Vanderbilt Journal of Transnational Law

Volume 55
Issue 5 *November 2022*

Article 1

11-2022

The Pivotal Role of International Human Rights Law in Defeating Cybercrime: Amid a (UN-Backed) Global Treaty on Cybercrime

Professor Fatemah Albader
Kuwait International Law School

VANDERBILT JOURNAL

of Transnational Law

Volume 55 November 2022 Number 5

The Pivotal Role of International Human Rights Law in Defeating Cybercrime: Amid a (UN-Backed) Global Treaty on Cybercrime

Dr. Fatemah Albader*

ABSTRACT

On May 26, 2021, the General Assembly of the United Nations adopted a resolution approving the drafting of a new global treaty on cybercrime, which commenced in February 2022. The proposed UN agreement on cybercrime regulation has garnered significant criticism among the international community, namely by state delegates, human rights advocates, and nongovernmental organizations. Fears stem from the belief that such a treaty would be used to legitimize abusive practices and undermine fundamental human rights. National cybercrime laws already unduly restrict human rights. However, at a time where the global community has moved toward a digital world, it becomes even more necessary to legislate on a global scale against the commission of cybercrime.

This Article aims to provide guidance on how to ensure respect for human rights in the drafting of a global treaty on cybercrime in the hopes that it will help guide the process and facilitate a smoother transition. The Article concludes that national security concerns stemming from threats of cybercrime should be viewed not as dichotomies but as complementary, where one cannot be achieved without respect for the other, concluding that the best approach is one that integrates human rights into the text of the treaty, thereby ensuring

---

* Dr. Fatemah Albader is an Assistant Professor of International Law at Kuwait International Law School. She also serves as Vice Chair of Publications of the American Bar Association International Law Section's Middle East Committee. The author would like to thank the Journal's editors for their immense contributions, revisions, and constructive feedback throughout the editing process.

that human rights are not trumped by national security concerns in the name of cybercrime regulation.

TABLE OF CONTENTS

I. INTRODUCTION

On May 26, 2021, the General Assembly of the United Nations adopted a resolution approving the drafting of a new global treaty on cybercrime, which commenced in February 2022.[1] This marks the first time that UN member states have begun to negotiate a legally binding treaty on any cyber-related topic.[2] The Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes has been tasked with developing the draft convention in consultation with the UN Office on Drugs and Crime (UNODC).[3] From the outset, the proposed UN agreement on cybercrime regulation has garnered significant criticism among the international community, namely by state delegates, human rights advocates, and nongovernmental organizations.[4] Fears stem from the belief that such a treaty would risk "legitimizing abusive practices and could be used as an excuse to

1. *See* G.A. Res. 75/282 (May 26, 2021).

2. *See* Joyce Hakmeh, *Can a cybercrime convention for all be achieved?*, CHATHAM HOUSE (Mar. 31, 2022), https://www.chathamhouse.org/2022/03/can-cybercrime-convention-all-be-achieved [https://perma.cc/2ZWR-3CXR] (archived Sept. 3, 2022).

3. *See* G.A. Res. 75/282, *supra* note 1.

4. *See, e.g.*, Deborah Brown, *Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights*, HUM. RTS. WATCH (Aug. 13, 2021), https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights [https://perma.cc/EX8U-MS5X] (archived Sept. 3, 2022).

silence government critics and undermine privacy in many countries."[5] It is true that national cybercrime laws already unduly restrict human rights, including, *inter alia*, freedom of expression and privacy rights.[6] There is ample evidence to suggest that cybercrime laws frequently exceed that which is necessary to prevent such crimes, thereby bordering on oppressive and limiting human rights to a degree that is prohibited under international law. However, it is equally true that, as the global community moves toward a digital world, it becomes even more necessary to legislate on a global scale against its commission. Thus, a balance must be struck, one that would allow for cybercrime regulation while at the same time respecting international human rights. Many examples illustrate, however, that this is not often the case.

In recent years, several digital criminal attacks have garnered significant media attention. The COVID-19 pandemic has resulted in an insurmountable increase in these cyberattacks, which continue to advance at an alarmingly fast rate, with newer ways to commit various acts of cybercrime constantly emerging.[7] In the first session of the ad hoc committee on the UN treaty on cybercrime, the UNODC itself has acknowledged that governments must act quickly to meet the difficulties posed by cybercrime because of the acceleration of such crimes owing to COVID-19.[8] Even before the pandemic hit, cybercrime was on the rise. Especially worrisome, given its lucrative nature, it is predicted that cybercrime will "be more profitable than the global trade of all major illegal drugs combined."[9] At the same time, cybercrime will cost the international community $10.5 trillion annually by 2025.[10] Accordingly, in May 2021, the United Nations General Assembly approved Russia's resolution to draft a global treaty to tackle the growing threat of cybercrime, with a draft convention to be submitted for review in 2023.[11] While these efforts are commendable, there is

---

5. *Abuse of Cybercrime Measures Taints UN Talks*, HUM. RTS. WATCH (May 5, 2021), https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks [https://perma.cc/HQW5-9Y9M] (archived Sept. 3, 2022).

6. *See id.*

7. *See* David Cripps, *Tackling the cybercrime pandemic in 2021*, SEC. MAG. (Sept. 21, 2021), https://www.securitymagazine.com/articles/96134-tackling-the-cybercrime-pandemic-in-2021 [https://perma.cc/A8S5-8UDC] (archived Sept. 3, 2022).

8. *See* U.N. OFF. ON DRUGS & CRIME, STATEMENT DELIVERED BY THE SECRETARY OF THE MEETING, MR. JOHN BRANDOLINO, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Statement_by_Secretary_UNODC.pdf [https://perma.cc/5Y4J-CMLK] (archived Sept. 3, 2022).

9. Steven Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [https://perma.cc/2NRZ-KCNA] (archived Sept. 3, 2022).

10. *Id.*

11. *See* Press Release, General Assembly, General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns Over 'Rushed' Vote at Expense of Further Consultations, U.N. Press Release GA/12328 (May 26, 2021),

significant potential for increased human rights violations amid a global treaty to combat cybercrime. Thus, drafters of the treaty must take into consideration, first and foremost, human rights concerns so as to reinforce the human rights framework in the digital arena.[12]

In considering this new cybercrime legislation, it is worthy to note that, while Russia spearheaded the process of establishing this global treaty on cybercrime, having initially been commended for its efforts, after the Russian invasion of Ukraine, criticisms grew. Many delegates expressed concern that negotiating with Russia at this time was inappropriate, given Russia's alleged use of cyberattacks in the ongoing conflict.[13] This has led to fears by those in support of a global treaty that the invasion would overshadow the negotiations process.[14] The committee chair rightfully urged the ad hoc committee "to focus on the substantive issues at hand."[15] Nonetheless, the first session of the ad hoc committee alone has revealed the tension between human rights and national security amid the ongoing conflict in Ukraine. But a global treaty on cybercrime, especially at this time, should be welcomed rather than feared, provided that governments exercise adequate care and due diligence to prevent the treaty from obscuring human rights concerns in the name of national security. It is clear that the COVID-19 pandemic as well as Russia's invasion of Ukraine have both complicated the process. However, as state cooperation is pivotal to the successful conclusion of this treaty, the delegates must set aside their political differences and focus on the outcomes that are required of them to address this pressing concern, especially given the current state of affairs.

Accordingly, this Article aims to provide guidance on how to ensure respect for human rights in the drafting of a global treaty on cybercrime in the hopes that it will help guide the process and facilitate a smoother transition. The Article concludes that national security concerns stemming from threats of cybercrime should be viewed not as

---

https://www.un.org/press/en/2021/ga12328.doc.htm [https://perma.cc/52BD-RSW7] (archived Sept. 3, 2022); G.A. Res. A/75/PV.71 (May 26, 2021).

12. *See* Fatemah Albader, *The Digital War on Human Rights: Guilty Until Proven Innocent: In Light of the Counter-Terrorism and Border Security Act of 2019*, 29 MINN. J. INT'L L. 21, 22 (2020).

13. *See, e.g.*, U.S. NATIONAL STATEMENT, U.N. OFF. ON DRUGS & CRIME, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/United_States.pdf (last visited Sept. 3, 2022) [https://perma.cc/2JJB-EZ2S] (archived Sept. 3, 2022); UNITED KINGDOM STATEMENT, U.N. OFF. ON DRUGS & CRIME, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/United_Kingdom.pdf (last visited Sept. 3, 2022) [https://perma.cc/BZ9E-JYTU] (archived Sept. 3, 2022).

14. *See* Ian Tennant & Summer Walker, *Cyber, fire and fury: Diplomats take first step towards a cybercrime treaty amid widespread condemnation and isolation of Russia*, GLOB. INITIATIVE AGAINST TRANSNAT'L ORGANIZED CRIME (Mar. 17, 2022), https://globalinitiative.net/analysis/un-cybercrime-treaty/ [https://perma.cc/PYV8-TVWW] (archived Sept. 3, 2022).

15. *Id.*

dichotomies but as complementary, where one cannot be achieved without respect for the other. In viewing the two as complementary rather than mutually exclusive, states would be able to guarantee respect for human rights while, at the same time, addressing key national security needs. This is especially pertinent in cybercrime regulation where the tendency is to curtail human rights in favor of national security.[16] This Article therefore addresses these arguments by establishing a framework that would reconcile the two, such that, in most instances, one does not prevail over the other. Accordingly, this Article is divided into two parts. Part II discusses the connection between cybercrime regulation and human rights, concluding that a UN-backed global treaty on cybercrime is necessary in order to properly regulate cybercrime so long as the treaty takes into consideration human rights in the drafting process. Part III discusses the possible governing frameworks to incorporate human rights considerations, concluding that the best approach is one that integrates human rights into the text of the treaty, thereby ensuring that human rights are not trumped by national security concerns in the name of cybercrime regulation.

II. INTERNATIONAL REGULATION OF CYBERCRIME: A DEADLY THREAT TO HUMAN RIGHTS LAW

Cybercrime breeds major national security challenges. At their core, the crimes are not a new phenomenon. Consider, for example, the crime of fraud. The crime has existed for many years. In the context of cybercrime, cyber fraud relies on technology to commit the same crime online. Due to the speed at which information is spread online, the level of sophistication, and the possibility for non-detection that is inherent in such attacks, cyber fraud has emerged as the most threatening type of fraud.[17] According to a 2021 study by Abnormal Security

---

16. *See, e.g.*, LAUREL E. FLETCHER & ASTHA SHARMA POKHAREL, GULF CTR. FOR HUM. RTS., WHO WILL BE LEFT TO DEFEND HUMAN RIGHTS? PERSECUTION OF ONLINE EXPRESSION IN THE GULF AND NEIGHBOURING COUNTRIES 1 (2021) (showing how countries in the Gulf have enacted anti-cybercrime legislation restricting a number of human rights, including the rights to freedom of expression, peaceful assembly, and the right to privacy); *id.* at 2. This tendency to curtail human rights in favor of national security is not only limited to countries in the Gulf. The United Kingdom, for example, has also in recent years limited fundamental human rights in the name of national security. *See* Albader, *supra* note 12, at 31.

17. *See* Morgan Rennie, *What is Cyber Fraud?*, DELTANET INT'L, https://www.delta-net.com/knowledge-base/compliance/fraud-awareness/what-is-cyber-fraud/#:~:text=Cyber%20fraud%20is%20the%20crime,protect%20their%20information%20from%20fraudsters (last visited July 28, 2022) [https://perma.cc/4YWD-R96T] (archived Sept. 3, 2022); Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=595878ca7864 [https://perma.cc/B6KD-ST8C] (archived Sept. 3, 2022).

Corporation, a new malware strategy using phone fraud has evolved.[18] Unsuspecting victims would receive an email asking them to call the scammers who would then instruct them to download virus-containing files. The study reported that "[t]his relatively new tactic increased dramatically throughout the last half of the year, with nearly a third of all organizations receiving at least one attack in the third quarter, and over half in the fourth quarter."[19] The chances of receiving this new phone scam attack was at a likelihood of 59.2 percent.[20] Another recent study found that the government/military sector, which saw 1,136 attacks per week in 2021—an increase of 47 percent from 2020—witnessed the second-largest volume of attacks, with the education/research sector being the most vulnerable and having the highest number of attacks.[21] Thus, these crimes affect both the private and public sectors at massive scales and range from typical identity fraud and online theft of data to drug trafficking and cyber pornography.

With advancements in technology, cybersecurity threats continue to develop. In addition, perpetrators often take advantage of public health emergencies and other crises that serve as a breeding ground for cybercrime. COVID-19 and the Russian invasion of Ukraine are two examples. During COVID-19, one phishing attack disguised itself as the World Health Organization, tricking individuals into opening emails they thought were from World Health Organization health officials but that actually contained dangerous malware.[22] Similarly, during the Russian invasion of Ukraine, cybercriminals exploited the ongoing war by launching phishing attacks and pretending to be Ukrainians or family members in need of financial support.[23]

All of these examples highlight just how lucrative cybercrime can be, illuminating the reasons as to why cybercriminals are driven to commit these crimes. Because of the anonymity involved in such crimes, cybercriminals have been able to thrive. It is generally understood that the right to privacy includes the right to communicate

---

18. *See* ABNORMAL SEC. CORP., FRAUDSTERS USE EMAIL IN PHONE FRAUD SCAMS, TARGETING 89% OF ORGANIZATIONS 2 (2022), https://medcitynews.com/uploads/2022/03/Abnormal-Security_H2-2021_Email-Threat-Report.pdf (last visited Sept. 12, 2022) [https://perma.cc/ZH37-H4DS] (archived Sept. 12, 2022).

19. *Id.*

20. *Id.* at 8.

21. *See Check Point Research: Cyber Attacks Increased 50% Year over Year*, CHECK POINT BLOG (Jan. 10, 2022), https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ [https://perma.cc/TG8E-RDQK] (archived Sept. 3, 2022).

22. *See* Piers Kelly, *Trends in Cybercrime in 2022 and Beyond*, GOVNET TECH. (July 28, 2022), https://blog.govnet.co.uk/technology/trends-in-cybercrime-in-and-beyond [https://perma.cc/C2XH-ZAW2] (archived Sept. 3, 2022).

23. *See* David Klein, *In Russia-Ukraine Crisis, Cybercriminals See New Opportunities*, ORGANIZED CRIME & CORRUPTION REPORTING PROJECT (Mar. 9, 2022), https://www.occrp.org/en/daily/16057-in-russia-ukraine-crisis-cybercriminals-see-new-opportunities [https://perma.cc/8RG6-ZW42] (archived Sept. 3, 2022).

privately and anonymously online.[24] On the positive side, this means that lawyers, journalists, and others who may be at risk for expressing their views online in more authoritarian countries are able to do so without risk of repercussion.[25] On the negative side, however, this has made it easier for criminals to commit wrongdoings online.[26]

Former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye has stated that "[l]aw enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigation into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives."[27] Thus, cybercrime poses a risk that was not envisaged before the development of technology, a risk that will continue to worsen with time. In order to stop its proliferation, states must therefore counter cybercrime by legislating against and cooperating to defeat the unprecedented threats posed by it. At the same time, however, cybercrime legislation often infringes on certain human rights. In its submission to the ad hoc committee, the UN Office of the High Commissioner for Human Rights stated that

> provisions regulating cybercrime and their application may pose significant human rights risks, as evidenced by the common use at national levels of cybercrime laws and policies to restrict freedom of expression, target dissenting voices, justify Internet shutdowns, interfere with privacy and anonymity of communications, and limit the rights to freedom of association and peaceful assembly.[28]

Thus, cybercrime regulation carries significant potential to violate human rights. For example, UK legislation undertaken to counter acts of terrorism online by prohibiting individuals from accessing material that may be of use to terrorists on the internet has been found to unduly restrict freedom of expression and privacy rights online.[29] Under the UK Counter-Terrorism and Border Security Act of 2019, individuals could be punished for merely viewing terrorist material online, bordering on thought crime, where persons may be punished

---

24. *See* David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/29/32, ¶ 12 (May 22, 2015).

25. *See id.*

26. *See id.* ¶ 13.

27. *Id.*

28. U.N. OFF. OF THE HIGH COMM'R, OHCHR KEY-MESSAGES RELATING TO A POSSIBLE COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES (Jan. 17, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf [https://perma.cc/XF45-ZJXA] (archived on Sept. 3, 2022).

29. Albader, *supra* note 12, at 23.

for their thoughts and not their actions, therefore violating the freedom of thought.[30] The UK example illustrates how governments are willing to trample on human rights in order to safeguard their national security interests. Thus, states often take measures that aim to tackle cyber-terrorism concerns, but more often than not these measures are far reaching and significantly exceed that which is necessary under international human rights. Similarly, during the COVID-19 pandemic, for example, when cybercrime increased drastically,[31] state measures taken to tackle such digital crimes have "put significant strain on the international human rights system."[32] One such example of a proliferated crime during the pandemic is ransomware.[33]

Ransomware is where hackers hack into a computer system and block access to the system until a demand, often a ransom, is settled.[34] In May 2021, the largest American gasoline pipeline system, Colonial Pipeline, was attacked, leading to the shutdown of the pipeline.[35] The hackers, said to be linked to a Russian cybercrime group, also threatened to leak private data belonging to Colonial unless the pipeline company paid the ransom. Shortly thereafter, Colonial paid the $4.4 million ransom.[36] Responses to these ransomware attacks pose immense human rights risks, namely with respect to the right to privacy. In order to counter and prevent ransomware attacks, many nations have considered adopting legislation prohibiting the payment of ransom.[37] The problem, however, is that if ransomware payments are not made, private individual information may be released, resulting in violations of privacy rights, which are protected under both

---

30. *Id.* at 24–25.

31. *See* Dan Patterson, *Cybercrime is thriving during the pandemic, driven by surge in phishing and ransomware*, CBS NEWS (May 19, 2021), https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/ [https://perma.cc/MP7B-YX3A] (archived Sept. 3, 2022).

32. Agnès Callamard, Ben Horton, Esther Naylor, Amrit Swali & Isabella Wilkinson, *Undercurrents: The global human rights system, and responding to ransomware*, CHATHAM HOUSE (Aug. 12, 2021), https://www.chathamhouse.org/2021/08/undercurrents-global-human-rights-system-and-responding-ransomware [https://perma.cc/H6MV-7DJS] (archived Sept. 3, 2022).

33. *See id.*

34. *See id.*

35. *See* William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [https://perma.cc/B8BC-VYY5] (archived Sept. 12, 2022).

36. *Id.*

37. *See Should Ransomware Payments Be Made Illegal?*, WALL ST. J. (Sept. 7, 2021), https://www.wsj.com/articles/ransomware-payment-illegal-ban-11631047209 [https://perma.cc/2SAN-YVPG] (archived Sept. 3, 2022); Jenni Bergal, *States Consider Legislation to Ban Ransomware Payments*, GOV'T TECH. (July 26, 2021), https://www.govtech.com/policy/states-consider-legislation-to-ban-ransomware-payments [https://perma.cc/36UL-NE9U] (archived Sept. 3. 2022); *Dutch government considering ban on ransom payments by insurers*, PINSENT MASONS (Sept. 28, 2021), https://www.pinsentmasons.com/out-law/news/dutch-government-considering-ban-on-ransom-payments-by-insurers [https://perma.cc/PL59-6S2N] (archived Sept. 3, 2022).

domestic and international law.[38] In May 2021, Tulsa, Oklahoma, fell victim to a ransomware attack.[39] The hackers threatened to release more than eighteen thousand city files containing private information including names, addresses, and driver's license numbers.[40] When the city refused to pay the ransom, the hackers published the eighteen thousand hacked files on the dark web.[41] Moreover, twenty-seven individuals' social security numbers were compromised.[42] Thus, the threat of not following through with a ransomware demand, no matter how risky or enticing for criminals behind such attacks, poses significant human rights concerns.

Like safeguarding human rights, countering ransomware and other cybercrimes is an international law obligation.[43] The Oxford Statement on International Law Protections in Cyberspace makes clear that "conduct carried out through information and communications technologies, such as ransomware operations, is regulated by international law."[44] This view is reiterated by the Tallinn Manual on the International Law Applicable to Cyber Operations.[45] Thus, where a state is responsible for conducting cyber operations, such as the introduction of malware into the cyber infrastructure of another state, violations of sovereignty and the principle of nonintervention have taken place.[46] While the Oxford Statement and the Tallinn Manual are promising, both are nonbinding. However, a comprehensive international treaty on cybercrime, the Council of

---

38. *See* International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; ADITYA VERMA, CENTRAL INFORMATION COMMISSION, RIGHT TO PRIVACY 12 (2019), https://cic.gov.in/sites/default/files/Right%20to%20Privacy%20and%20RTI%20by%20Aditya%20Verma%20%20%281%29%20%281%29.pdf [https://perma.cc/UTH2-X9QS] (archived Sept. 12, 2022).

39. *See Ransomware Update June 22 – Tulsa Police Citations Posted on Dark Web; Tulsa Residents Should Take Necessary Precautions*, CITY OF TULSA (June 22, 2021), https://www.cityoftulsa.org/press-room/ransomware-update-june-22-tulsa-police-citations-posted-on-dark-web-tulsa-residents-should-take-necessary-precautions/ [https://perma.cc/UD7M-9JUA] (archived Sept. 3, 2022).

40. *See Tulsa Says Network Hack Gained Some Social Security Numbers*, U.S. NEWS (July 14, 2021), https://www.usnews.com/news/best-states/oklahoma/articles/2021-07-14/tulsa-says-network-hack-gained-some-social-security-numbers [https://perma.cc/WX57-UYAF] (archived Sept. 3, 2022).

41. *See id.*; Bergal, *supra* note 37.

42. *Tulsa Says Network Hack Gained Some Social Security Numbers*, *supra* note 40.

43. *See* Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan B. Hollis, James C. O'Brien & Tsvetelina van Benthem, *The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations*, JUST SEC. (Oct. 4, 2021), https://www.justsecurity.org/78457/oxford-statement-on-international-law-protections-in-cyberspace-the-regulation-of-ransomware-operations/ [https://perma.cc/P5GZ-SN9E] (archived Sept. 3, 2022).

44. *Id.*

45. *See* INT'L GRP. OF EXPERTS, NATO COOP. CYBER DEFENCE CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 17–27, 312–25 (Michael N. Schmitt & Liis Vihul eds., 2017).

46. *See id.*

Europe Convention on Cybercrime, has been adopted and is thus binding on states that are parties to it.

The 2001 Cybercrime Convention, otherwise known as the Budapest Convention, is the first, and currently the only, international treaty to directly address computer-related crime.[47] With sixty-six parties, the Budapest Convention requires state parties to adopt legislation criminalizing certain cyber acts, such as, *inter alia*, illegal access of data, illegal interception of data, data interference, system interference, and misuse of devices.[48] The Cybercrime Convention Committee Guidance Notes clearly specify that the Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies."[49] Thus, newer forms of malware, including ransomware, are covered by the Budapest Convention.[50]

Procedurally, it is unclear whether or not the Budapest Convention permits the exercise of extraterritorial jurisdiction, which is one of the hotly contested issues in regard to criminalizing illegal conduct that takes place online. Article 22, which establishes the convention's jurisdiction, states, in full,

> Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
>
> (a) in its territory; or
>
> (b) on board a ship flying the flag of that Party; or(c) on board an aircraft registered under the laws of that Party; or
>
> (d) by one of its nationals, if the offense is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.[51]

Based on this provision, it is not known whether the Budapest Convention would provide for extraterritorial jurisdiction, given that it expressly provides for territorial and nationality jurisdiction, but it is silent on extraterritoriality. Even Article 32 of the treaty, which

---

47. *See* Council of Europe Convention on Cybercrime, Nov. 23, 2001, S. TREATY DOC. NO. 108-11, E.T.S No. 185 [hereinafter Budapest Convention]; *Budapest Convention*, COUNCIL OF EUR., https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/ (last visited Sept. 12., 2022) [https://perma.cc/TWE6-CDU3] (archived Sept. 3, 2022).

48. *See* Budapest Convention, *supra* note 47, ch. 2, § 1.

49. CYBERCRIME CONVENTION COMM. (T-CY), T-CY GUIDANCE NOTES *passim* (July 8, 2013), https://rm.coe.int/16802e7132 [https://perma.cc/4ATS-WETG] (archived Sept. 12, 2022).

50. *See id.*

51. Budapest Convention, *supra* note 47, art. 22, ¶ 1.

provides for trans-border access to stored computer data, does so only with state party consent or when the data is publicly made available.[52] This provision has led to considerable disagreement among state parties and international law scholars concerning its scope of interpretation.[53] With such uncertainty lies the risk that this provision may be read either too narrowly (that it does not apply at all) or too broadly (that it encroaches on fundamental human rights).

Article 32 is problematic for a number of other reasons. First, it is legally binding only on state parties such that only state parties can "access or receive, through a computer system in its territory, stored computer data located in another Party."[54] Article 32 will therefore not apply if the computer data is located on the territory of a nonstate party. As scholars have properly noted, this constitutes "a serious shortcoming as more than 130 states are not parties to the [c]onvention."[55]

Even among those that have ratified the convention, Article 32 is permissive, so state parties are not required to follow it. Finally, the issue of consent is troubling since the convention does not define who is able to provide such consent. Even so, not many individuals will voluntarily turn over data that will potentially subject them to criminal jurisdiction.[56] Also, not many data service providers will disclose data because they are not normally considered to own the data, but are merely holders of that data.[57] For all these reasons, since states may argue that the convention, on its face, does not provide for such jurisdiction, and when it does it is merely permissive, the convention is limited in terms of enforcement in a field that is practically reliant on the application of jurisdiction, given that cybercrimes often take place transnationally.[58] Although this view is not without its criticisms, there will inevitably exist limitations in the exercise of territorial jurisdiction for violations of cybercrime governed by international law. As Professor Mireille Hildebrandt states, "[t]erritorialization of cyberspaces easily generates cross-border communication, commerce, and crime, situating the same action

---

52. *See id.* art. 32.

53. *See* Cristos Velasco, Julia Hörnle & Anna-Maria Osula, *Global Views on Internet Jurisdiction and Trans-Border Access*, COUNCIL OF EUR., https://rm.coe.int/16806b8a7c [https://perma.cc/4QR8-GA58] (archived Sept. 4, 2022); Christian Walter, *Obligations of States Before, During, and After a Cyber Security Incident*, 58 GERMAN Y.B. INT'L L. 67, 85 (2015).

54. Budapest Convention, *supra* note 47, art. 32.

55. Jean-Baptiste Maillart, *The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime*, 19 ERA F. 375, 383 (2019).

56. *See id.*

57. *See id.*

58. *See* Mireille Hildebrandt, *Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace*, 63 UNIV. TORONTO L.J. 196, 199 (2013); Maillart, *supra* note 55, at 376.

seamlessly in different territories (both online and offline)."[59] This necessarily requires a reexamination of the legality of extraterritorial jurisdiction in cyberspace, while still ensuring respect for the international human rights law framework and, *inter alia*, the principles of sovereignty and non-intervention in cyberspace. This view has been recognized by INTERPOL at the ad hoc committee's second session concerning the drafting of a cybercrime convention.[60] Also, INTERPOL has stressed the importance of cooperation in order to "counter cybercrime given its cross-border nature."[61]

Article 23 of the Budapest Convention sets out the general principle of international cooperation.[62] But as a matter of procedure, it seemingly does not account for extraterritorial jurisdiction in any of its provisions. One of the matters that the new convention must seriously consider is how jurisdiction will operate in cyberspace. And if extraterritorial jurisdiction is permitted, to what extent it will be permitted. In its submitted statement to the ad hoc committee on the scope, objectives, and elements of a new convention on cybercrime, the Chilean delegate stated, "[t]he new convention is an excellent opportunity to discuss [the issue of jurisdiction], which is the basis for many of the procedural tools that can be addressed."[63] In so doing, it is vital to protect state sovereignty, while bearing in mind that the principle of sovereignty is not absolute. One way to guarantee this is to apply extraterritorial jurisdiction only to cases with a strong territorial nexus.[64] This might help in striking a balance between state sovereignty and extraterritorial enforcement.[65] In fact, the draft UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes seemingly promotes this balance. Draft Article 3 protects state sovereignty and states, "[t]his Convention shall not authorize the competent authorities of a State party to exercise in the territory of another State the jurisdiction and functions that are reserved exclusively for the authorities of that other State under its domestic law, *except as*

---

59. Hildebrandt, *supra* note 58, at 222.

60. *See* U.N. OFF. ON DRUGS & CRIME, STATEMENT BY INTERPOL AT SECOND SESSION OF THE AD HOC COMMITTEE ON CRIMINALIZATION (May 31, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/INTERPOL_Statement_on_Criminalization_vfinal_1.pdf [https://perma.cc/A7W4-SAYT] (archived Sept. 3, 2022).

61. *Id.*

62. *See* Budapest Convention, *supra* note 47, art. 23.

63. G.A. Res. A/AC.291/4, at 11/69 (Nov. 17, 2021).

64. *See* Sarah Miller, *Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention*, 20(4) EUR. J. INT'L L. 1223, 1236 (2010).

65. *See id.* at 1245.

provided for in this Convention."[66] In Article 39, concerning jurisdiction, the draft convention states, in pertinent part,

> [s]ubject to article 3 of this Convention, a state party may also establish its jurisdiction over any such offence and other unlawful act when: . . . (d) The offence is committed wholly or partly outside the territory of that State party but its effects in the territory of that State party constitute an offence or result in the commission of an offence.[67]

This appears to be a step in the right direction, grounding extraterritorial jurisdiction in some element of territorial jurisdiction, thereby defeating sovereignty concerns. Interestingly, the convention prohibits certain reservations, but not on Article 3, concerning sovereignty, nor on Article 39, concerning jurisdiction.[68] Thus, the parties are guaranteed respect for the principles and obligations laid out therein. Of course, the draft convention is still in its early stages, and there is still much work to be done. For one, it is recommended that the convention further specify whether extraterritorial jurisdiction applies and, if so, in which contexts. No matter the jurisdictional bases ultimately chosen, this will surely be raised as a point of contention among many states, one that the ad hoc committee sessions will hopefully tackle in the short amount of time it has to complete the draft.

Turning to the substantive provisions, the current Cybercrime Convention rightly envisions certain tensions with international human rights law. In its preamble, the convention clarifies "the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights," including freedom of expression, freedom of opinion, and privacy rights.[69] Thus, the convention somewhat requires adequate protection of the human rights framework in formulating cybercrime laws, striking a balance between human rights law and national security concerns. For this reason, many proponents of the Budapest Convention have stressed the importance of complementing the existing framework that follows the convention's rights-based approach.[70] Still, more effort can be undertaken to ensure that these fundamental human rights are more directly and fully integrated into cybercrime legislation in the form of

---

66. *Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, art. 3, U.N. OFF. ON DRUGS & CRIME (June 29, 2021), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf [https://perma.cc/SN8B-EF49] (archived Sept. 3, 2022) (emphasis added).

67. *Id.* art. 39, ¶ 2(d).

68. *See id.* art. 86.

69. Budapest Convention, *supra* note 47, pmbl.

70. *See, e.g.*, U.N. OFF. ON DRUGS & CRIME, STATEMENT ON BEHALF OF THE EU AND ITS MEMBER STATES 3–4 (Feb. 28, 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/EU.pdf [https://perma.cc/3NJG-97MH] (archived Sept. 3, 2022).

a new and comprehensive international treaty. It is further vital that adequate safeguards are implemented in order to ensure that states do not violate human rights in legislating against cybercrime. Such procedural safeguards necessarily include requiring "independent and competent judicial authorization of surveillance measures that intrude on privacy, meaningful oversight of surveillance measures, and respect for due process rights."[71]

Because the Council of Europe's Cybercrime Convention is already in effect, some states are reluctant to provide support for a UN-based international treaty regulating cybercrime due to human rights concerns.[72] These states fear that an international treaty regulating cybercrime will result in significant potential for government overreach where human rights are concerned.[73] Other states "believe a new instrument with global inputs is needed."[74] While the debate on who should regulate cyberspace is divided, a new UN treaty on cybercrime regulation should be welcomed, with the caveat that states must ensure respect for the basic human rights framework—taking into consideration the nine core international human rights treaties and the Universal Declaration of Human Rights—during the drafting process.

At the current time, the Budapest Convention does not go far enough. It is limited in both substance and procedure. Aside from the uncertainty about whether the convention applies extraterritorially, only sixty-six states are parties to the convention, and that is mostly due to nonparty state concerns that "these States were not involved in the drafting process of the Budapest Convention."[75] These nonparty states, namely Russia and developing countries, argued that the current convention does not take into consideration their concerns with respect to sovereignty, since Article 32(b) of the convention "allows States to obtain information in another country if the lawful owner of the data consents, without the need for government approval."[76] In 2000, the American Federal Bureau of Investigation hacked into Russian computers and managed to collect evidence that would later be used to prosecute two Russian men in US courts for defrauding

---

71. U.N. OFF. ON DRUGS & CRIME, SUBMISSION BY HUMAN RIGHTS WATCH TO THE UNITED NATIONS AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES FOR CRIMINAL PURPOSES 5 (Apr. 2022), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/HRW_contribution.pdf [https://perma.cc/7YJR-7JAC] (archived Sept. 3, 2022).

72. *See* SUMMER WALKER, GLOB. INITIATIVE AGAINST TRANSNAT'L ORGANIZED CRIME, CYBER-INSECURITIES? A GUIDE TO THE UN CYBERCRIME DEBATE 2–3 (Mar. 2019), https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf [https://perma.cc/JDG4-RJHU] (archived Oct. 10, 2022).

73. *See id.* at 3.

74. *Id.* at 2.

75. *Id.* at 6.

76. *Id.*

American banks.[77] This was viewed as a violation of state sovereignty. The new convention could therefore strike a balance between state sovereignty and other concerns.

Moreover, yet another point of contention raised by nonparty states is the claim that there is a lack of proper cooperation mechanisms within the Budapest Convention.[78] While Article 23, laid out above, establishes the general principles of international cooperation, opponents argue that, in terms of mutual legal assistance, "'the promise of cooperation [is] not firm enough' or that there are grounds for refusal to cooperate."[79] Thus, countries like India refused to become a party to the Budapest Convention but have become major proponents of an international treaty on cybercrime.

Regardless of whether these claims are properly substantiated, the new comprehensive international treaty must, as far as possible, take into consideration states' differences so as to ensure international cooperation and compliance. As stated by the Australian government, "[a] new convention will only be valuable if it can secure widespread support among the majority of Member States, based on consensus agreement obtained from good faith discussions under the auspices of the Ad Hoc Committee."[80] A UN-backed international treaty on cybercrime is better able to do so than the current Budapest Convention, as indicated by the fact that a number of states that are not signatories to the Budapest Convention have vigorously supported the adoption and drafting of the new treaty.[81] Moreover, as states contribute to the development of this new treaty, the higher the likelihood that the treaty will be viewed as internationally comprehensive rather than as a western innovation.

Considering the nonparty state concerns raised above, a universal, regulatory binding treaty on cybercrime regulation has become necessary to tackle the growing problem of cybercrime. International law must adapt in order to account for changes in the global regime stemming from issues raised by the regulation of cyberspace. Irrespective of whether the Budapest Convention is a proper means to regulate cybercrime, over twenty years after its adoption it still has relatively few signatories compared to other international treaties. So long as states view cybercrime legislation as a potential infringement on state sovereignty, high levels of

---

77. *See UN rejects Russian cyber-crime treaty*, ITPROPORTAL (Apr. 21, 2010), https://www.itproportal.com/2010/04/21/un-rejects-russian-cyber-crime-treaty/ [https://perma.cc/2NL9-T93X] (archived Sept. 4, 2022).

78. *See* WALKER, *supra* note 72, at 6.

79. ALEXANDER SEGER, CYFY 2016, INDIA AND THE BUDAPEST CONVENTION: WHY NOT? 7 (Aug. 10, 2016), https://rm.coe.int/16806a6698#:~:text=The%20Budapest%20Convention%20is%20a,and%20the%20securing%20of%20electronic [https://perma.cc/VW8X-G4LT] (archived Sept. 4, 2022).

80. G.A. Res. A/AC.291/4, *supra* note 63, at 3/69.

81. *See generally* SEGER, *supra* note 79.

commitment and cooperation across the international arena are highly unlikely. Accordingly, a more comprehensive UN-backed international treaty that could potentially attract more state parties is necessary if states are to regulate cybercrime while maintaining commitment and respect for human rights. The current treaty is often criticized for its weak protection for human rights.[82] Although some have criticized that a new cybercrime treaty is dangerous given the potential for further government regulation that may harm human rights, such as the right to freedom of expression and the right to privacy, a new cybercrime treaty could in fact provide an opportunity for stronger human rights protection. The best approach to solve this dilemma is to incorporate human rights protections in cybercrime regulation so as to ensure that one is not favored over the other. Otherwise, government regulation of cybercrime will almost always trump human rights.

It is true that many state laws on cybercrime far exceed that which is permissible under human rights law and, therefore, states oppose the establishment of an international treaty that would give states authority to do so.[83] However, given the potential this presents to regulate against cybercrime and protect against human rights violations inside the treaty itself, there is no reason to be afraid of the new UN convention. In sum, cybercrime regulation must not trump human rights. Rather, human rights must inform cybercrime regulation. Once a balance is struck, such that all sides are considered in the drafting of this treaty, the potential for greater state acceptance may increase. Of course, this consideration is not foolproof, and the more states who participate in the negotiation process, the more the likelihood for diverging views. Nonetheless, the more states who engage in the negotiating process, the more likely it is that those states will become parties to the new cybercrime convention, giving strength to it. That is, for example, one of the reasons provided as to why India, who did not negotiate during the drafting of the Budapest Convention, did not become a party to it, but India is a strong proponent of the new UN convention. States who participate in the drafting process have a stake in the treaty and are therefore more likely to feel included and that the treaty is more international than European focused, one that is more inclusive of their views. While the new convention should examine all points of view, it is crucial that states view human rights and cybercrime legislation as complementary rather than competing principles in order to prevent governments from passing laws that violate human rights.

---

82. *See* Brown, *supra* note 4.
83. *See, e.g., id.*

A. *Restrictions and Derogations to International Human Rights*

To guard against the threat of government control and overreach in formulating cybercrime regulation, states must continue to protect those human rights that are most likely to be implicated in cybercrime regulation policies, namely freedom of expression, freedom of opinion, and privacy. Although these rights are not absolute, meaning that they can be limited, they may only be restricted under certain circumstances. Thus, before discussing these rights in detail, this Article will provide an overview of how and when rights may be limited under international human rights law. Human rights can be either absolute, meaning they can never be suspended or limited under any circumstances, or limited, meaning that they can. Those rights that are absolute, include, for example, the freedom from torture or the right to recognition as a person before the law.[84] Most human rights, however, are not absolute, and rightly so given that some rights must be limited, but under very stringent circumstances in order to balance competing interests. Considering freedom of expression, for example, which is a right that may be limited, as such restriction is often necessary to ensure that freedom of speech does not extend to hate speech. Privacy rights may also necessarily be limited in accordance with lawfully executed search warrants. For the most part, then, rights may be limited or suspended, and that includes the right to freedom of expression, the right to freedom of opinion, and the right to privacy.

Accordingly, there are two ways in which rights may be suspended or limited under international human rights law. Article 4 of the International Covenant on Civil and Political Rights (ICCPR) allows state parties to derogate from their responsibilities under the convention "[i]n time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed."[85] When such an emergency exists, state parties can rely on the derogation clause in Article 4 to derogate from their international responsibilities so long as it is strictly required under the circumstances, "provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin."[86] The provisions under which derogation is not permitted are laid out in Article 4(2).

In addition to derogation, state parties may restrict certain rights so long as certain conditions are met. Article 19, which protects the freedom of expression, may be restricted so long as it is provided by law and is necessary "(a) [f]or respect of the rights or reputations of others; [or] (b) [f]or the protection of national security or of public order, or of

84. *See* ICCPR, *supra* note 38, art. 4, ¶ 2.
85. *Id.* art. 4, ¶ 1.
86. *Id.*

public health or morals."[87] Which rights may be restricted and which rights may be derogated depend on the convention. From a textual interpretation, it appears that some rights, like the right to privacy, cannot be restricted as the convention does not provide it with this right, but it can be derogated. At the same time, however, the Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, has stated that, although Article 17, which contains the right to privacy, is silent on restrictions, it "should also be interpreted as containing the said elements of a permissible limitations test."[88] That is because the language used in Article 17 is interpreted to support the view that it, too, contains this permissible limitations test.[89] Thus, the same test that applies to other rights, like the freedom of expression, applies to the right to privacy. That is, the right to privacy may be restricted where it (1) is provided by law, (2) is necessary in a democratic society, and (3) furthers one of the legitimate aims enumerated in the limitations provisions.[90]

For a restriction to be provided by law, "there must be clear legislation to enable individuals to understand exactly what forms a violation under the law."[91] Considering this, the law must be clear, accessible, and precise enough to allow for the regulation of conduct, and it must also provide protection from arbitrary state interferences.[92] In the context of cybercrime regulation, overbroad or vague laws that criminalize speech that, for example, "threatens public order" would violate this prong since it is not precise nor does it provide protection from arbitrary state interferences.[93] Such blanket restrictions are prohibited under international human rights law.

Next, in order for a restriction to satisfy the necessity prong, there must not exist other less restrictive alternatives that could also achieve one of the enumerated legitimate aims. The element of necessity is interrelated with proportionality such that the restriction must be the least intrusive means to protect that interest.[94] Taking the above example, blanket restrictions on cybercrime regulation can never be considered either necessary or proportional since they extend far beyond the limitations imposed under international human rights.

Finally, the restriction must be undertaken to achieve one of the enumerated aims within the convention, namely for the protection of

87. *Id.* art. 19, ¶ 3 (internal parentheses omitted).

88. Martin Scheinin (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism), *Report on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, U.N. Doc. A/HRC/13/37, ¶ 17 (Dec. 28, 2009).

89. *See id.* ¶ 18.

90. *Id.* ¶ 17.

91. Albader, *supra* note 12, at 27.

92. *See id.*

93. *See* FLETCHER & POKHAREL, *supra* note 16, at 2.

94. *See id.* at 18–19.

national security, public health, or public order. In the context of cybercrime, state parties will almost surely argue that the restrictions are undertaken to protect national security interests. Although this likely does not in and of itself violate the limitations test, the test tends to fail on the other prongs, since it is unlikely to be provided by law, and, even if so, it is often not necessary or proportional under the circumstances. In sum, restrictions are allowed for certain rights as provided under the ICCPR, but only when these stringent requirements are met.

It is worthy to note that, while Article 19(1)'s right to hold opinions without interference cannot be restricted, since the convention does not provide it with this right while allowing for restrictions on the freedom of expression contained in Article 19(2), it also is understood not to allow for any derogation even though it is not listed among the rights to which no derogation is permitted under Article 4(2) of the ICCPR. That is because the UN Human Rights Committee, in its General Comment No. 34 interpreting the freedom of opinion and expression stated,

> although freedom of opinion is not listed among those rights that may not be derogated from pursuant to the provisions of article 4 of the Covenant, it is recalled that, 'in those provisions of the Covenant that are not listed in article 4, paragraph 2, there are elements that in the Committee's opinion cannot be made subject to lawful derogation under article 4.'[95]

While general comments of the Human Rights Committee are not legally binding, they are considered highly authoritative given that the treaty body is interpreting the various provisions of its respective treaty, which in this case is the ICCPR.

In light of this framework, this Article will now consider the freedom of expression, the freedom of opinion, and the right to privacy and how they interplay with this system of derogations and limitations in the context of cybercrime regulation. Instead of a balancing test, this Article will suggest that the better framework would be to incorporate these rights into cybercrime legislation so as to ensure that one does not prevail over the other.

B. *Freedom of Expression*

Freedom of expression is protected under Article 19 of the ICCPR.[96] It is a binding obligation on the 173 state parties to the

---

95. Comment, Human Rights Committee, CCPR General Comment No. 34: Freedoms of Opinion and Expression art. 19, ¶ 5, U.N. Doc. CCPR/C/GC/34 (2011) [hereinafter General Comment No. 34].

96. *See* ICCPR, *supra* note 38, art. 19, ¶ 2.

ICCPR.[97] It is also protected by various regional and domestic instruments.[98] The right to freedom of expression is considered a norm of customary international law today.[99] Thus, all states are bound to ensure that everyone has the right to freedom of expression.

In the cyber context, cybercrime regulation often has the effect of chilling free expression.[100] In November 2021, a joint study by the University of California, Berkeley Law International Human Rights Law Clinic, and the Gulf Centre for Human Rights identified a growing trend of curtailment of freedom of expression online.[101] By examining the anticybercrime legislation of ten countries in the Gulf region, the study found that these countries effectively relied on such legislation to prosecute what is affirmatively protected expression under international law.[102] Many of these governments targeted human rights defenders who advocated for minority and women's rights online, charging them with violations of applicable provisions in their respective cybercrime laws.[103] In Saudi Arabia, for example, the government has relied on its Anticybercrime Law and the Law on Combatting Terrorism Crimes and Its Financing to arrest Saudi human rights defenders and journalists for their online human rights advocacy on various issues that stand in direct contrast with the position of the Saudi government.[104] This repression has resulted in various human rights violations, most notably the right to freedom of expression under the ICCPR.

While the right to freedom of expression under the ICCPR may be subject to certain restrictions under Article 19(3) of the ICCPR, such restrictions are only permissible when they are (1) provided by law, (2) necessary, and (3) undertaken to protect a legitimate state interest, such as respect of the rights or reputations of others or for the protection of national security or of public order.[105] Yet, most of the

---

97. *Id.* art. 2, ¶ 1; *see also Status of the International Covenant on Civil and Political Rights*, U.N. TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND (last visited Dec. 22, 2021) [https://perma.cc/V445-LUPF] (archived Aug. 24, 2022).

98. *See, e.g., Freedom of Opinion and Expression – International standards*, U.N. HUM. RTS. OFF. OF THE HIGH COMM'R, https://www.ohchr.org/en/issues/freedomopinion/pages/standards.aspx (last visited Dec. 22, 2021) [https://perma.cc/4DCM-RTK7] (archived Aug. 24, 2022); U.S. CONST. amend. I.

99. *See* Emily Howie, *Protecting the Human Right to Freedom of Expression in International Law*, 20 INT'L J. SPEECH LANGUAGE PATHOLOGY 12, 12 (2018).

100. *See* Wafa Ben-Hassine, Emma Sayadi & Dima Samaro, *When "cybercrime" laws gag free expression: stopping the dangerous trend across MENA*, ACCESS NOW (Sept. 12, 2018), https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/ [https://perma.cc/F3YQ-SFGG] (archived Aug. 24, 2022).

101. *See* FLETCHER & POKHAREL, *supra* note 16, at 1.

102. *See id.* at 2–3.

103. *See id.* at 3.

104. *See id.* at 190, 194.

105. ICCPR, *supra* note 38, art. 19, ¶ 3; Kaye, *supra* note 24, ¶ 31.

time, cybercrime regulation is defined as vaguely as possible such that it is used as a vehicle to curb free expression, thereby failing on the first prong.[106] Moreover, these laws extend far beyond what is necessary to combat cybercrime and far exceed the legitimate state interests used to further fuel the regulations.[107] For a requirement to satisfy the necessity prong, there must not exist other less restrictive alternatives that would not violate the provision to which it belongs.[108] For example, the transfer of a teacher to a non-teaching position because the teacher published material that was deemed hostile toward a particular religious community was viewed as necessary to protect children of that faith within that school district.[109] Similarly, in the cyber context, it is very much necessary to enact anticybercrime legislation that limits free speech bordering on incitement to violence. Even the ICCPR prohibits advocacy that constitutes incitement to discrimination, hostility, or violence.[110] Thus, cybercrime laws that seek to regulate such speech online are likely necessary, as in the example of the teacher, for the respect of the rights of others.[111] In the Saudi example, however, the laws cannot be considered necessary because holding as such would set a dangerous precedent, one that would chill free speech as all governments begin to cite national security concerns in order to limit their obligations to an extent far beyond what is permissible under international human rights law. And, in having to make a choice between national security and human rights, national security often prevails, meaning that if international cybercrime regulations permit states to make overbroad laws in the name of national security, human rights will almost always be of secondary concern.

In any event, the mass arrest of hundreds of human rights defenders and advocates cannot be said to comply with any of the requirements for permissible restrictions under Article 19(3) of the ICCPR. The Middle East is not alone in adopting cybercrime laws that have the effect of chilling free expression. In 2020, a Philippines Regional Trial Court prosecuted and convicted two journalists under the 2012 Cybercrime Prevention Act for cyber libel when the journalists re-published an article accusing a former justice of the

---

106. *See, e.g.*, JOYCE HAKMEH, CYBERCRIME LEGISLATION IN THE GCC COUNTRIES: FIT FOR PURPOSE? 4 (2018); *Libya's cybercrime law: A threat to freedom of expression and legalization of censorship*, ACCESS NOW (Nov. 10, 2021), https://www.accessnow.org/libya-cybercrime-law-threat-to-freedom-of-expression/ [https://perma.cc/M3EQ-856E] (archived Aug. 24, 2022) [hereinafter Libya's cybercrime law].

107. *See* HAKMEH, *supra* note 106; Libya's cybercrime law, *supra* note 106.

108. *See* General Comment No. 34, *supra* note 95, ¶ 33.

109. *See id.*

110. *See* ICCPR, *supra* note 38, art. 20, ¶ 2.

111. *See id.* art. 19, ¶ 3(a) (providing that freedom of expression may be subject to such restrictions that are necessary "[f]or respect of the rights or reputations of others").

Supreme Court of Philippines of impropriety.[112] Regardless of whether or not the information was true, criminal defamation must not be allowed to flourish, as it has the effect of chilling free expression.[113] Rather, civil defamation must be retained as the proper regulatory body of law. Western states have also fallen victim to far-reaching cybercrime legislation. In 2019, the United Kingdom passed antiterrorism legislation that effectively punishes the right to view terrorist material information online.[114] The UK act also prohibits expressions of opinion or belief supportive of proscribed terrorist organizations.[115] All these examples show that states have thus far managed to impose far-reaching, overly restrictive anticybercrime laws that extend well beyond what is a permissible restriction under international law.

Accordingly, the upcoming global treaty on cybercrime regulation must take steps to define as narrowly as possible the crimes within the convention so as to ensure adequate safeguards of the right to freedom of expression. Any restrictions on this right that would serve to muzzle human rights cannot be justified under international law.[116] Moreover, the forthcoming treaty must explicitly state how the permissible restrictions and/or derogations of this right interplay with cybercrime regulation, which the Budapest Convention does not explicitly address. Rather, the Budapest Convention merely states in its nonbinding preamble the need to respect fundamental human rights, including the right to freedom of expression.[117] Granted, Article 15 of the Budapest Convention ensures adequate safeguards of the international human rights framework described in subpart A.[118] However, in order to make these obligations clear and binding, the new global treaty must expressly define the scopes and limitations of these human rights, including the freedom of expression, and the limited situations in which states may restrict or derogate from these human rights obligations.

---

112. *See* Emerlynne Gil, *Philippines: Cyber-libel conviction of Maria Ressa and Reynaldo Santos a blow to freedom of expression and media online*, INT'L COMM'N OF JURISTS (June 16, 2020), https://www.icj.org/philippines-cyber-libel-conviction-of-maria-ressa-and-reynaldo-santos-a-blow-to-freedom-of-expression-and-media-online/ [https://perma.cc/CU6P-QNRQ] (archived Aug. 24, 2022); *Philippines: Rappler Verdict a Blow to Media Freedom*, HUM. RTS. WATCH (June 15, 2020), https://www.hrw.org/news/2020/06/15/philippines-rappler-verdict-blow-media-freedom [https://perma.cc/3B8M-3E5S] (archived Oct. 10, 2022).

113. *See id.*

114. *See* Albader, *supra* note 12, at 24.

115. *See* Counter-Terrorism and Border Security Act 2019, c. 1, § 1 (UK).

116. *See* ICCPR, *supra* note 38, art. 19, ¶ 3; *see also* General Comment No. 34, *supra* note 95, ¶ 23 (affirming that paragraph 3 of Article 19 may not, under any circumstance, "muzzle" advocacy of human rights).

117. *See* Budapest Convention, *supra* note 47, pmbl.

118. *See id.* art. 15.

C. *Freedom of Opinion*

Like freedom of expression, freedom of opinion is also protected under Article 19 of the ICCPR.[119] Freedom of opinion protects the right to hold opinions without interference. Unlike freedom of expression, Article 19 makes no provision for the restriction of this right.[120] In its General Comment, the United Nations Human Rights Committee on Civil and Political Rights (Committee) has explicitly stated that the freedom of opinion "is a right to which the Covenant permits no exception or restriction."[121] Moreover, Article 4 of the ICCPR permits state parties to take measures derogating from certain provisions of the ICCPR, where necessary, in times of public emergency threatening the life of the nation and whose existence is officially proclaimed.[122] Article 4(2) lists the provisions under which no derogation may be made. Article 19 is not one of them. Nonetheless, the Committee has, again, expressed that, "although freedom of opinion is not listed among those rights that may not be derogated from," no derogation is allowed from freedom of opinion, "since it can never become necessary to derogate from it during a state of emergency."[123] Thus, the right to freedom of opinion must be respected at all times.

A global treaty on cybercrime, therefore, cannot infringe on freedom of opinion, no matter the circumstance. Any interference on freedom of opinion will violate a state's obligation to respect this right. Concerning the UK act described above, the act punishes individuals who express an opinion as to a proscribed terrorist organization online, thereby violating freedom of opinion as well as freedom of expression.[124] Such cybercrime laws that attempt to limit the right to freedom of opinion must be repealed and amended. An international treaty that sets forth uniform standards for how to conform to international human rights in legislating against cybercrime is required so that all states understand their obligations both domestically and internationally.

D. *Right to Privacy*

The right to privacy, related to the rights of freedom of expression and opinion, is probably the most problematic in terms of state surveillance measures undertaken in the name of cyber security. For example, during COVID-19 alone, states justified extremely invasive, technologically furthered measures to tackle the pandemic. South Korea tracked the location of, and made publicly available, the names

---

119. *See* ICCPR, *supra* note 38, art. 19, ¶ 1.
120. *See id.* art. 19; General Comment No. 34, *supra* note 95, ¶ 9.
121. General Comment No. 34, *supra* note 95, ¶ 9.
122. *See* ICCPR, *supra* note 38, art. 4.
123. General Comment No. 34, *supra* note 95, ¶ 5.
124. *See* Counter-Terrorism and Border Security Act, *supra* note 115, c. 1, § 1.

and information of those infected with the virus.[125] Russia authorized "the use of facial recognition to find those suspected of evading a 14-day self-quarantine period upon their arrival in Russia."[126] These state measures were too invasive to be justified under the right to privacy.

The right to privacy is protected under Article 17 of the ICCPR, which prohibits "arbitrary or unlawful interference with [one's] privacy, family, home or correspondence."[127] This right is subject to derogation under Article 4, but such derogation must be both necessary and proportional given the circumstances, and the derogation must conform to other international law requirements, including nondiscrimination.[128] The measures taken to combat the spread of COVID-19 were neither necessary nor proportional, as they far exceeded their purpose. For the same reasons, the restrictions undertaken during COVID-19 also fail the permissible limitations test for valid restrictions under the ICCPR, as necessity entails that these measures were the least intrusive means to accomplish the legitimate state aim to be protected, which in this case is public health. Accordingly, in the context of cybercrime legislation, states must learn from the violative measures taken in response to COVID-19 so as to ensure that legislation does not surpass its limits and once again violate the human right to privacy.

In conclusion, human rights, including freedom of expression, freedom of opinion, and privacy, must be considered in cybercrime regulation. Given that some of these human rights are not absolute, necessary and proportional restrictions may be imposed upon them when balanced against legitimate state interests such as national security concerns. Often, the tendency of states is to limit human rights in favor of national security interests.[129] However, if national security interests were allowed to trump human rights, the basic human rights framework and its related limitations test would fail as states are forced to trump one (human rights) in favor of the other (national security). Rather than viewing human rights concerns as independent from national security concerns, a better and more sustainable alternative is to incorporate human rights into these national security

---

125. *See* Eun-Young Jeong, *South Korea Tracks Virus Patients' Travels – and Publishes Them Online*, WALL ST. J. (Feb. 16, 2020), https://www.wsj.com/articles/south-korea-tracks-virus-patients-travelsand-publishes-them-online-11581858000 [https://perma.cc/B8R2-QNKL] (archived Aug. 24, 2022).

126. *Chinese targeted in Russia raids as coronavirus fears spread*, S. CHINA MORNING POST (Feb. 23, 2020), https://www.scmp.com/news/world/russia-central-asia/article/3051964/chinese-targeted-russia-raids-coronavirus-fears [https://perma.cc/6GNZ-9TZE] (archived Aug. 24, 2022).

127. ICCPR, *supra* note 38, art. 17.

128. *See id.* art. 4; *see also* Statements, Hum. Rts. Comm., Statement on derogations from the Covenant in connection with the COVID-19 pandemic, ¶ 2, U.N. Doc. CCPR/C/128/2 (2020).

129. *See* Albader, *supra* note 12, at 37.

policies so as "to ensure respect for human rights at all times."[130] The next Part, therefore, briefly discusses how best to ensure a complementary framework, one that would not limit one concern in favor of the other, in the context of a global treaty on cybercrime.

III. INTERNATIONAL REGULATION OF CYBERCRIME: INCORPORATING HUMAN RIGHTS

In its open letter to the UN General Assembly, the Association for Progressive Communications, a non-governmental organization, advocated against the adoption of an international treaty on cybercrime regulation on the basis that it criminalizes what would normally be considered "ordinary online activities," thereby implicating various human rights in the process.[131] Clément Nyaletsossi Voule, UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, reported, "[a] surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world."[132] Thus, drafters of a global agreement on cybercrime must strike a balance, one that would properly safeguard the basic human rights framework, where fundamental human rights are respected in all circumstances except where permissible limitations are allowed.

State representatives must cooperate to establish a framework that would not be used as a pretext to commit serious human rights violations. Draconian measures used to stifle online freedoms must not be allowed to flourish. During negotiations, states must cooperate to ensure that the treaty clearly defines the cybercrimes it aims to regulate, so as to ensure that legislation does not become overbroad and far reaching, thereby defeating state concerns that a global treaty on cybercrime will lead to the criminalization of ordinary online behavior protected under human rights standards.[133] Clearly defining these standards will lessen the probability that offenses within the treaty will "lead to unnecessary or disproportionate interference with" human rights.[134] As an additional safeguard against possible human

---

130. *Id.* at 41.

131. *See Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online*, ASS'N FOR PROGRESSIVE COMMC'NS (Nov. 6, 2019), https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human [https://perma.cc/CAV4-C6EX] (archived Aug. 24, 2022).

132. Clément Nyaletsossi Voule (Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association), *Report on the Rights to Freedom of Peaceful Assembly and of Association*, U.N. Doc. A/HRC/41/41, ¶ 3 (May 17, 2019).

133. *See Open letter to UN General Assembly*, *supra* note 131 (contending that cybercrime laws must be narrowly defined so as not to hinder human rights or to create a chilling effect on the exercise of those rights).

134. General Comment No. 34, *supra* note 95, ¶ 46.

rights abuses, the treaty must expressly state the situations that would give rise to permissible restrictions and/or derogations under the applicable human rights regime. Accordingly, states must come together to ensure that, throughout the negotiation process, the treaty explicitly refers to and addresses at the forefront relevant human rights concerns.

In order to promote state cooperation, the treaty must, to the extent possible, incorporate the various views of the states involved. In so doing, the treaty must aim to strike a balance between national security concerns on the one hand and human rights on the other. The best approach, therefore, is to integrate human rights concerns into the cybercrime treaty so as to prevent misuse of cybercrime legislation resulting in a chilling effect on free expression and a hinderance of associated human rights online.[135] This view is reaffirmed by the UN Office of the High Commissioner for Human Rights in its submission to the ad hoc committee tasked with drafting the new convention on cybercrime.[136] A mere reaffirmation of the importance for the promotion and protection of human rights is not sufficient, and thus the Budapest Convention does not go far enough. The future global treaty must provide expressly for human rights safeguards within the text of the treaty itself while, at the same time, also providing a balance with national security interests. The best approach is to integrate a human rights–based approach into combatting cybercrime.

The 2021 Draft UN Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes could provide a starting point for a comprehensive international treaty on cybercrime regulation.[137] However, as it currently stands, the draft convention has garnered much criticism because of certain provisions that would allow cross-border access to data "by limiting the ability of a signatory to refuse to provide access to requested data."[138] While the draft convention does provide for respect for human rights in its preamble, and provides conditions and safeguards for the implementation of legislation in compliance with human rights in Articles 32 and 43, like the Budapest Convention, it does not clearly define the scopes and limitations of these safeguards.[139] Rather than leaving it to chance, the future international treaty on cybercrime must provide clearly the interplay of and prioritize human rights concerns, such as due diligence, relevant to all stakeholders.

---

135. *See id.* (stating that counter-terrorism measures should be clearly defined so as not to interfere with freedom of expression).

136. *See* OHCHR KEY-MESSAGES RELATING TO A POSSIBLE COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES, *supra* note 28.

137. *See Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online*, *supra* note 131.

138. *Id.*

139. *See id.*

While it is urged that states come together to clearly define the scope of the application of the treaty and its relation to human rights, in order to remain relevant for years to come, the international treaty must leave open-ended any definitions associated with current technology and methodology, in the form of a non-exhaustive list.[140] That is so as to ensure that the treaty is capable to deal with emerging threats of cybercrime and will remain effective in the future.

Given that the threat of cybercrime remains urgent and has proliferated due to COVID-19 and the Russian invasion of Ukraine, states must now begin to consider these essential elements that have been described that bear on whether the international community will ultimately adopt a global treaty on cybercrime come 2023. It is clear that, in order to maximize state cooperation, the global treaty must tackle, *inter alia*, the following objectives:

- ensure that the human rights framework is at the forefront of anticybercrime legislation,
- reform already-existing domestic cybercrime laws to comply with human rights law,
- safeguard state sovereignty and issues related to it, and
- provide effective mechanisms to guarantee international cooperation.

The best approach, therefore, is to integrate all these concerns into the treaty such that the treaty does not lead to a hostile environment hindering the protection of human rights.

IV. CONCLUSION

States have an obligation under international law to protect individuals against the rising threat of cybercrime. At the same time, states have an obligation to respect all human rights. The best way to ensure such respect is to incorporate human rights law into national security concerns in a way that the new UN-backed global treaty on cybercrime will have to address. States now have the opportunity to cooperate in the establishment of a cybercrime treaty that will hopefully garner more state support than previous conventions. The current war in Ukraine should not hinder cooperation during the drafting process of this proposed treaty. Responses from state delegates—including the United States—that, since Russia initiated the process on international regulation of cybercrime, and since Russia

---

140. *See* AUSTRALIA NATIONAL SUBMISSION, U.N. OFF. ON DRUGS & CRIME, AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON CYBERCRIME: AUSTRALIAN SUBMISSION ON SCOPE, OBJECTIVES, AND STRUCTURE (Oct. 29, 2021), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Australia_-_National_Submission.pdf [https://perma.cc/2XZP-PCA2] (archived Aug. 24, 2022) (stating that criminalization standards should be drafted in a fashion that is neutral regarding technology and methodology).

is alleged to have committed a number of cyberattacks during the conflict, negotiating with Russia at this time is not appropriate, should not intrude on this domain.[141] Now is the most urgent and pressing time to negotiate with Russia and focus on the task at hand, which is to draft a cybercrime treaty that aims to legislate against cyberattacks while at the same time protecting human rights. Safeguarding human rights, such as freedom of expression, freedom of opinion, and privacy, will ensure such enhanced support and cooperation among the international community, which is vital if the treaty will be successful in passing muster in 2023, when a draft convention is expected to be submitted for review.

This Article has stressed the need for human rights standards to be fully integrated into a global treaty addressing cybercrime regulation. The Budapest Convention has provided a good starting point for a new, comprehensive global treaty on cybercrime regulation. Now, it is up to states to cooperate in the establishment of a new treaty that will complement the already existing international law framework, with due regard to human rights law.

Cybercrime is a global threat, one that requires global attention. Given its immediacy, the time is ripe for states to consider how best to effectively combat the threat of cybercrime operations while simultaneously safeguarding the basic human rights framework. If adopted, the new treaty on cybercrime will provide states with the unprecedented opportunity to legislate against cybercrime on an international basis. At the same time, states must remain vigilant in making sure that implicated human rights, such as freedom of expression, freedom of opinion, and privacy, remain protected. Only then will a true global treaty on cybercrime emerge.

---

141. *See, e.g.*, U.S. NATIONAL STATEMENT, *supra* note 13.