DGAP MEMO
German Council on Foreign Relations e. V.
No. 36
July 2025

A Lack of Action in UN Cyber Discussions Is Partly the Fault of the West

By Valentin Weber, Senior Research Fellow, Center for Geopolitics, Geoeconomics, and Technology

In July, the UN's Open-ended Working Group (OEWG) on cybersecurity successfully concluded five years of negotiations by agreeing on the Global Mechanism, a permanent body that will address issues of international cybersecurity from 2026 onward. Germany and partners successfully defended their interests – notably, preventing the body from advancing Russia's proposal for a legally binding cybersecurity treaty. Despite this success, the Global Mechanism runs the risk of following the OEWG's example, i.e., becoming a forum for debates that lack depth. This is also partly due to a Western tendency to make broad general statements in plenary sessions. Therefore, Germany and partners should focus their national statements on one topic, working systematically through issues in detailed commentary. For example, rather than merely mentioning the threat of quantum computing to current encryption methods, Germany and the EU should share best practices on how they plan to migrate to post-quantum cryptography.

The 2021-2025 Open-Ended Working Group on cybersecurity, which concluded in July, was the second UN-wide discussion of the topic after the 2019-2021 OEWG. A Russian initiative, it enabled UN member states to exchange views on cyber threats, the application of international law in cyberspace, norms of responsible state behavior, confidence-building measures and cyber-capacity building.

Previously, a select few states had negotiated for decades within UN Groups of Governmental Experts (UN GGEs) on how cyber operations affect international peace and security. These mechanisms had one thing in common – they were temporary. By passing the OEWG's final report in July, state delegates cleared the way for a permanent mechanism on cybersecurity, the "Global Mechanism on developments in the field of ICTs [information and communications technologies] in the context of international security and advancing responsible State behaviour in the use of ICTs" (the UN Global Mechanism or UN GM).

To ensure that the mechanism leads to concrete action in the future, member states must change their approach to national statements in plenary sessions. Future plenary sessions can only advance ideas significantly if they evolve into proactive, agenda-setting forums. This requires a shift in culture among a critical mass of countries. Instead of making broad statements or rattling off a litany of cyber threat concerns, Germany, for example, should coordinate with like-minded countries primarily within the EU, but also beyond, to steer discussions toward a single, specific threat each year – whether ransomware, risks to encryption from quantum computing or another priority threat. They should also outline best practices for dealing with it. This will bring focus and momentum to action-oriented ideas in the plenary discussions.

UNDERSTANDING THE OEWG NEGOTIATIONS: PUSHBACK AGAINST INTERNATIONAL LAW

The primary aim of the OEWG negotiations was to adopt by consensus a final report recording the global priorities for cybersecurity and to set the foundation for a permanent UN body on international cybersecurity. Germany and other EU countries were keen to thwart Russia's goal of making the new UN body a vehicle for a legally binding treaty. This outcome would have given Russia a win in its pushback against

international law. The United States under the administration of Donald Trump also focused on this problem, in addition to its rivalry with China and opposition to gender issues and the UN Sustainable Development Goals. The overall aim of the West was to achieve a mechanism focused on concrete action for the future rather than on forging a treaty in Russia's interest. The negotiations of both the OEWG and the future Global Mechanism are consensus-based.

The high-stakes negotiations were not easy. A group consisting of Russia, Nicaragua, Belarus, Venezuela, Iran, China, Cuba, Sudan, Niger, Zimbabwe, and Eritrea continuously questioned the applicability of international law to cyberspace. However, this issue had already been agreed on in the General Assembly working group by all states in the 2021 final substantive report of the previous OEWG.

Western countries strongly pushed back against the prospect of a Russian-proposed cyber treaty, arguing that international law in its entirety already applies to cyberspace. Ukraine also reflected this sentiment in saying there was no point in negotiating a convention when Russia was not upholding its current international obligations.

The consequence of Russia's multi-year effort against international law is evident in the final report: it is very slim and void of key issues such as how international humanitarian law or international human rights law apply in cyberspace. More broadly, this is crucial for multilateralism, as the interpretation of international law in cyberspace could have repercussions for international law generally and thereby weaken the rules-based international order.

However, the Singaporean chair, Ambassador Burhan Gafoor, managed to weaken some of Russia's advances and consider the concerns of the EU (Germany) and US. In the last revision of the report, the OEWG's presiding chair slightly accommodated concerns of Switzerland, the European Union and other states, by adding language on state responsibility and due diligence in the context of international law.

The chair also rejected a part of the report that foresaw the establishment of a dedicated thematic group on international law within the Global Mechanism. By deleting this provision, the chair accommodated the United States, which feared that Russia and its small circle of partners would use this opportunity to table a convention on international cybersecurity. Russia's call for an additional dedicated thematic group on new norms was ignored as well.

While Russia succeeded in weakening provisions on international law and human rights, it did not manage to advance its convention proposal.

TOUGH NEGOTIATIONS ON THREATS AND OTHER ISSUES

The section on threats was also hotly debated, as the mention of threats usually signals an accusation of foul play involving another country. For instance, when a country mentions ransomware, it usually refers to a threat emanating from Russian territory. Or when South Korea mentions cryptocurrency threats, it alludes to North Korea. It is in the interest of Russia and North Korea to minimize discussions within the UN on these topics. For Germany, positioning ransomware as a priority threat could lead to in-depth exchanges in the Global Mechanism's dedicated thematic working groups and potentially to actionable outcomes that improve international security.

The EU, Mauritius, Canada, Thailand and many developing countries wanted to prioritize emerging threats such as quantum computing and artificial intelligence. However, the United States and Israel were against in-depth discussions on emerging threats. The United States made comments related to artificial intelligence and deep fakes, which it deemed to be out of scope for this process. Israel mentioned that there was an overemphasis on quantum risks at the cost of the opportunities that new technologies bring. This ignores the concerns of developing countries, which have genuine fears of emerging threats due to a lack of cybersecurity capacity at home.

An important point in the discussion on emerging cyber threats was the transition to post-quantum cryptography, as encryption-breaking quantum computers could arrive as soon as 2030. At DGAP, we have conducted in-depth research to support **countries' transition to post-quantum cryptography**. It is therefore crucial and very welcome that the final OEWG report notes the importance of this transition, which the United Kingdom also advocated for during the discussions.

The final report also importantly retained provisions on the **impact of ransomware and cryptocurrency** theft on international security, which countries including Germany and Mauritius had pushed for. Russia and like-minded states did not support these provisions, as they play a key role in facilitating such malicious activities from their territories.

There were no major surprises on **confidence-building measures**, except one: a provision that the Global Mechanism might discuss a new CBM regarding states' access to ICT products and tools was inserted in the final report. This benefits countries that intend to weaken Western sanctions, such as Iran, Russia, or China. Emphasizing the need for all states to gain access to technologies makes it more difficult for Western states to argue that some should not have such access.

On **capacity building,** the report very much strengthens developing countries,

noting there will be a dedicated thematic group on improving the cybersecurity capacity of least-developed states. But too much emphasis on this in the Global Mechanism would come at the expense of discussions on international law, threats, the implementation of existing norms and confidence-building measures.

Finally, the **participation of NGOs**, industry, think tanks and academia was a central topic of discussion. Russia, China and other like-minded states do not want non-state stakeholders contributing to UN cyber discussions. Russia, in particular, has regularly objected to their participation. A group of 41 states therefore suggested during the weeklong negotiations on this topic that if a country vetoed a stakeholder without the agreement of all countries, a majority vote would decide. The chair did not include this proposal in the final report, but he also did not give in to Russia, which went further than ever to prevent the participation of stakeholders, proposing that even UN Economic and Social Council (ECOSOC)-accredited stakeholders could be barred from participating in the future mechanism.

HOW DID GERMANY AND ITS PARTNERS DO IN THE NEGOTIATIONS?

Germany and Europe can be largely satisfied with the outcome. Germany's main points were that the threat of ransomware should be highlighted in the report and that paragraphs 34 q and r, which pointed to non-consensus language and would have strengthened Russia's proposal for a treaty, should be deleted. Ransomware is prominently referenced in the threat section of the final report and paragraph 34 q was deleted entirely, while the chair also removed important bits of 34 r that referred to legally binding language.

More broadly, Germany and its partners managed to have a direct reference to the Russian proposal for a cyber treaty deleted from the final document. This is the strongest roadblock to Russian advancements in this direction. Germany, the EU, and other Western states managed to stave off the erosion of non-state stakeholder modalities. The final document amplifies stakeholders' voices, as they will be able to present their expertise on threats, international law, critical infrastructure protection, and other fields in direct briefings to member states.

What is more, the past two OEWGs were initiated by Russia, which enhanced its diplomatic credibility. Russia should receive credit for expanding the cybersecurity discussions from a few states (UN GGEs) to all states (UN OEWGs). Even though the large number of participants watered down the discussions compared to the UN GGE, it did make most states for the first time part of UN negotiations on cybersecurity. Their participation was facilitated by Western financial support through initiatives such as the Women in International Security and Cyberspace Fellowship, which allowed dozens of female state representatives from least-developed countries to participate in the New York-based negotiations.

Western states, in particular France, which took a leading role in the negotiations, prevented Russia from steering cyber negotiations toward its own interests. The five-year discussions could have resulted in yet another successive OEWG. Instead, the UN Global Mechanism, which is likely to become operational in 2026, is an amalgamation of ideas that emerged from two separate groups of like-minded states, one formed around Western states and a smaller one around Russia. In the Global Mechanism, Russian proponents will welcome the continuation of plenary discussions, while Western states appreciate the more action-oriented, dedicated thematic groups.

While Germany and its partners managed to hold their ground, they made little progress in bringing greater reflection to the report on international law or even human rights. Russia was never forced to take a real step back in its positions. As Western states did not genuinely threaten to derail the process, there was no real progress. Instead, the status quo prevailed.

NEXT STEPS: AN ACTION-ORIENTED STRATEGY FOR THE GLOBAL MECHANISM

Germany and the West need to retake the initiative in negotiations. Therefore, they should work to shape the boundaries of the future mechanism in a way that suits their interests.

Germany should actively push to turn the plenary sessions into an extension of the action-oriented, dedicated thematic groups. In the short-term, Western states and their partners should ensure all their statements in these sessions are action-oriented, making discussions in the plenary more focused and proactive and less repetitive. For instance, if a dedicated thematic group were to discuss best-practices in migrating to post-quantum cryptography in 2026, these ideas should dominate the plenary discussion on threats that year. Germany and its partners should thus refrain from enumerating the dozens of threats (as they usually do), and instead focus in 2026 on quantum security. This will bring greater focus to the plenary discussions.

In 2027, the plenary discussions on threats could emphasize ransomware, as a pressing issue for states across all continents. A similar singular focus should apply to plenary discussions on other pillars of the framework, such as international law. Western states have largely refused to apply international law to real-life cyber incidents during peacetime or wartime. Even if they do not go so

far as to apply it to real-life cases, they could make a concerted effort in plenaries to establish, for example, whether data is a civilian object that should not be targeted in conflict,rather than making blanket comments that international humanitarian law applies. 2026 could focus on international humanitarian law and 2027 on state responsibility. Russia would not have to agree to this, as a critical mass of countries would make statements on a specific topic in a given year and thereby steer discussions. The principal benefit of this approach would be to measurably advance discussions if, say, more than 50 member states would in a single plenary session voice how international humanitarian law applies in cyberspace. Remarks would have to be specific, as, for instance, whether data can be considered a civilian object.

Through this strategy that focuses on proactively shaping the debate, the Global Mechanism could for the first time in history have a tangible impact on global cybersecurity. UN member states should grasp this opportunity. Germany can play an important role by leading the effort.

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
𝕏 @dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2749-5542

Editing Ellen Thalman

Layout Marie Bauer