Principles of International Law in Cyberspace

Joanna Kulesza

Report on the Third Meeting of the Sino-European Expert Working Group on the Application of International Law in Cyberspace

Principles of International Law in Cyberspace

Joanna Kulesza

Report on the Third Meeting of the Sino-European Expert Working Group on the Application of International Law in Cyberspace

Disclaimer

The views, information, and opinions expressed in this publication are the authors' own and do not necessarily reflect those of the four facilitating organisations of the Sino-European Expert Working Group on the Application of International Law in Cyberspace, namely the China Institutes of Contemporary International Relations, EU Cyber Direct – EU Cyber Diplomacy Initiative, the Geneva Centre for Security Policy and Xiamen University. The facilitating organisations are not responsible for the accuracy of the information provided.

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
E-mail: info@gcsp.ch
www.gcsp.ch

About the author

Joanna Kulesza Executive Director of Lodz Cyber Hub at the University of Lodz, Poland and a tenured assistant professor at its Faculty of Law and Administration, specializes in various aspects of international law in cyberspace. As the head of Lodz Cyber Hub, she manages the standing curriculum expert course on "Cybersecurity and International Law" at the European Security and Defense College (ESDC). She participates in the work of the UN Ad-Hoc Committee aimed at developing a comprehensive international convention to counter the criminal use of information and communication technologies. At UniLodz she coordinates several research projects, including "Enhancing Security Cooperation in and with Asia" (ESIWA) and the "Global Digital Human Rights Network" COST Action (CA19143). Joanna represents European Internet users in the ICANN At-Large Advisory Committee (ALAC) as its Vice Chair. Previously, she co-chaired the Advisory Board of the Global Forum on Cyber Expertise (GFCE) and was a member of the Scientific Committee of the European Union Agency for Fundamental Rights (EU FRA). Her specializations include Public International Law, Internet Governance, Cybersecurity, Artificial Intelligence, Lethal Autonomous Weapons Systems (LAWS), Cyber Diplomacy, Human Rights, Privacy, Personal Data, Media Law, and Disinformation.

Acknowledgments

The author wishes to extend thanks to the individuals and institutions given below whose support and contributions were instrumental in the creation of this report. Their dedication to the fields of international law, cyberspace, cyber security, and Internet governance has enriched the content of these pages, specifically by contributing to a better understanding of the application of international law in cyberspace.

These institutions are the Geneva Centre for Security Policy, the European Union Institute for Security Studies (EUISS), the China Institute of Contemporary International Relations, and Xiamen University, which the author wishes to thank for their ongoing support. Special thanks are also due to Dr Fan Yang, Dr François Delerue, Dr Linda Maduz, Dr Andrea Salvi and Ms Alice Jorda for their contributions to this work. Their expertise and commitment have been invaluable.

In Europe the EWG-IL is kindly sponsored by the Swiss Federal Department of Foreign Affairs, the European Union and the Dutch Ministry of Foreign Affairs.

Note: Written by a European expert, this report has also been reviewed and approved by the Chinese experts group, led by Dr Fan Yang.

Contents

1. Introduction and general overview

The Third Meeting of the Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL) took place on 14-15 September 2023 in Xiamen, China. This collaborative effort has been jointly implemented by the China Institutes of Contemporary International Relations, Xiamen University, the EU Cyber Direct project of the European Union Institute for Security Studies and the Geneva Centre for Security Policy. The purpose of this EWG is to provide a platform for legal experts from Europe and China to explore the application of international law in cyberspace, address related legal issues from a theoretical perspective, and offer practical policy guidance.

The EWG-IL typically convenes once a year. It brings together a select group of experts in international law, while also welcoming the active participation of government and non-government representatives from both China and European countries. The composition of the EWG-IL varies to best reflect the specific subject matter to be discussed and expertise required for each meeting.

Key points from the meetings are documented by facilitators and conveyed to subsequent consultations of the Sino-European Cybersecurity Dialogue. They are presented as a joint public report summarising areas of agreement and divergence among participants. Additionally, the process provides the opportunity to set up smaller research groups to discuss specific legal issues and deliver joint research outcomes during upcoming meetings.

2. Main themes

2.1. Theme I: Review of small research groups' working reports

Building on the discussions of the EWG-IL meeting in 2022, the partners agreed to establish two parallel small research groups to conduct in-depth research on two specific topics. This joint effort was intended as preparation for the annual meeting, with the groups providing working draft documents to be discussed during the event. The objective of this exercise was to provide analyses of selected subjects and identify areas of agreement and disagreement between European and Chinese stakeholders. The overarching purpose was to ensure a well-informed and trust-based environment for policy discussions.

In 2022 the partners collectively decided to focus their attention on two significant themes: "due diligence" and "sovereignty". Subsequently, two draft reports were prepared and shared among the participants in May 2023. Their objective was to identify well-founded policy recommendations based on the extensive analysis of these selected aspects of international law in cyberspace. The draft reports differed in methodology, with the work on sovereignty reflecting two specific regional perspectives and the due diligence report reflecting a shared position, but with identified points of divergence. Each draft report consisted of up to 5,000 words and was presented for discussion with the aim of finalising them and publishing them after the meeting, reflecting possible amendments resulting from the discussion in Xiamen.

The second overall objective of the Xiamen meeting was to identify further steps for mutual cooperation, whether by finding new themes for in-depth analysis or pursuing deeper research into those already identified. For this purpose the meeting agenda included a discussion on sovereignty and due diligence, but also the exploration of mutual positions on non-intervention, countermeasures, state responsibility, and cybercrime. A report on these proceedings and proposed further steps is presented below.

2.1.1. Subtheme A: Sovereignty in cyberspace – small research group working report and discussion

The researchers engaged in the discussion of the issue of sovereignty in the context of cyberspace decided to present their report as a compilation of two independent position statements. This reflected varying perspectives on the nature of cyberspace and the structure of the regulatory framework behind it. Both sides agreed to reflect on the application of international law in various layers of the Internet. While various methodologies can be used to identify such layers and approach related regulatory challenges, the group agreed to focus on the four specific layers identified below.

The compiled report reflected on commonalities and differences in research group members' understanding of sovereignty, pointing out its crucial role as a fundamental principle of international law that serves as the foundation on which many other principles are built.

Both groups agreed that cyberspace is a conceptual construct and that the application of international law in this domain requires going beyond this conceptualisation to understand its practical implications. This resulted in the group presenting two positions on how sovereignty and its application in the ever-evolving landscape of cyberspace are to be understood.

The Chinese perspective presented sovereignty in cyberspace as a layered concept comprising four distinct layers in which sovereignty may manifest itself:

- The *physical layer* encompasses technical and territorial sovereignty over physical infrastructure in a state's territory, including the right to take all related necessary measures.
- The *logical layer* is where states can independently formulate or adopt technical standards ensuring the interoperability of the Internet. The Chinese perspective is that coercing a state into adopting a particular technical standard may result in problematic "legal consequences".
- The *application layer* allows for the representation of "legitimate" data and information related to national security so that they are protected from "foreign theft and destruction". It also allows states to restrict the dissemination of unlawful information, content undermining social interests, or information fabricated or distorted in other countries that might jeopardise national interests.
- The *social layer* reflects the way in which a state manages its Internet users and platforms, fostering a conducive environment for independent Internet governance and supporting the digital economy.

From the Chinese perspective, the principle of sovereignty is integral to these layers and serves as a means for states to regulate the dissemination of information in their territories, especially when such information infringes on social interests or poses a threat to national sovereignty and security.

Equally, from the Chinese perspective, sovereignty in cyberspace is not just a concept, but a legally binding principle and rule. It was emphasised that certain cyber operations may violate sovereignty, the principle of non-intervention, and even the prohibition of the use of force in specific circumstances. Sovereignty was recognised as a primary rule with implications for state behaviour. The concept of sovereignty was discussed in the context of its legal identity, the capacity to govern and the potential to assume responsibility. It was closely linked to the concepts of both due diligence and non-intervention, emphasising the complementary nature of these principles of international law. The standard for determining violations of sovereignty in cyberspace was explored, with factors such as the unauthorised penetration of network systems in the territory or jurisdiction of another state being considered as potential violations. The extent of harm was also discussed as a crucial factor in determining such violations.

Additionally, the question of whether cyber violations could be qualified as a use of force was considered. The attribution of responsibility for cyber violations was recognised as an important concept for understanding sovereignty, although the authors agreed that the specifics of attribution fell beyond the scope of the meeting. It was, however, recognised that the operations of non-state actors could only constitute violations of sovereignty if they could be attributed to a

state. Violations of sovereignty implied responsibility and could trigger a state's right to institute countermeasures. Depending on the threshold of harm, the principle of the use of force might be violated, constituting an infringement of sovereignty that could potentially lead to self-defence measures being taken.

In conclusion, the Chinese perspective recognised the existence of different approaches to sovereignty in cyberspace. The report's authors underscored that states should strive to find common ground on basic principles and reach agreements on more specific rules. The need for mutual understanding and cooperative efforts in the realm of international law in cyberspace was emphasised.

The European perspective was also presented as a dedicated component of the report. It reflected the focus on the first three layers of cyberspace referred to above (the physical, logical and application layers). The physical layer was identified as the most significant, with the location of related hardware components within its territory allowing a state to exercise sovereignty. This perspective emphasised the expectation that states should respect each other's territorial sovereignty and jurisdiction, and that this principle also applied in cyberspace. Jurisdiction was a key discussion point, because it was derived from sovereignty. Notably, the intersection between sovereignty and jurisdiction was brought up. The discussion focused on whether violations of sovereignty were essentially instances of extra-territorial jurisdiction, highlighting the complexity of these interconnected principles. Divergent views on this issue were reported, with some believing that any form of cyber operation could constitute a violation of sovereignty, while others assumed that the very nature of cyberspace made such violations different from those in other domains. This territorial aspect of the sovereignty discussion was also reflected in the European perspective on cyber operations. The European rapporteurs highlighted that cyber operations are likely to breach the principle of territorial sovereignty rather than other norms of international law. The authors also addressed the concepts of intervention and the use of force. The overlap between these concepts and sovereignty was discussed, as well as the need to distinguish and define the elements that differentiate them.

The relevance of the Westphalian system in the contemporary globalised world was touched on, with the point being made that it continues to be important in protecting weaker states, but was not found appropriate to fostering the current discussion, given the transboundary nature of cyberspace, with due regard to the fundamentally different theoretical approaches to the nature and structure of cyberspace and its impact on the application of international law in this realm.

The key takeaways from the sovereignty discussion amounted to the identification of divergence in regional perspectives on the structure and nature of cyberspace, as well as a focus on jurisdiction as a more specific topic derived from the broad sovereignty debate. As noted below, jurisdiction was also the common denominator for the discussion on cybercrime covered on Day 2 of the meeting.

2.1.2. Subtheme B: Due diligence – small research group working report and discussion

The due diligence joint paper discussed in session 1 was structured differently, presenting a joint statement from the two research groups highlighting points

of alignment and identifying specific points of contention that could potentially be the subjects of further debate. In the experts' comprehensive discussions ahead of the meeting, a consensus emerged regarding the recognition of due diligence as an essential standard in international law.

One prominent point of agreement was the recognition of technological neutrality, signifying that due diligence standards should maintain their relevance across different technological contexts. The researchers also managed to identify common ground that justified the validity of due diligence as a standard in international law. They pointed to specific case law and other sources of international law to set the framework for the joint reference.

Most significantly for possible further work, the identified differences focused on the status of the duty bearer and their associated obligations. A notable area of contention arose when the group considered whether the scope of the due diligence obligation should encompass preventive measures. One perspective, in line with European practices, advocated for the taking of proactive steps to prevent harm as an obligation of conduct, while an alternative viewpoint, presented by the Chinese position, leaned towards a more limited approach focused on halting and redressing harm. These discrepancies underscored divergent approaches to the extent of the duty bearer's responsibilities, with one viewpoint emphasising due diligence as a preventive principle and the other primarily concentrating on redress.

Furthermore, the standard of knowledge emerged as a significant point of reference. Identifying potential threats while respecting individual privacy remains a prominent area of international discussion. It was also reflected in the draft paper discussed during Day 1. The parties referenced the work of the International Law Commission, which drew the line of duty at clandestine activities, which no state is under obligation to prevent. This relatively low standard of consensus and its intentionally ambiguous nature make the enforcement of this obligation on an international scale an ongoing challenge.

The question of prevention, repression and restitution became a pivotal aspect of the discussion. Differing perspectives were evident in the language used to describe harmful activities, with one viewpoint highlighting the need to prevent such activities and the other emphasising the importance of addressing malicious activity that had already been performed.

In the Chinese view, implementing cyber due diligence as a duty primarily involves actions that can be internationally classified as wrongful acts. However, the European viewpoint suggests that it can also stem from actions that harm a nation, but may not necessarily meet the criteria of internationally classified wrongful acts where the law on international liability could be applied.

In summary, these discussions brought to light both consensus and divergence. A consensus was reached regarding the existence of due diligence in international law, thus recognising its significance. Nevertheless, the discussions illuminated significant differences in how this standard is understood and applied, underscoring the multifaceted and complex nature of this concept in the context of international law.

2.2. Theme II: Non-intervention

In the course of the public debate, the principle of non-intervention, which is derived directly from the UN Charter and customary international law, has faced substantial criticism due to its frequent breaches. Originally, it primarily pertained to military non-intervention, but has gained new relevance in the modern world, which is characterised by extensive economic exchanges and overseas interests. However, it has also become one of the most frequently violated legal obligations. When an attempt was made to extend this principle to the governance of cyber operations, new challenges emerged. For this reason the experts agreed to address these challenges in two dedicated sessions.

The first session involved a theoretical examination of the principle of non-intervention and the complexities of applying it in cyberspace by exploring the issues of identifying an alleged illegal intervention, establishing its target and assessing the level of "coercion" exerted. In the second session a hypothetical case study proposed by the European participants was presented. This case study served as a practical illustration of the theoretical considerations discussed by offering an opportunity to apply and test the principles of non-intervention in cyberspace in a specific scenario.

The opening discussion highlighted the absence of a single European perspective on this issue. As the experts reported, Western states had previously considered the principle to be redundant, particularly during the Cold War, when the focus was on the prohibition of the use of force. Nevertheless, the session underscored the contemporary importance of the principle of non-intervention due to the significant role of activities in cyberspace designed to influence recent elections.

Coercion was a central theme during the discussion. Two forms of coercion were examined: dictatorial and forcible. Dictatorial coercion is the term used to refer to demands and threats aimed at compelling a state to take specific actions or refrain from certain activities, often accompanied by explicit threats of harm. In contrast, forcible coercion entails a state exercising power in the territory of another state without valid consent or a rule of international law permitting the activity. However, as the experts emphasised, coercion is not inherently unlawful: its legality depends on whether it is employed in the internal affairs of another state.

The session also covered the question of which cyber operations are considered coercive. Cyber operations causing material damage to individuals or physical objects may be seen as violations of the non-intervention principle. Similarly, cyber operations that disrupt or damage infrastructure without proper consent can be viewed as dictatorial coercion. Unauthorised extra-territorial access to non-public data through cyber operations was considered a complex issue, often intersecting with the rules of sovereignty. When carried out without consent, such operations may be viewed as violations of the principle of non-intervention. The use of cyber operations to influence the internal affairs of a sovereign state remained contentious due to the blurred line between persuasion and coercion.

Further discussion revolved around the evolving application of the non-intervention principle in cyberspace. Western countries in particular have become vocal

proponents of extending this principle into the digital realm, with legitimate concerns driving this shift. This change is seen as an opportunity for both Western and non-Western countries to engage in realistic discussions regarding their concerns and potential areas of agreement. This may contribute to making the principle, historically one of the most violated, more effective. The primary focus in recent discussions regarding non-intervention in cyberspace has been on the issue of coercion. Some states attempt to broaden the principle of non-intervention and expand its interpretation. However, there is a concern that this broadening might lead to an over-interpretation of this principle to encompass actions that may not genuinely violate it. The shift in focus from the freedom to decide to the freedom to control could lead to an excessively expansive interpretation. This shift may replace the principle of sovereignty with that of non-intervention, raising concerns about the stability of cyberspace. The session emphasised the need for non-Western countries to play a more active role in interpreting and applying the principle of non-intervention in cyberspace. Encouraging their active participation in shaping the interpretation and application of this principle, including countries like China, was deemed crucial.

In the ensuing discussion, questions were raised about the nature of manipulative coercion, the differentiation between information from authorities and citizens, the role of specific intent in assessing coercion, and the balance between existing principles and the development of new rules in cyberspace. The session also considered the possibility of composite acts and their relation to other norms of international law. Ultimately, the first session highlighted the dynamic and complex nature of interpreting and applying non-intervention principles in the evolving cyberspace landscape.

The session concluded by highlighting that the prohibition of cyber operations supporting subversive, terrorist, or armed activities aimed at overthrowing another state's government or interfering in its political affairs had achieved consensus across various blocs. This prohibition on providing such support is a fundamental aspect of non-intervention that is applicable to both the physical and cyber domains.

This insightful discussion was followed by a second dedicated session involving a case-study analysis. The European perspective presented during this session focused on the principle of non-intervention in the context of cyber operations, particularly in the run-up to elections. Several key points emerged:

- *Domaine reserve:* The European perspective noted that the issue no longer belongs to the domain reserve when it is regulated by international law, which constitutes a horizontal approach. However, a vertical understanding of the issue argues that certain elements, like conducting elections, pertain to the political affairs of the state, and therefore fall under the non-intervention principle.
- *Coercion vs influence:* The session highlighted a distinction between wrongful intervention and influence. While some states claim that any form of influence is unlawful, European states tend to differentiate between these concepts. The quality and content of the information disseminated were considered crucial in assessing whether it breaches the non-intervention principle.

- *Information and disinformation:* The session emphasised the importance of distinguishing between information and disinformation. Disinformation, including deep fakes and trolling, can lead to intolerance and violence both online and in real life. The distinction between cyber information operations and cyber effect operations was also briefly discussed. The discussants agreed that cyber effect operations in their strict sense mean operations carried out through cyber means aimed at having disruptive or destructive effects. Complementarily, cyber information operations are usually performed in the information domain, and it is there that disinformation and misinformation can have a cognitive impact on recipients. Effectively, non-intervention analysis should be applied according to the definitions of these two types of operations.
- *Cyber operations and non-intervention:* The experts discussed the relationship between cyber operations and the principle of non-intervention. Foreign intrusion into a state's cyber election infrastructure could constitute wrongful intervention, but a comprehensive assessment of relevant circumstances is necessary before concluding that it is an illegal intervention.
- *Coercion in cyber operations:* Traditional formulations of coercion were framed narrowly, often focusing on changing the policy of the target state. However, coercion in cyberspace can encompass various means, including political ones. The effects-based approach that looks at the scale and effects of the results of such operations was emphasised. Cyber operations affecting a state's essential functions, such as its energy supply, could be seen as coercive.

From the Chinese perspective, three types of cyber operations were discussed, including influencing elections, affecting the voting website and affecting election infrastructure. The key points included the following:

- *Domain reserve and coercion:* The Chinese perspective emphasised that state interference in other states' elections and their accession to treaties fell within the domain reserve. For an act to be coercive, it must either compel the target state to change its behaviour or deprive it of control over protected matters.
- *Accuracy of information:* The element of truthfulness of information was a focal point. It was argued that the impact of an act of intervention should be considered, but is not the decisive factor. Even the release of truthful information could be seen as coercive, and the impact of an act does not necessarily determine its legality.
- *Seriousness of cyber attacks:* Cyber attacks on critical infrastructure, such as the power grid, were deemed to be serious issues with serious consequences. Priority should be given to the actual impact of the attack on the valid interests of the state, including its critical infrastructure.

In summary, this session highlighted the complexity of interpreting and applying the non-intervention principle in the context of cyber operations, particularly concerning elections and critical infrastructure. It underlined the need to consider the quality of information, the distinction between influence and coercion, and the seriousness of cyber attacks on critical infrastructure.

The discussion during this session raised the following issues:

- **Misinformation and credibility**

One participant was unsure of whether a misinformation operation should be considered a breach of the non-intervention principle, and suggested that the accuracy of the statements made could affect the assessment. There was a question about the extent to which the insertion of truthful information into a manipulative narrative designed to exert influence should be considered. The issue of who decides what is truthful was raised. While reports of truthful events can be circulated, due attention must be paid to the disclosure of reliable information consisting of national secrets or sensitive personal information. The discussion highlighted the complexity of defining truth in this context. Certain communications, like deep fakes, disinformation and deliberate lies, might directly reflect the intent of the actors behind them. The discussion highlighted the importance of addressing this kind of manipulation. The trend in international agreements, such as the Global Compact on Migration, suggesting that states should engage in internal debates based on true, verifiable facts to prevent misinformation in public arenas was also mentioned.

- **Standard of intervention**

The issue of the standard of permitted state intervention was raised, particularly in the context of sovereignty. Respecting sovereignty means respecting a state's political independence. The discussion pointed out that without a clear international standard on this issue, the answer might require considering the target country's perspective, circumstances and reasons for implementing a particular policy or taking a particular course of action.

In summary, the discussion highlighted the challenges of addressing misinformation and manipulation, determining a standard for intervention, and assessing whether various cyber operations breach the principle of non-intervention in cyberspace.

2.3. Theme III: Applying the law of state responsibility in cyberspace

The attribution of state responsibility in cyberspace is seen as a vital aspect of future developments in the cyber domain. While some states have publicly attributed responsibility for particular cyber operations, they have yet to invoke international law to establish the responsibility of alleged wrongdoers. The next step is likely to involve holding the responsible state to account before an international tribunal or arbitration proceeding. Complementarily, countermeasures are likely to play a crucial role, allowing target states to respond to international law breaches and justify their response. In this context new debates have arisen about the use of countermeasures in cyberspace. Theme III allowed for a general discussion on attributing state responsibility in cyberspace, followed by a focused debate on countermeasures in this context.

2.3.1. General discussion

In the European narrative, references to state responsibility explicit in state practice, understanding its forms, and expected consequences are not well documented. Understanding the reference to state responsibility involves

examining remedies, measures to be taken by the state perpetrating the infringement, expectations of guarantees of non-repetition, and the type of reparation requested. Yet whereas the practice of raising the issue of state responsibility is limited, public attribution is common. Experts also observed that determining when a cyber operation constitutes an internationally recognised wrongful act is possible only with reference to primary rules. Secondary rules are applicable when identifying the degree of illegality and the nature of cyber operations, particularly when multiple operations are involved. Defining the nature of an operation, formulating a claim and determining the claim's scope are critical aspects.

Attributing state responsibility involves:

- the target state formulating claims, which requires the provision of substantial cyber security information to support these claims;
- identifying remedies, such as measures to be taken by the wrongdoing state, expectations of guarantees of non-repetition and the forms of reparation; and
- giving notice of the claim to the wrongdoing state.

The claim for state responsibility can be implemented through diplomatic or judicial means. Yet challenges arise concerning the relationships among state and non-state actors, diplomatic protection, private company damages, and insurance claims. The collective dimension of attributing state responsibility requires considering multi-operation scenarios, the potential involvement of multiple states and reparations. Non-targeted states may also make claims in support of other states, potentially safeguarding collective interests.

The participants agreed that the principles of state responsibility apply in cyberspace, and that the attribution of responsibility is a fundamental aspect of this process. Attribution falls into three categories: legal, political and technical. In cyberspace injuries are often caused by non-state actors, but they can be attributed to a state, particularly when proxies act under state instruction or control. The rules outlined in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) are relevant to cyberspace. However, attributing acts of proxies to a state is a contentious issue, with varying standards like those of "effective control", as identified by the International Court of Justice, and "overall control", as identified by the International Criminal Tribunal for the former Yugoslavia. These differences in standards can impact attribution claims and their viability.

When assessing events occurring in cyberspace, lawyers, including investigators and judges, may adopt different standards of proof due to the technical challenges of attribution. Given the difficulty of technical attribution, some suggest reversing the burden of proof, shifting from a standard requiring "proof beyond reasonable doubt" to one requiring a "preponderance of evidence", while the obligation to publicly attribute responsibility or disclose evidence remains a contentious matter. While some argue for transparency, emphasising the importance of public attribution and evidence disclosure for accountability, there are differing approaches globally, including joint attribution by multiple states and various attribution methods in the US and UK courts when prosecuting cybercriminals. The discussion also covered a proposal for setting up a voluntary non-partisan technical attribution centre under UN auspices.

2.3.2. Subtheme: Countermeasures

The experts defined countermeasures as actions that are normally unlawful, but can be considered lawful due to prior unlawful conduct. It is in this context that significant questions were raised about their applicability in cyberspace. Under the ARSIWA, most states view countermeasures as lawful actions in international law, while a few, including Greece, India, Mexico and Cuba, hold a different view. China has expressed cautious support for countermeasures.

Challenges related to countermeasures in cyberspace include four key issues:

- *Notice:* Targeted states are required to notify the responsible state or states before engaging in countermeasures. Some European Union (EU) states argue for exceptions, particularly in urgent cases where there is no time for extensive procedures.
- *Timing:* The timing of countermeasures in cyberspace is a complex issue. The challenge lies in determining when the underlying breach has occurred, especially in cases where the operation has not yet begun or has already concluded.
- *Attribution:* Misattribution can occur when states engage in countermeasures against the wrong party, risking violations of innocent states' rights. Different countries have varying approaches to assessing countermeasures.
- *Collective countermeasures:* The notion of collective countermeasures is a complex and controversial one, with countries like Estonia supporting it, while France and others disagree. Defining the legal basis for collective countermeasures is a challenge.

In the discussion, the question arose regarding anticipatory countermeasures, particularly in the context of the United States' "defend forward" strategy in cyberspace. This strategy involves preparing for pre-emptive measures in response to perceived threats that fall below the threshold of armed conflict. The discussion revolved around whether these actions could be deemed anticipatory countermeasures and their implications.

The conversation also touched on the difficulty of ensuring proportionality in anticipatory countermeasures. It was suggested that one way to address this was to assess the harm the state would have suffered in the absence of countermeasures and ensure that the countermeasures are limited to the least harm they can cause.

Overall, the discussion highlighted the complexities and challenges associated with anticipatory countermeasures, particularly in the realm of cyberspace, where the nature of threats and responses can be complex and intricate. In the discussion, several questions were raised and answers given concerning various aspects of unlawful cyber operations, countermeasures and their implications:

- *Definition of unlawful cyber operations:* The question arose as to whether there is a clear definition of unlawful cyber operations. The answer provided was that an unlawful cyber operation would violate any of the rules of international law, including principles related to sovereignty, non-intervention in a country's internal affairs, the use of force, and the violation of diplomatic bodies or posts.

- *Composite acts:* The discussion touched on composite acts, particularly in the context of a campaign of cyber attacks. The focus was on whether these composite acts affect the permissibility to deploy countermeasures. The understanding was that composite acts generally involve continuing unlawful activity conducted by the same actor over time against the same target.
- *Collective countermeasures:* Questions were raised about the legality of and differences in scenarios of collective countermeasures. The term "collective countermeasures" was discussed as a non-legal term, often referring to countermeasures taken by non-injured states. The difference between state obligations *erga omnes* and requests for assistance was addressed, and it was acknowledged that more research into the related methodology is needed.
- *Fundamental norms of international law:* The question focused on which rules of international law would be considered fundamental and whether countermeasures could violate fundamental rules, including human rights such as freedom of speech. The answer emphasised the need to evaluate whether specific human rights are fundamental and highlighted the potential differences in interpretations among countries.
- *Temporary nature of countermeasures:* The nature of countermeasures as temporary and their purpose in compensating for harm was discussed. The question raised was how countermeasures could be set up after the internationally recognised wrongful act is over and whether they serve as a punishment or a solution. The response clarified that countermeasures taken after the fact could be a response to a state's failure to provide reparation and not necessarily an escalation.
- *Basis of collective countermeasures:* The basis for collective countermeasures was discussed from both the political and legal perspectives. While alliances and political considerations may play a role, the legal aspects were characterised as requiring a more nuanced approach, because collective countermeasures often challenge established norms.

Overall, the discussion highlighted the complexities and ambiguities surrounding unlawful cyber operations and countermeasures in international law, underscoring the need for further research and international consensus on these issues.

2.4. Theme IV: International governance of cybercrime

Addressing cybercrime is directly relevant to all cyber security concerns. Distinguishing state-sponsored cyber attacks from criminal activities carried out by non-state actors can be challenging. Establishing effective global cyber security rules is currently unattainable due to the lack of a normative framework for cybercrime, both domestically and internationally. Theme IV explored the intersection of cybercrime and cyber security in the light of ongoing UN negotiations on the issue. It also offered an opportunity to analyse a hypothetical case scenario prepared by the Chinese participants. The discussion centred on the intersection of cybercrime and international law in the context of ongoing cybercrime treaty negotiations. Key points from the discussion include the following:

- *Jurisdictional principles of public international law:* Cybercrime must be addressed under the jurisdictional principles identified in public international

law. The discussion emphasised the importance of understanding how international law governs enforcement jurisdictions beyond a state's territory, especially in the cyber context.

- *International human rights law (IHRL):* Participants discussed the extent to which IHRL influences cybercrime laws, especially in cases where online criminal activities may impact human rights such as privacy and freedom of expression.
- *State obligations in cybercrime cases:* The conversation raised the question of how states should respond to cybercrime groups causing harm to other states. The experts discussed the legal obligations of states when dealing with cross-border cybercrime incidents. From the EU perspective, the Budapest Convention on Cybercrime was raised, and its link to the European Convention on Human Rights. Both agreements play a crucial role in addressing cybercrime in the context of international law. It was noted that the Budapest Convention is supported by a community of experts, fostering exchanges and confidence-building efforts.
- *Challenges and trends in cybercrime:* Trends in cybercrime were discussed, such as the digitalisation of traditional crimes, the industrialisation of cybercrime and its internationalisation through cross-border criminal activities.
- *Ongoing UN treaty negotiations:* The ongoing negotiations for a UN cybercrime treaty were mentioned. The positive developments, consensus on principles and constructive attitudes of participating countries were highlighted. China's advocacy of a more open approach to cybercrime criminalisation and additional proposals for criminalisation were also noted.
- *International cooperation:* The importance of international cooperation in addressing cybercrime was stressed, particularly in terms of the exchange of e-evidence. It was suggested that states may voluntarily expand international cooperation to address crimes not covered by the proposed UN treaty.
- *Prevention and the role of service providers:* Preventing cybercrime requires raising public awareness, capacity-building and effective preventive measures. The role of service providers in facilitating efficient preventive measures was underscored, although differing perspectives exist on including obligations for service providers in the proposed UN convention and in the existing internet governance model.

3. Ways forward

The discussions provided valuable insights and touched upon various key takeaways for future sessions of the EWG-IL. In their final interventions experts emphasised the need for focusing more research on the issues of attribution, cybercrime, jurisdiction and capacity-building, and reflected, among other things, on the current work of the UN Open-Ended Working Group. Personal reflections highlighted participants' trust in and commitment to the EWG-IL process, with due regard to the valuable reports on identified divergences, allowing for further steps to be taken. Exploring ways forward, the suggestions include:

- building on what has already been achieved, emphasising the consensus on the issues of due diligence and sovereignty;
- developing existing processes, but introducing new topics within the same framework, such as dedicated policy papers on cybercrime or territorial jurisdiction;
- further work on the concept of state responsibility in cyberspace, including countermeasures and attribution; and
- joint capacity-building efforts on the application of international law in cyberspace, which could lead to a better understanding of vital issues and further consensus.

The need to explore new topics and connect them thematically was also proposed, potentially introducing subtopics under overarching themes. The discussions also highlighted the significance of addressing new technologies in cyberspace and the potential threats they pose. This included the need to discuss issues like artificial intelligence and its impact on cyber security. The discussions also emphasised the value of case studies in the practical application of international law. Regarding international relations, potential topics included the possibility of engaging international institutions in countering cybercrime and the regulation of non-state actors, including private companies.

Finally, there were suggestions for further research on the attribution of responsibility and its relationship with technical and political aspects. Additionally, the need to make the dialogue reactive to real-life challenges, not just technical legal questions, was emphasised. The parties considered a dedicated focus for the next meeting of the EWG-IL, possibly that of attribution, with a specific emphasis on exploring subthemes of this topic, whereas the details of intersessional work are yet to be decided on. These might include the limits of state jurisdiction online, state responsibility and international liability for non-state actors, and technical attribution, all of which should be accompanied by targeted capacity-building efforts. Overall, these discussions have provided grounds for future academic research and collaborative efforts aimed at shaping the application of international law in cyberspace.

About the partner organisations

China Institutes of Contemporary International Relations

The China Institutes of Contemporary International Relations (CICIR) is a long-standing, extensive, and multifunctional research and consultation complex focusing on international strategic and security studies. It covers all geographic areas and major strategic and comprehensive issues in the world. The CICIR has a staff of about 300, including researchers and administrative and logistical personnel, who work for 15 institutes, a number of centres, and several offices. For years it has participated in wide-ranging, thorough and high-end international academic exchanges. The CICIR is authorised to confer master's and doctoral degrees, and publishes three academic journals: *Xiandai Guoji Guanxi*, *Contemporary International Relations* and *China Security Studies*.

EU Cyber Direct

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen a rules-based order in cyberspace and build cyber-resilient societies. To fulfil this aim it conducts research, supports capacity-building in partner countries and promotes multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 54 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

Xiamen University

Xiamen University (XMU), established in 1921, has long been listed among China's leading universities. With a graduate school, six academic divisions consisting of 33 schools and colleges, and 16 research institutes, XMU boasts a total enrolment of nearly 44,000 full-time students, and has over 3,000 full-time teachers and researchers, of whom 32 are members of either the Chinese Academy of Sciences or the Chinese Academy of Engineering.


CICIR
中国现代国际关系研究院
CHINA INSTITUTES OF CONTEMPORARY
INTERNATIONAL RELATIONS


EU
CYBER
DIRECT


GCSP
Geneva Centre for
Security Policy


UNIVERSITAS AMOIENSIS