GCSP
Geneva Centre for Security Policy

EU CYBER DIRECT

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

Countermeasures in Cyberspace

Hui Chen, Antonio Coco, François Delerue, Lixin Zhu

Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL), Research Group Report 2024

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
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-019-8

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 (GCSP) is an international foundation that aims to advance global cooperation, security, and peace. Governed by 55 Member States, this flagship foundation is supported by the Swiss government to provide a unique 360° approach to learn about and solve global challenges. Our mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions for 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.

Background

This report has been produced in the context of a larger research and dialogue project: The China Institutes of Contemporary International Relations (CICIR), the EU Cyber Direct, the Geneva Centre for Security Policy (GCSP), and Xiamen University convene a joint Sino-European Expert Working Group on the Application of International Law in Cyberspace (WG IL). The working group provides a platform for exchange among European and Chinese legal experts to examine the application of international law in cyberspace. The main goal of the work in research groups is to provide more thorough analysis of the selected topics and identify points of divergence and convergence between European and Chinese side with the purpose to create more evidence-based and trusted environment for the policy discussions in track 1.5. and track 1 processes.

Authors

Hui CHEN, Assistant Researcher, Institute of Cyberspace Governance, Wuhan University

Antonio COCO, Associate Professor (Senior Lecturer), Essex Law School, University of Essex

François DELERUE, Assistant Professor of Law, IE University

Lixin ZHU, Researcher, Xi'an Jiaotong University Institute of Techonlogy and Education Development

Acknowledgement

On the European side, this report was sponsored by the Swiss Department of Foreign Affairs, whose generous support is greatly appreciated. The constructive feedback and valuable insights of the reviewers, Liis VIHUL and Fan YANG, whose expertise has contributed to the quality of this publication, are also acknowledged with gratitude.

Contents

1. The concept of countermeasures and its applicability in cyberspace

The term "countermeasure" generally refers to a measure taken to counteract or offset another.[1] It has been used in various contexts, including law, defence, medicine, engineering, pollution prevention, and computer security.[2] In international law, however, the concept of countermeasures[3] has a specific meaning. Over the past century, "countermeasures" gradually replaced the concept of reprisals.[4] In 1978, the arbitral tribunal in the *Air Services Agreement* case[5] was one of the first to use the term "countermeasures," and the International Court of Justice (ICJ) referred to it for the first time in the *Tehran Hostages* case in 1980.[6]

The International Law Commission (ILC) selected the topic of "the law of State responsibility" in 1949[7] and published the final version of the *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA) in 2001.[8] The ILC's work, aimed at codifying customary international law on state responsibility, devotes considerable attention to clarifying the rules on countermeasures, as well as other principles, such as those governing the attribution of conduct to a state. Although ARSIWA does not define countermeasures, the term is widely understood to refer to unilateral acts that would otherwise be internationally wrongful, but whose wrongfulness is precluded because they are taken in response to a prior internationally wrongful act by another state.

Even after more than two decades, countermeasures remain one of the most controversial aspects of the work of the ILC and ARSIWA.[9] On the one hand, the acknowledged value of countermeasures lies in the fact that, in an international community lacking a centralised authority that could uphold the legitimate interests of each state and ensure compliance with international law, they provide states with a means to safeguard their interests and restore international order in a decentralised manner. On the other hand, countermeasures may provide powerful states with a strong justification for engaging in controversial behaviours. James Crawford, the last special rapporteur on state responsibility for the ILC, noted that "countermeasures — especially collective countermeasures — remain

1 A. Stevenson (ed), "Countermeasure", Oxford Dictionary of English (3rd edn.), Oxford University Press 2015.

2 F. Delerue (2020) Cyber Operations and International Law, Cambridge, Cambridge University Press, p. 434.

3 On countermeasures, see, generally: C. Leben, "Les contre-mesures inter-étatiques et les réactions à l'illicite dans la société internationale" [1982] Annuaire français de droit international 9; O.Y. Elagab, *The Legality of Non-Forcible Counter-Measures in International Law* (Oxford University Press 1988); E. Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational 1984); L.A. Sicilianos, *Les réactions décentralisées à l'illicité: des contre-mesures à la légitime défense* (LGDJ 1990); C. Focarelli, *Le contromisure nel diritto internazionale* (Giuffrè 1994); Y. Matsui, "Countermeasures in the International Legal Order" [1994] The Japanese annual of international law 1; D. Alland, *Justice privée et ordre juridique international: étude théorique des contre-mesures en droit international public (A Pedone 1994); M. Noortmann, Countermeasures in International Law: Five Salient Cases* (Gadjah Mada University Press 2005); M.E. O'Connell, *The Power and Purpose of International Law: Insights from the Theory and Practice of Enforcement* (Oxford University Press 2008); J. Crawford, A. Pellet and S. Olleson (eds), *The Law of International Responsibility* (Oxford University Press 2010) 1127–1214; J. Crawford, *State Responsibility: The General Part* (Cambridge University Press 2013) 684–712.

4 M. Noortmann, *Enforcing International Law: From Self-Help to Self-Contained Regimes* (Ashgate 2005) 35; O'Connell (n 3) 233.

5 *Air Service Agreement of 27 March 1946 between the United States of America and France* (1978) 18 RIAA 417.

6 *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (Judgment) [1980] ICJ Reports 3, 27–28 para 53.

7 ILC (International Law Commission) (1949) "Survey of International Law and Selection of Topics for Codification", Yearbook of the International Law Commission, 1, pp. 279, 281; Crawford, 2013, pp. 35-44.

8 ILC (International Law Commission) (2001) "Articles on Responsibility of States for Internationally Wrongful Acts", adopted at the fifty-third session, annexed to UN General Assembly Resolution 56/83, 12 December, A/56/49(Vol I)/Corr4.

9 Crawford, 2013, p. 675.

deeply controversial, associated as they are with a history of power politics and gunboat diplomacy in international relations."[10]

Therefore, both European and Chinese teams converge in emphasising the pivotal role of countermeasures within the framework of existing international law. They unanimously recognise countermeasures as a firmly established set of rules of customary nature, making them applicable in cyberspace. Consequently, those digital actions taken in cyberspace in response to an unlawful operation, such as retaliatory hacking or disrupting an adversary's networks, could be categorised as cyber countermeasures. However, they also acknowledge the potential for abuse inherent in the notion's application, necessitating stringent substantive and procedural requirements to ensure their proper use.

During the discussion, the authors diverged in their approaches to the question of whether resorting to countermeasures is automatically permitted in cyberspace.

The European team believes that, as a general rule and unless more specific rules emerge, customary international law is applicable to state activity in cyberspace,[11] and this includes the law relating to countermeasures. In this respect, the substantive and procedural conditions for resorting to countermeasures outlined in the ILC work on state responsibility represent the law applicable by default with respect to state activity in cyberspace and provide guarantees against abuse of the notion of countermeasures.

However, the Chinese team tends to adopt a different approach, emphasising that countermeasures involve a complex interplay of authorisation and restriction. They argue that countermeasures can only be considered permissible if it is ensured that every rule within this framework remains diligently observed and fulfils a practical, equivalent role in the cyber context.[12] In other words, the Chinese team observes that, unless a new consensus emerges, cyber countermeasures are only generally permissible under the condition that the balance between the ease with which a state can take countermeasures and the restrictions necessary to prevent abuse in cyberspace mirrors that found in traditional environments. However, as countries are still debating how various elements should be applied in cyberspace, it is unclear whether this balance can be maintained. Therefore, it is difficult to provide a definitive answer on whether resorting to countermeasures is permitted at present. The Chinese team emphasises that, in the future, if guided by this principle, permissibility could be achieved through countries clarifying how countermeasures are applied in cyberspace.

Most interpretative statements, predominantly from developed states, regarding how international law applies to cyberspace include the possibility for an injured state to resort to countermeasures against the wrongdoing state.[13] Conversely,

10 Ibid., p. 684.

11 D. Akande et al. (2022) "Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies", International Law Studies, 99, pp. 4-36.

12 The Chinese team provide "electronic signature" as an illustrative example. When determining whether electronic signatures should be permitted in the digital environment, we apply the principle of functional equivalence. An electronic signature can only be recognised as having the same legal effect as a traditional handwritten signature if it can identify the signer's identity and intention through certain technical means, providing comparable functionality. Therefore, only a "Reliable Electronic Signature", as defined in the UNCITRAL Model Law on Electronic Signatures, or a "Qualified Electronic Signature", as defined in the EU eIDAS Regulation, is legally recognised.

13 CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) "Countermeasures", Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Countermeasures.

some developing countries express greater apprehension over the difficulty of clearly articulating and imposing restrictions on cyber countermeasures, leading to their reluctance to publicly endorse their permissibility. For instance, among the nations that have publicly stated their positions or opinions, four states — Iran,[14] Kazakhstan,[15] Kenya,[16] and Pakistan[17] — along with the African Union, have remained silent on the issue of cyber countermeasures. Additionally, Brazil took a critical stance and called into question the ILC's approach, questioning whether they went further than codifying existing customary international law regarding countermeasures.[18]

In this regard, the Chinese team cited China as a specific example to explore whether the requirements for applying countermeasures in cyberspace can be clearly defined through universal and equal negotiation within the United Nations framework.[19] In particular, they questioned whether these requirements could be appropriately restricted — such as by reinforcing the principle of peaceful settlement of international disputes and limiting erroneous attribution.[20] The outcome of this process will influence whether developing countries like China are willing to affirm both the applicability and feasibility of countermeasures.

In 2001, when commenting on ARSIWA, the Chinese government generally acknowledged the status of countermeasures in international law, providing that "countermeasures must be accompanied by appropriate restrictions on their use, in order to strike a balance between the recognition of the legitimacy of countermeasures and the need to prevent their abuse."[21] However, in 2017, precisely due to concerns about the abuse of countermeasures, along with the militarisation of cyberspace, which could escalate conflicts between states, China strongly opposed the United Nations Group of Governmental Experts on Information Security's (UNGGE) report on introducing cyber countermeasures.[22] However, given China's urgent need to counter foreign sanctions, including but not limited to those imposed in cyberspace, some punitive measures outlined in the Anti-Foreign Sanctions Law may require justification as countermeasures.[23] Therefore, China is unlikely to oppose, and indeed no longer strongly opposes,

14 Iran (2020) "General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat", NOURNEWS Analytics & News Agency, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

15 UNGA (UN General Assembly) (2021) "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266", UN Doc A/76/136, pp. 51-52.

16 Ibid., pp. 52-54.

17 Pakistan (2023) "Pakistan's Position on the Application of International Law in Cyberspace", https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf.

18 United Nations General Assembly (n 15) 21.

19 China (2021) "China's Positions on International Rules-making in Cyberspace", https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf; China (2017) "International Strategy of Cooperation on Cyberspace", Xinhua, 1 March, http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm.

20 A.E. Levite et al. (2022) "Managing U.S.-China Tensions Over Public Cyber Attribution", Carnegie Endowment for International Peace, 28 March, https://carnegieendowment.org/research/2022/03/managing-us-china-tensions-over-public-cyber-attribution#a-chinese-perspective-on-public-cyber-attribution.

21 State Responsibility: Comments and observations received from Government, A/CN.4/515, 2001, p.82.

22 Permanent Mission of the People's Republic of China to the UN (2017) "Statement by Counsellor Sun Lei of the Chinese Delegation at the Thematic Discussion on Information and Cyber Security at the First Committee of the 72nd Session of the UNGA", 23 October, http://un.china-mission.gov.cn/eng/chinaandun/disarmament_armscontrol/unga/201710/t20171030_8412335.htm.

23 For example, measures such as "sealing up, seizing and freezing movable, immovable and other types of property in China" and "prohibiting or restricting organisations and individuals within the territory of China from conducting transactions, cooperation or other activities with them" may conflict with China's trade obligations under WTO rules or other bilateral or multilateral trade and investment agreements. Therefore, countermeasures can serve as a legal basis for those measures. For relevant Chinese academic papers, see Z. Hui, "Whether Unilateral Sanctions Have Legality: A Framework Analysis" (2022) 3, China Legal Science. H. Zhengxin, "An Interpretation of the Anti-Foreign Sanctions Law of China under International Law" (2021) 4, Journal of Comparative Law.

the application of countermeasures in cyberspace. Instead, it typically maintains silence and welcomes thorough discussions regarding the requirement of cyber countermeasures, particularly the restrictive components, while remaining vigilant against any potential excessive development.

In this context, experts from both the European and Chinese sides recognise the importance of the following detailed discussion on the substantive and procedural requirements of countermeasures with respect to activity in cyberspace.

2. The substantive conditions for resorting to countermeasures with respect to activities in cyberspace

The substantive conditions for resorting to countermeasures — specifying both the circumstances under which a state can take countermeasures and the limitations with which a state must comply in the process — established in general international law apply equally with respect to activities in cyberspace.

2.1 Prior existence of an internationally wrongful act

Both teams agreed that the right to resort to countermeasures arises exclusively after an internationally wrongful act has occurred.[24] The concept of countermeasures in international law is fundamentally reactive, not proactive, and therefore simply cannot be invoked to justify conduct that is anticipatory, preventive, or pre-emptive of a (possible, future, or even imminent) internationally wrongful act.

In keeping with the general principle that damage is not a requirement for the existence of an internationally wrongful act, both teams agreed that the lack of physical damage does not impede justified countermeasures. However, the European team notes that lack of physical damage may affect the assessment of the necessity and proportionality requirements. The Chinese team added that, given the lack of clear international consensus on what constitutes wrongful acts in cyberspace, countermeasures taken before actual damage occurs risk leading to disputes and conflict.

As recognised by the ILC, a state taking countermeasures acts at its peril. Both teams agreed that, if a state's assessment of the prior existence of an internationally wrongful act is incorrect, that state risks incurring responsibility for its own wrongful conduct.[25] Simply believing in good faith that a prior internationally wrongful act existed is insufficient. Without an objectively established wrongful act, the countermeasures taken will be unjustified and, thus, unlawful.[26]

National positions of European states on this matter confirm the critical need for accurate attribution and justified grounds before taking countermeasures.[27] For the European team, the strict substantive and procedural requirements for lawfully engaging in countermeasures exist also to prevent abuse. The state taking countermeasures becomes responsible for an internationally wrongful act of its own if it does not satisfy these conditions.

The Chinese team, on its part, believes that relying solely on a state's self-confidence in the pre-existence of an internationally wrongful act leaves too much

24 "Fundamental prerequisite" per ARSIWA Commentaries Art 49, p. 130, § 2. See *Gabčíkovo-Nagymaros Project* (Hungary/Slovakia) [1997] ICJ Rep 7, 55, para 83; *Naulilaa* (Portugal v Germany) (1928) 2 RIAA 1011, 1027; *Cysne* (Portugal v Germany) (1930) 2 RIAA 1041, 1057. See also Delerue (n 2) 438.

25 ARSIWA Commentaries Art 49, p. 130, § 3.

26 F. Paddeu (2015) "Countermeasures", Max Planck Encyclopedia of Public International Law, para. 18, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1020.

27 Estonia (2019) "President of Estonia: International Law Applies Also in Cyberspace", 29 May UNODA (United Nations Office for Disarmament Affairs) (2021) "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States", A/76/136, August, p. 73.

room for abuse[28] and that more study and legal developments are required with respect to the question of attribution, which is a prerequisite for lawfully engaging in countermeasures.

2.2 Aim of countermeasures

Both teams agree that countermeasures serve an instrumental purpose in international law; they are designed to prompt the cessation of and reparation for an internationally wrongful act, not to punish the responsible state. The primary aim of countermeasures is to restore a condition of legality between the injured state and the responsible state. If they successfully induce the responsible state to fulfil its obligations of cessation and reparation, countermeasures should be terminated.[29] In fact, according to Article 49(1) ARSIWA, countermeasures may *only* be taken by an injured state to induce the responsible state to comply with its obligations under Part Two of the Articles. These include ceasing the internationally wrongful act, if it is ongoing, and providing reparation to the injured state. Thus, countermeasures are a tool for enforcing compliance with international law, emphasising the restoration of legal order and rectification of wrongful acts rather than retribution.[30]

2.3 Addressee of countermeasures

According to Article 49, paragraphs 1 and 2 ARSIWA, countermeasures must be directed only at the responsible state and not at third parties.[31] They work as a circumstance precluding wrongfulness in the relationship between an injured state and the state that has committed the internationally wrongful act.[32]

However, this does not exclude incidental effects on third states or other third parties. For example, the suspension of a trade agreement may affect trade with the responsible state, potentially causing business losses or bankruptcies for companies; such indirect effects are sometimes unavoidable.[33] A question remains as to whether the indirect effects of countermeasures on third states and other third parties should be considered as part of the proportionality assessment. The European team is inclined to answer that it should. Additionally, the Chinese team emphasises that taking into account the proliferation and amplification effect of cyberspace, when an injured state considers various countermeasures, it should prioritise those with minimal incidental impact on other states or take necessary steps to mitigate potential collateral effects.

Both teams agree that if a harmful cyber operation originates from a third state (e.g., from a controlled zombie server located in a third country's territory), the

28 Chinese Delegation to the Open-ended Working Group on ICT Security (2021) "Statement at the Seventh Plenary Meeting on the Application of International Law", 16 December, https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-7th-plenary-meeting_international-law_DEC-16-AM_CHN.pdf.

29 ARSIWA Commentaries Art 49, pp. 130-131, § 7.

30 ARSIWA Commentaries Art 49, p. 130, § 1. In this sense, among other states: New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, 3.

31 ARSIWA Commentaries Art 49, p. 130, § 4.

32 ARSIWA Commentaries Art 22, pp. 75-76, § 5, citing *Cysne* (n 22) at 1055-1056) and *Gabcíkovo-Nagymaros Project* (n 22), p. 55, para. 83.

33 ARSIWA Commentaries Art 49, p. 130, § 5. In this respect, it must be noted that, per Denmark's national position, this 'does not necessarily exclude that actions may in some circumstances be directed against non-State actor as part of countermeasures.' See Government of Denmark, "Denmark's Position Paper on the Application of International Law in Cyberspace"(4 July 2023).

injured state can only take countermeasures against that third state if it claims that the third state committed an internationally wrongful act of their own by having, for instance, failed to comply with its ("due diligence") obligation to not knowingly allow its territory (or infrastructure under its control) to be used for acts contrary to the rights of other states.[34] If the third state has committed an internationally wrongful act by breaching its due diligence obligations — like the one just mentioned — then the injured state may resort to countermeasures, provided the relevant substantive and procedural requirements are met.

The state engaging in countermeasures remains responsible for any damage caused to states other than the state responsible for the initial internationally wrongful act. If the rights of a third state are impaired by the countermeasure, the injured state will be responsible for breaching its obligations vis-à-vis the third state[35] and, as such, will be obliged to cease its own internationally wrongful act, offer guarantees of non-repetition and provide reparations. In this case, each state injured by an internationally wrongful act has an independent right to take countermeasures proportional to the harm it suffered.

2.4 Prohibited countermeasures

Both teams agree that, under Article 50(1)(a) of ARSIWA, countermeasures must be non-forcible. The ILC notes that the prohibition on forcible countermeasures is widely supported by extensive literature and consistent judicial decisions. This principle has also been explicitly stated in numerous international legal instruments, such as the *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States* in accordance with the Charter of the United Nations.[36] Thus, no matter the seriousness of the internationally wrongful act in question, the injured state cannot lawfully invoke countermeasures to justify conduct (even by cyber means) that amounts to the use of force.[37] The Chinese team notes how keeping countermeasures below the use of force threshold is especially significant in preventing them from being abused as a tool of military intervention.

Both teams note that Article 50 ARSIWA specifies obligations that cannot be suspended through countermeasures, including those protecting fundamental human rights. The Chinese team notes that although international law does not clearly define fundamental human rights, they understood them as involving the core parts of a person's right to life, liberty, and security, as codified in the Universal Declaration of Human Rights.[38] Some interpretations or issues that have emerged in cyberspace may provide new understandings of traditional

34 *Corfu Channel* (United Kingdom v. Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22.

35 Paddeu, 2015, para. 41.

36 ARSIWA Commentaries Art 50, p. 132, § 5. Citing *Corfu Channel*, (n 32) at 35; and Military and Paramilitary Activities in and against Nicaragua, p. 127, para. 249. See, e.g., Security Council resolutions 111 (1956) of 19 January 1956, 171 (1962) of 9 April 1962, 188 (1964) of 9 April 1964, 316 (1972) of 26 June 1972, 332 (1973) of 21 April 1973, 573 (1985) of 4 October 1985 and 1322 (2000) of 7 October 2000. See also General Assembly resolution 41/38 of 20 November 1986.

37 M. Roscini (2014) Cyber Operations and the Use of Force in International Law, Oxford, Oxford University Press, pp. 105-107; H. Lahmann (2020) Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution, Cambridge, Cambridge University Press, p. 130; Delerue, 2020, pp. 442-443.

38 UNGA (United Nations General Assembly) (1948) "Universal Declaration of Human Rights", Article 3.

human rights,[39] may constitute human rights themselves,[40] or may act as ancillary rights that can facilitate the realisation of fundamental human rights.[41] However, whether any rights in cyberspace have individually become fundamental human rights is still doubtful. At least at this stage, when observing national practices, it appears that the right to internet access is still frequently restricted under specific circumstances, and, thus, it is not yet unequivocal that it constitutes a fundamental human right.

The European team notes that, by reading the ILC commentary on the point, it appears that the "fundamental" human rights in question are those that cannot be derogated in times of emergency or that are necessary for survival.[42] It would be, at the very least, a stretch to argue, at present, that these rights include a right to internet access. However, any countermeasure impinging on human rights is bound to respect the principles of necessity and proportionality to be lawful.

Both teams further note that Article 50 ARSIWA also lists other obligations that cannot be suspended through countermeasures. These include obligations of a humanitarian character prohibiting reprisals,[43] obligations under peremptory norms of general international law (*jus cogens*)[44] and those established for the protection of the inviolability of diplomatic or consular agents, premises, archives, and documents.[45] This ensures that essential principles and norms of international law are upheld even during the implementation of countermeasures. Additionally, obligations under any dispute settlement procedure applicable between the injured and responsible state must be upheld to ensure fair and effective resolution processes.[46] Countermeasures may also be prohibited by a *lex specialis*: for instance, resort to countermeasures is excluded within the legal systems of European Union Law and of the World Trade Organization.[47]

2.5 Necessity and proportionality

Article 51 ARSIWA requires that countermeasures taken in response to an internationally wrongful act must be proportionate — a requirement additional to that of necessity.[48] This means that the countermeasures should be commensurate with the injury suffered and the gravity of the wrongful act. Proportionality must be assessed in terms of both a quantitative element (the injury suffered) and qualitative factors like the interests protected and the seriousness of the breach.[49] Proportionality must also take into account "the rights in question", an expression encompassing the rights of the injured state, those of the responsible state and, if relevant, the position of other states.[50] It has been acknowledged

39 E.g. it could be argued that freedom of online speech could be a new manifestation of the right to liberty and of the right to freedom of expression.

40 E.g. a right to internet access.

41 E.g. a right to cybersecurity, which could more fully safeguard the right to liberty and security.

42 ARSIWA Commentaries Art 50, p. 132, §§ 6-7.

43 ARSIWA Commentaries Art 50, § 8, p. 132.

44 ARSIWA Commentaries Art 50, pp. 132-133, § 9.

45 ARSIWA Commentaries Art 50, pp. 133-134, §§ 14-15.

46 ARSIWA Commentaries Art 50, p. 133, §§ 12-13.

47 Paddeu, 2015, para. 22. See Article 55 ARSIWA on the point.

48 ARSIWA Commentaries Art 51, p. 135, § 7.

49 ARSIWA Commentaries Art 51, p. 135, § 6.

50 ARSIWA Commentaries Art 51, p. 135, § 6. See also Paddeu (2015) para 23.

that assessing the proportionality of countermeasures is a task that may require some level of approximation.[51] The ILC noted that the proportionality requirement is essential to ensure that countermeasures are lawful and do not escalate conflicts unnecessarily.[52]

The Chinese team notes that, in practice, the question of how to determine the proportionality of a countermeasure is still a controversial issue because it is difficult to make comparisons when combining different qualitative and quantitative judgments, so even the criteria adopted by the ICJ, for instance in the *Gabčíkovo-Nagymaros Project case*, remain unclear in practice.

Both teams agree that there is no requirement that countermeasures amount to the non-performance of the same obligation breached in the internationally wrongful act in question or a closely related obligation.[53] Resort to countermeasures may even entail the non-performance of more than one obligation.[54] With respect to countermeasures relating to cyber operations, it has been acknowledged by several states that "countermeasures against cyber operations can be non-cyber in nature, and cyber countermeasures may be adopted in response to non-cyber wrongful acts."[55]

Both teams note that the adoption of "in-kind" countermeasures (i.e. the non-performance of the same obligation breached by the allegedly responsible state or of closely related obligations) may make it easier to establish their proportionality.[56] However, the Chinese team warns that the position warrants further consideration. Although the actual damage may be comparable, the degree of perception of the harm may vary. For example, the same cyber-attack that disconnects the internet causes significantly different implications for cyber-developed and underdeveloped countries, so they may respond to the same obligation breached with different countermeasures to ensure proportionality. This is particularly evident when considering the non-performance of the same obligation breached may not necessarily trigger similar feelings of being aggrieved by the responsible state. For example, responding in a manner that violates cyber sovereignty will be treated significantly differently by China, which highly values it, and the UK, which doesn't recognise it as an applicable international rule. Ultimately, to urge the responsible state to correct its behaviour, the pressure exerted by countermeasures lies precisely in the perception of harm, rather than the actual harm. Response in-kind only provides a convenient starting point for thinking about proportionality rather than an endpoint.

The European team notes that the proportionality principle ensures that the countermeasures are not excessive and aim to induce the responsible state to comply with its obligations rather than to punish. The Chinese team notes that countermeasures should be limited to what is necessary to restore the legal relationship between the responsible state and the injured state. In this view, the

51 *Air Service Agreement* (n 5), 443 para. 83.

52 ARSIWA Commentaries Art 51, p. 135, § 7.

53 ARSIWA Commentaries Art 22, pp. 75-76, § 5, *Cysne* (n 22) at 1055-1056) and *Gabcíkovo-Nagymaros Project* (n 22), p. 55, para. 83. See also ARSIWA Commentaries p. 129, § 5.

54 ARSIWA Commentaries Art 49, p. 130, § 6.

55 "Countermeasures" (*International cyber law: interactive toolkit*, 20 May 2024) https://cyberlaw.ccdcoe.org/wiki/Countermeasures accessed 9 June 2024. See e.g. the positions of Canada, Germany, Italy, Japan, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

56 Air Service Agreement, 1978, p. 443, para. 83

assessment of proportionality should focus more on achieving this restorative purpose rather than on imposing equivalent harm.

2.6 Temporariness and reversibility

Both teams agree that countermeasures are a tool to induce compliance with the breached rule and with the responsible state's obligations to cease the internationally wrongful act and provide reparation. For this reason, countermeasures are temporary and must be "as far as possible" reversible in their effects.[57] By effect of the expression "as far as possible", the injured state — if faced with the choice of several lawful and effective countermeasures — must resort to the one(s) that would allow it to resume performance of the related obligations after their purpose has been served.[58]

57 Arts 49(2-3), and 53 ARSIWA.

58 ARSIWA Commentaries Art 49, p. 131, § 9.

3. The procedural requirements for the adoption of countermeasures with respect to activities in cyberspace

Article 52(1)(a) of ARSIWA requires an injured State to call upon the responsible State to fulfil its obligations of cessation and reparation before taking countermeasures. This requirement of prior demand, sometimes referred to as "sommation", is supported by general practice and relevant judicial decisions. This requirement, from which Article 52 does not envisage derogations, ensures that the responsible state is given a chance to provide a response and, if the case, cease the wrongful act and provide reparations, with the aim of avoiding immediate escalation.[59] Although there is controversy over how to specifically comply with these regulations in practice, both teams believe that this procedural requirement should apply to countermeasures related to cyber operations, ensuring the allegedly responsible state is aware of the issue and has a chance to rectify it.

3.1 Prior recourse to dispute settlement procedures

During the further discussion, a divergence emerged as to whether any available dispute settlement procedures should be resorted to before resorting to countermeasures.

The European team follows the position of the ILC articulated in ARSIWA 2001. Countermeasures, in accordance with Article 52(1)(b) ARSIWA, must normally be preceded by an offer to negotiate. Moreover, Article 52(3) requires countermeasures to be suspended (or not to be adopted in the first place) if the internationally wrongful act has ceased and the dispute is pending before an adjudicative body that has the authority to take binding decisions for the parties. This ensures that countermeasures are temporary and respect judicial processes. Article 52(4) ARSIWA, instead, allows the continuation of countermeasures if the responsible State fails to engage in dispute settlement in good faith, seeking to prevent abuse of these mechanisms and encouraging genuine resolution efforts.

The Chinese team prefers to go a step further, arguing that by stating in Article 52(1)(b) of ARSIWA that "injured states shall notify the responsible State of any decision to take countermeasures and offer to negotiate with that state" before taking countermeasures, the ILC intended to encourage the resolution of disputes through peaceful means beforehand. However, considering that more and more states advocate for the adjustment of some procedural requirements for countermeasures in cyberspace, especially emphasising the exclusion of the application of Article 52(1)(b) in urgent circumstances, the Chinese team, based on the balanced approach proposed in Section 1, believes that the requirement articulated in the second half of Article 52(1)(b) should be further strengthened to balance the insufficient restrictions caused by the exemption from the obligation to provide prior notice of countermeasures in urgent circumstances. Therefore, when a responsible state commits an internationally wrongful act, the injured

59 ARSIWA Commentaries Art 52, p. 136, §§ 4-5.

state should first seek to settle the dispute in any circumstances through "any" available means of dispute settlement rather than through countermeasures. Since it is not required to exhaust all available settlement procedures, they consider it acceptable as negotiation is always an available and simple way through which one party can request the other to resolve actual disputes, even in urgent circumstances.[60]

3.2 The requirement of prior notification

The requirement of prior notification continues to apply in cyberspace. It is a necessary step to encourage the responsible state to self-correct its wrongful conduct or to promote the peaceful resolution of disputes between the two states in good faith. In fact, considering the difficulty in tracing activities in cyberspace, prior notification also provides the parties with an opportunity to further clarify the facts and avoid misjudging responsibility.

According to Article 52(1)(b) ARSIWA, a state taking countermeasures is required to notify the responsible state of any decision to take countermeasures and offer to negotiate with that state. The commentary clarifies that this allows the responsible state another opportunity to comply with its obligations before countermeasures are applied.[61]

The injured state is under no obligation to specify which countermeasures it plans or intends to adopt, even though specificity could be more effective in inducing the allegedly responsible state to abide by its obligations.[62]

No predetermined temporal relationship exists between the two kinds of notification referred to in subparagraphs (a) and (b) of Article 52(1) ARSIWA — meaning that they could be made at the same time or close to each other.[63]

3.3 Urgent countermeasures

Article 52(2) ARSIWA provides that the injured state can take urgent countermeasures as necessary to preserve its rights. The article acknowledges an exception to the requirement contained in Article 51(1)(b), namely that of notifying the allegedly responsible state of the decision to take countermeasures and of offering to negotiate with that state. The exception reported in Article 52(2) ARSIWA does not extend to the requirement to call upon the allegedly responsible state to cease and repair the internationally wrongful act, which remains a procedural condition for resorting lawfully to countermeasures.

However, the word "urgent" encompasses both substantive and procedural aspects. Due to the lack of discussion and consensus on what constitutes "urgency" in cyberspace in terms of substantive conditions, there are different views on how "urgent countermeasures" should be applied procedurally. The European

60 C. Tomuschat (1994) "Are Counter-measures Subject to Prior Recourse to Dispute Settlement Procedures?", European Journal of International Law, 5, pp. 84-87.

61 ARSIWA Commentaries Art 52, p. 136, § 5.

62 Paddeu, 2015, para. 27.

63 ARSIWA Commentaries Art 52, p. 136, § 5.

team believes that the exception to prior notification comes into play for urgent countermeasures that are necessary to preserve the rights of the injured state, meaning both the injured state's rights in the subject matter of the dispute and the injured state's right to take countermeasures.[64] Specifically, a state may take urgent countermeasures without such prior notification if giving notice would defeat the purpose of the countermeasures, for instance by revealing sensitive methods or capabilities. In cyberspace, where threats can materialise rapidly and cause significant damage, urgent countermeasures may be thus justified, provided they are then notified to the responsible state and terminated once the need for urgency ceases. Several states have espoused the application of this rule to countermeasures related to cyber operations.[65]

The Chinese team agrees that this special provision for urgent situations does not exclude the applicability of Article 52(1)(a) ARSIWA, which means that the injured state is still required to inform the responsible state of its illegal behaviour and demand it to fulfil its obligations before taking countermeasures.[66] The urgent countermeasures without prior notification must be taken only when necessary, though what constitutes "necessary" in cyberspace is still worth exploring. States may resort to countermeasures in cyberspace for effectiveness, yet the extent to which notification requirements can be waived to prevent abuse remains a critical question. In this regard, the Chinese team, after considering the often-covert nature of cyber countermeasures, believes that even urgent countermeasures must be perceivable for the responsible state to be motivated to rectify its wrongful conduct, thereby achieving the fundamental objective of the countermeasures. Thus, the Chinese team holds the same view that notification required by Article 52(2) of ARSIWA, though not necessarily prior notification, should still be given simultaneously with or promptly after implementing urgent countermeasures.

64 ARSIWA Commentaries Art 52, p. 136, § 6.

65 Costa Rica (2023) "Position on the Application of International Law in Cyberspace", 21 July, pp. 4-5, § 14;Netherlands (2019) "International Law in Cyberspace", 26 September, pp. 7-8;France (2019) "International Law Applied to Operations in Cyberspace", 9 September, pp. 7-8;Israel (2020) "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", 8 December;UNODA (United Nations Office for Disarmament Affairs) (2021) "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States", A/76/136, August, p. 73;Sweden (2022) "Position Paper on the Application of International Law in Cyberspace", July, p. 6;UK (United Kingdom) (2018) "Cyber and International Law in the 21st Century", 23 May;UK (United Kingdom) (2021) "Application of International Law to States' Conduct in Cyberspace", 3 June.

66 ARSIWA Commentaries Art 52, p. 136, § 6.

4. Measures by states other than the injured state

Countermeasures by a state other than the injured state are not unanimously accepted as *lex lata* and remain a highly controversial issue. Both teams agreed on these two observations.

In 2001, states were unable to reach a consensus on whether international law permits such countermeasures while adopting ARSIWA. As a compromise, ARSIWA only permits the invocation of responsibility (Article 48) and the taking of "lawful measures"[67] (Article 54) by a state other than an injured state. The commentary under Article 54 affirms that it is uncertain as to whether "countermeasures taken in the general or collective interest" are permissible under existing international law and, therefore, "includes a saving clause which reserves the position and leaves the resolution of the matter to the further development of international law."[68]

Countermeasures by a state other than the injured state may take three different forms:

- The first form covers countermeasures by a non-injured state in reaction to the breach of an *erga omnes* obligation.
- The second form covers countermeasures by a non-injured state in reaction to the breach of an *erga omnes partes* obligation.
- The third form covers countermeasures taken by a non-injured state at the request of the injured state regardless of the nature of the obligation breached.

It is important to note that the vocabulary on these different forms of countermeasures is not settled, and different terms are used, sometimes interchangeably, depending on the source. The first and second forms are sometimes referred to as "third-party countermeasures" or "countermeasures taken in the general or collective interest", while the third form is generally referred to as "collective countermeasures" or "proxy countermeasures".[69] The remainder of this section will use these expressions accordingly.

In recent years, scholars and some states have commented on countermeasures by a state other than the injured state in relation to cyber operations. Since 2012, states have publicly released interpretative statements on international law and cyber operations. Over the 33 positions, only ten States – Austria,[70] Canada,[71]

67 Some scholars argue that this could include countermeasures because their wrongfulness is precluded. See, generally, L.A. Sicilianos, "Countermeasures in Response to Grave Violations of Obligations Owed to the International Community" in J. Crawford and others (eds), *The Law of International Responsibility* (Oxford University Press 2010) 1145–1146; M. Longobardo, "The Contribution of International Humanitarian Law to the Development of the Law of International Responsibility Regarding Obligations *Erga Omnes* and *Erga Omnes Partes*" (2018) 23 Journal of Conflict and Security Law 383, 388.

68 ILC (International Law Commission) (2001) "Commentary to the Articles on State Responsibility", Yearbook of the International Law Commission, Vol. 2(II), p. 139, para. 6 to Article 54.

69 M. Jackson and F.I. Paddeu (2024) "The Countermeasures of Others: When Can States Collaborate in the Taking of Countermeasures?", American Journal of International Law, 118, p. 231.

70 Austria (2024) "Position Paper of the Republic of Austria: Cyber Activities and International Law", p. 9.

71 Canada (2022) "International Law Applicable in Cyberspace", para. 37, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx.

Costa Rica,[72] Denmark,[73] Estonia,[74] France,[75] Ireland,[76] New Zealand,[77] Poland,[78] and the United Kingdom[79] – commented on countermeasures by states other than the injured state. It can be observed that over the different interpretative statements mentioning countermeasures by a state other than the injured state, some focus on third-party countermeasures, others on collective countermeasures, and a few on both. They adopt different approaches:

- Third-party countermeasures: Poland, Ireland, Costa Rica, and Austria consider them as permitted, while Denmark seems to be in favour.
- Collective countermeasures: Estonia, Ireland, and Costa Rica consider them as permitted, while New Zealand seems to be in favour. France and Canada oppose.

Estonia, in May 2019, was the first state to introduce the question of countermeasures by states other than the injured state in its interpretative statement on international law and cyberspace.[80] Interestingly, the Estonian position and several subsequent positions focus on collective countermeasures. In other words, the focus is on the possibility for an injured state with fewer capabilities to request other states to assist it and conduct countermeasures on its behalf. Yet, the most recent positions tend to discuss both collective countermeasures and third-party countermeasures. These observations are important because, outside of the cyber-related discussion, collective countermeasures are more rarely discussed. The general approach stems from the development of *erga omnes* obligations. Indeed, third-party countermeasures are considered by some scholars to be necessary for the effective enforcement of *erga omnes* obligations.[81] The Chinese team noted that the absence of a clear list of *erga omnes* obligations and the clear understanding of their application in cyberspace makes the question even more challenging in this respect. More generally, it has been asserted by some scholars that since 2001 and the adoption of ARSIWA, the practices developed by some states in certain circumstances may be considered as forms of third-party countermeasures.[82]

---

72 Costa Rica (2023) "Position on the Application of International Law in Cyberspace", p. 5.

73 J.M. Kjelgaard and U. Melgaard (2023) "Denmark's Position Paper on the Application of International Law in Cyberspace", Nordic Journal of International Law, pp. 446-455.

74 Kersti Kaljulaid (2019) "Opening Address at the 11th Annual Conference on Cyber Conflict of the NATO Cooperative Cyber Defence Centre of Excellence", https://president.ee/en/official-duties/speeches/2525-president-republic-opening-cycon-2019; United Nations General Assembly, 28.

75 France (2019) "International Law Applied to Operations in Cyberspace", ministère des Armées, p. 7.; France (2021) "International Law Applied to Operations in Cyberspace", United Nations Office for Disarmament Affairs, Paper shared by France with the Open-ended working group established by resolution 75/240, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

76 Ireland (2023) "Position Paper on the Application of International Law in Cyberspace", Department of Foreign Affairs, p. 6, para. 26, https://www.dfa.ie/our-role-policies/international-priorities/international-law/internationallawandcyberspace/.

77 New Zealand (2020) "The Application of International Law to State Activity in Cyberspace", p. 4, https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf.

78 Poland (2022) "The Republic of Poland's Position on the Application of International Law in Cyberspace", Ministry of Foreign Affairs of the Republic of Poland, https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace.

79 S. Braverman (2022) "International Law in Future Frontiers", UK Attorney General's Office, https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

80 Kaljulaid, 2019.

81 G. Gaja (2013) "The Protection of General Interests in the International Community: General Course on Public International Law (2011)", 364 Collected Courses of the Hague Academy of International Law, p. 130.; C.J. Tams (2005) Enforcing Obligations *Erga Omnes* in International Law, Cambridge University Press, pp. 198–251.; M. Dawidowicz (2017) Third-Party Countermeasures in International Law, Cambridge University Press, p. 11.

82 T. Dias (2024) Countermeasures in International Law and Their Role in Cyberspace, Chatham House, Research Paper, pp. 39–42.

No sufficient state practice currently complements the limited number of states' positions on countermeasures by a state other than the injured state in cyberspace. Both teams agreed that these different positions do not necessarily demonstrate an evolution of existing international law and that it is sounder to assume that countermeasures by a state other than the injured state are not permitted so far, including in cyberspace.

The distinction between countermeasures by states other than the injured state, on the one hand, and forms of aid or assistance, on the other hand, is important and might be more challenging in cyberspace. In certain circumstances, a non-injured state providing aid or assistance might be considered to be contributing to an act breaching international law or committing an internationally wrongful act itself and see its international responsibility engaged. These observations are particularly relevant regarding the development of capacity-building efforts. Certain capacity-building activities, for instance, providing support that may be used to develop cyber capabilities to be used in cyber operations, may, in certain circumstances, either contribute to an internationally wrongful act by the assisted state or constitute an internationally wrongful act themselves when violating international obligations. Both teams agreed on these observations.

Building Peace Together

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
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-019-8