Towards a UN-Centric Cybercrime Treaty

Chinese positions and interests at the UN Ad Hoc Committee for a cybercrime convention

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Eric Siyi Zhang,
Rogier Creemers

February, 2024

The LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society.

More information can be found on our website:

www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl

M. de Vrieshof 3, 2311 BZ Leiden, The Netherlands

LEIDEN ASIA CENTRE

Partners in Research and Knowledge

Abstract

Since 2021, an international convention on tackling cybercrime is being negotiated at the UN. As positions of states for the UN Cybercrime Treaty vary, this report focuses on China's role at the negotiations. While there is a long list of issues at stake at the current AHC negotiations, this report focuses on Chinese positions on four issues: (1) a UN-based cybercrime treaty as China's primary objective, (2) states' sovereignty in cyberspace as a principle to be enshrined in the convention, (3) the range of criminalisation, and (4) conditions of transborder access of data. Also, this report analyses China's role in the establishment of the AHC negotiation process and its role during the first six sessions of the negotiation. This report argues that using a typology of states based on whether they are 'like-minded' or not is not conduicive to correctly understanding states' preferences, as they are largely determined by domestic legislation. The extent of alignment of states' positions on various issues at the AHC is discussed by applying a text-scaling model - wordscore on positions papers submitted by delegations to the AHC. It shows that while an absolte majority of states have positions similar to the EU on criminalisation, preferences on other chapters of the Convention are more diverse. In the conclusion of this report, this report also briefly discusses how states coordinate their positions. From a European perspective, it also explores the strengths and weaknesses of the EU delegation's position.

Contents

1. Introduction

As digital technologies bring more promises to the global economy and the quality of life worldwide, the perils carried by crimes committed with those technologies also grow in tandem. A typical kind of cybercrime is ransomware, where the perpetrator can use malware to threaten to withhold/publish compromised data unless a ransom is paid off. Besides, crimes that existed before the internet age, such as theft and fraud, are increasingly being committed with digital technologies. Cybersecurity threats have emerged as a systemic risk for the global economy.[1] Moreover, emerging digital technologies such as Internet of Things, are making a variety of new devices[2] cyber-dependent, thus making them also vulnerable to cybersecurity risks. Another challenge posed by cybercrime stems from the fact that the internet by design is borderless, as cybercrimes can be easily committed against targets located in another state. Moreover, activities in cyberspace are also covert in nature, i.e., cyber forensics often falls short of establishing the identity of the perpetrator behind the cyber incident.

Because of the reasons mentioned above, governments worldwide, at least in their official positions, agree on the need for collective action in tackling cybercrime, while there are significant divergences on how. To begin with, states have long disagreed about whether there should be a binding, UN-based treaty on tackling cybercrime. Issues such as the range of criminalisation, jurisdiction, and human rights safeguards are also contentious, due to states' differences in domestic laws, normative preferences in the global governance of the internet, and other foreign policy considerations. Since 2021, an international convention on tackling cybercrime is being negotiated at the UN's Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications

[1] World Economic Forum. (7 July 2021). Only cross-border, cross-sector collaboration will be enough to beat cybercrime. Retrieved from: https://www.weforum.org/agenda/2021/07/cross-border-cross-sector-collaboration-cybercrime/.
[2] e.g., autonomous driving vehicles.

Technologies for Criminal Purposes (hereinafter AHC).[3] Prior to the establishment of the AHC, Western governments maintained that there was no need for a new international binding treaty on cybercrime under the framework of the UN, and advocated for the 'globalisation' of the Budapest Convention. The current process at the UN is initiated by Russia in 2019 through a draft resolution tabled at the United Nations General Assembly. Although Western and 'like-minded' countries generally opposed the initiative, the resolution was able to pass with a margin of 19 votes.

This report focuses on China's positions and interests at the AHC negotiations. The rest of the report proceeds as follows: firstly, it discusses Chinese preferences in the making of international law in tackling cybercrime based on an extensive review of relevant Chinese literature. While there is a long list of issues at stake at the current AHC negotiations, this part of the report focuses on Chinese positions on four issues: (1) **a** UN-based cybercrime treaty as China's primary objective, (2) states' sovereignty in cyberspace as a principle to be enshrined in the convention, (3) the range of criminalisation, and (4) conditions of transborder access of data. Then, the second analytical task of this report is to analyse China's role in the establishment of the AHC negotiation process and during the first six sessions of the negotiation. Besides, the extent of alignment of different positions at the AHC is discussed by applying a Natural Language Processing (NLP) model - wordscore to positions papers submitted by delegations to the AHC. Qualitatively, this report also provides a detailed analysis of the AHC's consolidated negotiating documents on selected issues.[4] In the conclusion of this report, apart from summarising its findings, this report also discusses how states coordinate their positions with each other, and some possible developments and dynamics in the final session of the AHC. From a European

[3] Walker, S. (2 June 2021). Contested domain: UN cybercrime resolution stumbles out of the gate. Global Initiative against Transnational Organised Crime. Retrieved from: https://globalinitiative.net/analysis/un-cybercrime-resolution/.

[4] As articles in the draft treaty text are re-numbered by the Chair in draft treaty text prepared for different sessions, it is important to note that the article numbers this report refers to are the article numbers used in the document referenced in the footnote.

perspective, it explores the strengths and weaknesses of the EU delegation's position and possible room for negotiation with the Chinese delegation on a few contentious issues.

2. Chinese interests in the making of international law on cybercrime

China's most important objective on the issue of international law on cybercrime is to have a UN-based international treaty in itself,[5] rather than specific provisions that must be included in that treaty. The making of the UN Cybercrime treaty is not only about devising a functional legal project, but also consolidating the UN as the platform for issues on the global governance of cyberspace. At the regional level, there are currently a few conventions on tackling cybercrime, including (1) Council of Europe Convention on Cybercrime (hereinafter Budapest Convention), (2) Arab Convention on Combating Information Technology Offences, and (3) African Union Convention on Cyber Security and Personal Data Protection.[6] Among them, the Budapest Convention, with 70 signatory states,[7] is likely the only project with realistic prospects of becoming a global standard for tackling cybercrime. It has served as a de facto guideline or reference for cybercrime legislation worldwide: many states used the Budapest Convention as the basis for their national cybercrime legislation, even though some of which are not parties to it.[8] Besides, the Budapest Convention comprises institutional mechanisms (T-CY and C-PROC)[9] which further contributes

[5] Yu, Z. (2015). China's Position on Concluding and Joining the International Convention on Cybercrime[缔结和参加网络犯罪国际公约的中国立场]. Tribune of Political Science and Law 2015(5). p.105.

Wu, S. (2017). China's Practices in Preventing and Combating New Types of Cybercrime[防治新型网络犯罪的中国实践]. China Information Security, 2017(3), pp. 97-99.

[6] Zhang, P. & Wang, Y. (2020). Actively Participate in the Negotiations of the United Nations Convention on Combating Cybercrime and Build a Community of Shared Future in Cyberspace[积极参与联合国打击网络犯罪公约谈判 构建网络空间命运共同体]. China Information Security 2020(9): 68-72.

[7] Council of Europe. (n.d.). Chart of signatures and ratifications of Treaty 185. Retrieved from: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

[8] Hakmeh, J. (13 Jan 2020). A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet. Council on Foreign Relations. Retrieved from: https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

Yang, F. (2019). The current situation, goal and promotion path of international rule codification of cybercrime [网络犯罪国际规则编纂的现状、目标及推进路径]. Network Communication and Privacy 2019(5): 21-24.

[9] The Cybercrime Convention Committee (T-CY) provide states with guidance on interpreting the Convention. The Cybercrime Programme Office provides countries worldwide with capacity-building assistance on cybercrime. In
Council of Europe. (n.d.). Action against Cybercrime. Retrieved from: https://www.coe.int/en/web/cybercrime.

to the dissemination of its norms, standards, and procedures. However, China has been a vocal opponent of the globalisation of the Budapest Convention. In this context, China's objection to specific provisions in the Budapest Convention (e.g., unilateral transborder access of data) is only a secondary reason for opposing the Budapest Convention's globalisation: after all, China is not a party of the Budapest Convention, so China would in any case not be bound by those provisions. Rather, many Chinese scholars see the globalisation of the Budapest Convention as a threat to the UN-centred world order, which is a key element in China's worldview.[10] In principle, Chinese foreign policy has maintained in the long-term that any governance issue of global relevance, including the tackling of cybercrime, should be addressed (preferably exclusively) under the framework of the UN. Along this line of thinking, the potential globalisation of the Budapest Convention would be a challenge to UN-centred world order as China sees it. As Lu (2018) argues, the Budapest Convention, or any other regional treaties and organisations, should not replace the UN in international affairs, as it could set a precedent with a serious impact on the UN and the post-WWII security order.[11]

Another reason why China prefers a UN-based cybercrime treaty is that it has not negotiated the Budapest Convention. Most Chinese experts argue that it poorly reflects the interests of developing countries, as it is negotiated by a 'small number of Western states'.[12] States could be reluctant to accede to an international treaty which they did not negotiate purely due to foreign policy considerations, even if they otherwise believe the accession to be in their interests. It needs to be emphasised that such foreign policy considerations are not unique to China, but shared by some others,

[10] Ghiasy, R.; Zhang, E. S.; & Ferchen, M. (March 2023). Sino-Russian Global Reordering? Comparing visions and assessing practical cooperation. LeidenAsiaCentre Report.
[11] Lu (2018).
[12] Yu, Z. (2015). China's Position on Concluding and Joining the International Convention on Cybercrime[缔结和参加网络犯罪国际公约的中国立场]. Tribune of Political Science and Law 2015(5):91-108.
Hu, J. & Huang, Z. (2016). The Problems and Prospects of the International Legal Regimes in Combatting Cybercrimes – from the perspective of CoE's Convention of Cybercrime[打击网络犯罪国际法机制的困境与前景——以欧洲委员会《网络犯罪公约》为视角]. International Law Studies 2016(6): 21-34.
Yang, F. (2019). The current situation, goal and promotion path of international rule codification of cybercrime.

such as India.[13] In fact, many Chinese scholars positively evaluate the Budapest Convention from a legalist perspective, referring to the Convention as 'having a preeminent quality of legislation',[14] some even point out that the Budapest Convention has been instructive for China's own domestic cybercrime legislations.[15]

Regarding what the UN cybercrime convention should look like at a more granular level, while various Chinese scholars named a few issues which the UN cybercrime convention should address (which following paragraphs of this report will discuss), many (correctly) argue that it would most likely be unrealistic for states to obtain adequate support for its preferences on wide ranges of issues at the UN, since preferences and priorities of states at the UN are diverse in all potentially contentious areas, inter alia the range of criminalisation, applicability of human rights, and grounds for refusal legal assistance.[16] Therefore, states that participate in the UN cybercrime convention negotiation will unavoidably have to make compromises and work constructively on issues where reaching an agreement is possible. Several Chinese legal experts thus suggests that China should take a constructive approach during the AHC negotiation, which they refer to as 'finding the common denominator'.[17]

---

[13] India, for instance, has already aligned its domestic legislations fully in line with the Budapest Convention in the 2000s; it would also be the largest beneficiary of the Convention's technical assistance provisions. However, not having negotiated the Convention remains one of the most important reasons for India's non-accession. See e.g.
Seger, A. (2016). India and the Budapest Convention: Why not? Observer Research Foundation. Retrieved from: https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/.

[14] 先进立法水平 in Yang, F. (2019). The current situation, goal, and promotion path of international rule codification of cybercrime.

[15] Yu, Z. (2015). China's Position on Concluding and Joining the International Convention on Cybercrime;
Hu, J. & Huang, Z. (2016). The Problems and Prospects of the International Legal Regimes in Combatting Cybercrimes – from the perspective of CoE's Convention of Cybercrime;
Yang, F. (2019).

[16] E.g. Yu, Z. (2015). China's Position on Concluding and Joining the International Convention on Cybercrime

[17] 最大公约数, in
Jiang, S. (2023). Commentary on the "Criminalization" Section of the United Nations Convention against Cybercrime[《联合国打击网络犯罪公约》"刑事定罪"部分评述]. China Information Security 2023(3), 58-60.;
United Nation News. (12 December, 2022). [Special report] Looking for the common denominator of international governance in cyberspace——Interview with Wu Shenkuo, Senior Adviser on Cyber Security and Cybercrime at the United Nations[【专题报道】寻找网络空间国际治理的最大公约数——专访联合国网络安全与网络犯罪问题高级顾问吴沈括]. Retrieved from: https://news.un.org/zh/story/2019/12/1047311.

One issue which most likely constitutes a red line for the Chinese delegation in the AHC is the reference to sovereignty in the UN cybercrime convention. Various Chinese scholars argue that sovereignty should not only be enshrined as a general principle in the convention, but also be strictly interpreted and sufficiently considered in the design of provisions on issues such as jurisdiction and transborder access of data.[18] In this context, it should be reminded that the concept of cyber sovereignty is inherently securitised in the Chinese conceptualisation, as it is defined as a part of national security.[19] The concept serves as a normative basis for the Chinese government to make domestic regulation as it sees fit in order to defend against perceived foreign interference and cyber espionage.[20] While it is beyond the scope of this report, it should also be mentioned that the Chinese conceptualisation of cyber sovereignty also has important geoeconomic underpinnings, such as reaching technological and industrial self-sufficiency for China's digital industry.

Regarding criminalisation, China advocates the inclusion of a wide range of crimes[21] in the UN cybercrime convention, most importantly cyber-enabled crimes.[22] Chinese experts have argued that the Budapest Convention has a narrow range of criminalisation – it merely criminalises cyber-dependent crimes, with a few exceptions (infringement of copyrights, fraud).[23] Such criticisms have often been cited as one of

[18] Yu, Z. (2015). China's Position on Concluding and Joining the International Convention on Cybercrime; Zeng, L. & Wang, Z. (2023). China's Approach to International Cooperative Governance of Cyber Crimes from the Perspective of Cyber Sovereignty —Taking the Drafting of the Countering the Use of Information and Communications Technologies for Criminal Purposes as an Opportunity [网络主权视域下网络犯罪国际合作治理的中国路径——以《联合国打击网络犯罪公约》的起草为契机]. Information Security and Communications Privacy,2023(2):135-148.

[19] Cyber Administration of China. (2016). National Cybersecurity Strategy[国家网络空间安全战略].

[20] Yu, Z. (2015). China's Position on Concluding and Joining the International Convention on Cybercrime.

[21] Crime that can exist purely in physical space, but are being committed more often through cyber means, e.g. theft.

[22] Ma, X. (6 June, 2023). The Current International Law Situation and China's work on Diplomatic Treaty and Law Work—Keynote Speech of Director of the Department of Treaty and Law of the Ministry of Foreign Affairs Ma Xinmin at the 2023 Academic Annual Conference of the Chinese Society of International Law[当前国际法形势与我国外交条法工作——外交部条法司司长马新民在中国国际法学会 2023 年学术年会上的主旨报告]. Retrieved from: http://qmyfzgyjy.cupl.edu.cn/info/1016/1265.htm.

[23] Qu, X. & Zhao, Q. (2019). Development of China's cybercrime evidence collection rules from an international perspective [从国际视角看中国网络犯罪取证规则发展]. China Information Security 2019(5).

the reasons why a new international cybercrime treaty is needed.[24] States' priorities in the issue of criminalisation during the AHC negotiations are primarily shaped by existing challenges their law enforcement agencies face, as well as provisions in domestic legislations. As for China, a report on cybercrime in China published by the Chinese Judicial Big-data Institute [中国司法大数据研究院] shows that all ten most common subcategories of cybercrime convicted in China during 2016-2018 are in fact cyber-enabled crimes, with the most common one being fraud (31.83%), followed by online gambling (10.45%).[25] Besides, China's gradually tightening online real-name regulations[26] [网络实名制] in the 2010s brought new challenges to tackling cyber-enabled crimes, as organised crime groups have typically relocated their operations to South-Eastern Asian countries, where no similar regulations are in place. Apart from law enforcement, this trend also creates challenges on the determination of jurisdiction, collection of evidence, and more importantly legal assistance and repatriation.[27] Below is a list of cyber-enabled crime which should be addressed in the UN cybercrime treaty often mentioned in the Chinese sources reviewed by this report:

[24] Jiang, S. (2023). Commentary on the "Criminalization" Section of the United Nations Convention against Cybercrime.

[25] Chinese Judicial Big-data Institute. (2019). Characteristics and Trends of Cybercrime Special Report on Judicial Big Data [网络犯罪特点和趋势 司法大数据专题报告].

[26] E.g Cyber Administration of China. (2016). Cybersecurity Law of People's Republic of China[中华人民共和国网络安全法]. Article 24. Retrieved from: http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm.

[27] An, K. (2019). China's Involvement in International Governance of Transnational Cybercrime[跨国网络犯罪国际治理的中国参与]. Journal of Yunnan Minzu University (Social Sciences), 36. p.157.

(1) Fraud,[28] (2) money-laundering,[29] (3) drug-related crimes,[30] (4) facilitation of gambling, [31] (5) Arms trafficking, [32] (6) child pornography, [33] and (7) facilitation of cybercrime.[34]

Some of those offences are relatively less contentious between China and the EU, as they are also criminalised in the Budapest Convention, including fraud[35] and child pornography. However, there are divergences between Chinese and European positions on the exact wording and provisions of those issues, as observed during the previous sessions of the AHC negotiations.

Regarding content-related crime, there seems to be little consensus in the Chinese literature reviewed by this report: unlike cyber-enabled crime, far from all Chinese sources has argued for the inclusion of content-related crimes in the convention. However, the inclusion of content-related crime (e.g., incitement of hatred, terrorism, spreading disinformation) is advocated in a commentary written by two Chinese in their capacity as observers at the United Nations Office of Drugs and Crime,[36] which should somewhat reflect China's official position. Chinese scholars seem to be aware that the inclusion of content-related crime in the UN cybercrime convention is only supported by a handful of states. However, there seems to be no consensus among them on how important it is for China to include content-related crimes. While some argues that specific content-related crime, especially terrorism, is

[28] Yu, Z. (2015).;
Zhang, L. & Gong, W. (2020). States Positions on Legal Issues Related to the United Nations Convention against Cybercrime [联合国打击网络犯罪公约相关法律问题的各国立场]. China Information Security 2020(9): 85-88.;
Yang, F., & Lu, C. (2021). Observer's comments (Shanghai Institute for International Studies)[观察员单位意见（上海国际问题研究院）]. United Nations Office on Drugs and Crime. Retrieved from: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Comments/Additional-comments/Shanghai_Institute_for_International_Studies.pdf.
[29] Yu, Z. (2015).
[30] Yu, Z. (2015).
[31] Zhang, L. & Gong, W. (2020). States' Positions on Legal Issues Related to the United Nations Convention against Cybercrime; Yang, F., & Lu, C. (2021). Observer's comments (Shanghai Institute for International Studies).
[32] Yang & Lu. (2021).
[33] Yang & Lu. (2021).
[34] Ibid.
[35] It should be reminded that the cyber-enabled crime with the highest priority for China is online fraud and online theft.
[36] Yang & Lu. (2021).

'controversial yet important',[37] other Chinese scholars argue that proposals for 'content-related crime' should be treated with somewhat lower priority than issues that are a core Chinese national interest (e.g. cyber sovereignty) and issues where reaching an acceptable outcome for all is plausible (e.g. cyber-enabled crimes).[38] Nevertheless, at this stage, policymakers should be aware that the discussion on the possible inclusion of content-related crimes in the UN cybercrime convention is unlikely: the AHC chair did not include articles on content-related crime in the draft treaty text prepared for the sixth session, as they did not have enough support among states. This is also true in the drafty treaty text prepared by the Chair for the seventh session.[39] Re-introducing those articles in the upcoming session is possible, whereas they would still need significantly more support to become a part of the final draft treaty text. As it stands at the end of the sixth session, content related crimes introduced at the AHC include Article 15 ter (Encouragement of or coercion to suicide), Article 15 quarter (Incitement to subversive or armed activities), Article 15 quinquies (Extremism-related offences), Article 15 sexies (Denial, approval, justification or rehabilitation of genocide or crimes against peace and humanity), Article 15 septies (Terrorism-related offences), and Article 16 bis (Prohibition of incitement to violence).[40] While they are supported by a group of hardliner states on content-related crimes including Russia, North Korea, and Egypt, China has not co-sponsored the amendments of their inclusion.[41] On the other hand, China supports Article 15 duodecies (Acts threatening public safety),[42] of which the wording[43] is fairly ambiguous. While this could appeal to states that are in favour of the inclusion of

[37] Li, Y. (2020).
[38] 'These points should be proposals China pushes for, instead of being treated as matters of principle or red lines' 上述观点作为中国的力推主张而不是底线原则 in
Yu, Z. (2015). China's Position on Concluding and Joining the International Convention on Cybercrime.
[39] AHC seventh session. (6 November 2023). Revised draft text of the convention. A/AC.291/22/Rev.1.
[40] AHC sixth session. (2 September 2023). Draft text of the convention Status as of 2 September 2023 with updates from Member States.
[41] Ibid.
[42] Ibid.
[43] 'Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, the organization, planning, and commission of violent acts that pose a serious threat to public safety, including but not limited to explosions and indiscriminative violences, through the use of information and communication technology.'

aforementioned content-related crimes, it is unlikely that this proposal would be supported by the majority of states which favours a narrow scope of criminalisation. This article, in its current form, are also prone to abuse.

Another substantive issue frequently discussed in Chinese literature reviewed by this report is transborder access of data, if the data is not publicly available. As is the case with criminalisation, this debate similarly emerges from the provisions (or the lack thereof) in the Budapest Convention: Budapest Convention's Articles 32b permits unilateral transborder access of computer data without the procedure for mutual assistance under limited circumstances.[44] In other words, national governments of the jurisdiction where data is stored can be circumvented, if the controller of said stored data consent to the transborder access. Chinese scholars argue that this provision violates the principle of non-interference of internal affairs and undermines states' judicial sovereignty,[45] which could also be used as a pretext for 'long-arm jurisdiction' in cyberspace, as Chinese commentators often describe it.[46] More importantly, there are also concerns that this provision would be used as a loophole for state-sponsored actors for cyber-espionage. Hu & Huang (2016) point out that 'computer data' in Budapest Convention's Article 32b is not clearly defined, and data with military or national security relevance is therefore also not excluded.[47] There are also concerns that data-controllers (often a multinational company) can be enticed or even compelled to provide consent, which they otherwise would not. As this issue is understood by at least some Chinese commentators from a national security scope, it is expected that China would categorically oppose proposals at the AHC similar to

[44] T-CY. (2014). T-CY Guidance Note # 3 Transborder access to data (Article 32). Retrieved from: https://rm.coe.int/16802e726a#:~:text=Article%2032%20(Trans%2Dborder%20access,computer%20system%20in%20its%20territory%2C.

[45] E.g. Qu, X. & Zhao, Q. (2019). Development of China's cybercrime evidence collection rules from an international perspective;

[46] Liang, K. (2019). Criminal Evidence Collection Jurisdiction Model Based on Data Sovereignty[基于数据主权的国家刑事取证管辖模式]. Chinese Journal of Law 41, 188-208.

[47] Hu, J. & Huang, Z. (2016). The Dilemma and Prospect of the International Legal Mechanism to Combat Cybercrime——From the Perspective of the Council of Europe Convention on Cybercrime[打击网络犯罪国际法机制的困境与前景———以欧洲委员会〈网络犯罪公约〉为视角]. Chinese Review of International Law. 2016(6). p.27.

the provisions of Budapest Convention Article 32b. Incidentally, a Chinese article from 2023 explicitly argues so.[48]

On the other hand, Chinese experts recognise that requesting transborder access of data through mutual legal assistance procedures, by obtaining the consent of the law enforcement agencies of the jurisdiction where data is stored, can be inadequate for the need of tackling crime in terms of efficiency and practicality. They call for balancing the respect for national judicial sovereignty and the need to fight crime, by devising generally accepted rules for cross-border access to electronic data under the framework of the United Nations.[49] Liang (2023) suggests two alternatives to provisions in Article 32b: First, the interpretation to Article 32a, i.e. unilateral transborder access is allowed if the data is open-access, can be expanded. For instance, if the data can be accessed after registration. Second, an exception could be made for unilateral transborder access of non-open-access data with the consent of the controller: if the controller of the requested data stored in another jurisdiction is located on the territory of the requesting state party.[50] During the fourth and fifth sessions of the AHC, those debates and proposals are centred around the wording of Article 45 (Production Order), Article 72 (Cross-border access to stored data). Another proposal mentioned by a few Chinese experts is to sort data into three categories, i.e. (1) subscriber data, (2) content data, and (3) traffic data.[51] For those three categories, different rules for transborder access should apply: less restrictions should apply for subscriber data, as it implicates issues such as privacy to a lesser extent.[52]

[48] Liang, K. (2023). Analysis of Cross-border access to data provisions in the United Nations Convention against Cybercrime[《联合国打击网络犯罪公约》中跨境获取数据条款设置分析]. China Information Security 2023(3). p.63.
[49] Zhang, L. & Gong, W. (2020). States Positions on Legal Issues Related to the United Nations Convention against Cybercrime [联合国打击网络犯罪公约相关法律问题的各国立场]. China Information Security 2020(9): 85-88.
[50] Liang, K. (2023). Analysis of Cross-border access to data provisions in the United Nations Convention against Cybercrime.
[51] Yang & Lu. (2021).; Qu, X. & Zhao, Q. (2019). Development of China's cybercrime evidence collection rules from an international perspective [从国际视角看中国网络犯罪取证规则发展]. China Information Security 2019(5).
[52] Ibid. and Qu, X. & Zhao, Q. (2019). Development of China's cybercrime evidence collection rules from an international perspective.

3. China's role in the UN cybercrime convention negotiation

Among the states which prefer a new UN cybercrime treaty, Russia and China (to a lesser extent), played an active role in initiating the process of negotiation since the 2010s. While China-Russia relation in cyberspace is beyond the scope of this report, it is necessary, given the significant role Russia has been playing in the AHC, to briefly discuss their normative convergence in cyberspace which enabled their similar positions during the current UN cybercrime convention negotiation. Those shared visions are first and foremost expressed in their shared problematisation of cybersecurity: Contrary to the common approach in the West which mostly emphasises the security of data and infrastructure, both China and Russia prefer the term 'information security' over 'cybersecurity', where information (or content) is also securitised.[53] Besides, both Russia and China adopt a maximalist interpretation of sovereignty in cyberspace, instead of regarding sovereignty merely as a general principle in international law applied in cyberspace.[54] In the issue of countering cybercrime, they emphasise that any transborder operation, in particular access of data, should be coordinated by national governments. In the area of international law, whereas Russia takes a positive approach to international law in cyberspace, pushing for UN treaties on both cybercrime and acceptable state behaviour, China has habitually preferred to leverage Russia's greater experience in the UN realm while taking less of its own initiative.[55]

In addition to cooperating with each other, Russia and China have consolidated their positions within regional and multilateral organisations, inter alia the BRICS and the Shanghai Cooperation Organisation (SCO). In 2014 at the organisation's Fortaleza Summit, BRICS countries declared the commitment to the negotiation of a 'universal

[53] Zhang, E. S.; Creemers, R. (2021). Russian Perspectives on China as an Actor in Cyberspace. LeidenAsiaCentre Report. Retrieved from: https://leidenasiacentre.nl/report-russian-perspectives-on-china-as-an-actor-in-cyberspace/.
[54] Ibid.
[55] Broeders, D.; Adamson, L.; & Creemers, R. (2019). A coalition of the unwilling? Chinese & Russian perspectives on cyberspace. The Hague Program for Cyber Norms.

legally binding instrument' on combatting cybercrime with the central role of the UN,[56] which is again reaffirmed at BRICS's Ufa Summit in 2015.[57] In 2017, BRICS has further coordinated their positions and delegated Russia to submit a draft cybercrime convention to the United Nations General Assembly later that year.[58] Similar to BRICS, SCO also concluded agreements on committing to negotiating a UN cybercrime treaty in 2020, and it furthermore agreed to coordinate member states' positions during the negotiation process.[59] However, as following paragraphs of this report will discuss, the extent of coordination between China and Russia is limited to submitting a common position paper, while the Chinese and the Russian delegations do not seem to act in cohort during the negotiation process.

As several Chinese commentators correctly point out,[60] as UNGA resolution 74/247 decides to establish an ad hoc committee to elaborate a UN cybercrime treaty,[61] it has transformed the interstate contention on cybercrime in the UN from 'whether there should be a UN cybercrime convention' to 'how should the UN cybercrime convention look like'. The draft of resolution 74/247 was sponsored by Russia and twenty-six other states, and it was adopted by the UNGA with 79 states voting yes, 60 voting no, 33 abstention, and 21 states not voting.[62] Regardless of how the final text of

---

[56] BRICS. (15 July, 2014). The 6th BRICS Summit: Fortaleza Declaration. Retrieved from: http://www.brics.utoronto.ca/docs/140715-leaders.html.

[57] MFA of China. (17 July, 2015). The 7th BRICS Summit: Ufa Declaration[金砖国家领导人第七次会晤乌法宣言]. Retrieved from: https://www.mfa.gov.cn/gjhdq_676201/gjhdqzz_681964/jzgj_682158/zywj_682170/201507/t20150717_9383530.shtml.

[58] An, K. (2019). China's Involvement in International Governance of Transnational Cybercrime[跨国网络犯罪国际治理的中国参与]. Journal of Yunnan Minzu University (Social Sciences), 36, 155-160.

[59] Deng, H. & Li, T. (24 Sept, 2021). SCO Information Security Cooperation: Progress, Challenges and Future Paths[上合组织信息安全合作：进展、挑战与未来路径]. China Institute of International Studies. Retrieved from: https://www.ciis.org.cn/yjcg/sspl/202109/t20210924_8175.html.

[60] Huang, Z. & Wang, X. (2023). Disagreements and Prospects in the Negotiations of the United Nations Conventin against Cybercrime[《联合国打击网络犯罪公约》谈判分歧及展望]. China Information Security 2023(3): 50-53; Zhang, P. & Wang, Y. (2020). Actively Participate in the Negotiations of the United Nations Convention on Combating Cybercrime and Build a Community of Shared Future in Cyberspace[积极参与联合国打击网络犯罪公约谈判 构建网络空间命运共同体]. China Information Security 2020(9): 68-72.

[61] UN Digital Library. (2019). Countering the use of information and communications technologies for criminal purposes : resolution / adopted by the General Assembly.

[62] Ibid.

the UN cybercrime treaty turns out to be, the adoption of resolution 74/247 itself is a significant success for states against the globalisation of the Budapest Convention.

The AHC had its first meeting in New York in May 2021, where it determined the rules and procedures of the drafting process. The importance of this first meeting should not be overlooked, primarily because it determined what kind of voting the AHC should operate on: although delegations in the AHC formalistically should strive for reaching consensus on all provisions in the convention text,[63] while states are mostly incentivised to negotiate and to compromise to the extent that they expect to receive enough votes. Theoretically, a proposed article that fails to receive enough votes would simply not be included in the final text, while references across different articles and negotiation tactics such as issue linkage likely to be used by delegations during the AHC negotiation would unavoidably complicate states' positioning and the consideration of gaining support. During the meeting, two draft resolutions were initially submitted by the US and Russia respectively: while the US preferred a consensus-based process, Russia proposed that a simple-majority voting process should be applied to the AHC.[64] For the US and other states which support the globalisation of the Budapest Convention,[65] a consensus-based process would mean that the UN cybercrime treaty would be no more than the fairly narrow common denominator of states' positions on cybercrime. A UN cybercrime treaty in this form would probably not be specific enough to have significant practical relevance, let alone becoming an alternative cybercrime treaty which can compete with the Budapest Convention. As for the simple-majority voting, although one obvious shortcoming is that a convention based on this voting rule would unlikely be signed by those opposed, it is possible that Russia and China, which leads the effort of drafting a new UN cybercrime convention, is not looking for a draft treaty with wide

[63] UNGA. (26 May, 2021). Resolution A/RES/75/282.
[64] Walker, S. (2 Jun, 2021). Contested domain: UN cybercrime resolution stumbles out of the gate. Global Initiative against Transnational Organised Crime. Retrieved from: https://globalinitiative.net/analysis/un-cybercrime-resolution/.
[65] This should not be equated with all signatories of the Budapest Convention, there are a number of Budapest Convention signatories which are at least not against negotiating a new cybercrime treaty at the UN.

acceptance,[66] but merely an UN-based cybercrime treaty to compete with the Budapest Convention. Eventually, the AHC decided to adopt an amendment submitted by Brazil by a wide margin (88 for, 42 against, 32 abstain), which proposed the committee to introduce a 2/3-majority voting.[67] Interestingly, while all Western delegations, which initially backed a consensus-based process, ended up voting for Brazil's amendment, China and Russia voted against. This development might seem counter-intuitive, as 2/3-majority seems at least equidistant from simple-majority and consensus-voting. However, a 2/3-majority voting in fact favours states supporting the Budapest Convention, as it would mostly likely lead to the AHC drafting a cybercrime convention with a narrow scope. Especially on the issue of criminalisation, most states' positions at the AHC are closely aligned with the provisions in the Budapest Convention.[68]

In 2022, the AHC has held two sessions for the first reading of the draft text, where states are invited to submit their contributions on eight proposed chapters and the preamble as follows: (1) general provisions, (2) provisions on criminalization, (3) procedural measures and law enforcement, (4) international cooperation, (5) technical assistance, (6) prevention measures, (7) mechanism of implementation and (8) final measures. A debate on the appropriate terms the UN cybercrime convention should adopt run through all parts of the negotiation: while states that seeks an expansive treaty prefers 'information-centric' terms, including 'using information and communication technology for criminal purposes', and 'digital information', states that prefers the convention to have a narrow scope favour 'data-centric' terms, such as 'cybercrime', and 'computer data'.[69] Among specific chapters, divergences are the

[66] Walker, S. (2 Jun, 2021). Contested domain: UN cybercrime resolution stumbles out of the gate. Global Initiative against Transnational Organised Crime.
[67] Ibid.
[68] It needs to be emphasised that this line of thinking is only logical in retrospect, because many states' positions on substantive matters remained unknown in May 2021, as position papers on substantive issues are only submitted to the AHC during the 2nd and 3rd sessions of the AHC in 2022. In particular, many developing countries' positions would also be difficult to estimate, as they do not have a clear stance on normative issues such as what should be criminalised, but are more interested in technical assistance.
[69] Walker, S. (June, 2023). Still poles apart – UN Cybercrime Treaty Negotiations. Global Initiative against Transnational Organised Crime. p.8.

widest in criminalisation, jurisdiction, and procedural measures and law enforcement, as they comprise some most contentious issues of the UN cybercrime convention. First, states' priorities in combatting cybercrime are diverse. Apart from political and normative considerations, the divergence is often to a greater extent caused by the different substantive challenges states are confronted with.[70] In this context, it should be emphasised that a simplistic dichotomy between democracies defending a free and open internet and autocracies aiming to re-write the rules is not conducive to understanding states' real interests and needs on criminalisation beyond their stated positions. Of course, several proposals such as 'incitement to subversive or armed activities'[71] are indeed mostly motivated by political considerations. China's interests on criminalisation are elaborated in previous chapters of this report. Disagreements also exist on safeguard measures, i.e. if procedures specified in the chapter should be subject to normative conditions such as privacy and human rights.[72] Divergence in procedural measures and law enforcement mainly entails the scope of sharing electronic evidence, while some Budapest Convention signatories insist on a narrow scope, i.e. only for crimes to be listed in UN cybercrime convention, some other states propose that the scope should apply to any criminal offence. A middle ground supported by the EU delegation on the condition of double criminality, proposes to include all serious crimes (crimes that can lead to imprisonment for more than four years).

[70] e.g. drug crimes, fraud.
[71] AHC Second Session. (9-20 January, 2023). Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, A/AC.291/16: Article 26. Retrieved from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/222/255/1E/PDF/2222551E.pdf?OpenElement.
[72] AHC fourth Session. (21 January, 2023). Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes – Status as of 21 January 2023: Article 42. Retrieved from: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf.

In order succinctly summarise and present states' positions on those issues, this study applies a computer-assisted scaling model [73] to the position papers/contributions submitted to the AHC's second and third sessions. Three groups of states have chosen to submit a single coordinated document[74] to represent their positions: (1) EU and its member states, (2) Jamaica's position papers were submitted on behalf of the Caribbean Community, (3) Russia's position papers were submitted on behalf of China, Belarus, Burundi, Nicaragua, and Tajikistan during the AHC's second session. During the AHC's third session, they were submitted also on behalf of Mali, in addition to the five aforementioned states. This study has placed the EU and Russia's positions on two sides (1 and -1) of the dimension of positions, then the scaling model estimates where other states position themselves between Russia and the EU.

[73] A computer-assisted Natural Language Processing scaling model - wordscore is used in the analyses. Wordscore is a scaling model for estimating the positions (mostly of political actors) for dimensions that are specified a priori, based on the distribution of word frequencies. Wordscore has been widely applied to study states positions and their alignment in the UN. See
Laver, M.; Benoit, K. & Garry, J. (2003). Extracting Policy Positions From Political Texts Using Words as Data. American Political Science Review 97(2): 311-331.

[74] Readers of this report therefore need to be aware that points for Russia, EU, and Jamaica in the document position plots below carry more voting power than others.

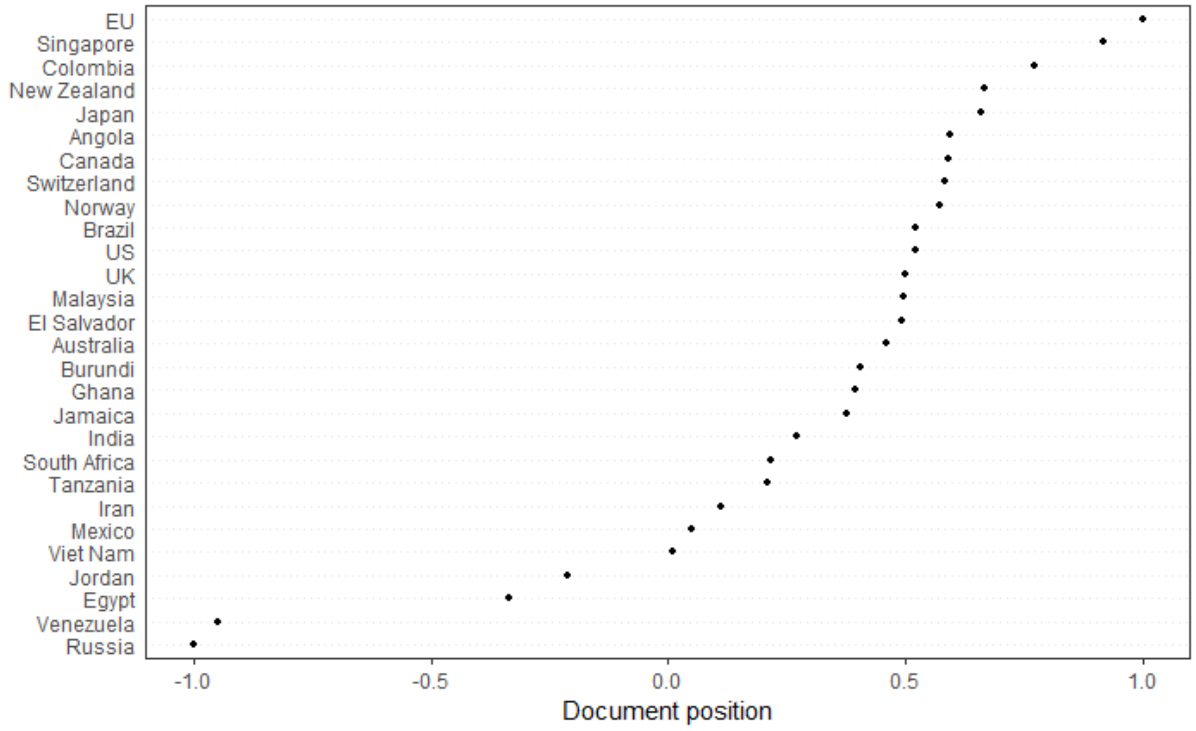

Figure 1: Positions (as submitted to AHC during the second session) relative to the EU and Russia in the AHC on Chapter 2 (criminalisation)

On the issue of criminalisation, as figure 1 shows, among the states which has submitted their contribution, there is an overwhelming majority of states which are more aligned with the EU's position (which is based on the provisions of the Budapest Convention), than with Russia. In particular, many contributions submitted by those states that are often perceived to have preferences divergent from the EU's, are also notably more aligned with the EU. This includes several African states, and more notably also three BRICS states - Brazil, India, and South Africa, despite coordination efforts within BRICS since the 2010s, as mentioned in this report's previous chapter. The wide distance between Russia's position and that of almost all other states as shown in figure 1 is most likely because Russia has put forward a few proposals which are shared by almost no others. There are of course a few exceptions: for example, Venezuela and Egypt's position papers also made reference to 'incitement to

subversive or armed activities'.[75]Those proposals are mostly the criminalisation of activities with a likely political motive and no apparent financial gain, which is unlikely to be committed by non-state-sponsored actors. Parenthetically, it is extremely hard to conceive that Russia made those proposals in good faith, given its long record of using malign cyber activities for geopolitical objectives.

As there are no separate proposals submitted by China during the second session of the AHC,[76] understanding China's position would require a more detailed analysis of the Chinese delegation's input during the negotiation process. During the fourth session of the AHC, many of Russia's proposals in criminalisation were in fact not supported by China during the negotiation process. Russia is the sole sponsor of its proposal of Article 10 ter on interference with critical information infrastructure.[77] China also did not sponsor Russia's amendment[78] to retain Article 13 on computer-related theft.[79] Those examples on the divergence of China and Russia's positions on criminalisation are not exhaustive. As shown in the consolidated negotiating document, China's main priority during the fourth session seems to be the inclusion of cyber-enabled crimes typically[80] faced by its own law enforcement agencies. They include the facilitation of cybercrime, (cyber) money-laundering, and mostly likely some other issues which the AHC chair designated to informal consultations due to insufficient support (including violation of personal information and drug-trafficking).[81]

[75] AHC fourth session. (2022). Compilation of proposals and contributions submitted by Member States on the provisions on criminalization, the general provisions and the provisions on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. A/AC.291/9: p.21, p.70.
[76] As aforementioned, Russia's contributions for the negotiation's first reading during the second and third sessions were also submitted on behalf of China.
[77] AHC fourth Session. (21 January, 2023). Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes – Status as of 21 January 2023: Article 10 ter.
[78] Incidentally, Russia's amendment to retain the article was supported by Iran and Syria.
[79] AHC fourth Session. (21 January, 2023). Consolidated negotiating document Status as of 21 January 2023: Article 13.
[80] discussed in the previous chapter of this report
[81] AHC fourth Session. (21 January, 2023). Consolidated negotiating document Status as of 21 January 2023.

In preparation for the sixth session, the chair compiled a draft text of the convention, based on the outcomes of the second reading of the draft chapters of the convention during the fourth and the fifth sessions.[82] Most of the articles concerning cyber-enabled crime were into included in the draft convention, due to insufficient support among states in the AHC. It should be reiterated that a convention covering a wide range of cyber-enabled crimes is not supported by the starting positions of most states in the AHC, and building support for them would prove to be difficult. Despite the distant prospect of attaining sufficient support, states that advocate for broader criminalisation once again tabled a wide range of cyber-enabled crimes during the sixth session. It also became increasingly clear that priorities among this group of states also vary: while some other hardliner countries on a wide range of criminalisation (such as Russia and Iran) focus on the inclusion of acts that are likely to be committed with political motives (e.g. interference with critical infrastructure, terrorism and extremism-related crimes), China's priority lies in the following two categories: (1) cyber-enabled crimes currently most committed in China, and (2) 'acts threatening public safety'. They are motivated respectively by challenges faced by its law enforcement and concerns over societal/regime stability.

However, the level of priority those issues receive in the China's agenda might not yet fully explain why the Chinese delegation repetitively tables proposals for those issues at such late stages of the AHC negotiation. While solicitating sufficient support for those proposals seems fruitless if solely judging from states' starting positions submitted during the second reading of the AHC, it is possible that those proposals are a part of the Chinese delegation's negotiation strategy. Those proposals can be used as 'quid pro quo' to extract concessions in other contentious issues in the draft text, such as jurisdiction and ground for refusing cooperation. Moreover, China's positioning and negotiation strategy might (have) enable(d) it to be in the position to potentially influence other (more) hardliner countries, since it has gradually appeared as a relatively constructive negotiator among states favouring a wide range of

[82] AHC sixth session. (29 May 2023). Draft text of the convention. A/AC.291/22.

criminalisation, assuming that they are prepared to reach a compromise. As it currently stands, there seems to be some progress for China on at least one of its proposals – it has become likelier that computer-related theft would be addressed by the Convention. During the sixth session, the discussion on Article 12 (Computer-related fraud) and Article 13 (Computer-related theft) negotiated during the fourth session[83] were merged into a single article – Article 12 (Computer-related theft or fraud), and the discussion on the article has become more technical and detailed.[84] While consensus is far from being reached in this article, it is included in the revised draft text of the convention prepared by the Chair for the seventh session of the AHC, indicating the Articles growing acceptability among states.[85]

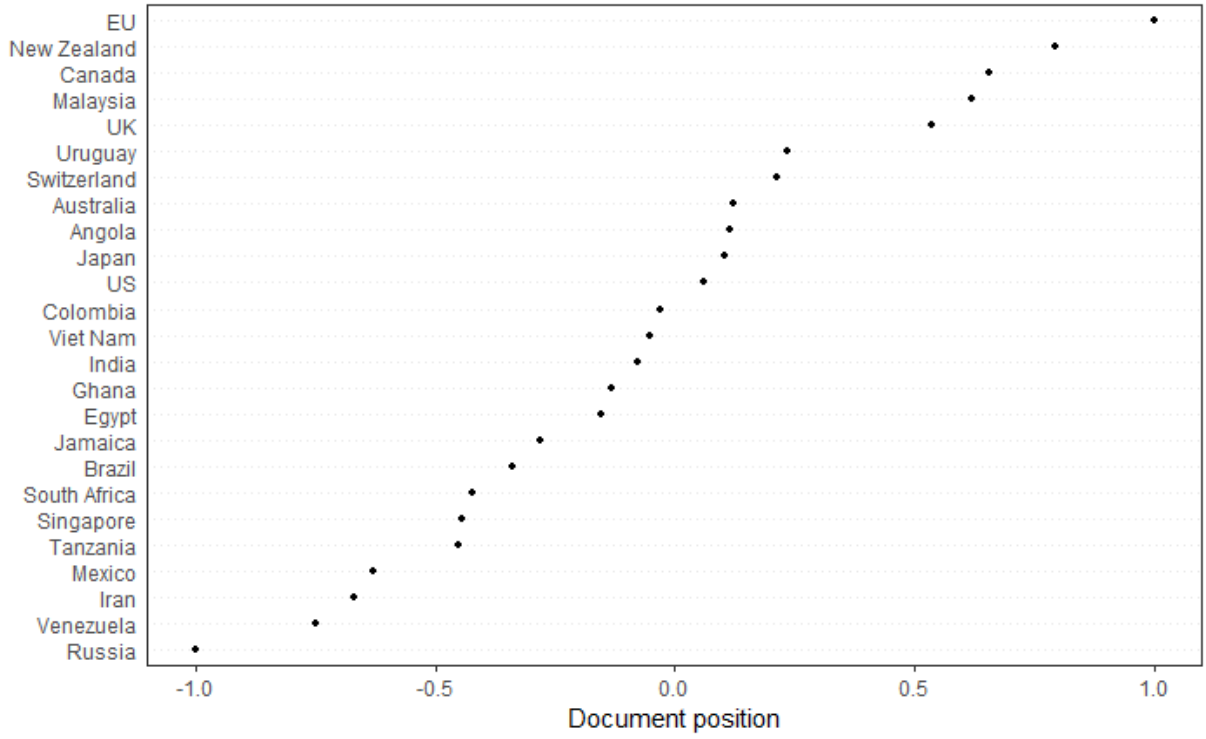

Figure 2: Positions (as submitted to AHC during the second session) relative to the EU and Russia in the AHC on Procedural measures and law enforcement.

[83] AHC fourth session. (21 January 2023). Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, Status as of 21 January 2023.
[84] AHC sixth session. (2 September 2023). Draft text of the convention, status as of 2 September 2023.
[85] AHC seventh session. (6 November 2023). Revised draft text of the convention.

On procedural measures and law enforcement, preferences in the AHC are more diverse, compared with criminalisation where most states' positions are closely aligned with the EU. Perhaps, the most salient issues of contention in this regard primarily entails the debate of whether powers and procedures specified in the treaty text should be subject to normative conditions (as favoured by the EU), this debate runs through multiple articles in relevant chapters. Notably, several states, including Japan and Singapore, that are more aligned with the EU in the area of criminalisation also argue that excessive safeguards could limit the opportunities for cooperation and the efficiency of the convention.[86] For instance, during the fourth session, Singapore is among the states that support deleting the article on conditions and safeguards altogether, along with Egypt, Malaysia, Pakistan, Oman, Russia, and Iran. [87] Incidentally, China did not support this deletion request, but proposed to amend the article by removing the reference to specific human rights and protection of privacy, but only to refer more generally to state party's domestic law and their obligations under applicable international human rights.[88] During the fourth and fifth sessions, there are also disagreements on data protection between the US and the EU, which is caused by the difference in personal data protection standards provided for in their respective laws and regulations.[89] In particular, the US proposed to remove references to 'protection of personal data' under Article 42 Section 1, which is opposed by the EU.[90] In the sixth session, while there is progress in the negotiation on conditions and safeguards – less states now propose the complete deletion of the article and the negotiation has become more technical and engaging. However, divergences remain on various issues, including the reference to legality, necessity, and proportionality, (2) whether the articles should be applicable only to the chapter or the entire convention, and (3) exact wordings of reference to human rights.[91]

[86] Walker. (June 2023). p.5.
[87] AHC fourth Session. (21 January 2023). Consolidated negotiating document Status as of 21 January 2023: Article 42.
[88] Ibid.
[89] Ibid.
[90] Also by Liechtenstein, Switzerland and Norway.
[91] AHC sixth session. (2 September 2023). Draft text of the convention, status as of 2 September 2023: Article 42.

Regarding the international cooperation chapter, ongoing debates are both technical and overarching,[92] where one of the most contentious issues is the range of mutual legal assistance: some states are vocal supporters of limiting cooperation, i.e., only for crimes specified in the convention, while some others seek the widest range possible, preferring the wording 'any criminal offence'. There have been intensive negotiations during the AHC fifth session, and efforts to compromise have been made. The EU has already indicated during the third session that it remains open to discussing the collection of electronic evidence for any type of crime, other than the crimes defined in this Convention, if the Convention provides for appropriate conditions and safeguards.[93] A notable idea inspired by the United Nations Convention against Transnational Organized Crime (UNTOC) is introducing the concept of 'serious crime', defined as 'an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty'.[94] The application of the concept of 'serious crime' is supported by both China and the US, while the EU proposed to further subject this provision to dual criminality. Table 3 is an overview of existing proposals on the range of mutual legal assistance and their supporters according to the AHC Fifth session consolidated negotiating document. As can be seem in Table 3, none of these proposals seem to have the support of even a single majority. Besides, although proposal 3 and 4 appear similar, what they could entail is very different, because not all offences established in the UN cybercrime convention would be considered 'serious crime'. In a domestic context, 57.23% of cybercrimes in China between 2016 and 2018 were in fact convicted with less than three years of imprisonment.[95]

[92] Walker. (June, 2023). p.8.
[93] AHC Third Session. (29 August–9 September, 2022). Compilation of proposals and comments submitted by Member States on provisions on international cooperation, technical assistance, preventive measures and the mechanism of implementation, the final provisions and the preamble of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. A/AC.291/12, p.57.
[94] United Nations. (2004). United Nations Convention against Transnational Organized Crime and the protocols thereto. Article 2.
[95] Chinese Judicial Big-data Institute. (2019). Characteristics and Trends of Cybercrime Special Report on Judicial Big Data.

Proposal	During AHC fifth session supported by
offences set forth in this Convention	Egypt, Mexico, Indonesia, US, Malaysia, Turkey, Nigeria, Iran, New Zealand, Canada, Syria, China, South Africa, Namibia, Costa Rica, Singapore
any criminal offence	Russia, Japan, Caribbean Community, Brazil, Argentina, Turkey, S. Korea, Australia, Algeria, Armenia, Cabo Verde, Nicaragua, Tonga
serious crimes	Norway, Japan, China, US, Georgia, Chad, Nigeria
serious crimes in addition to the offences established under this convention	China
offences provided that those are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least four years	EU

Table 3: Proposals presented during the fifth session for Article 61 Section 1(General principles and procedures relating to mutual legal assistance) and their supporters[96]

Another contentious issue is grounds to refuse mutual legal assistance: while China proposes to delete the section on grounds to refuse mutual legal assistance altogether, other states vastly differ in what those grounds should be. Table 4 offers an overview of a selection of proposals made during the AHC fifth session.

[96] AHC Fifth Session. (11-21 April, 2023). Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes - Status as of 21 April 2023: Article 61. Retrieved from: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf.

Proposal	Supported by	Opposed by
Request made is contrary to domestic law	Russia	EU, US
Risk of inhuman treatments, among others death penalty	EU, Liechtenstein, Georgia, Paraguay	US, Egypt, Singapore, Caribbean Community
The offence is considered a political offence	EU, Norway, Liechtenstein, Ghana, US, Georgia, New Zealand, Paraguay	Egypt, Singapore, Caribbean Community
Lack of dual criminality	EU, Japan, Egypt, Liechtenstein, China, Switzerland, Indonesia, Ghana, India, Georgia, S. Korea, New Zealand, Canada, Palestine, Syria	Russia, Argentina

Table 4: Selected Proposals presented during the fifth session for Article 61 Section 19 (Refusal of mutual assistance)[97]

[97] IbId.

4. Conclusion and discussion

This report has discussed China's interests in the making of international law on cybercrime, and its key findings are as follows: first and foremost, establishing a UN-based international treaty **in itself** is China's primary objective. Contrary to what existing (Western) literature often argue, China does not seem to envisage a UN cybercrime convention which should replace the Budapest Convention, as the diversity at the UN would hamper the AHC's ability to agree on unavoidably contentious issues which are meanwhile important to the functionality of the convention as a legal project. Rather, a UN-based treaty is preferred because China's view of the world order is UN-centric. On criminalisation, apart from cyber-dependent crimes, China also advocates to include a wide range of cyber-enabled crimes. While there are other valid hypotheses, this report argues that this position primarily stems from the challenges faced by Chinese law enforcement agencies in tackling those crimes. Some Chinese proposals are instead likely to be political in nature, for example that on 'act threatening public safety'. Unlike crimes such as online fraud and money laundering, 'acts threatening public safety' is not among the cybercrimes frequently prosecuted at Chinese courts according to available data.

Although Russia and China submitted a single position paper, which also proposed to include cyber operations targeting states,[98] such as attacking critical infrastructure, almost no Chinese literature reviewed by this report has discussed those issues under the framework of the UN Cybercrime Convention. This could mean the following: those issues, which would be better addressed under the framework of acceptable state behaviour in cyberspace, became a part of China's stated position principally as a result of coordination[99] with Russia, but they do not necessarily form a part of China's real concerns, interests or needs. Overall, various Chinese commentators recommended China to take a constructive approach of 'finding the common denominator', even if it could result in a treaty with a narrow scope (which is not preferred by China). This report's analysis of the consolidated negotiating documents also shows that the approaches taken by the Chinese delegation have been mostly constructive. For

[98] Which are unlikely to be committed by non-state-sponsored groups or individuals.
[99] Of course, it means that China has no overt objection to including those issues in the convention.

proposals which apparently contradict China's initial positions, the Chinese delegation has habitually suggested amendments, rather than deleting the article altogether.

Regarding China's coordination with other states prior to and during the AHC negotiation: it is true that the AHC negotiation is a Russian initiative, and Russia was also able to secure enough support in 2019 at the UNGA for its draft resolution to establish the AHC. Reasonably so, some existing literature written by Western commentators took a rather alarmist tone about Russia's clout in terms of its ability to shape the draft treaty text.[100] However, this report argues that it should not be overestimated. Indeed, there had been coordination efforts within BRICS and SCO regarding the UN cybercrime convention negotiation since the 2010s, while the coordination was about initiating the process of a UN-based cybercrime treaty, instead of about specific provisions in that treaty. Similarly, the Sino-Russian coordination was important in setting up the AHC under the framework of the UN, but the extent of their coordination during the negotiations should not be overestimated. Although Russia and China (along with several others) submitted a single position paper, they have most likely done so out of expediency – as a tactic to extract more compromises from Western delegations. The two consolidated negotiating documents as analysed in the previous chapter suggest that the Chinese delegation and their Russian counterparts have been acting independently from each other.

More generally, policymakers should be aware that a dichotomy between states that support a free and open internet against those that support the centred role of national government would be a poor predictor of states' preferences in the AHC negotiation. The negotiations at the AHC are nuanced and technical, although authoritarian countries overall tend to prefer a more expansive treaty with less safeguards, there is no generalisable pattern which is accurate enough to be relevant for delegations participating in the negotiation. States' positions need to be understood separately on different issues, taking into account their interests and needs in a contextualised manner.

[100] See e.g. Article 19. (17 February, 2022). Russia: Proposed UN Cybercrime Convention must uphold free speech. Retrieved from: https://www.article19.org/resources/russia-proposed-un-cybercrime-convention-must-uphold-free-speech/.;
Peters, A. (16 September, 2019). Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime. Foreign Policy. Retrieved from: https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/.

This report's analysed the positions in the AHC on the UN cybercrime convention's most contentious chapters: it shows that the EU is in a good negotiation position mostly in the area of criminalisation, whereas it could prove to be more laborious to achieve a preferred outcome in the treaty text on issues such as human rights safeguards and principles of mutual legal assistance. On criminalisation, a predominant majority of states are more aligned with the proposals initially presented by the EU. AHC chair has prepared a draft text of the convention for the sixth session in August 2023, based on the second reading of the negotiation: most of proposals that were previously under informal consultation, proposed by non-signatories of the Budapest Convention are not included in this draft convention,[101] and the draft text on criminalisation is so far fairly similar to the provision of the Budapest Convention. This most likely means that proposals from states favouring a wide range of criminalisation at the time did not expect to receive sufficient support.

During the sixth session, proposals to include a wide-range of cyber-enabled crimes and content-related crimes are once again tabled at the AHC, while there has been more progress and compromises made in other chapters.[102] This might seem counterintuitive, as it is unlikely that those proposals would ever receive sufficient support. However, there are two reasons why hardliner countries on a wide range of criminalisation would be motivated to do so. First, it is conceivable that some delegations at the AHC adopts an instrumentalist rather than a legalist approach to the formation of the UN Cybercrime Convention: they believe that the Convention will not/should not become a functional legal project, and the Convention should rather be devised as a normative project. This means a wider scope/criminalisation of the convention enjoys higher priority than specific provisions on procedures and international cooperation on delegations' agenda. Second, as mentioned earlier in the report, proposals on criminalisation at such late stage of the negotiation can be a part of a 'quid pro quo' negotiation strategy, since issue linkage could be an expedient tactic when the negotiation is deadlocked. Third, it is also

[101] Article 13-17, 20-24, 26-32, 34, and 37 from the fourth session's negotiating document are not included in the draft treaty text prepared for the sixth session. Among which, only article 17 on the infringement of copyrights is likely proposed by signatory-states of the Budapest Convention.
AHC fourth Session. (21 January, 2023). Consolidated negotiating document.
AHC Sixth Session. (29 May, 2023). Draft text of the convention. A/AC.291/22. Retrieved from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V23/039/51/PDF/V2303951.pdf?OpenElement.
[102] AHC sixth session. (2 September 2023). Draft text of the convention, Status as of 2 September 2023 with updates from Member States.

possible that some states' delegation at the UN does not have the full mandate to make changes to the instructions they have received, and they re-table proposals to include other offences because it was the pre-determined course of action. Contrary to what the alignment of states' positions on criminalisation might suggest, criminalisation is likely to remain a contentious issue during the seventh session.

In comparison with criminalisation, states' preferences in procedural measures and law enforcement and international cooperation are much more diverse, and there seems to be little unity/coordination among signatories of the Budapest Convention. Apart from political and foreign policy considerations which are already extensively discussed in existing literature, states' preferences in those chapters are also strongly determined by their domestic laws.[103] This brings difficulties to assessing the possibilities of compromise, as states' priorities are often shaped in their distinct domestic political contexts. Regarding China's position, although Chinese scholars have generally advocated for fewer safeguards to be included in the convention, fearing that safeguards would hinder cooperation, they do not elaborate on exactly which safeguards should not be included in the convention: this could mean that although China prefers less safeguards to be referred to in the convention in general, none of the specific safeguard would constitute a 'deal-breaker'. Of course, one 'safeguard' that China insists should be referenced in chapter 3 and 4 is sovereignty: this includes primarily the issues of jurisdiction and transborder access of data. Parenthetically, sovereignty is usually not considered to be a 'safeguard', as the term usually exclusively refers to human rights considerations. However, it is imperative to point out that the discussions of sovereignty (favoured by Russia and China among others) and human rights in chapter 3 and 4 are identical in the sense of limiting the functionality of the convention: they both would serve as grounds for refusing cooperation.

Besides, one dynamic delegations to the AHC need to proactively consider is that many developing countries take no principled position on substantive issues such as criminalisation or the range of sharing evidence, while calling for the widest measure of beneficiary-driven technical assistance for collecting e-evidence for investigations and prosecutions. Provisions on technical assistance could entice would-be beneficiaries to align their positions with would-

[103] E.g. US and Singapore oppose including 'risk of death penalty' as a reason to refuse legal assistance.

be funders. Some African countries voiced against reference to transparency, accountability, human rights, and gender-mainstreaming training, citing concerns that it would hinder access to assistance.[104] However, it is unlikely that the EU would, or could, compromise on those issues, as it is constrained by its long-standing normative commitments. Other contentious issues regarding technical assistance include possible technology transfer under the framework of technical assistance. Among would-be funders, a number of European countries and the US have voiced against, while China expressed support for technology transfer.[105] Overall, China would probably have more manoeuvrability than the EU and thus be in a better position to use technical assistance as a leverage to secure more support for its proposals in other chapters from the group of would-be beneficiaries, which, as needs to be stressed, is sizable in the number of votes. Moreover, enlisting the support of developing countries in the AHC by advocating for narrowing the digital gap and offering technical assistance is indeed suggested by some Chinese experts as a negotiation strategy.[106]

Lastly, while reaching compromise on the draft treaty text in the way that is acceptable to a wide majority of states is essential for the AHC to move forward, adopting more ambiguous languages inevitably entails its own risks. As Walker (2023) points out, such risks has potential to advance state repression and establish new international norms that would formalise these practices into international law.[107] Such risk is most pronounced when states with harsh punitive laws interact with each other.

[104] Walker. (June, 2023). p.10.
[105] Ibid. p.11.
[106] E.g. Li, Y. (2020).
[107] Walker, S. (2023). Closing Pandora's Box – UN Cybercrime Treaty Negotiations. Global Initiative against Transnational Organised Crime.