The Legal Pitfalls to Ratification of the United Nations Convention Against Cybercrime

Murdoch Watney
University of Johannesburg, South Africa

mwatney@uj.ac.za

Abstract: A safe and secure digital space benefits all countries. The growth and development of information and communication technologies (ICTs) are now moving at such a fast pace that keeping up with the threats that ICTs present to businesses, governments, and individuals necessitate a response on an international level. As far back as the early 2000's, the Council of Europe recognised the threat that cybercrime presents to a safe and secure internet. It adopted a multilateral Convention on Cybercrime (Budapest Convention) in 2001 which came into effect in 2004. Since its adoption 68 countries have ratified it, but the Budapest Convention never achieved ratification on a global level, with the unfortunate consequence that a void existed on international level. As the risks to the cybersecurity landscape escalated, it became apparent that critical issues such as international consensus on which behaviour in cyberspace should be criminalised, how cooperation in the investigation of crime and sharing of evidence should be achieved, had to be addressed by the United Nations (UN). It is against this background that the first international Convention against Cybercrime is explored. The Convention traces its roots back to a United Nations General Assembly (UNGA) vote in 2019, when Russia challenged the Budapest Convention calling for an international framework to address cybercrime. Such a call was supported by BRICS nations and other developing countries but some Western countries were not enthusiastic. Following an arduous 5 year negotiation process, the UNGA adopted the Convention against Cybercrime on 24 December 2024. he adoption of the Convention may be a landmark achievement, but it cannot be considered a victory if the key players do not ratify it. For example, the United States' (US) tech sector holds most of the world's data and if the US does not ratify it, it will impact negatively on the operational value of the Convention. Furthermore, if countries decide not to ratify, it may heighten geo-political tension. The discussion highlights the objections and reservations to the Convention against Cybercrime, whether the concerns are justifiable and the possible impact of non-ratification.

Keywords: United Nations Convention against cybercrime, Budapest convention, Objections to the convention against cybercrime, Operational effect of non-ratification on the convention against cybercrime

1. Introduction

Digital transformation brought many benefits to governments, businesses and individuals, such as global connectivity, rapid exchange of information and improved efficiencies. The growth of the digital population, quicker and easier access to the internet and the use of information and communication technologies (ICTs) have resulted in an increase of potential threat actors who may exploit the benefits of the internet and ICTs to their advantage. The cybersecurity landscape is also exacerbated by artificial intelligence (AI) and the growth in mobile connected devices. Globally and domestically there are several vulnerabilities that cyber criminals may exploit, and this has resulted in an unprecedented rise in the frequency, sophistication, and costliness of cybercrime. International consensus on which conduct and communication constitute a cybercrime, cooperation in the investigation and sharing of evidence have become critical to address the rapidly evolving risks that these crimes present to states, businesses, and individuals (Plumb, 2024).

It is commendable that as far back as the early 2000's the Council of Europe (CoE) recognised the serious threat cybercrime presented in securing a safe and secure digital space which culminated in the Convention on Cybercrime (referred to as the Budapest Convention) of 2001 which came into effect in 2004. However, for various reasons which will be explored in the discussion, it never reached full global acceptance.

Over the years, it became clear that a convention against cybercrime on international level was urgently needed to address the fight against cybercrime. When Russia spearheaded the notion for a comprehensive international convention on countering the use of information and communication technology for criminal purposes to the General Assembly in 2019, the international community was sharply divided. Russia, China and most Southeast Asian countries were among those that cast the 79 votes in favour, while 60 delegations (including Australia, most European states, Japan, Britain and US) voted against it. The latter countries opined that the Budapest Convention was sufficient to address cybercrime as it establishes a comprehensive legal framework for countries to participate in the fight against cybercrime (theinterpreter, 2022).

Although a large number of countries had ratified the Budapest Convention, there are a number of countries that did not ratify it. Some countries perceive it as a regional European Union (EU) instrument with the negotiations primarily conducted by European countries (Bannelier and Lostri, 2024b; Priyandita and Hogeveen,

2024). The absence of a convention against cybercrime negotiated on UN level by all countries presented a serious void in respect of the criminalisation of cybercrime, cooperation in the investigation of crimes and sharing of electronic evidence on international level.

After 5 years of rigorous and strained negotiations, the United Nations General Assembly (UNGA) adopted on 24 December 2024 the Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, (referred to as the UN Convention against Cybercrime). It is the first cybercrime convention to have been negotiated on UN level (Mishra, 2024).

As the discussion will show, it is victory in itself that the UN member countries – which comprise of developed and developing countries, western and non-western countries with divergent social, economic and cultural backgrounds and different stances on human rights' protection – reached consensus on the adoption of a Convention. It opens in 2025 for signature at a formal ceremony to be hosted in Hanoi, Vietnam. It requires at least 40 signatures by 31 December 2026 to come into force (Priyandita and Hogeveen, 2024).

Although the adoption may be a victory, it may not result in a celebration if the key players do not ratify it as this will impact negatively on the operational implementation of the Convention against Cybercrime. The discussion explores from a South African legal perspective, the legal pitfalls that may hinder ratification resulting in the much needed Convention from reaching its full potential aimed at improving the global community's ability to combat pervasive and evolving cybercrime threats.

2. Brief Synopsis of the Council of Europe Convention on Cybercrime (Budapest Convention)

The Council of Europe (CoE) Convention on Cybercrime (commonly known as the Budapest Convention), is the oldest and most important regional initiative combating cybercrime. It was the first multilateral pact aimed at combating cybercrime by standardizing national laws, strengthening investigative procedures, and increasing international cooperation.

It was made available for signing in Budapest, Hungary, in 2001, and went into effect in 2004. Five non-EU countries, namely Japan, the US, South Africa, Canada, and the Philippines were involved in the drafting of it and of the 5 countries who signed it, only South Africa as a BRICS member country, never ratified it.

The Budapest Convention had a global impact on domestic cybercrime legislation, and several states outside of Europe embraced it as well. For example, South Africa may not have ratified it, but the Cybercrimes Act 19 of 2020 which came into effect in December 2021 is modelled on the Budapest Convention. The Council of Europe's chart of signatures and ratifications provides at the start of 2025 that the number of ratifications/accessions to the Budapest Convention is 68.

Unfortunately, the Budapest Convention never reached global acceptance as some countries perceive it as an Euro-centric instrument with not enough focus on the actual cybercrimes (Priyandita and Hogeveen, 2024). As far back as 1999, Russia which was a CoE member at the time of the drafting and adoption of the Budapest Convention, began initiating a debate on a cybercrime treaty on UN level (Jakobi and Herbst, 2024). Over the years, it became apparent that there is a void regarding cybercrime governance on international level and it is this void that the UN Convention against Cybercrime aims to address.

3. UN Convention Against Cybercrime

3.1 Background to the UN Convention Against Cybercrime

Almost twenty years after its initial attempt to establish a UN treaty process, Russia with the support of BRICS nations and developing countries such as China, Cambodia, Belarus, North Korea, Myanmar, Iran, Venezuela, and Nicaragua, presented in 2019 a resolution for such an international cybercrime treaty to the UN General Assembly. Although some western countries were not eager to support this notion, many countries did support such an initiative. In 2021, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes held its first organizational session, with the goal of drafting a convention to address cybercrime. The UN Office on Drugs and Crime (UNODC) served as secretariat to the negotiations. On 11 August 2024 member states finally agreed on the text of the Convention. On 11 November 2024 the General Assembly's Third Committee recommended its adoption, and on 24 December 2024 the General Assembly adopted the Convention against Cybercrime.

It consists of 9 chapters which covers various issues, such as general provisions (chapter 1), criminalisation of online activity (chapter 2), jurisdiction (chapter 3), procedural measures and law enforcement (chapter 4), international cooperation (chapter 5), preventative measures (chapter 6), technical assistance and information exchange (chapter 7), mechanism implementation (chapter 8) and final provisions (chapter 9). Most of the chapters will be referred to in the discussion.

The negotiations between the UN member countries were fraught with disagreements on various issues, such as which cyber conduct should be considered as cybercrime and the manner in which human right protection should be effected (Bannier and Lostri, 2024). The division between the member countries is not surprising as the countries have different cultural, social and economic stances. Central to the UN Convention was the following question: How can the UN Convention achieve robust international cooperation and sharing of electronic evidence in the fight against cybercrime while offering strong protection of fundamental freedoms?

Bannier and Lostri (2024) opine that the interest blocs during the negotiations were fairly straightforward: China and Russia, and a small constellation of states around them, prefer broad criminalization that captures a wide range of cyber conduct. At the other end, states more closely aligned with the Budapest Convention saw Russia's position as a thinly veiled attempt to use the UN Convention to weaken fundamental principles of human rights. In between these blocs stands a group of countries, including Caribbean states and South Africa, that "want to ensure that the treaty provides them with access to wide-ranging opportunities for cooperation, capacity building and technical assistance." Ultimately, the member states compromised on the central question and adopted the Convention. The countries that had compromised will have to decide whether they will ratify the Convention.

3.2 Brief Overview of the Convention Against Cybercrime

The UN Cybercrime Convention is a legal framework aimed at strengthening international cooperation for combatting certain crimes committed by means of information and communications technology and for the sharing of electronic evidence in respect of serious crimes.

Walker and Oliveira (2024) opine that the ability to collect and share electronic evidence drove the negotiations and shaped core elements of the final treaty. They furthermore contend that the main objective for many countries was a wide scope for the collection of data. In the end, it was also written into the subtitle, namely "United Nations convention against cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes".

Chapter 2 provides for various cybercrimes. There is not international consensus on what constitutes a cybercrime, and the Convention does not provide an explicit definition on cybercrime. It does provide for electronic evidence collection for serious crimes which compromise of crimes punishable by over four years' imprisonment. Cybercrime is used as an umbrella term for a range of unlawful online activity which can be divided into two broad categories, namely cyber-enabled and cyber-dependent crimes (Watney, 2022). Most traditional criminal activity is conducted online but it does not specifically require the use of a computer. These are called cyber-enabled crimes. Examples include drug and weapons trafficking, theft, fraud, and incitement of violence. Cyber-dependent crimes, on the other hand, are crimes that can be committed only using Information and Communication Technology (ICT) devices. For example, a threat actor cannot spread malware if there is no computer or network to infect. Some stakeholders believed that the Convention should only cover cyber dependant crimes, so-called core cybercrimes (Falchetta, 2024). These would be offences inherent to cyberspace which are committed against the confidentiality, integrity and availability of data and systems.

Chapter 2 covers a range of core cyber-dependent crimes, and a limited number of cyber-enabled crimes, such as information and communications technology system-related forgery (article 12), information and communications technology system-related theft or fraud (article 13) and laundering of proceeds of crime (article 17). Articles 61 and 62 provide that the Conference of the States Parties may supplement the Convention with one or more additional protocols. It is therefore possible to expand the Convention in future to cover for example crimes that are not included in chapter 2 (Bannelier and Lostri, 2024b). These protocols must be submitted by at least 60 states, and while they should preferably be adopted by consensus, a two-thirds majority vote of the states' parties present and voting would be enough to adopt them

As most "traditional" crimes are now committed online, the South African Cybercrimes Act 19 of 2020 provides for not only cyber-dependant crimes, but also for a few cyber-enabled crimes such as fraud, forgery and uttering

and extortion as well as a limited number of content (communication) crimes such as incitement to damage property or violence, threats to persons to damage property of violence as well as non-consensual sexual images, so-called revenge pornography (Watney, 2022).

The Convention also obligates States to develop digital investigation and enforcement capabilities, and to apply these new powers to other crimes conducted using computer networks. The procedural obligations in terms of law enforcement (chapter 9) and international cooperation (chapter 10) go well beyond the 11 cybercrimes identified and defined by the Convention. As the sub-title of the Convention indicates, the aim is to strengthen international cooperation not only for the cybercrimes identified by the Convention but also for "serious offenses" (Bannelier and Lostri, 2024b). The Convention's procedural obligations (chapter 9) apply to the collection of evidence in electronic form for "any criminal offense, cyber or not, serious or not". Bannelier and Lostri (2024) provides that the scope of the Convention's offenses is therefore extremely broad, going well beyond the fight against cybercrimes to include any such "serious offense" whose identification relies on each state's domestic criminal law. Walker and Oliveira (2024) provide that while the treaty could be used to build up responses to crippling incidents, such as ransomware attacks, every indication so far is that the focus of implementation will be data collection. The articles relating to mutual legal assistance (chapter 10) and technical assistance (chapter 12) are also focused primarily on collecting, sharing and using electronic evidence. Technical assistance will depend on which countries ratify, who is available to provide support on technical assistance and who drives the limited resources for treaty implementation while the UN is under austerity measures.

Jakobi and Herbst (2024) compares the EU Budapest Convention with the UN Convention against Cybercrime. They provide that while many paragraphs of the UN Convention resemble those of the Budapest Convention, noticeable changes and gaps exist, such as

- The crimes covered include more recently emerging crimes, like the dissemination of intimate pictures, but exclude copyright infringements (Art. 10 in the Budapest Convention).
- The jurisdiction of the UN Convention is relatively broad and includes cybercrimes committed abroad but directed against a state party (article 22).
- The Budapest Convention refers to human rights treaties (article 15), including those of the UN, but the UN Convention does not contain the same references. Additionally, paragraphs transferred from the Budapest Convention have been changed, such as article 29 of the UN Convention on real-time cooperation, which is based on the wording of article 20 of the Budapest Convention, but without its reference to the protection of human rights.

Although the Budapest Convention played a major role in the drafting of the Convention against Cybercrime, it cannot be expected for it to be a replica of the Budapest Convention. Since the drafting of the Budapest Convention, technology has radically evolved and the threat of cybercrime has escalated and become more complex. Furthermore, the Convention was negotiated on an international level which involved various member states worldwide with divergent views that had to be accommodated.

4. Obstacles That may Hinder the Ratification of the Convention

Although the Convention against Cybercrime has been adopted, member countries need to ratify it in order for it to come into force. There are obstacles that may prevent some of the UN member countries from ratifying it.

Some of the challenges facing the ratification of the Convention are discussed hereafter.

4.1 Multilateral Versus Multi-Stakeholder Model of Cyberspace Governance

Traditionally, the UN is the realm of state actors (Bannelier and Lostri, 2024b). However, the role that the private sector and civil society play in curbing cybercrime meant that there was significant interest in including their perspectives. Over the years their participation has become commonplace in many of the cyber discussions that have taken place. Therefore, at the invitation of Western countries, the views of the private sector and civil society were given serious consideration (Bannelier and Lostri, 2024b).

Priyandita and Hogeveen (2024) concedes that for some time "cyberspace was thought to be most effectively governed through collaborative multi-stakeholder interactions, in which governments, civil society, industry and the technical community would take responsibility for their share of the domain". The UN Cybercrime Convention, however, shows government-led proceedings took precedence and that cyber sovereignty was the rallying concept around which states found consensus. Cyber sovereignty is protected in article 5 of the Convention.

US President Trump's attitude to multilateralism and the tech industry's opposition to the Convention against Cybercrime, may result in US ratification slipping away, leaving the world's newest multilateral treaty without its most crucial player (Tennant, 2024). Without US participation and access to its vast pool of data, the treaty's operational value will be close to zero as the Convention will be without access to the most rich and relevant data needed for it to have any criminal justice impact (Tennant, 2024).

In summary: It may be that the multilateral model approach is one of the reasons for non-ratification. Although the emphasis during the negotiations were on the governments participating in the drafting of the Convention, the views of other stakeholders were also considered. In future this type of approach may pave the way for government-to-government treaties to reach an agreement on critical infrastructure protection, state-on-state cyber operations during peacetime and ethical principles of AI on international level (Priyandita and Hogeveen, 2024).

4.2 Human Right Protection Concerns

The Convention against Cybercrime contains human right provisions, but many have warned that the human right provisions in the Convention does not provide sufficient protection. Living in an intelligent age means that the issue of human right protection is an ongoing concern, not only on an international level, but also on a domestic level. On domestic level, countries should have human right safeguards in place and be vigilant in upholding the protections.

Some of the concerns are as follows:

- Article 6 contains a core human rights clause.

It guarantees respect for human rights for all the provisions, and provides:

> *"1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.*
>
> *2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law".*

Rodrigues (2024) argues that the treaty fails to adopt specific safeguards necessary to protect human rights. However, article 6(2) provides that if a state attempts to invoke the treaty to suppress rights like freedom of expression, religion, or association it would be acting contrary to this provision.

- Chapter IV provides for procedural measures and law enforcement.

Article 23(1) states that "Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings. Article 24 mandates that surveillance powers respect human rights safeguards and proportionality, but Rodriquez (2024) as well as Bannelier and Lostri (2024b) opine that it lacks explicit requirements for the core human rights principles of legality, necessity, and non-discrimination. Rodriquez (2024) provides that although article 24(2) adopts a number of safeguards including the need for judicial review and the need for grounds justifying the use of an investigative power, it is not sufficient as it leaves them as potentially discretion and contingent on domestic law.

Stakeholders have indicated that the provisions of the Convention against Cybercrime may be abused to conduct mass surveillance, thus violating human rights such as free speech and privacy (Jakobi and Herbst, 2024). Surveillance without proper safeguards is not only a challenge in terms of the Cybercrime Convention but it is an ongoing concern on domestic level. For example, spyware, including the controversial Pegasus software, enables agencies to directly access data stored on devices. These tools allow surveillance, including reading encrypted messages, viewing photos, and accessing call logs, without needing to intercept communications in transit. It is for this reason that the US adopted in 2023 an Executive Order that is aimed at the regulation of commercial spyware. The US provides in its policy for specific government action that is aimed at limiting the use, sale, and procurement of commercial spyware that poses a risk (Kitchgaessner, 2024). Furthermore, the United Kingdom and France has initiated the Pall Mall Process (PMP) in 2024 which aim to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities by means of a normative framework (Landi, 2024). One of the purposes of the PMP is holding states accountable when behaviour is inconsistent with international human rights law.

The provisions in the Cybercrime Convention should therefore not be seen in isolation, but other initiatives such as those by the US and the PMP should be kept in mind. Protecting human rights in the digital realm requires vigilance on domestic and international level.

4.3 Jurisdiction With Specific Focus on Passive Personality Jurisdiction

Chapter 3 provides for jurisdiction. Scher-Zagier (2024) opines that article 22 authorizes states to exercise jurisdiction over extraterritorial conduct that harms their nationals—known as passive personality jurisdiction – is controversial. By signing this treaty, states would essentially cede sovereignty to other states, eliminating what would be states' ordinarily exclusive jurisdiction to regulate—including, importantly, to permit—the conduct of their citizens in their territory (Scher-Zagier, 2024). Jakobi and Herbst (2024) opine that non-democratic states could use this to claim the application of this Convention against criticism abroad.

The Budapest Convention does not contain an endorsement of passive personality jurisdiction. Scher-Zagler (2024) provides that "passive personality jurisdiction undermines the fundamental treaty purpose of unifying the cybercrime regime. Rather than encouraging cooperation on a shared core of cybercrimes, the treaty permits fragmented criminal enforcement that legitimizes states exercising jurisdiction over many cyber offenses—defined as each state chooses—against any of their nationals".

Although the criticism may be justifiable, it should be noted that a state could invoke its obligation to comply with international human rights law under article 6 and decline to assist in electronic monitoring or extradition.

4.4 IT Sector Warns Legitimate Cybersecurity Research may be Criminalised

The IT sector has been particularly vocal in its criticism (Rodriquez, 2024; Tennant, 2024). The Cybersecurity Tech Accord, a global industry group representing more than 157 large tech companies, including Microsoft, Meta, Oracle, Cisco, SalesForce, Dell, GitHub, HP and more, has warned of the treaty's potential to criminalise legitimate cybersecurity research. By criminalising unauthorised access to computer systems without distinguishing between malicious actors and ethical hackers, it could expose security professionals to legal repercussions even when their actions aim to enhance security. Moreover, the treaty's prohibition on intercepting non-public data transmissions fails to recognise the necessity for security researchers to validate vulnerabilities. Similarly, its stipulations against manipulating or deleting data could misapply to legitimate practices like penetration testing and red-teaming which are crucial for identifying weaknesses.

Cybersecurity measures ensure prevention which is crucial to mitigate cybercrime commission. Countries will therefore have to be mindful that cybersecurity research and testing cannot be criminalised. However, cybersecurity is not infallible and many crimes are committed across borders. A cybercrime convention on international level is a therefore a step in the right direction.

4.5 Geo-Political Differences

While countries such as Russia, China and Vietnam enthusiastically support the convention, others, such as the EU, UK, Australia, New Zealand, Canada, Switzerland and Liechtenstein have expressed reservations. Egypt and Iran meanwhile expressed reservations from the opposite perspective – that the treaty is overly focused on protecting human rights. Russia, and other key convention supporters – including Brazil, South Africa and India – were silent at the November 2024 session that moved the Convention to its final stage in December 2024 (Tennant, 2024).

When it comes to ratification, it may be that the divide between countries based on geo-political differences is too big to overcome. To ensure a safe and secure cyberspace, countries need to trust each other that they will act in the best interest of the digital society but this trust may be lacking. Non-ratification will not bide well for any future negotiations. It could even contribute to the escalation of tension between the countries.

5. Conclusion

The solution to the ever-evolving cybercrime threats, such as combatting ransomware, widespread cyber-enabled fraud, and illegal intrusions into computers and networks, requires a two-fold approach, namely criminal and procedural laws on domestic level, and consensus on criminalisation, cooperation in the investigation and sharing of electronic evidence on an international level.

The discussion shows that defining the precise purpose and scope of such a convention on an international level, has been fraught with complexities. Balancing the need for effective law enforcement with the protection of human rights remains a significant challenge. Nick Ashton-Hart, Tech Accord's Head of

Delegation to the Negotiations, opined in 2024 that "they are choosing to believe that a bad treaty is better than no treaty" (McKann, 2024). Maybe a compromise is the solution for cooperation in the investigation of cybercrime and sharing of electronic evidence on international level? Bannelier and Lostri (2024) opine that the UN Convention against Cybercrime has "left everyone unhappy". It depends from which perspective the Convention is viewed. From a South African perspective, such a Convention is welcomed as it would mean global assistance, capacity building and technical assistance.

If countries decide not to ratify the Convention against Cybercrime, the fallback option could be the Budapest Convention (Jakobi and Herbst, 2024). However, if countries do elect to fall back on the Budapest Convention, it may result in the divide between those that ratify and those that do not ratify the Convention against Cybercrime, becoming bigger. It could also result in a power shift in cyberspace governance on an international level. By ratifying the Convention, countries have the opportunity to monitor human right protection and safeguard human right protection on an international level (Tennant, 2024). The Conference of States Parties (COSP), in particular, will constitute an important mechanism for bringing to light and repudiating any abuses committed under the alleged auspices of the Convention and mobilizing to prevent future misuse.

Countries should be mindful of the consequences of non-ratification as it could have a negative impact on cyberspace governance which does not bode well for future negotiations nor ensuring a safe and secure cyberspace.

References

Bannelier, K. and Lostri, E. (2024a) "So close, So far: UN Committee tasked with Cybercrime Convention Hits Snooze", [oline], https://www.lawfaremedia.org/article/so-close-so-far-un-committee-tasked-with-cybercrime-convention-hits-snooze.

Bannelier, K, and Lostri, E (2024b) "Is anyone happy with the UN Cybercrime Convention", [online], https://www.lawfaremedia.org/article/is-anyone-happy-with-the-un-cybercrime-convention.

Falchetta, T. (2024) "The Draft UN Cybercrime Treaty is overbroad and falls short on human rights protection", [available], https://www.justsecurity /91318/the-draft-un-cybercrime-treaty-is-overbroad-and-falls-short-on-human-rights-protection/.

Jakobi, A. and Herbst, L. (2024) "Between a Rock and a Hard Place: The UN Cybercrime Convention", [online], https://blog.prif.org/2024/12/09/between-a-rock-and-a-hard-place-the-un-cybercrime-convention/.

Kitchgaessner, S. (2024) "US announces new restrictions to curb global spyware industry", [online] https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions Landi, E. (2024) "Harmonizing recent campaigns to tame the hacking marketplace", [online], https://carnegieendowment.org/r USesearch/2024/06/us-europe-cyber-policy-joint-statement-pall-mall-process?lang=en.

McKann, K. (2024) "UN Cybercrime Treaty: Why is the Tech Industry up in Arms?", [online], https://cybermagazine.com/articles/un-cybercrime-treaty-why-is-the-tech-industry-up-in-arms.

Mishra, V. (2024) "UN General Assembly adopts milestone cybercrime treaty", [online], https://news.un.org/en/story/2024/12/1158521.

Plumb, C. (2024) "Understanding the UN's new international treaty to fight cybercrime", [online], https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime.

Priyandita, G. and Hogeveen, B. (2024) "The UN cybercrime convention: a victory for state sovereignty", [online]. https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/.

Theinterpreter. (2022) "The hypocrisy of Russia's push for a new global cybercrime treaty", [online], https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

Rodriguez, K. (2024) "The UN Cybercrime Convention: Analyzing the risks to human rights and global privacy", [online], https://www.justsecurity.org/98738/cybercrime-convention-human-rights/.

Sayce, S. (2024) "3 trends set to drive cyberattacks and ransomware in 2024", [online], https://www.weforum.org/stories/2024/02/3-trends-ransomware-2024/.

Scher-Zagier, E. (2024) "The New UN Cybercrime Treaty is Bigger than Even Its Critics realise", [online], https://www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-deal-than-even-its-critics-realize#:~:text=Rather%20than%20encouraging%20cooperation%20on,against%20any%20of%20their%20nationals.

Tennant, L. (2024) "UN Cybercrime Treaty faces uncertain future under Trump", [online], https://globalinitiative.net/analysis/un-cybercrime-treaty-faces-uncertain-future-under-trump/.

United Nations (2024) United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes, [online], https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf.

Walker, S. and Oliveira, A.P. (2024) "The final call UN member states adopts a new cybercrime treaty" [online], https://globalinitiative.net/analysis/the-final-call-un-member-states-adopt-a-new-cybercrime-treaty/.

Watney, MM. (2022) "Chapter 13 Cybercrime" in Papadopoulos and Snail Cyberlaw@SA pages 463 – 465.