 'dark web' allow distribution of and access to various products and services – from viruses and botnets to drugs and weapons – all are just 'one click away' and almost risk-free. A particularly flourishing offer is that of cyber-weapons (e.g. exploits, malware kits, and botnets). Each day, the headlines feature updates about millions of passwords for online services, or the new 'zero-day' exploits – all for sale. The abundance of hacked information and exploits enables the emergence of cheaper and simpler to use, yet more sophisticated malware (such as Trojans or ransomware) and social engineering techniques (such as phishing and spear-phishing), and even cyber-attack services (distributed denial-of-service or DDoS attacks, hacking and defacement, spam and malware distribution) – with customer support. For instance, a smaller botnet can be rented for about €100, or a DDoS attack ordered for less than €50 per day; no specific skills are required except for how to find such offers online. Available, affordable, ready-made, and simple-to-use cyber-weapons, combined with the low risk of prosecution due to anonymity, in turn invite greater interest from various individuals and groups, who want to purchase tools and hire services online. In addition, certain security companies – Vupen and Hacking Team are among the most out-spoken – have created a lucrative legal business out of discovering vulnerabilities, producing exploits, building them into hacking tools, and finally selling them to security services and governments, among others.

Different terminology

Cyber policy is a policy field in the making. Thus, there is still a lot of terminological confusion, ranging from rather benign differences such as the interchangeable use of prefixes (cyber/e/digital/net/virtual) through to core differences, when the use of different terms reflects different policy approaches. In policy and political discussions about cybersecurity, different organizations and governments use different terminology, but they also view cybersecurity concepts differently

Differences start from the very terms delineating the field: cybersecurity and information security. The European Union has its Cybersecurity Strategy within which it describes cybersecurity as 'safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure'. This understanding of cybersecurity is related to cyber-threats against networks and infrastructure. US laws define information security as 'protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction' to provide integrity, confidentiality, and availability. Within its foreign policy endeavors and documents, however, the US government strictly uses the term cybersecurity and relates it toprotection from cyber-threats and cyber-attacks against critical infrastructure and information systems, while at the same time promoting open Internet and online freedoms.

On the other hand, Russia, China, and their partners from the SCO predominantly use the term information security in their foreign policy efforts. More importantly, in their view, the term relates to the strategic control of ▸

information and implies a broader understanding of threats including information that could endanger 'societal-political and social-economic systems, and spiritual, moral and cultural environment of states', as defined in the 2015 pact between Russia and China. Within this foreign policy platform, SCO countries strongly opt for clear national sovereignty in the case of cyberspace, which would allow countries to consider content control measures as an 'essential aspect of 'information security'– a concept which conflicts with the open Internet and online freedoms promoted by the USA and the EU.

Human rights communities have also tried to offer a definition of cybersecurity, which suggests that it should be about people rather than about systems: it is a matter of individual security rather than national security. The Working Group of the Freedom Online Coalition– a partnership of 30 governments working to advance Internet freedom – has codified a similar perspective, de-fining cybersecurity as protecting information and the Internet infrastructure for the sake of enhancing the security of individuals, both online and offline.

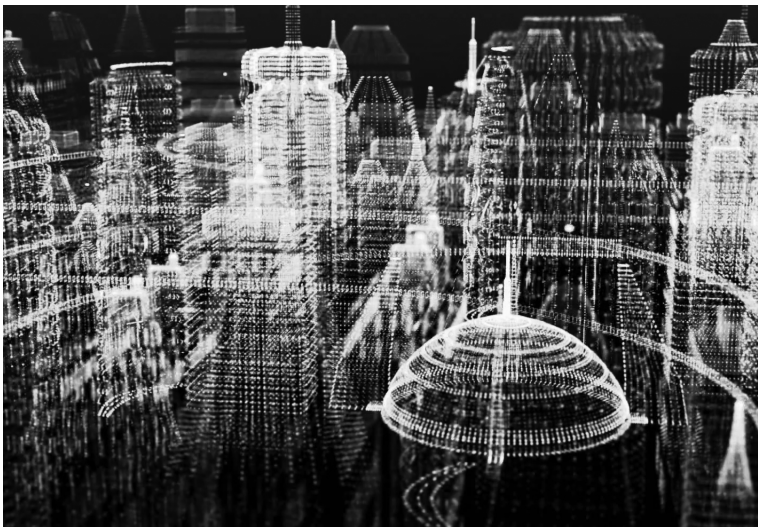
These terminological differences are of fundamental importance for international co-operation and negotiation about cyberspace. Lack of common language in-creases the risk of miscommunication that could, at best, confuse messages and, at worst, lead towards conflict escalation.

Major initiatives and instruments

In response to increasing cyber-armament, diplomatic initiatives have emerged attempting to codify state behavior in cyberspace and encourage co-operation to reduce the risk of conflicts. On an international level, the UN has established dialogue among a number of states through the GGE, while several regional organizations. Such as the OSCE in Europe, ASEAN Regional Forum, and the OAS have also set up their own mechanisms for discussing ways to reduce risks from the misuse of ICT. The SCO has proposed the International Code of Con-duct for Information Security. The European Union and the African Union are addressing the broader context of cybersecurity through their policy documents, while NATO, the OECD, and the G20 are focusing on particular aspects related to their agenda. Interestingly, even the private sector – namely, Microsoft – has joined in with proposed international cybersecurity norms for states and industry.

Bangladesh e-Government CIR Thas started its journey from January 2015 and has already achieved the membership from FIRST (https://first.org/members/teams/bgd_e-gov_cirt). Ithas membership from APCERT and have signed mutual cooperation agreements with many foreign national CSIRT. It has also signed bilateral agreement with many Government CIRT in Asia, Europe, Africa etc. It has also Government mandate to act as National CERT until now.Today itis only the legal government CIRT in Bangladesh (www.cirt.gov.bd) which work 24/7 to secure Bangladesh cyber space.

The two common political instruments shaped in these initiatives are voluntary norms of state behavior in cyberspace and CBMs to reduce



conflict; specific aspects of capacity building are also suggested. Norms are understood in the broader context of regime theory as 'standards of behaviour defined in terms of rights and obligations'. The UN GGE report states that 'norms reflect the expectations of the international community, set standards for responsible State behavior and al-low the international community to assess the activities and intentions of States.' CBMs, on the other hand, are 'planned procedures to prevent hostilities, to avert escalation, to reduce military tension, and to build mutual trust between countries', according to the UN Office for Disarmament Affairs (UNODA).22 CBMs can 'increase interstate co-operation, transparency, predictability and stability', and 'enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs'. Capacity building is observed as needed assistance, especially to developing countries, to improve 'the capacity of states for co-operation and collective action'; importantly, it is recognized that capacity building 'involves more than a transfer of knowledge and skills from developed to developing State, as all States can learn from each other about the threats that they face and effective responses to those threats'.

Bilateral cyber-relations

Bilateral cyber-dialogues and agreements

With the increasing frequency and intensity of cyber-attacks and their geopolitical and economic consequences, many countries are turning to bilateral relations concerning cyberspace. Relations vary from bilateral meetings to strategic partnerships (such as between Canada and Israel), from continuous dialogue (such as the EU-Japan cyber-dialogues) to statements and communiqués (such as the joint statement by the Prime Ministers of Sweden and India, or a joint declaration of Czech Republic and Israel), from Memorandums of Understanding (such as between the UK and Singapore) to bilateral agreements (such as be-tween Brazil and Russia or between India and Russia).

Thematic coverage of bilateral arrangements varies from specific coverage such as co -operation in combating cybercrime and terrorist use of the ICT, cyber-defence, and non-aggression by information weapons, to broader coverage of cybersecurity co-operation (such as between India and Malaysia) or cyber-policy issues (such as between Japan and Australia) – often including privacy and data protection as well (such as between Brazil and the USA). Cybersecurity is often also part ▸

of co-operation agreements in the field of ICT, the information society, or Internet governance (such as the trilateral India-China-Russia meeting of Foreign Ministers).

A non-exhaustive mapping of bilateral cyber-relations, graphically represented in Figure , accounts for over 100 already established relations in the field of cybersecurity, cyber policy, ICT, and the information society. It is expected that the list will grow further as cyber comes tothe forefront of the diplomatic agenda, and as capacities and awareness also increase in developing countries.

Bilateral cyber-relations among major economies

The lead economies are also the leaders in establishing mutual relationships on cyber issues. Some of the key bilateral arrangements and dialogues include:

EU with third countries: The EU cyber-dialogues with China, India, Japan, South Korea, and the USA had started by 2015,while the dialogue with Brazil is pending. Most formal negotiations are accompanied by informal dialogue with other experts and stakeholders in these countries, such as the Sino-European Cyber Dialogue.

USA and China: In September 2015, the presidents of the USA and China met to discuss, among other issues, increasing concerns about cyber-incidents.They agreed not to knowingly support cyber-espionage against the corporate sector.

USA and Russia: In 2013, the USA and Russia engaged in dialogue to reduce the danger from cyber-threats. The agreement envisaged establishing a direct 'cyber-hotline' between the White House andthe Kremlin, an operational link between CERTs, anda bilateral working group to extend co-operation related to national security concerns. The co-operation, however, was frozen in 2014 due to tensions over the situation in Ukraine. Meetings between US and Russian cybersecurity officials in Geneva in April 2016 focused on the work of the UN GGE and the OSCE CBMs.

Russia and China: The presidents of Russia and China concluded a cyber-agreement according to which both sides will refrain from carrying out cyber-attacks against each other, will support each other's cyber-sovereignty, and will jointly respond to technologies that may 'destabilize the internal political and socio-economic atmosphere'.

USA and India: The Indian prime minister and the US president agreed to finalize a joint Framework for the US-India Cyber Relationship focusing on cyber-security.66 The framework should include developing co-operation among law enforcement agencies and CERTs, strengthening the security of CI, restraining from cyber-espionage, combating various cyber-attacks by state and non-state actors, and investing in research and development of cybersecurity products. The agreement supports the multistakeholder model of Internet governance, which moves India closer to the position of the USA and its allies and further from the position of China and Russia.

India and Russia: On the margins of the October 2016 BRICS Summit, India and Russia signed a formal bi-lateral cybersecurity agreement covering cyber-crime co-operation but also matters of combating cyber-terrorism and protecting the critical infra-structure, as well as defense and national security co-operation. This means that India is the only major power to have established formal cybersecurity frameworks with both Russia and the USA.

China and Germany: Chinese and German officials have started working on a cybersecurity no-spy agreement similar to the one between China and the USA, as was confirmed after the visit of German Chancellor Merkel to Beijing.

China and Canada: Canada and China have started a series of negotiations on a possible bilateral agree-ment on cybersecurity, which may be similar to the China-US agreement, focusing particularly on pre-venting economic cyber-espionage to protect the in-tellectual property of the Canadian industry.

China and Bangladesh: Bangladesh and China signed three cooperation documents here on Friday as the two countries are seeking close cooperation and intelligence sharing over issues like terrorism, transnational crimes and cybercrimes.The Home Minister said the issues related to counterterrorism, cybercrimes, militancy, transnational crimes, narcotics, fire service and visa issues were discussed at the meeting.

India And Bangladesh: The Indian Computer Emergency Response Team (CERT-In) and its Bangladeshi counterpart Bangladesh Government Computer Incident Response Team (BGD e-Gov CIRT) have signed a Memorandum of Understanding (MoU) on cyber security cooperation. The MoU was originally signed in April 2017, and will be implemented through a Joint Committee on Cyber Security, which is yet to be set up. As per the MoU, CERT-In and BGD e-Gov CIRT will:Exchange information on cyber-attacks and cyber security incidents; cyber security technology cooperation; exchange cyber security policies and best practices; and Human Resource Development in this field in accordance with the relevant laws and regulations of each country and on the basis of equality, reciprocity and mutual benefits.

While these relationships vary in form and content, it is evident that there is a growing need for enhancing the co-operation, to prevent misunderstanding and possible conflicting situations. These bilateral relations, however, should not replace or reduce the importance of international and regional processes; on the contrary, the two should feed into and fuel each other.

Conclusion : The fast-changing online environment, driven by the marked demand for ever more powerful rather than more secure products, results in an increasing number of intrinsic vulnerabilities in software and hardware. The flourishing cybercrime markets have exploited these vulnerabilities to create an abundance of cyber-weapons that are readily available and easy to use – yet potentially causing detrimental consequences for their targets and society in general. The increasing interest of states in cyber-armament as a potential means of defending society's critical resources and infrastructure, is accompanied with their growing capacity to produce highly sophisticated offensive tools based on discovered or purchased exploits. The lack of widely agreed norms of state behavior in cyberspace, as well as the lack of common terminology used to discuss cyber issues, is increasing the risks of possible misperception which could escalate cyber-incidents into conflicts.

In response to frequent cyber-attacks, including those less- visible involving intrusion into computer systems of state agencies, the corporate sector, and CI, states are turning to bilateral relations and agreements ◙