Navigating Sino-European Approaches to the Application of International Law in Cyberspace

François Delerue and Fan Yang

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

Navigating Sino-European Approaches to the Application of International Law in Cyberspace

François Delerue and Fan Yang

Report on the Second 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 authors

François Delerue is an Assistant Professor of Law at IE University Law School, Spain.

Fan Yang is an Assistant Professor and Deputy Director of Cyberspace at the International Law Centre of Xiamen University School of Law, China.

Contents

1. Introduction

The China Institutes of Contemporary International Relations, EU Cyber Direct – EU Cyber Diplomacy Initiative, the Geneva Centre for Security Policy (GCSP) and Xiamen University jointly convened the second meeting of the Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL) in Geneva and online from 22 to 23 June 2022.

The working group provides a platform for exchanges to examine the application of international law in cyberspace and promote exchanges among Chinese and European legal experts on their legal positioning across diverse cyber scenarios. The EWG-IL is also uniquely designed to examine specific legal questions in the periods between meetings of the more widely focused EU-China Cyber Task Force (Track 1) and Sino-European Cyber Dialogue (Track 1.5) meetings, thereby advancing the discussion in all forums.

The second meeting hosted by the GCSP on 22-23 June brought together over 20 legal experts to discuss topics under three broad, standing themes:

- the overarching legal framework applicable to cyberspace;
- the rules and principles of international law in cyberspace; and
- case studies of the application of international law to a cyber operation.

The meeting provided an opportunity for an expert discussion of the following issues: (1) perspectives on cyber sovereignty and the peaceful settlement of disputes; (2) interpretations of legal issues stemming from fictional cases dealing with due diligence and the law of armed conflict; and (3) the identification of areas of consensus and issues for further study and discussion.

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.

2. General overview

The second meeting of the EWG-IL comprised four thematic sessions on cyber sovereignty, due diligence, the peaceful settlement of disputes and the law of armed conflicts. The next section of this report summarises the discussions and main outcomes of these thematic sessions.

This second meeting allowed the EWG-IL to restart the dynamic initiated by the first meeting in 2019, after which subsequent meetings were halted due to the global COVID-19 pandemic. Overall, it is to be commended that the participants approached this meeting in a constructive way, allowing for interesting and fruitful discussions, including on convergences and divergences among the Chinese and European participants, and on determining possible topics and formats for further engagements.

3. Core themes

3.1 Cyber sovereignty

The first session was dedicated to the subject of sovereignty.[1]

Sovereignty is a cornerstone and pivotal principle of international law, and is also the foundation on which various rules and principles of international law are grounded, such as territorial sovereignty, sovereign equality and the principle of non-intervention. Part of the discussion during this first session focused on the specific nature of the principle of sovereignty and on its relationship with its corollaries. It was notably pointed out that there is no single definition of sovereignty, and the discussion showed that in using similar terms we might sometimes be referring to different concepts. From this perspective the concepts of "cyber sovereignty" and "digital sovereignty" were discussed, notably highlighting that they were used as political concepts in general, rather than legal concepts. This remark is important in showing that behind the use of the term "sovereignty", states and other actors are not always referring to either the relevant principle of international law or one of its legal corollaries.

In recent years an important focus of discussions and work on sovereignty and cyberspace relates to the question of the extent of a state's territorial sovereignty in cyberspace. While forming part of the discussion, territorial sovereignty was only briefly discussed, and it did not raise any specific questions or debate among workshop participants.

[1] It should be noted that during this session the third report jointly launched in 2021 by Wuhan University, the China Institutes of Contemporary International Relations, the Shanghai Academy of Social Sciences, Fudan University, Beihang University, the National Institute for Global Strategy, the Chinese Academy of Social Sciences, Tsinghua University and the University of International Business and Economics on *Sovereignty in Cyberspace: Theory and Practice* was presented and formed the focus of some of the discussion. This report can be found online at: https://subsites.chinadaily.com.cn/wic/2021-09/28/c_815431.htm .

Questions of how a cyber operation may breach sovereignty or one of its corollaries led to an interesting discussion on the fact that, like any other type of activity, a cyber operation may simultaneously breach more than one rule or principle of international law. An act amounting to a prohibited use of force, for instance, may also simultaneously constitute a breach of territorial sovereignty and the principle of non-intervention. Yet it is important to distinguish the different legal rules or principles that could apply to a particular cyber operation and to avoid conflating them. From this perspective, an important dimension of the discussion focused on the relationship between sovereignty and the principle of non-intervention, which are sometimes perceived to be closely related. This formed the starting point of the discussion. Yet the principle of non-intervention is notably characterised by a coercive criterion, which clearly distinguishes it from territorial sovereignty, as the participants discussed and generally highlighted. The discussion also revolved around the relationship between sovereignty and due diligence, which constituted the theme of the second session.

The question of espionage was also discussed, and the diversity of approaches on how international law regulates espionage activities. Both the Chinese and European participants expressed similar views on the matter, highlighting that there is no distinction from an international law perspective based on the purpose of a cyber operation. In other words, whether the purpose of the cyber operation is espionage is irrelevant in determining whether it constitutes a breach of international law.

The closely related question of jurisdiction in relation to cyberspace and cyber activities led to some interesting discussions, notably on extraterritorial jurisdiction and conflicts of jurisdiction. It was notably observed that there is a developing practice on these matters in private international law and criminal jurisdiction cases. Generally, the development of the Internet has radically increased conflicts of jurisdiction among states because it facilitates transboundary activities, and state practice will be key in determining the outcome of these conflicts.

Internet governance was also discussed, focusing on the relationship between states' sovereignty and multistakeholder governance. Some participants argued that, as a human-made technical space, the architecture of the Internet required substantial input from private parties, especially at the logical layer, where technical protocols abound. However, this fact does not in any way preclude governance by states in terms of fundamental issues such as content regulation, privacy protection and cyber security.

In general, the presentations and discussions on sovereignty showed a high level of convergence between the European and Chinese participants. From the discussion summarised above it appears that various unsettled questions remain. Yet these questions are not linked to a divergence of views between European and Chinese scholars, but are more general questions that are still to be debated by both states and scholars around the world.

3.2 Due diligence

The second session was dedicated to the issue of due diligence. A case study formed the basis for the subsequent discussion.

Due diligence is a flexible standard of conduct that has developed in various branches of international law. The polymorphous nature of this concept explains why part of the discussion focused on the definition of due diligence and different related standards, as well as on questioning whether a general rule or principle of due diligence exists under public international law.

One of the Chinese participants highlighted that the polymorphous nature of due diligence may be seen as a source of uncertainty regarding its legal nature and content, while a European participant argued that its polymorphous nature was a feature of due diligence that allowed an important level of adaptation. From there, the experts discussed the sources of due diligence obligations and their relationship with the law of state responsibility. This discussion notably focused on the work of the United Nations (UN) International Law Commission (ILC) and its work on state responsibility and transboundary harm.

The legal status and sources of due diligence were also discussed. Some participants highlighted that in the reports of the UN Group of Governmental Experts (UNGGE), due diligence is discussed in the section dedicated to "Norms, rules and principles for the responsible behaviour of States" (norm 13(c)) and not in the section dealing with international law. It was argued that this observation reinforces the uncertainty of the legal status of due diligence. However, a European participant noted that the norms of responsible state behaviour coexist with the rules of international law, and there is a certain degree of overlap between norms and existing international law. Moreover, it was mentioned that some states are generally opposed to due diligence as an international legal obligation, notably the United States. However, some European participants noted that most states that have expressed their position on the matter have accepted the existence of one or more obligations that establish due diligence standards. Various obligations of due diligence and their legal sources and consequences were discussed; for instance, Article 194(2) of the UN Convention on the Law of the Sea and Article 1 of the Convention on the Prevention and Punishment of the Crime of Genocide.

Due diligence is an obligation of conduct, not of result. Various experts restated this during the discussion, and the concept seemed to be rather uncontroversial among the participants. Other aspects of due diligence were also discussed, notably regarding a state's knowledge of the activities taking place on its territory. This notably led to some discussion on the relationship between due diligence and jurisdiction.

Due diligence is sometimes perceived as being closely related to attribution, if not a substitute for it. This observation led to discussions among the participants on the rules on attribution in the law of state responsibility and the different thresholds of control identified by the International Court of

Justice (ICJ), the ILC and the International Criminal Tribunal for the former Yugoslavia for the imputation of conduct by a non-state actor vis-à-vis a state. Yet comments from both Chinese and European participants pointed out to the meeting on several occasions that attribution and due diligence should not be conflated, and that due diligence is not a secondary rule of attribution. Several Chinese participants indicated that the perceived tendency of Western states to consider due diligence as a substitute for attribution explains why China and Chinese scholarship tend to take a cautious approach to the issue of due diligence.

The presentations and discussion during this session showed a degree of divergence among the participants on several questions related to due diligence. As summarised above, many questions were raised and many comments made during this session. Yet finding answers to these questions was not the objective of the session; instead, participants indicated various paths that could be followed for a subsequent engagement on the subject of due diligence.

3.3 Peaceful settlement of cyber disputes

The third session was dedicated to the issue of the peaceful settlement of cyber disputes.

The basic consensus is that, just like other types of international disputes, cyber disputes should be settled by peaceful means. This international legal obligation is principally stipulated in Articles 2(3) and 33(1) of the UN Charter, and has been generally recognised as customary international law in ICJ judgments. UNGGE reports have confirmed the applicability of such an obligation in a cyber-related context.

Quite notably, disputes regarding cyber operations seldom take the form of an international legal confrontation. Multiple participants designated the issue of the attribution of a cyber operation as the obvious reason for this, as it includes not only difficulty at the technical level and uncertainty in the political calculation regarding to whom a particular cyber operation could be attributed, but also ambiguity in terms of legal imputation on how to substantiate the claim. The lack of an incontrovertibly applicable rule of international law on cyber operations also makes the decision to initiate a legal confrontation less appealing to disputing parties.

For comparison, international disputes around cyber-related measures – such as digital surveillance measures, data localisation measures, cyber security review measures, etc. – are more often brought to courts as legal disputes. Chinese participants tended to ascribe this to the maturity of the relevant international rules, because disputes around cyber-related measures involve a natural link to more developed branches of international law such as international human rights law and international investment law.

Both groups of participants agreed on the importance of a clearer cyber attribution mechanism. The political willingness of relevant states to deal

with this issue was repeatedly mentioned in the discussion of this problem. Citing the Budapest Convention as an example, in particular its Second Protocol on enhanced cooperation and the disclosure of electronic evidence, some participants expressed concerns that although regional consensus may be easier to reach, it would be very hard to establish any binding mechanism for the attribution of cyber operations that major players would accept. Still, some discussants expressed their belief in the feasibility of a concrete cooperative arrangement, such as a joint programme for developing expertise on cyber security or a commonly approved standard procedure for the attribution of cyber operations.

The state party in a cyber dispute is likely to adopt self-help measures such as unilateral sanctions and so-called restrictive measures, the legality of which was briefly touched upon in the discussions. These measures may be carried out according to domestic law, targeting individuals or private entities from the opposing state disputant. In such a case the legality test for countermeasure under international law may not necessarily be fulfilled. However, to justify self-help measures targeting the opposing state as a possible countermeasure, one should first verify various procedural and substantive conditions required for a legal countermeasure, mostly set out in Article 52 of the Articles on the Responsibility of States for Internationally Wrongful Acts. No detailed discussions were held on exactly how such conditions should be evaluated or developed to adapt to a cyber-related scenario.

The participants also referred to an international forum suitable for resolving disputes over cyber operations. A Chinese speaker offered a tentative explanation of why the ICJ may not be an ideal candidate for such a forum, because relevant states tend to perceive – if not overemphasise – cyber disputes as an issue of high politics closely related to their core national interests. To hand such a case over to the ICJ means uncertainty as to the possible outcome, which powerful states desperately try to avoid.

A few points on the peaceful non-settlement – instead of the settlement – of cyber disputes were made to diversify the discussion. In this regard, analogies were drawn with actions such as shelving the dispute and seeking joint development in the Sino-Japanese territorial dispute in the 1970s, and the proposal to freeze all claims of sovereignty over any part of Antarctica in the 1959 Antarctica Treaty. This indicates the need for more theoretical research, rather than mere doctrinal research on how to apply international rules to cyber-related matters.

Presentations and discussions in this session showed a high level of convergence between the European and Chinese participants, especially on the severity and nature of the cyber operation attribution problem, as well as its ability to impede the settlement of cyber disputes. The importance of clarifying existing international rules on cyber operations and potentially developing them further – both primary and secondary – was once again affirmed.

3.4 Law of armed conflict

The fourth session was dedicated to applying the law of armed conflict (LOAC) in cyberspace. Once again, a concrete case study was used to initiate discussion.

A fundamental divergence between the two groups was notable throughout this session. European participants tended not to question the applicability of LOAC rules in cyberspace, and identified the key issue as being how to reasonably interpret these rules. From the perspective of Chinese participants, however, the uniqueness of cyberspace renders the application of outdated LOAC rules quite challenging, if not unrealistic. It was brought to the participants' attention that the current system and wording of LOAC rules were developed at a time when mechanised warfare dominated and a specific pattern of international political relationships was in place. Key pairs of concepts in the LOAC such as peace v. wartime, neutrality v. co-belligerency and civilians v. combatants all become blurred in a cyber scenario. As a result, Chinese speakers suggested that we should inherit the spirit rather than the rules of the LOAC, so that principles such as the protection of civilians and restrictions on the misuse of military power could be better applied in the modern context.

There was some discussion on whether and when cyber operations constitute an attack within the meaning of international law. As a starting point, discussants generally referred to the *Tallinn Manual* approach, which evaluates this threshold problem mainly from the effect that cyber operations cause. A European participant clarified that while the *Tallinn Manual* is in no way a formal source of law, a similar approach of applying a legal test can be found in the ILC's 2001 *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*. Questions were raised as to what kind of non-physical effects caused by cyber operation may be seen as an attack, but no conclusions were reached. In this regard, confusing definitions of critical infrastructure were also raised as a problematic issue.

A number of legal issues emerged from the case study of a crowd-sourced cyber attack. To determine the legal consequence of private entities participating in a pre-existing international armed conflict, relevant International Committee of the Red Cross standards on direct participation in hostilities could arguably apply, the three constitutive elements of which are threshold of harm, direct causation and belligerent nexus. A Chinese discussant expressed scepticism regarding the possibility of evaluating the element of harm or causality in such an analysis. This is consistent with the overall Chinese view on the possibility of applying the LOAC in cyberspace. Whether or not a private entity that participated in a conflict would lose both its civilian status and the accompanying LOAC protections during the conflict, and whether or not its participation would make its home state a co-belligerent to an armed conflict could only be determined after the provision of more details in different scenarios.

A European discussant suggested that the term "ensure respect" in Article 1 common to the four Geneva Conventions could be read as imposing a type

of “due diligence” obligation on contracting parties. This led the discussion back to the thematic topic of the second session. A Chinese discussant pointed out that, even if the due diligence rule in the *Tallinn Manual* were accepted, the risk of imposing an excessive burden on states would be stark, especially if the aim of exercising due diligence is to avoid “serious adverse consequence” by adopting “reasonable available measures”, both of which are terms that may lack quantified criteria for their interpretation.

Chinese participants suggested the possibility of absorbing specifically hackers and hacking activities into the LOAC regime. They believed this might help to enhance the legal clarity of the issues involved, which could in turn help to bind the actors and promote conformity with international law. No strong echo by the European side was recorded vis-à-vis this suggestion.

As the presentations and discussions during this session showed, the level of divergence among the participants with regard to applying the LOAC in cyberspace may have been the highest of all four sessions. This divergence goes all the way to the fundamental methodological choice that needs to be made regarding this issue: should we adopt primarily a doctrinal approach to focus on the interpretation of existing LOAC rules as they could apply in cyberspace, or an evolutionary approach that would inherit the key values of the LOAC while adapting LOAC rules to the specific features of cyberspace?

4. Ways forward

The closing session of the second meeting of the EWG-IL was notably dedicated to reflecting on both the discussions that had taken place during the meeting and possible ways forward for the EWG-IL process.

The participants highlighted the quality of the exchanges and their interest in the interactive process that characterised the meeting, which notably allowed them to identify convergences and divergences between European and Chinese scholars. In addition to identifying differences in the approaches of each group, this interactive process also allowed participants to identify the differences in both the development and maturity of the discussed topics in European and Chinese scholarship and in the approaches and practices of states.

Building on these observations, three elements were discussed for future attention. The first was the process of organising the third meeting of the EWG-IL in 2023, which is to be convened by the Chinese facilitators. The participants expressed their interest in holding this meeting in person. Secondly, the possibility was discussed of convening small research groups comprising a more limited number of participants who would meet more regularly and focus on a specific topic in preparation for the next meeting. Thirdly, the participants discussed the need for concrete outcomes to emerge from the EWG-IL process such as joint EWG-IL publications.

About the partner organisations

China Institutes of Contemporary International Relations

The China Institutes of Contemporary International Relations (CICIR) is a longstanding, 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 is an international foundation serving a global community of organisations and individuals. Its mission is to advance peace, security, and international cooperation by providing the knowledge, skills, and network for effective and inclusive decision-making through executive education, diplomatic dialogue, research, and policy advice.

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