

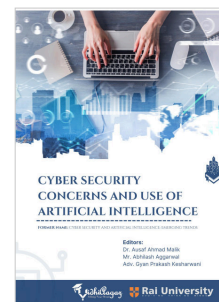
CHAPTER 43

UN Convention on Cybercrime: The Concept, Concerns and Negotiations

Sneha M. and Pooja Shree

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 360–368

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Sneha M. & Pooja Shree, *UN Convention on Cybercrime: The Concept, Concerns and Negotiations*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 360 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Sneha M. and Pooja Shree, 'UN Convention on Cybercrime: The Concept, Concerns and Negotiations' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 360.

CHICAGO (17TH ED.)

Sneha, M., and Pooja Shree. "UN Convention on Cybercrime: The Concept, Concerns and Negotiations." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 360–368. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-43/>.

APA (7TH ED.)

Sneha, M., & Shree, P. (2024). UN convention on cybercrime: The concept, concerns and negotiations. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 360–368). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-43/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-43/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

UN CONVENTION ON CYBERCRIME: THE CONCEPT, CONCERNS AND NEGOTIATIONS

Sneha M.⁸⁰ and Pooja Shree⁸¹

ABSTRACT

Is the new draft of the United Nations Convention on Cybercrime an advancement in policy or diplomacy? This paper aims to answer the same. The rapidly evolving cyber threat landscape necessitates robust international cooperation, prompting the development of the UN Convention on Cybercrime. This landmark agreement aims to harmonize national laws, enhance international cooperation, and safeguard human rights in the face of escalating cyber threats. However, its implications for global cybersecurity governance warrant critical examination.

This study provides an in-depth analysis of the UN Convention on Cybercrime, focusing on the interplay between cybersecurity, human rights, and state sovereignty. A comprehensive review of the Convention's provisions reveals both strengths and weaknesses. On one hand, the Convention addresses emerging cyber threats, promotes international cooperation, and establishes guidelines for cybersecurity governance. On the other hand, concerns persist regarding human rights protections, the effectiveness of international cooperation mechanisms, and the Convention's adaptability to technological advancements.

The research investigates key questions inclusive of,

- 1. Human Rights Protections: How effectively does the Convention balance cybersecurity concerns with human rights safeguards?*
- 2. International Cooperation: What mechanisms does the Convention establish for inter-state cooperation, and how can they be improved?*
- 3. Technological Adaptability: How well does the Convention accommodate emerging technologies and evolving cyber threats?*
- 4. State Sovereignty: How does the Convention navigate tensions between national sovereignty and global cybersecurity governance?*

The findings contribute to the ongoing discourse on cybersecurity governance, informing policymakers, scholars, and stakeholders. This research aims to:

- 1. Inform policy decisions on cybersecurity governance and human rights protections.*
- 2. Enhance understanding of international cooperation mechanisms in cybersecurity.*
- 3. Foster dialogue on the Convention's limitations and potential revisions.*

By examining the UN Convention on Cybercrime through a critical lens, this study sheds light on the complexities of cybersecurity governance and offers recommendations for addressing the challenges ahead.

INTRODUCTION

Cybercrime has emerged as a pervasive and insidious threat to modern society, the exponential growth of the internet and interconnected technologies has created vast opportunities for malicious

⁸⁰ Student at KLE Society's Law College, India.

⁸¹ Student at KLE Society's Law College, India.

actors to exploit vulnerabilities, steal sensitive information, and disrupt critical infrastructure.

The far-reaching consequences of cybercrime transcend national borders, affecting individuals, businesses, governments, and entire economies. From identity theft and financial fraud to ransomware attacks and cyber espionage, the scope and complexity of cybercrime have escalated dramatically.

As the digital revolution continues to reshape the global landscape, the need for effective cybersecurity measures and international cooperation has become imperative. The UN Convention on Cybercrime attempts to address its global impacts, and the imperative for collective action to combat this burgeoning threat.

THE BUDAPEST CONVENTION

The first multilateral instrument to attempt global cybercrime regulation would be The Europe-led Budapest Convention, an international treaty focused on harmonizing national laws, and improving investigative techniques.

India is not a signatory to this convention, as it was negotiated and drafted without its participation, another primary contributor towards India's disinterest in the Budapest Convention would be, according to the Intelligence Bureau (IB), India, exchanging data with foreign law enforcement agencies would violate India's national sovereignty.

More prospective signatories opted out with the primary concern stemming from the limited involvement in its drafting process, leading to reservations about ratifying the treaty. India, for instance, has opted out, citing a lack of participation in its creation.

Another significant obstacle is the perceived threat to national sovereignty. Russia, among others, had expressed opposition, arguing that the Convention would undermine their autonomy and compromise law enforcement cooperation.

Major drawbacks of the Budapest Convention would be that it reflected Eurocentric focus, it faced negotiations from Russia and China as it was perceived to overstep national sovereignty of the party states, this would also be a primary cause for the lack of interest in the instrument.

The Budapest Convention also faced criticism due to the lack of safeguards provided for privacy and freedom of expression in varied regimes, and thusly didn't attract more signatories, it lacked universal adoption and thus failed at garnering global cooperation, the convention remained lost on the world with minimal impact.

UNITED NATIONS CONVENTION AGAINST CYBERCRIME

India is reconsidering its stance on a global instrument dealing with cybercrime since 2018 due to the surge in cybercrime.

India voted in favor of a separate convention under a Russian-led UN Convention against cybercrime (henceforth 'UNCAC') that would offer more measures on the ever evolving nature of the issue, with safeguards to the sovereignty of the party states. The then proposed convention received substantial push back from America and likeminded states, civil societies, and human rights institutions across the

globe, here the issues raised were that, with broad powers vested in legislations, it opens up more avenues for regimes to prosecute dissent and activism, and allows massive rampant surveillance, violating privacy.

The UNCAC is the second such global effort at cybercrime regulation, the deliberations towards this 41 paged document lasted over three years with the title being settled mere weeks before the adoption by the UN ad-hoc Committee (henceforth ‘UNAHC’).

The Deliberations for this global instrument lasted over three years, throughout which different countries moved motions in support of their national needs and agendas. An analysis of the said deliberations would provide us with insights into the future implications of the UNCAC in different nations.

Developing countries stressed the need for capacity-building and technical assistance to bridge cybersecurity gaps, thus, Article 1(c) from the statement of purpose pledges resources towards developing countries to ensure harmonious global co-operation in tackling all the facets of cybercrime, this move is seen necessary from the global community as the weak policies and enforcement mechanism in developing countries shelters the sources of cybercrime.

Article 1(c) also makes an effort to move away from the criticism of euro-centrism of its predecessor, potentially attracting more developing countries for signatories to bridge the gap that the Budapest Convention left. This addition could potentially save the move from failing.

Article 5 of the same document addresses the impact on sovereignty of the party states addressing the concerns and reassuring the sovereignty of the party states, so Article 1(c) and 5 seems to address the primary flags that were raised against the adoption of the Budapest Convention.

Article 6 - “Respect for human rights” adds directions for the state legislations towards compliance with Human Rights, the provision comes after much insistence by numerous civil societies and human rights institutions.

The draft United Nations convention against cybercrime draws the core resolutions against cybercrime from the Budapest Convention on Cybercrime, 2001, it also includes provisions adapted from the UN conventions on Transnational Organised Crime, 2000 and Corruption, 2003. But it is interesting to note here that the new draft does not include the advanced tools that are employed in the 2nd protocol to the Budapest Convention that would be critical for enhanced cooperation and disclosure of electronic evidence.

Inclusion from the Budapest Convention establishes the relevance of the document in today’s landscape of cybercrime, and might reduce the present draft to a mere diplomatic advancement, as Australia and likeminded states were throughout of the opinion that the Budapest convention, already in place, addresses cybercrime offences, jurisdiction and international co-operation along with establishing procedural law, mutual assistance and extradition sufficiently.

DELIBERATIONS

The UN convention on cybercrime is the first legally binding global instrument to tackle cybercrime,

as it involves a complex, open ended ad hoc committee process, the deliberations saw participation from developing countries, making it a more inclusive and widely acceptable instrument, something that the Budapest Convention had failed to do with its 76 signatories, it was thusly was much criticized for excluding the developing countries during its deliberations. The UN convention on the other hand is expected to bridge the gaps in the global map that were left by the Budapest Convention, this would implicate a greater possibility of the convention being more successful in achieving its objectives.

The UN Conference on Cybersecurity convened with 70 speakers sharing insights on threats, national experiences, and the Security Council's role in addressing cybersecurity concerns. UN Secretary-General António Guterres stressed the importance of leveraging digital breakthroughs for global betterment, emphasizing conflict prevention and cybersecurity, leading the deliberations. The conference highlighted the alarming integration of digital tools with weapons systems, creating vulnerabilities, and the growing use of AI in cyberoperations. Another area of concern and deliberation was ransomware surge, as ransomware payments skyrocketed to \$1.1 billion in 2023, compromising public institutions, electoral processes, and online integrity.

The conference emphasizes global cooperation, as Speakers underscored the need for international collaboration to combat cyber threats, acknowledging resource gaps in many countries, as reflected in the third statement of purpose.

During the deliberations of the UNCAC, nations adopted diverse stances and made substantial contributions. Delegations from different countries put forth motions in advancement of their national concerns and agendas,

The UNCAC has sparked a global debate, reflecting the complex and often conflicting interests of various countries regarding how to regulate and combat cybercrime. These discussions are part of an ongoing international effort to establish a comprehensive legal framework for addressing the rapidly growing threat of cybercrime, which has evolved with the expansion of digital technologies. However, the participating nations are “poles apart” on many critical issues, such as the scope of the treaty, the balance between security and human rights, and the implications for state sovereignty and internet freedom.

The primary divide in the negotiation's centers on two competing visions for the treaty: one focused on combating specific criminal activities in cyberspace and another that seeks to extend the treaty's scope to include broader control over digital content and information.

On one side, Western nations, including the United States, members of the European Union, and several other democracies, advocate for a narrow and targeted treaty. These countries want the treaty to concentrate on addressing defined cybercrimes such as hacking, ransomware attacks, identity theft, and fraud. They emphasized the importance of ensuring that the treaty does not infringe on human rights, particularly the rights to privacy, free expression, and access to information. Many Western countries are also concerned about the potential for the treaty to be used as a tool for state surveillance or to justify repressive measures, especially in authoritarian regimes.

For instance, the European Union pushed for language in the treaty that would explicitly protect individual privacy rights and guarantee that any law enforcement cooperation in cybercrime investigations adheres to established human rights standards. The EU's concern is that a poorly defined or overly broad treaty could undermine the fundamental freedoms that underpin democratic governance and the open nature of the internet.

On the other side, Russia, China, and some other authoritarian-leaning states advocate for a broader interpretation of cybercrime that includes regulations on online content, misinformation, and other forms of digital communication. Their stance reflects a desire to exercise greater control over the internet within their own borders, using cybercrime as a justification for increasing state regulation and censorship of digital spaces. For these countries, issues like disinformation, online extremism, and political dissent are seen as threats that can and should be controlled through legal means.

Russia has been a particularly vocal proponent of this approach, suggesting that the treaty should not only target cybercriminals but also regulate content that undermines state authority or spreads harmful information. This position has led to significant criticism from human rights groups, who warn that such provisions could enable states to crack down on legitimate political dissent or restrict the free flow of information online.

The positions of developing countries further complicate the negotiations. Many developing nations are concerned about their limited capacity to deal with cybercrime, as they often lack the technical resources and expertise to combat sophisticated cyber threats. As a result, these countries have called for greater international cooperation, capacity building, and resource sharing as part of the treaty. They seek assurances that wealthier nations will provide the necessary support to help them address cybercrime effectively.

At the same time, some developing countries also support broader provisions that would give states more control over digital content, reflecting concerns about the destabilizing impact of misinformation, especially in fragile political environments.

For these countries, cybercrime is not just about financial theft or data breaches but also about the potential for digital platforms to undermine governance and social stability.

The negotiations are at a delicate juncture, with wide-ranging views on what the final treaty should look like. Finding a balance between security and freedom is the central challenge. Many observers worry that without careful safeguards, the treaty could be used to justify overreach by authoritarian governments, while others are concerned that too narrow a focus might leave significant cyber threats unaddressed.

Despite the divide, there is broad agreement that international cooperation is essential in tackling cybercrime. Cyber threats are global, and no country can effectively address them in isolation. However, the path to a treaty that satisfies the concerns of all parties remains fraught, with countries continuing to be “poles apart” on key issues. The outcome of these negotiations will shape the future of international cybersecurity policy and the balance between state security and individual freedoms in the digital age.

During the deliberations on the provisions of human rights, India backed Iran's proposal to delete clauses allowing states to refuse personal data requests that may lead to prosecution based on political views, race, or ethnicity.

Furthermore, India, alongside 22 other nations, voted to eliminate Article 6(2), a vital human rights safeguard. This clause ensured that the convention wouldn't be used to suppress fundamental freedoms, though the Iran's proposal failed to have its motion passed the convention lacks robust human rights protections, assuming countries will act in good faith. This assumption is flawed given the diverse human rights standards globally.

The delegation from South Korea urged for a strengthened security council engagement to counter cyber threats, citing North Korea's sanctions evasion through digital means.

Ukraine put forth a plea against Russia's cyber aggression, including sophisticated attacks on government, security agencies, businesses, and critical infrastructure.

Russia, Belarus, China, Nicaragua, and Cuba, in consensus proposed expansive criminalization of cyber-enabled crimes, including content-based offenses like inciting subversion or armed activities and ICT-facilitated coercion.

Russia has taken a robust stance on the UN Convention on Cybersecurity, advocating for an expansive definition of cybercrime. This includes content-based offenses such as inciting subversion or armed activities and ICT-facilitated coercion, sparking concerns among Western officials and human rights groups.

They worry that Russia's approach could legitimize authoritarian digital sovereignty models, undermining online freedoms. In 2019, Russia, China, Iran, and North Korea supported a UN General Assembly resolution aimed at establishing an international convention to counter criminal uses of ICTs.

Critics argue that Russia's efforts aim to shift global cyber norms toward authoritarianism, potentially criminalizing free expression and circumventing humanitarian law obligations.

Chile, Canada, and the UK, these countries championed integrating a gender perspective into the treaty, acknowledging unique cybersecurity risks and experiences across genders.

EU member states, the US, the UK, Japan, and Australia, these nations advocated for a focused approach, targeting core cyber-dependent crimes and select cyber-enabled crimes, such as child exploitation.

Key Concerns of the UNCAC would be the threat it poses to free speech, dissent and activism through Surveillance Expansion, Russia's proposal may justify increased state surveillance and censorship.

It could hinder free speech further in authoritarian regimes, as it would restrict expression due to availability of provisions to prosecute the same, the broad cybercrime definition could limit online freedom of expression, thus hindering digital sovereignty, Russia's push may undermine global human rights and democracy promotion online.

The United States has taken an active role in discussions on cybersecurity at the United Nations, with a focus on establishing a safe, open, and interoperable cyberspace. During deliberations at various UN conventions, the U.S. has consistently pushed for certain key proposals and policies, aimed at shaping international cybersecurity governance.

The U.S. strongly advocated for the application of existing international law to cyberspace, particularly the principles laid out in the United Nations Charter. During UN discussions such as those led by the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG), the U.S. has argued that international law, including state sovereignty and non-interference, must extend to cyber operations. This includes a clear prohibition on the use of force or interference in domestic matters via cyber activities.

One of the primary U.S. proposals is the promotion of confidence-building measures (CBMs) to reduce cyber-related risks between states. These measures, which include increased transparency, information sharing, and the creation of communication channels between nations, aim to prevent misunderstandings and potential conflicts that could arise from cyber incidents.

In terms of combating cybercrime, the U.S. supports the use of existing international legal frameworks, particularly the Budapest Convention on Cybercrime, which provides a comprehensive international legal standard for addressing cybercriminal activities. The U.S. opposes efforts to create new, potentially conflicting frameworks, as proposed by some countries like Russia and China, which could undermine current efforts and restrict digital freedoms.

The U.S. has consistently voiced its opposition to proposals supporting cyber sovereignty, a model championed by countries such as Russia and China. These proposals argue for greater national control over cyberspace, allowing governments to restrict or monitor the internet within their borders. The U.S. opposes this vision, advocating instead for a global and open internet, which would preserve the free flow of information and protect freedom of expression.

The U.S. also emphasizes the importance of capacity building in developing countries, arguing that many nations lack the expertise and infrastructure to effectively counter cyber threats. The U.S. supports international cooperation in strengthening technical knowledge, improving cybersecurity infrastructure, and building frameworks to assist developing nations in securing their cyberspace.

The U.S. consistently links cybersecurity to the protection of human rights. It argues that cyber regulations should not infringe on fundamental rights such as privacy, freedom of expression, and access to information. The U.S. has repeatedly called out authoritarian regimes for using cybersecurity as a pretext for limiting internet freedoms and human rights.

In line with its broader internet governance philosophy, the U.S. supports a multi-stakeholder approach to cybersecurity, which includes contributions from not only governments but also the private sector, civil society, and academic institutions.

This model ensures a more open and collaborative approach to internet governance, in contrast to the state-controlled models advocated by countries like China and Russia.

Throughout various United Nations discussions, the U.S. has sought to balance the need for robust cybersecurity with the preservation of human rights and an open, global internet. It has consistently pushed for the application of international law to cyberspace, promoted collaboration and capacity building, and resisted efforts to impose more restrictive, state-centric internet governance models. The U.S. approach focuses on international norms, cooperation, and the protection of digital freedoms, often in opposition to authoritarian countries proposing stricter control over cyberspace.

IMPLICATIONS FOR INDIA

The UN Draft Convention's adoption will significantly impact India's cybercrime and cybersecurity legal framework, potentially requiring amendments to existing legislation (e.g., Information Technology Act, 2000) or enacting new laws.

India's Cybercrime Laws are dispersed across Information Technology Act (2000), CERT-IN Framework, Digital Personal Data Protection Act (2023), Criminal laws, and Sectoral regulations. The National Cyber Security Policy (2013) is currently in effect, with an updated strategy aligned with international standards anticipated.

Several human rights institutions expressed their discontent with the present draft that would empower different regimes against dissent and activism, their concerns revolved around the overly broad scope and definition potentially leading to misuse. The insufficient human rights safeguards, particularly freedom of expression and privacy, require strengthening.

The same institution has written to the UNCAC before the adoption of the draft addressing the same concerns and recommendations, primarily to establish clear, concise definitions of cybercrime and cyber-dependent crimes. To lean towards robust human rights protections and targeted capacity building and provide tailored technical assistance to address state capacity disparities.

The Knowmad Institut, an organization focused on human rights and drug policy, made several key recommendations to the United Nations convention on cybersecurity, emphasizing a balance between security, human rights, and digital freedoms. Their approach is centered on ensuring that cybersecurity frameworks respect fundamental freedoms, avoid excessive government control, and promote ethical use of technology.

1. Human Rights-Centered Approach

The Institut advocates for a cybersecurity framework that prioritizes the protection of human rights, particularly freedom of speech, privacy, and access to information. They argue that cybersecurity measures should not become tools for government surveillance or the suppression of dissent.

The Knowmad Institut warns against overregulation in cyberspace, which could lead to mass surveillance or the curbing of digital freedoms. They recommend that any international cybersecurity framework be designed to prevent states from infringing on individual privacy and digital rights under the guise of security measures.

2. Transparency and Accountability

The Institut stresses the importance of transparency in cybersecurity governance. They argue that any

cybersecurity policies developed at the UN level should ensure that states are held accountable for their actions in cyberspace, particularly in the use of surveillance technologies.

3. Promotion of Ethical Technology Development

The Institut recommends promoting the development and use of technology that is ethical and respects human rights. They suggest that cybersecurity efforts should not only focus on defending against cyberattacks but also consider the long-term societal impacts of technological innovations.

4. Collaboration Across Sectors

The Institut emphasizes the need for a multi-stakeholder approach, bringing together governments, civil society, the private sector, and technical experts to create a comprehensive and inclusive cybersecurity framework. This approach would ensure that diverse perspectives are considered, reducing the risk of authoritarian policies being adopted.

In summary, the Knowmad Institut's recommendations to the UN on cybersecurity call for a balanced approach that protects security while safeguarding human rights, promoting ethical technology, and ensuring transparency in governance.
