The Impact of Stereotyping on International Cyber Norm-making: Navigating Misperceptions and Building Trust

Fan Yang

February 2025

GCSP Policy Brief No.19

GCSP
Geneva Centre for
Security Policy

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 55 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

The GCSP Policy Briefs Series

The GCSP Policy Briefs series addresses current security issues, deduces policy implications and proposes policy recommendations. It aims to directly inform policy- and decision-making of states, international organisations and the private sector.

Under the leadership of Ambassador Thomas Greminger, Executive Director of the GCSP, the series is edited by Professor Nayef Al-Rodhan, Director of the Geopolitics and Global Futures Department, and Doctor Tobias Vestner, Director of the Research and Policy Advice Department & Head of Security and Law, and managed by Ms Christine Garnier Simon, Administration and Coordination Manager, GCSP Geopolitics and Global Futures.

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

ISBN: 978-2-88947-436-3

The views, information and opinions expressed in this publication are the author's own and do not necessarily reflect those of the GCSP or the members of its Foundation Council. The GCSP is not responsible for the accuracy of the information.

About the author

Dr Fan Yang leads the Cyberspace International Law Center at the Xiamen University School of Law and provides consultancy to the Chinese government on negotiations and consultations at various international forums, including the UN Ad Hoc Committee on Countering Cybercrime and the UN OEWG process. He is also actively involved in a series of Track 1.5 and Track 2 dialogues on international governance in cyberspace, notably serving as the liaison and expert for the Sino-European Expert Working Group on the Application of International Law in Cyberspace.

Introduction

Over the past three decades, cyberspace – a digital realm shaped by both technological and social dynamics – has evolved into a domain where a wide range of human activities now take place. These activities are marked by their anonymity, which complicates attribution, and their instantaneity, which challenges timely regulation. To address these challenges, states focus on two approaches: applying existing laws and creating new ones. While there is a general consensus that cyberspace should be governed by the rule of law, including international law, the application of existing legal frameworks to cyberspace remains an evolving challenge both in terms of state practice and academic discourse. At the same time, the international community has consistently sought to develop new norms to promote good governance in cyberspace.

Against this backdrop, states – especially those with advanced cyber capabilities – are engaging in a competitive game of norm-making, striving to exert influence in shaping international rules to govern cyberspace.[1] As part of this process, states often categorise each other by trying to highlight their counterparts' most distinct characteristics. While such labelling is common in diplomatic interactions, it is particularly problematic in the context of international cyber norm-making. Labels reflect and reinforce stereotypes, which often oversimplify the complexities of states' behavioural patterns in cyberspace and their underlying logic. States are thus roughly grouped by opposing indicators, such as those viewing cyberspace as a global commons versus sovereign territory, those advocating for an interconnected free Internet versus a fragmented "splinternet", or those favouring multistakeholderism versus multilateralism as the dominant approach to the governance of cyberspace. Once established, these stereotypes are difficult to dismantle and can lead to distorted perceptions that obstruct constructive dialogue.

This GCSP Policy Brief aims to identify the potential security challenges posed by stereotyping in international cyber norm-making processes. It then illustrates the policy implications of this problem and offers policy recommendations.

[1] See, e.g., D.B. Hollis, "China and the US Strategic Construction of Cybernorms: The Process Is the Product", Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1704, 7 July 2017, https://www.hoover.org/sites/default/files/research/docs/hollis_china_and_the_us.pdf.

Security challenges

States' stereotyping of their counterparts can be witnessed in various multilateral cyber norm-making forums. This is evident in almost all the leading processes for states to debate international norms in cyberspace, such as the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, its predecessor, the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace, and the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes (Ad Hoc Committee). The phenomenon of such stereotyping and its impact become especially apparent when we examine specific cases, such as the recent example of the negotiation of a multilateral convention on combatting cybercrime.

In August 2024, the Ad Hoc Committee concluded its negotiations[2] when the contracting parties adopted by consensus the draft UN Cybercrime Convention (UN Convention),[3] which was adopted by the UN General Assembly[4] just days before the end of 2024 and will come into force once it is ratified by at least 40 UN member states. Aiming to enhance domestic law enforcement and international cooperation to combat cybercrime, the UN Convention closely resembles the Budapest Convention on Cybercrime (Budapest Convention)[5] in terms of both the structure of its chapters and the wording of specific articles. This is not at all surprising, because states representing differing interests engaged one another in the negotiations and were likely to ultimately reach a consensus that only reflects the common denominators of their divergent positions. For those who have long supported expanding the Budapest Convention into the global legal foundation for international cooperation in combatting cybercrime, the adoption of the UN Convention in its current form should have been deemed a favourable outcome, if not a de facto "globalisation" of the Budapest Convention. However, the reactions we saw from public opinion expressed in various English-speaking media outlets do not seem to support this view.

Although few states parties have released official statements on the UN Convention, human rights organisations, advocacy groups, and academic voices have actively expressed their critiques, and the criticisms are likely to continue to grow. These voices have largely converged into a mainstream position that

[2] UNODC (UN Office on Drugs and Crime), "Reconvened Concluding Session of the Ad Hoc Committee", https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main.

[3] UNGA (UN General Assembly), Countering the Use of Information and Communications Technologies for Criminal Purposes, A/79/460 of 27 November 2024, https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf.

[4] V. Mishra, "UN General Assembly Adopts Milestone Cybercrime Treaty", UN News, 11 December 2024, https://news.un.org/en/story/2024/12/1158521.

[5] Council of Europe, Convention on Cybercrime, Budapest, 23.XI.2001, https://rm.coe.int/1680081561.

is either critical of the UN Convention[6] or expresses disappointment with the draft that was adopted.[7] This stands in stark contrast to the acclaim the Budapest Convention keeps receiving since its adoption.[8] An examination of the possible reasons for this difference is particularly intriguing. It seems that many of the critics of the UN Convention are influenced by negative stereotypes. A typical line of such thinking may look like the following: the UN Convention's negotiation process was mainly advocated by the anti-Budapest Convention camp, a particular group of states that did not participate in the negotiation of the Budapest Convention and consistently opposed its expansion; most of the states from this camp are labelled as "digital authoritarians"; and any negotiation outcomes yielded by this inherently flawed process are thus born with this "original sin", even though the UN Convention extensively follows the legal philosophy and legislative technique of the Budapest Convention. Criticisms grounded in such stereotypes are often overly simplistic. A nuanced examination will show that these assumptions are, in many cases, unfounded.

Stereotypes

Stereotypes in existing commentaries include, among others, claims that the UN Convention could enable state parties to tighten control over online expression, impact press freedom, or overemphasise state sovereignty at the expense of human rights protections. This policy brief does not aim to examine all such stereotypes in depth, but will focus on two typical examples in the following analysis.

One typical stereotype is that the provisions in the criminalisation chapter of the UN Convention are vaguely worded, allowing states parties to misuse them in the name of fighting cybercrime and disproportionately target civil society – especially the tech community. For example, Articles 7 and 11 of the UN Convention criminalise "illegal access" and "misuse of devices", respectively. Critics argue that "digital authoritarian" states could leverage these provisions as a basis to strengthen control of network system vulnerabilities, with cybersecurity practitioners potentially being prosecuted for conducting vulnerability tests or publishing discovered vulnerabilities.[9]

At first glance, this stereotype seems plausible; however, it fails under closer examination. Firstly, the two articles in question largely replicate Articles 2 and

[6] T.B. Bacherle, "The UN Cybercrime Convention Is a Victory for Digital Authoritarianism", EURACTIV, 16 August 2024, https://www.euractiv.com/section/law-enforcement/opinion/the-un-cybercrime-convention-is-a-victory-for-digital-authoritarianism/.

[7] K. Bannelier and E. Lostri, "Is Anyone Happy With the UN Cybercrime Convention?", LAWFARE, 2 December 2024, https://www.lawfaremedia.org/article/is-anyone-happy-with-the-un-cybercrime-convention.

[8] See, e.g., Cybercrime Convention Committee, *The Budapest Convention on Cybercrime: Benefits and Impact in Practice,* Council of Europe, 2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac; see also A. Adams and D. Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention", LAWFARE, 9 December 2024, https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention.

[9] Bacherle, 2024.

6 of the Budapest Convention, respectively. A doctrinal reading reveals that the "misuse of devices" article explicitly requires *intent* to establish criminal liability, clarifying that the "authorized testing or protection of ICT systems" is not punishable. Secondly, the criminalisation provisions in the UN Convention are not automatically applicable to domestic laws: state parties must enact corresponding laws in their own legal frameworks, which are often subject to national legislative procedures and constitutional oversights. This ensures that the UN Convention's provisions will not automatically result in overly broad criminal laws. Finally, the UN Convention's negotiation history shows that after extensive debate, the "narrow" approach to criminalisation that states agreed upon largely mirrors the Budapest Convention's practice. This outcome should have been recognised as a diplomatic achievement of the pro-Budapest camp.

Another typical stereotype focuses on the UN Convention's human rights protections, claiming that they are weak and insufficient to safeguard against the potential misuse of state power in the enforcement of laws to deal with cybercrime. Critics argue that the "conditions and safeguards" provisions in the UN Convention (Articles 24 and 35, corresponding to Articles 15 and 23 of the Budapest Convention, respectively) are overly formalistic and inoperable, and fail to meet international human rights standards. Some critiques dismiss the inclusion of the "principle of proportionality" as inadequate, arguing that it neglects the necessity and legality principles central to international human rights law.[10]

This stereotype overlooks the core purpose of the UN Convention, which prioritises the effective prevention and combatting of cybercrime, with human rights protection being a secondary but important concern. A cybercrime convention cannot be expected to serve as the primary instrument for human rights protection in the digital age; this issue is better addressed by other international mechanisms. Furthermore, the UN Convention includes Article 6, which mandates respect for human rights, explicitly listing fundamental freedoms such as freedom of expression, conscience, and assembly. This also represents an advance compared to the Budapest Convention, which lacks such a dedicated human rights article. However, due to the lack of parity of legal protections conferred by international instruments of human rights, one cannot deny that criticisms grounded in comparisons to European legislation to protect human rights, particularly that conferred by the European Convention on Human Rights, would be more logically coherent. Nevertheless, few cases have been brought before the European Court of Human Rights concerning the Budapest Convention, which, it could be argued, undermines the validity of these critiques.

[10] K. Mahadik, "Should India Vote to Adopt the UN Cybercrime Treaty? Tech Policy Expert Weighs In", *Indian Express*, 23 August 2024, https://indianexpress.com/article/technology/tech-news-technology/should-india-vote-to-adopt-un-cybercrime-treaty-9527899/.

Reverse stereotypes

Stereotyping is not a one-way practice, and reverse stereotypes exist. It is therefore important to examine the biases that appear mainly in discussions within the anti-Budapest Convention camp, and evaluate how these shape the commentators' perceptions of the Budapest Convention and its supporters.

A common reverse stereotype is that the criminalisation clauses of the Budapest Convention are outdated and no longer suited to the practical needs of states to collaboratively combat malicious activities in cyberspace. This critique had served as one of the justifications for initiating the UN's multilateral process. However, since the criminalisation chapter of the UN Convention closely mirrors that of the Budapest Convention, this stereotype needs to be reassessed. In reality, the proponents of the UN Convention have not given adequate attention to updating these clauses as they have claimed. Instead, the issue seems to remain open for further discussion. Freeing ourselves from this stereotype would enable us to engage more openly with at least two related key questions.

If additional criminalisation clauses were to be introduced into the UN Convention through subsequent negotiations, it would be important to assess whether the proposed need to criminalise certain cyber activities are shared broadly across the international community. For example, online gambling is a major concern in China's cybercrime governance, but may not occupy the same priority for many states within the pro-Budapest Convention camp. Similarly, while Article 291(a) of China's Criminal Law criminalises the fabrication and dissemination of false information,[11] introducing this as an international crime would likely face significant opposition due to ideological and value differences, because some states would value freedom of speech over the regulation of disinformation and misinformation.

We should also reconsider whether the “narrow” approach to criminalisation could already provide sufficient foundation for cooperation in combatting cybercrime. Think about the provisions of the UN Convention on "illegal access", "illegal interception”, "interference with electronic data", "interference with an ICT system" and "misuse of devices". Because these clauses are broad and general, other criminal activities than those prescribed in the UN Convention may trigger these behaviours when they are perpetrated in cyberspace. For example, the infringement of laws governing personal information may likely involve illegal access to a computer system or the misuse of devices. Although the UN Convention has not yet criminalised such an infringement, states could still devise prosecution strategies to bring such acts into the scope of the convention by linking them to existing clauses. This method is not always applicable, particularly when the perpetrators are legitimate holders of personal information. But it allows for some flexibility and adaptability in

[11] Criminal Law of the People's Republic of China, Article 291(a), 1 July 1979, as amended, http://en.npc.gov.cn.cdurl.cn/2020-12/26/c_921604_13.htm.

addressing cybercrimes within the limitations caused by the “narrow” approach to criminalisation.

Another reverse stereotype involves the caution surrounding invasive cross-border evidence-collection provisions. Critics usually argue that these provisions pose a threat to judicial sovereignty and law enforcement power. This stereotype is particularly associated with Article 32(b) of the Budapest Convention, which allows law enforcement agencies of one contracting party to access data held by a data controller in the jurisdiction of another contracting party without that party's prior consent, provided that data controller expresses its legal and voluntary consent. Given the rise of unilateral cross-border data collection for law enforcement, this concern warrants further consideration.

In practice, when law enforcement agencies or judicial bodies seek to obtain electronic evidence from abroad, they are more likely to rely on domestic laws than international treaties. For example, US law enforcement agencies may use the Clarifying Lawful Overseas Use of Data Act (the so-called CLOUD Act) to collect data from US-based data controllers overseas, while US courts may compel parties to submit electronic evidence stored abroad based on the rules of evidence disclosure. This means that the real threat to a country’s judicial and law enforcement sovereignty may come from extra-territorial domestic laws enacted by foreign governments rather than international treaty provisions that are often more cumbersome to enforce.

Security challenges

The preceding discussion of the bidirectional stereotypes associated with the UN Convention can be logically extended in order to examine the security challenges that stereotyping may cause in international cyber norm-making. It goes without saying that any obstacle – such as stereotyping – that impedes the effective norm-making process as a promising way to address security threats would in itself become a threat to security. This is because international society promotes cyber norms primarily to address various cyber governance challenges, and the effectiveness of the norms created directly affects how well states could cooperatively counter those challenges. More specifically, stereotyping in the context of international cyber norm-making poses security challenges, because it may hinder meaningful negotiations, perpetuate misperceptions, magnify antagonism into hostility that spills over to broader diplomatic relations, and exacerbate cybersecurity dilemmas.

Firstly, when states enter into diplomatic dialogues discussing cyber norms, they may be driven by stereotypes to instinctively object to a proposal without substantive grounds simply to express opposition for its own sake, hence blocking meaningful and constructive negotiations. Instead of pursuing a reasoned and objective debate, states might simply affirm their pre-established positions spurred by preconceived biases, rather than undertake a proper evaluation of the merits of the issue at hand. This dynamic makes it harder to reach consensus or compromise. For instance, the negotiating process of the

UN Convention was at times protracted because states would reject proposals (such as criminalising a particular type of harmful cyber activity) initiated by specific states based on their preconceived negative impressions of these states (such as suspicions that the pretext of fighting cybercrime might be used as a cover for persecution or repression).

Secondly, stereotyping perpetuates misperceptions, because by their very nature, biases are static and one-sided. They tend to capture only simplified or exaggerated aspects of a state's behaviour, failing to adequately reflect the complexity of political calculations or the nuances in deciding on priorities and taking actions in the international arena. What is more troublesome is that stereotyping is often self-fulfilling and self-reinforcing. States that hold stereotypical views are more likely to interpret subsequent interactions in a way that validates their preconceptions. This can lead to a cycle where misconceptions become entrenched.

Thirdly, antagonism generated by stereotyping in a specific track of cyber-related dialogue can extend beyond the immediate negotiations and affect other diplomatic processes, because different stereotypes regarding the same targets often corroborate each other. States deemed to support multilateralism in cyber norm-making are labelled digital authoritarians, while states in favour of multistakeholderism are seen as discouraging or opposing cyber sovereignty. This is why we can observe similar patterns of confrontation and division into camps of states with broadly opposing approaches emerging in diplomatic processes vis-à-vis responsible state behaviour in cyberspace and on combatting cybercrimes.

Fourthly, stereotyping in international cyber norm-making exacerbates a basic cybersecurity dilemma. As a well-known phenomenon in international relations, the security dilemma refers to the paradoxical situation where actions taken by one state to enhance its security inadvertently threaten other states, leading to an arms race or heightened tensions.[12] In the context of cyber governance, if one state stereotypes another as a potential cyber threat, this may lead to an aggressively defensive posture or may even provoke pre-emptive measures. This security dilemma may even result in negotiations or other types of international interaction ending up in deadlock, because stereotyping involves imposing malicious intent or motivation on actors even when they may not possess such intent. Once a stereotype regarding malicious intent is established, it is difficult to dispel. States labelled as "cyber threat actors" find it particularly difficult to prove that this is not the case, even if their actions are based on defensive or neutral motives. This dynamic makes it challenging to foster trust and confidence in cyber-related diplomacy.

In light of these challenges, it becomes clear that the presence of stereotypes in international cyber norm-making not only undermines the potential for

[12] See, e.g., A. Wivel, "Security Dilemma", in B. Badie et al. (eds), *International Encyclopedia of Political Science*, pp.2389-2391, https://www.researchgate.net/publication/320211391_Security_dilemma.

cooperation, but also exacerbates existing international tensions. Overcoming these biases requires intentional efforts to promote self-awareness and more nuanced understandings of this problem, and to create opportunities for open, objective, constructive dialogue.

Policy implications

The findings related to the problem of stereotyping in international cyber norm-making have the following policy implications.

Stereotyping hinders the international legalisation of cyberspace

International society relies on norm-making to promote the legalisation of cyberspace, which refers to the extent to which cyberspace is regulated in terms of established legal rules and accompanying legislation. States engage in this process to achieve three policy goals: (1) to address shared challenges associated with cyber activities, (2) to foster a more regulated digital realm, and (3) to assert influence over the norm-making process to strengthen their geopolitical standing. To illustrate, we can look again at the negotiating process that led to the adoption of the UN Convention. Through this multilateral norm-making endeavour, the contracting parties primarily focused on crafting an international legal framework that would enhance the collective ability to combat transnational criminal activities occurring in or through cyberspace. Naturally, ensuring human rights protections is a central concern during these negotiations, particularly since the criminalisation, investigation, and prosecution of cybercrimes and the imprisonment of the perpetrators all involve significant exercises of state power. In the negotiation process one can detect a distinct pattern of states vying to exert influence. The debates often revolved around whether this multilateral law-making process at the UN should be initiated; who got to set the agenda; and the specifics of proposals on criminalisation, the collection of electronic evidence, and international cooperation.

Among the three policy goals, stereotyping poses a significant barrier to achieving the first two, but paradoxically serves as a convenient – albeit counterproductive – tool for pursuing the third.

Firstly, stereotyping significantly impedes the development of substantively effective international cyber norms. The process of creating norms requires a nuanced understanding of the diverse perspectives and concerns of the states involved in the negotiations. Stereotypes reduce this complexity by forcing states into narrow, predefined categories. When states are perceived through biased lenses, the scope of negotiations becomes limited, and the development of comprehensive and balanced cyber norms is hindered. This lack of nuance can result in the creation of norms that fail to adequately address the challenges faced by all states.

Secondly, as states become entrenched in their belief in specific stereotypes, the negotiation process itself becomes less about aligning values and more about reinforcing preconceived ideas. States may dismiss proposals or resist compromises that they believe are not aligned with their stereotypical view of another state. The inability to move beyond stereotypes thus makes it more difficult to establish cyber norms that are inclusive, progressive, and capable of advancing norms for a more responsible and ethical cyberspace.

Thirdly, in the game of exercising influence in norm-making, labelling and stereotyping can be a useful skillset because they may help states to identify "friends" and "foes". But they often oversimplify what should ideally be nuanced discussions, fostering antagonism and reducing dialogues to binary conflicts. This dynamic not only obstructs constructive engagement, but also diminishes the likelihood of meaningful progress in developing international cyber norms.

Stereotyping entrenches cyber divides

The presence of stereotypes in international cyber norm-making discussions risks entrenching existing divides between different states, regions and groups. Many current cyber governance frameworks are influenced by the priorities and perspectives of powerful states, particularly in the West. Less advanced states are more often on the receiving end of this process, allowing them to contribute relatively little to global processes and thus to have only a marginal impact on global discourse. Stereotypes can perpetuate these divides by framing certain regions or states as ICT technology abusers, safe havens for cybercriminal, or reactionary agents that oppose human rights protection in the digital sphere, etc.

Moreover, these entrenched stereotypes create a feedback loop where states on the receiving end of this kind of labelling may become resistant to adopting global norms, perceiving them as biased or imposed by particular state actors rather than negotiated by all concerned. As a result, global cyber governance risks becoming increasingly fragmented, with the various global regions adopting conflicting approaches to cyber norms based on their own interests and concerns. The concern that the decoupling of tech standards would lead to a “splinternet” is not merely a fantasy. In this regard, the divergence in values and approaches to governance will weaken the international community’s ability to address common cyber-related challenges that are spreading rapidly into emerging areas such as AI safety.

In addition to deepening cyber divides, stereotyping erodes states’ mutual trust, which is foundational to successful diplomacy. Trust between states allows for the sharing of sensitive information, the negotiation of compromises and the implementation of collective actions. When states stereotype each other, trust is undermined by preconceived notions about intentions and capabilities. This leads to a more cautious, less open approach to international negotiations. Such a lack of trust fosters a hostile or competitive environment, making it challenging to develop meaningful and lasting cyber norms.

Professionalism can counter stereotyping

One key lesson learned from years of experience in cyber dialogues on Confidence Building Measures (CBMs) is that professionalism – referring to the expertise-driven prioritisation of technical specifics and neutral benchmarks – can play a crucial role in curbing stereotyping. This can be corroborated by the various discussions on applying existing international laws in cyberspace that function as a parallel endeavour to international cyber norm-making. While the latter is primarily driven by diplomatic negotiations, the former involves academic input, which enriches the nuances of the process and helps mitigate biases.

Professionalism can significantly assist international norm-making because it can establish a framework for dialogue that fosters clarity, precision and mutual understanding. Firstly, dialogue among professionals relies on a uniform and mutually agreed lexicon, so that the participants are more likely to share a common understanding of terms, concepts and issues. This reduces the risk of misinterpretation and the imposition of biased assumptions. Secondly, professional discussions dive into the details, which goes beyond superficial assessments and addresses the complexities of the issues at hand. This depth of engagement allows for more nuanced understandings of these issues and discourages oversimplifications. Thirdly, professional debates follow structured formats, ensuring that exchanges remain focused and respectful. Organisational patterns of this kind help to maintain the integrity of the conversation, preventing it from descending into emotionally charged or simplistic adversarial exchanges.

Like other processes for enacting rules, international cyber norm-making crucially hinges on how relevant actors participate in the process. In line with the theory of communicative action, professionalism enables participants to engage in a process of dialogue aimed at reaching mutual understanding and consensus that is as free as is humanly possible from distortion. It has been argued that communicative action, grounded in rational discourse and the pursuit of common ground, provides the ideal conditions for overcoming misunderstandings and biases.[13] In this sense, professionalism does not merely mitigate the impact of stereotypes, but creates the conditions necessary for constructive and inclusive dialogue.

[13] See J. Habermas, *Between Facts and Norms*, trans. W. Rheg, Massachusetts, MIT Press, 1998.

Policy recommendations

The international cyber norm-making process is becoming increasingly geo-politicised and crippled by stereotypes. To mitigate this trend, several adjustments are needed. Heightened awareness of the problem itself should be a critical first step. Based on the preceding analysis, this policy brief offers the following three policy recommendations.

Firstly, diplomats directly involved in international cyber norm-making must recognise the problem of stereotyping and its negative impact. They should approach negotiations in terms of professionalism, a willingness to engage constructively, and an open mind. It is crucial for diplomats to build personal connections with their counterparts to foster mutual understanding and reduce the likelihood of stereotyping, allowing for more effective dialogue and cooperation.

Secondly, professionals with different affiliations – such as government officials, think tank researchers, consultants and critics – can exercise constructive influence over each specific track of the international cyber norm-making process. They should actively highlight the dangers of stereotyping and its corrosive effects on international cooperation. Instead of reinforcing harmful stereotypes, professionals should advocate for more accurate and more nuanced understandings of the issues at hand. They can also help states to identify common ground and align their priorities, contributing to a more substantive and cohesive international dialogue.

Lastly, and more broadly, states should periodically review the impact of stereotyping on their diplomatic efforts to establish norms to govern cyberspace. It is important for states to incorporate discussions of this problem into inter-state dialogues and explore ways to minimise its effects. States should also examine domestic processes and institutions that may perpetuate stereotypes, whether in policy development, media production, or public discourse, and work to counter these influences to prepare for more informative and constructive international engagements.

Conclusion

In conclusion, the issue of stereotyping in international cyber norm-making presents significant challenges to the development of effective, cooperative and inclusive frameworks for addressing global cyber threats. As has been demonstrated throughout this policy brief, stereotypes distort perceptions, fuel antagonism and obstruct meaningful collaboration. These biases are not only self-reinforcing, but also exacerbate existing tensions, ultimately undermining the goals of international cooperation, effective norm development, and the management of the security dilemma.

The policy implications of stereotyping in international cyber norm-making are far-reaching. Stereotyping weakens trust between states, hinders the development of comprehensive cyber norms and deepens cyber divides. These outcomes threaten not only the progress of norm-making processes, but also the broader goal of creating a secure, stable and cooperative global cyberspace.

To address these issues, enhancing professionalism is key, and a multifaceted approach is required. Diplomats must remain vigilant to the dangers of stereotyping, and attempt to engage in discussions with other countries with an open mind that can foster human connections to build trust and cooperation. Professionals in related fields should advocate for a nuanced understanding of global actors, highlighting the destructive impact of stereotyping. Finally, states must recognise the problem, incorporate it into diplomatic dialogues and examine domestic processes that may perpetuate harmful stereotypes.

The path forward is not without its challenges, but with collective effort and a commitment to overcoming biases, there is ample opportunity to strengthen international cyber governance. By mitigating the impact of stereotyping, we can create a more collaborative and effective approach to managing the complexities of cybersecurity and its governance in the digital age.

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
E-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-436-3

GCSP
Geneva Centre for
Security Policy