Cyber
Niskanen Center and Article 36

Background

"Cyber security" constitutes a broad spectrum of activity and concerns that may hinder individuals, private industry, society, and governments. The aspects most relevant to the First Committee are likely that of cyber conflict or cyber-attacks, concepts which include mass espionage and surveillance, privacy intrusions, denial-of-service attacks, and malware operations with the potential to disable or destroy infrastructure vital to the general population. It is worth noting that there is no universal agreement on what these terms mean, however, particularly at a political level. Potential impacts from such activities include impairment of government administration, damage to critical infrastructure, and the undermining of human rights. In approaching these issues, it is important to be wary of responses that overinflate the threat, and in doing so promote militarisation and facilitate escalation.

If normative progress is to be made in this area, states will need to go beyond a reiteration of existing, general rules and recognise that cyberspace needs to be addressed on its own terms, with consideration of its specific characteristics. The Internet is essentially civilian infrastructure as such it should not be made the target of or the medium for attacks because of the inability of the attacker to keep the effects directed on specific targets. States should establish the strongest norms against such attacks and not drift into an acceptance or legitimation of problematic emerging practice. To this end, we see merit in the negotiation of new principles, procedures, rules, and norms.

Agreement that existing international law, including international human rights law and international humanitarian law, applies to activities in cyberspace provides a shared baseline, but this should not be taken to mean that the existing legal framework is sufficient. There is a lack of clarity regarding which legal framework should have primacy in relation to certain actions, and challenges to the application of legal frameworks, including in terms of accountability. Furthermore, these existing frameworks may not adequately reflect a wider social interest in developing and preserving the public space of the Internet as a shared, non-militarised resource.

Current context

Over the last year, the public imagination has continued to be seized with the concept of cyber conflict and this is increasingly reflected in policy discussions at multiple levels and in multiple fora. In the context of the United Nations, cyber security has been addressed primarily in the context of the Group of Governmental Experts on Internet Communications Technologies (GGE on ICTs). The Group of 20 experts met four times

between 2013 and 2015 and agreed a substantive consensus report last year.[1] The report is said to break new ground in three areas: by explicitly referencing the possible applicability of the international legal principles of humanity, necessity, proportionality, and distinction; by noting that states should substantiate public accusations of state-sponsored cyber activity; and by recommending that states "should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts."

Across the three aspects there are nuances worth noting.[2] In the first, it's not clear if the group has endorsed the application of these principles to state activity in cyberspace, or merely take note of their existence. There are wide differences of opinion on this, notably between the United States and China. Further, as noted above, there remains great uncertainty about the parameters for applying IHL or IHLR frameworks, and these existing legal frameworks may still be permissive of behaviours that there is a wider social benefit to preventing in the context of the shared cyber medium. The reference to assistance perhaps the most significant development in the report because at present, coordination between national computer emergency response teams (CERTs)—which act as focal points to coordinate national and international responses to cyber incidents—is slow and ineffective, hampering adequate response.

On 23 December 2015, the UN General Assembly unanimously adopted resolution 70/237, which welcomed the outcome of the 2014/2015 GGE and requested the UN Secretary-General to establish a new GGE that would report to the General Assembly in 2017. It will hold its first meeting in New York in August 2016. During last year's First Committee, there

were calls from government and civil society to make further work by the GGE more inclusive, including more participation from developing countries, as some also noted that developing countries might benefit from technology transfer and capacity-building measures.

At national levels, there continues to be a growth in the articulation of cyber doctrines and the establishment of relevant bodies, units, or departments. In some instances these relate to potential cyber conflict and in others they are established to manage issues of cyber crime or espionage. For example, the United States, United Kingdom, and Russia all articulate doctrines noting the importance of cyber security and delineating this space as a zone of conflict, with NATO also recently taking this stance. This is juxtaposed with Brazil's notable instance that the internet should be the domain of research and education, not warfare. The EU primarily frames cyber security in the domain of crime rather than national security.

It is important to be mindful that the realities of so-called cyber war are far more restrained and less "war-like" than one might think, given the profile sometimes given to this issue. It is true that some cyber-attacks can have impacts similar to those of kinetic attacks, but these modes of conflict are as yet purely speculative. In practice, the majority of attacks have had information security implications (privacy, access, espionage, information technology transfers) without having direct physical effects. For example, espionage conducted using various cyber or online technologies constitutes the vast majority of aggressive cyber interactions between states, often with a view to learning more about a nation's industrial or commercial assets. Treating cyber primarily as a military and security issue risks institutionalising the broad idea of cyber conflict without a thorough examination of its real impact and full dimensions. It can also lead to responses that can unnecessarily escalate incidents, including misunderstandings, into armed conflict. A recent example is how the term "cyber bombs" is being used increasingly despite a lack of understanding about what is being referred to and how such engagements might be used against insurgent targets in a low technology environment. Inflammatory rhetoric such as this can be effective in media headlines but is misleading in the policy world, as it tends to overlook that the vast majority of malicious cyber activities revolve around crime or espionage and not necessarily war.[3]

Where there has been an increase in negative use of cyber technology by state actors is in the repression of human rights, notably the right to freedom of expression, and cracking down on the ability of civilians to communicate electronically or access email, news, or social media platforms.[4] It is a human rights imperative to protect privacy and respect for Internet freedoms. This part of the agenda is rightly being pursued in other forums, including in the Third Committee, but should not be completely divorced from how delegates in First Committee approach this subject.

Recommendations

During First Committee, delegations should:

- Express concern about the risk of cyber attacks and the militarisation of cyberspace and promote a vision of the Internet as a shared public space that should not be the target of or medium for attacks;
- Promote a fact-based discussion, avoiding language that over-inflates the threat and tacitly promotes militarisation;

- Advocate for common understandings within the international community around key terms, in order to facilitate common approaches; and
- Indicate support for the current GGE to develop concrete recommendations on preventing the development, deployment, and use of cyber weapons, cyber attacks or other intrusions of interference.

Beyond First Committee, states should:

- Seek to establish new avenues for wider discussions on these issues open to all states and inclusive of civil society and other relevant actors, noting that including the voices of states from all regions, including low and middle income countries, will be crucial in this process;
- Seek to support one another in addressing cyber threats and communicate between CERTs and interested public parties;
- Refrain from any repression of human rights or freedoms through digital means; and
- Work towards adopting an effective international legal framework that will prevent cyber attacks, intrusions, or interference and protect the networked infrastructure upon which societies rely for their wellbeing.

NISKANEN CENTER

Article 36

1 See https://www.un.org/disarmament/topics/informationsecurity.

2 Grigsby, Alex. "The 2015 GGE Report: Breaking New Ground, Ever So Slowly" Council on Foreign Relations, 8 September 2015 http://blogs.cfr.org/cyber/2015/09/08/the-2015-gge-report-breaking-new-ground-ever-so-slowly.

3 Brandon Valeriano, "Stop Saying We're Dropping 'Cyber Bombs' On ISIS" *Defense One*, 24 May 2016 http://www.defenseone.com/ideas/2016/05/stop-saying-were-dropping-cyber-bombs-isis/128581.

4 *Freedom on the Net 2015 Report*, Freedom House, https://freedomhouse.org/report/freedom-net/freedom-net-2015.