First Committee, Item 94

Statement by Ambassador Dr Thomas Fitschen

Director for the United Nations, Cyber Foreign Policy and Counter-Terrorism,
Federal Foreign Office of Germany

Mr. Chairman,

The German position on our agenda item is fully reflected in the statement delivered by the representative earlier today, so I don't have to repeat all my points on the work of the GGE. Allow me instead to pick up, and react to, some of the arguments we heard this morning on issues that seem to have contributed to our not having a GGE report this year.

First of all I sensed some general reservation in the room concerning the question whether certain parts of traditional international law, for example on what states are entitled to do in response to a malicious cyber operation, are really applicable "in cyberspace". That is, I'm afraid, the wrong question. I know that we all use the "cyberspace" metaphor every day, but here it is actually misleading. If a state agent or someone else whose acts are attributable to a state carries out a cyber operation in another state to stop an electricity plant, to disable machinery, to suppress or forge data stored in electronic governmental archives, to open the gates of a dam or to bring down the financial markets in another State, that does not happen somewhere "in cyberspace". It happens on the territory and in the jurisdiction of those two countries. It affects the bilateral relations between those two countries. And these relations between sovereign states are governed by international law as we know it. This is what the 2015 GGE report has clearly said, and if I remember correctly, all delegations present here today supported this straightforward statement on the applicability of international law two years ago.

I have also noted that some delegations were reluctant to even touch upon the issue of lawful countermeasures in response to a malicious cyber operation, citing the difficulty of proper attribution. Here again we have a problem which, from a legal standpoint, is not cyber-specific at all. Under general international law - as laid out by the International Law Commission in the 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts - a state can be held "responsible" for an action that (a) constitutes a breach of an international obligation and (b) is "attributable" to that state. It is attributable if the action was actually *carried out by* a state organ or a person or entity exercising elements of governmental authority, or if this conduct is acknowledged and adopted by that State as its own. There is of course more to be said on that but I don't want to go into details here. My point is just to show that the issue of attribution of a certain conduct to a state - as a precondition for the question of whether the state can indeed be held responsible - is not new at all. International law *does* provide the necessary criteria for that. I concede that for cyber operations it may be technically challenging to apply these criteria in practice. The 2015 GGE Report quite rightly underlined that any decisions in this context should be taken very carefully and without undue haste. But that does not mean that we don't have any binding criteria at all when having to decide on these issues.

Clearly the most contentious issue is the question to what extent key provisions of the UN Charter, namely Art. 2 (IV) on the prohibition of the use or threat of force and Art. 51 on the right to self-defense in case of an armed attack, are applicable to cyber operations.

Distinguished delegates, we are the First Committee here: Of course we can imagine, given the rapid development of IT capacities worldwide over the past 15 years, cyber operations carried out by one state against another that cause as much damage as the deployment of more classical means of using "force". So why should digital operations be somehow miraculously exempt from the general prohibition to use force if they cause the same kind of damage as the deployment of physical force? I do of course agree that we need to be extra cautious here and must not rush to conclusions. But I find it hard to deny that a cyber operation against the territorial integrity or political independence of another state – to put it in legal terms: *which in its scale and effects is comparable to a non-cyber operation that rises to the level of a use of force* - can in itself constitute a use of force in the sense of Art. 2 (IV) and is thus *unlawful.*

The same line of argument applies in principle to Art. 51. Again, First Committee experts probably have no difficulty sketching cyber operations by one state against another that – if one looks at their scale and effects – could be as grave as a classical "armed" attack. So here again I would like to ask: Why should we privilege a cyber operation which in its scale and effects *does* rise to the level of an armed attack by *exempting* it from the application of the UN Charter and its Art. 51? Can we really deny the right to self-defence to a state targeted by a cyber operation that is a grave and serious as a classical armed attack just because it is carried out via cyber means rather than by tanks and missiles?

Mr Chairman

It is an entirely different – and terribly difficult - question how states falling victim to such types of unlawful cyber operations may react - or to be more precise : react in a way that in itself is lawful. That is a box that I certainly do not want to open here. But let me, as an international lawyer, just make one point: the fact that it has never been easy to interpret the prohibition of the use of force and the concept of self-defence as contained in the UN Charter has never meant that Article 2.4 or Art. 51 are not relevant, or cannot be applied.

The same holds true for the law of countermeasures: difficulties to apply it in practice are no reason to deny that in case of a cyber operation that is in breach of an international legal obligation below the level of the use or threat of force prohibited by Art. 2 (IV) States are also entitled to take countermeasures as allowed by international law.

Mr Chairman,

some countries, thanks to the size of their IT industry and their big pool of smart IT experts may not feel too concerned about the lack of agreement among GGE experts this year. They think they can take good care of themselves. The vast majority of countries represented in this room, however, know for sure that they cannot.

They – and that includes my own country - are concerned about securing peace, sovereign equality, the protection of human rights "online" and friendly relations among all states in the digital age.

They want clarity about the norms, rules and laws that should guide all states in our digital age.

They want a predictable and reliable framework for responsible state behavior that prohibits and deters internationally wrongful cyber acts.

They insist on having rules that protect them against manipulation, interference, economic espionage, the theft of business secrets and intellectual property, and the threat or use of force against their political independence via cyber operations carried out by state agents or non-state actors of all kinds.

They worry about the dangers of escalation of minor cyber incidents into a real political crisis and look for measures to build trust and confidence in their relations with neighbors, regional organizations and beyond.

They wonder about mechanisms or procedures to cooperate in the investigation of IT incidents and to address issues they may have with other states.

Mr Chairman,

Previous GGE Reports, and the 2015 Report in particular, contained a lot of consensus language on many of the issues I have just mentioned. We may not have a GGE Report this year, but that does not leave us empty-handed. There is still a lot that we can build on. That's why I would like to appeal, through you, Mr Chairman, to all states to continue working together. It is up to us to keep our digital world free, open and secure.