Despite cyberattacks: Russia, China and the U.S. reach surprising agreement on cybersecurity

Article in Neue Zürcher Zeitung (NZZ) by Lukas Mäder on 29 March

Translated with www.DeepL.com/Translator (free version)

For six years, nothing went right in the UN on the subject of cyber security. The fronts between the world powers had hardened. Now, for the first time, all member states have been able to agree on recommendations - thanks in part to Switzerland.

Relations between the cyber superpowers USA, Russia and China are poor. In recent months, two spectacular cases of cyber espionage have come to light, most likely involving state-backed groups from Russia and China, respectively: the so-called Solarwinds attack and the Exchange breach. The USA is threatening to take countermeasures.
These are not good conditions for a new agreement in the field of cyber security. It is therefore all the more surprising that the major powers were recently able to reach an agreement within the framework of the UN. Under the chairmanship of Swiss diplomat Jürg Lauber, the 193 UN member states agreed in mid-March - unanimously - to recommendations for greater cybersecurity.

"At a time of increased conflict between Russia, China and the U.S., the agreement is a major breakthrough," says Jovan Kurbalija of the non-governmental organization Diplo-Foundation in Geneva. In fact, the last joint statement on cybersecurity was six years ago. Since then, conflicts in cyberspace have intensified; the three major powers are taking an increasingly offensive stance.

For example, Russia is believed to be responsible for two power outages in Ukraine brought about by cyberattacks, for hacking into Democratic Party servers before the 2016 U.S. presidential election, or for the hacking attack on several U.S. government departments that came to light last December.

China is primarily credited with espionage operations against companies or research institutions, including in the health sector. The goal: to steal intellectual property or know-how in specific areas, such as for the development of an ocean-going navy.

Russia had an interest in success

The fact that Russia, China and the U.S. have now been able to reach an agreement despite this is also due to a special history. After the UN body that used to discuss security in cyberspace was unable to reach agreement after 2015, Russia launched a new process. Instead of only a select group of states, a new body (OEWG) was to allow all U.N. member states to participate in discussions. Russia hoped this would give it more influence.
Because Russia had launched this working group, it wanted agreement at all costs. Observers assume that this is why it finally persuaded critical states such as Iran, Venezuela and Cuba to give in. Until recently, these countries had protested in pithy terms. Now Russia can chalk up a success for itself. At the same time, the new working group is likely to have established

itself as a future body for cyber security within the UN. It has already decided to continue its work.

No agreement reached on international humanitarian law

Because the fronts between individual states have hardened, the content of the new report is largely based on the last decision from 2015. Only just the most important points could be saved, says a person close to the Swiss delegation.
The report states that basic international law also applies in cyberspace. It includes recommendations for good behavior by states, including, for example, the protection of so-called critical infrastructure. But the request by Switzerland and other states to reaffirm the validity of international humanitarian law in cyberspace did not pass because of strong opposition.

Nevertheless, there is hope that the latest development could give new impetus to the issue of cybersecurity. That's what Jürg Lauber, chairman of the working group, says when asked, for example. On the one hand, he hopes that the dialogue between the major cyber powers will continue, and on the other, that regional initiatives will emerge. After all, capacity building at the regional level is a new objective of the report. For Lauber, one of the most important findings of the OEWG is that awareness of cybersecurity has grown. "Many states were not aware, or not aware enough, of the threats to their IT infrastructure," he says. Now, he says, there is a common understanding that the outstanding issues need to be addressed.

Those issues include, in particular, cyberattack attribution ("attribution") and state accountability ("accountability"). "These are the two big elephants in the room that no one wants to address," says Kurbalija of the Diplo Foundation.

The significance of these questions is evident in countermeasures that the U.S. could currently take regarding the Solarwinds hacking attack. The US assumes Russian authorship. But what this attribution is based on is not publicly known.

In order to create more transparency, a network of independent IT laboratories would be conceivable, for example. **Security expert Serge Droz** and former **Swiss diplomat Daniel Stauffacher** from the Swiss non-governmental organization ICT4Peace suggest this possibility.

Accordingly, several institutes would separately analyze the technical aspects of a cyber attack. This task is comparable to that of the Spiez Laboratory, a recognized testing laboratory that analyzes chemical warfare agents on behalf of international organizations. The technical findings would be published, and the affected states could make a political attribution of the cyberattack based on them. Compared to today, the process would be transparent and independent, even if the thorny issue of state responsibility is not yet resolved.

However, a new UN body could at least address the behavior of states in cyberspace. Stauffacher of ICT4Peace envisages a mutual assessment of states. For example, specific cyberattacks that violate internationally recognized recommendations could be discussed, says Stauffacher. "As with the Human Rights Council, members could address when a country is conducting cyberattacks against medical facilities, for example."

The U.N. could create a permanent body

Whether the UN will actually agree on such far-reaching instruments in the next few years is questionable. But it is possible that in the future a new UN body will take on the issue of cybersecurity on a permanent basis. This idea is part of an action program put forward by France and Egypt. The proposal now has the support of around 50 member states, including Switzerland.

This could result in a kind of guideline on how the existing provisions of international law should be implemented in cyberspace in concrete terms. This point is crucial, many observers say. There is hardly any need for new legal cyber provisions.

But processes within the UN are slow, and agreement is uncertain. That's why there are also voices that place more emphasis on other international organizations that are closer to the private sector and civil society. IT companies in particular need to be involved in the discussion on how to increase cybersecurity around the world.

Switzerland could play an important role in this. Lauber has now shown what it can achieve as a neutral player with an integrative approach as part of the working group. This progress is also in Switzerland's interest. Cyberattacks are now a threat to local infrastructure, even if they are actually directed against targets abroad - the international interdependencies are so great that consequential damage can easily occur worldwide.

That is why Switzerland has the will to play an important role. It is involved not only within the framework of the UN, but also, for example, in an OECD working group for more cyber security.

Back in 2018, the Department of Foreign Affairs launched the Geneva Dialogue, which involves companies such as Cisco, Huawei, Kaspersky and Microsoft. The advantage of this initiative is that it deals with tangible issues such as the security of digital products and services. And the major cyber powers Russia, China and the USA cannot block the process.

Translated with www.DeepL.com/Translator (free version)