Summary of discussions at the Workshop on “Cyber Resilience and Norms for International Stability” at the international conference “Shaping Cybersecurity”

The workshop on “Cyber Resilience and Norms for International Stability” aimed to discuss different normative elements in advancing cyber resilience at the global, regional and national level. The first part of the workshop focused on the implementation of norms of responsible state behavior, confidence building measures and international law in cyberspace. The second part of the session addressed questions how to achieve cyber resilience and cyber stability. The session provided useful insights on abovementioned topics, drawing on the wide experience of speakers from the UN, OSCE, EU as well as national governments, and academia.

During the last decade, international diplomatic community has been working intensively on increasing cyber stability at global, regional and national level. Under the aegis of the UN Disarmament Committee, the United Nations member states have developed a framework for responsible state behaviour that consists of the application of existing international law, norms of responsible state behaviour, confidence and capacity building measures.

As a key element of this framework, the UN member states agreed that the existing international law offers sufficient guidance for state conduct in cyberspace, just as in any other domain of operations. The International Humanitarian Law and customary international law principles apply for states’ cyber activities, both during armed conflicts and in peacetime.

The voluntary non-binding norms of responsible state behaviour agreed during the 2014-2015 UN Group of Governmental Experts (GGE) and elaborated further during the 2019-2021 GGE, offer important additional guidelines for states on resilience, cooperation, assistance and protection of their vital cyber assets.

The implementation of these norms contributes to cyber resilience and should be advanced globally. International law and cyber norms also provide required reference framework for countries how to respond to malicious cyber activities, as well as offer direction on related issues such as attribution of cyber operations, and assistance and cooperation options in case countries fall victims of cyber attacks.

At the UN level, there have been two distinct processes in the field of information and telecommunications in the context of international security: the Open Ended Working Group (OEWG) and the Governmental Group of Experts (GGE). The successive GGEs have developed norms of responsible state behavior in cyberspace, affirmed the applicability of international law, including International Humanitarian Law and human rights law in cyberspace, as well as stressed the key role of confidence and capacity building measures. The OEWG in 2019-2021 has confirmed these elements as a basis for the framework of responsible state behavior in cyberspace.

Since 2021, the newly established OEWG discusses the implementation aspects of norms, but there are attempts by Russia and other authoritarian countries to revise existing cyber norms and make new binding commitments that might lead to a greater state control over the Internet while emphasizing state sovereignty. To achieve its goals, Russia argues that because the OEWG involves all interested UN member states, it represents a more comprehensive process and therefore should have the power to fundamentally change existing cyber stability framework agreed by the GGEs. The United States and European countries, on the other hand, argue that while the OEWG can help to develop better understanding among the global community on agreed norms and international law, establishing new binding obligations is far beyond its mandate.

Thus, in the deliberations on cyber norms, there is currently a disagreement on fundamental issues, with democratic and autocratic blocks opposing each other. This fundamental disagreement as well as the need to reach agreement among the 193 UN member states has prevented further progress in implementing the agreed normative framework in cyberspace at a global level.

The discussion on norms and resilience in cyberspace will continue also in other international forums and at national level. The new UN initiative, “Program of Action” (PoA) by France and Egypt is an important addition to existing UN achievements within the GGE and the OEWG. The goal of this bottom-up approach is to promote the application of international law in cyberspace, and implement the framework for responsible state behavior. It is hoped that the PoA will further advance cyber stability at the global level as it offers a shared vision how the implementation of norms contributes to cyber resilience.

In general, it can be observed that there are challenges in implementing cyber norms. Important aspects of any kind of norms implementation are compliance and reassurance. For example, sanctions can be used as a means to achieve this. Hence, it is necessary to identify and clearly communicate the challenges that exist in these areas. It is also important to make the topics more mainstream and not just to discuss them in expert communities. There is already a great deal of expertise in the private sector and in academia, for example, which can be helpful in gathering evidence in the event of cyberattacks.

It is clear that not all states adhere to the agreed upon cyber norms. This can be seen in various incidents around the world. Nevertheless, agreements on normative frameworks are important components of international relations, because they build a basis for expected behavior on which norms violations can be publicly condemned and sanctioned.

The discussion during the workshop also stressed that the **EU is instrumental** to provide joint response to violations of shared values in the context of responsible state behavior, for example through its coordinated attribution statements and sanctions. Nevertheless, there is still room for improvement on how to deal with violations of these shared values on the global level and how to enforce cyber norms. Another important contribution the EU makes to stability in cyberspace is through the adoption of cybersecurity regulations, the "EU Cyber Resilience Act" being the most recent example of the EU’s regulatory power. These regulations intend to create a framework that allows to include security by design principle to the ICT ecosystem supporting our economies and societies.

Based on these observations, it can be summarized that different international forums are needed to strengthen stability in cyberspace globally. Some forums are more relevant to the implementation of adopted norms, while others are more relevant to the creation of new normative elements.

At the regional level, confidence-building measures are important building blocks for strengthening stability in the cyber domain by increasing predictability, transparency and cooperation. The OSCE's task is to support states in the voluntary implementation of CBMs aimed at reducing conflict stemming from the use of information and communication technologies. There is a wide range of different CBMs: from the establishment of a point of contact network, to the exchange of best practices and national views on aspects of national and transnational threats to and in the use of ICTs, to the organization of coordinated vulnerability disclosure. In the OSCE, 16 cyber CBMs have been adopted - highlighting that there is no "one size fits all" solution. OSCE member states represent a very diverse community, both in terms of the maturity level in cybersecurity and in terms of political interests. Currently, the focus is on implementing the agreed CBMs rather than adding new ones. OSCE is closely engaged in cooperation activities with other regions in order to support global partners in implementing the framework of responsible state behavior. The discussion highlighted the fundamental role of trust and confidence building between the states in order to achieve stability in cyberspace.

The experts at the workshop analyzed that different aspects have to be considered for capacity building to be effective, with a major conclusion that **capacity building** must be sustainable. Therefore, it is relevant to work according to the need-based principle instead of demand-based principle, and to focus not only on governments but also on community-building and public-private cooperation. In order to improve capacity building delivery, best practices should be identified. It would be a great improvement if cyber capacity building projects were officially recognized as development assistance, hence, more political awareness needs to be raised among the development assistance community.

Another relevant aspect in current debates of cyber stability is deterrence. Deterrence means discouraging or preventing something from happening, for example, through the punishment or by denying the access or increasing the cost of attacking. Many experts find that traditional strategies of deterrence do not work in cyberspace. Some states resort to offensive methods such as “hackbacks” or interfering with the attackers' infrastructure as part of cyber deterrence. Even if the public debate is dominated by these ideas, Germany should choose a different path here. The priority should be to **strengthen resilience** in order to mitigate the effects of attacks. In addition, as part of this strategy, promotion of better cyber protection such as by "security by design” as well as closing backdoors should be key aspects. At the same time, there should be realistic ways found to implement "security by design" principle and the new EU Cyber Resilience Act. For example, not every product can be easily certified for cybersecurity and could increase the prices to an unreasonable level, making the effort almost impossible to manage.

In conclusion, in order to increase cyber resilience on the global, national and regional level capacity building, deterrence and response as well as advancing cyber protection should be prioritized. The mere existence of a normative framework is not sufficient to ensure stability and responsible state behavior in cyberspace; implementation of that framework and strengthening of resilience are also required.

Based on the discussions, the following recommendations can be derived:

- Germany should position itself at the global level as a **reliable cyber power**. Accordingly, Germany should be able to defend itself in cyberspace, but also have the capacity to help others and play a role in global discussions
- It will be vital to advance the **implementation of norms of responsible state behavior**, confidence building measures and apply existing international law in cyberspace

- The goal should be to build **superiority in terms of cyber resilience**, adding different measures as protection layers

- Different measures should be used to **minimize the impact of cyber operations**, including signaling on more visible domains and providing response, either on EU level or individually

- Germany should work with global partners to make **cyber capacity building more systematic** and sustainable, including promoting this assistance area as the subject of **ODA- eligibility**

- In capacity building efforts, it is always important to raise awareness on political level and build **public-private partnerships** as well as invest into community building

- Germany should work **towards strengthening the democratic Internet model** where all stakeholders – the private sector, government and civil society share their responsibility to maintain free flow of information, freedom of speech online and protection of fundamental rights in cyberspace