Chicago Journal of International Law

Volume 24 | Number 1 Article 10

The Honeypot Stings Back: Entrapment in the Age of Cybercrime and a Proposed Pathway Forward

Renée N. Girard

The Honeypot Stings Back: Entrapment in the Age of Cybercrime and a Proposed Pathway Forward

Renée N. Girard*

Abstract

Cybercrime's transnational nature has rendered conventional methods of domestic policing ineffective. The international community must cooperate to combat cross-border cybercriminals. Law enforcement efforts to respond to the threat through cyber sting operations call into question the degree to which individuals are protected by the entrapment defense. There is disagreement in the international community about the validity of the defense. The lack of consensus threatens effective law enforcement cooperation in responding to cybercrime, posing a global security risk. Furthermore, if countries with dissimilar entrapment rights cooperate to share data and carry out cyber stings, there is a heightened risk of the rights of the private citizen being diluted. After summarizing existing international agreements that discuss transnational crime and cybercrime, this Comment proposes that the international community modify the Budapest Convention to establish a "minimum floor" of entrapment rights. This approach would require countries, at a minimum, to consider entrapment as grounds for mitigation at sentencing or discretionary exclusion of evidence. While countries have been hesitant to explicitly codify entrapment in legislation, there has been an observed acceptance of entrapment-based rights in practice.

* B.A. 2020, Cornell University, College of Arts and Sciences; J.D. Candidate 2024, The University of Chicago Law School. I would like to thank Professor Curtis Bradley, Katherine Koza, and Marin Murdock for their thoughtful guidance and encouragement. Thank you to the editorial board and staff of the *Chicago Journal of International Law* for their assistance and support throughout the publication process.

Table of Contents

I. INTRODUCTION

Cybercrime is a dynamic threat with a global dimension.[1] The number of cyberattacks is growing each year, and by 2025, it is predicted that the global cost of cybercrime will total $10.5 trillion annually.[2] For the purposes of this Comment, cybercrime is defined as "activities in which computers, telephones, cellular equipment, and other technological devices are used for illicit purposes such as fraud, theft, electronic vandalism, violating intellectual properties rights, and breaking and entering into computer systems and networks."[3]

Cybercrime is an extraordinarily transnational crime;[4] members of cybercriminal "gangs" can span across a series of international borders.[5] Even when a cybercriminal is working alone, they can operate via a "proxy" IP address, which makes it time-consuming and difficult for law enforcement to trace cybercrime to an individual.[6] Intelligence agencies can recognize when a cybercriminal uses a similar IP address or software to carry out several crimes, but the cybercriminal's true identity and location are much more difficult to ascertain.[7] Due to the frequent uncertainty about a cybercriminal's whereabouts, law enforcement may be tracking and executing investigations on individuals beyond their jurisdiction, even across the world. The "cross-national nature" of cybercrime has rendered traditional methods of policing ineffective, even in advanced countries.[8] In order to effectively investigate, combat, and prosecute

---

1 PEDRO VERDELHO, THE EFFECTIVENESS OF INTERNATIONAL CO-OPERATION AGAINST CYBERCRIME: EXAMPLES OF GOOD PRACTICE 4 (Council of Eur. Project on Cybercrime, 2008).

2 Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://perma.cc/SN5A-G2WC; *see* Olena Sviatun et al., *Combating Cybercrime: Economic and Legal Aspects*, 18 WSEAS TRANSACTIONS ON BUS. & ECON. 751, 756–59 (2021); *see also* Steve Morgan, *IBM's CEO on Hackers: 'Cyber Crime is the Greatest Threat to Every Company in the World'*, FORBES (Nov. 24, 2015), https://perma.cc/F7LB-J48V (explaining that cybercrime poses a grave threat to companies around the world and can have a "negative impact on revenues, company valuation when raising capital, customer acquisition and retention, and their ability to recruit top talent").

3 David L. Speer, *Redefining Borders: The Challenges of Cybercrime*, 34 CRIME L. & SOC. CHANGE 259, 260 (2000).

4 *See* VERDELHO, *supra* note 1. *See generally* Marina Caparini, *Transnational Organized Crime: A Threat to Global Public Goods*, STOCKHOLM INT'L PEACE RSCH. INST. (Sept. 1, 2022), https://perma.cc/AGN9-YY7W (identifying that transnational crimes include "trafficking in humans, arms, drugs, minerals and wildlife; production and trade of counterfeit goods; fraud and extortion; money laundering and cybercrime").

5 *Id.*

6 *See* Alan Woodward, *Viewpoint: How Hackers Are Caught Out by Law Enforcers*, BBC NEWS (Mar. 12, 2012), https://perma.cc/6KSU-UTDG; *see also* Alexander Fox, *How Are Hackers Identified and Brought to Justice*, MAKE TECH EASIER (May 24, 2017), https://perma.cc/SWQ9-KQR5.

7 *See* Fox, *supra* note 6.

8 *See* Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-Crime*, 29 POLICING 408, 408 (2006).

cybercrime, international cooperation is required.[9] There are thus several "challenges to international cooperation and establishing international guidelines to fight global cybercrime across borders."[10]

Given the elusive nature of cybercrime, sting operations play a crucial role in combatting cybercriminals.[11] Police create a deceptive opportunity to commit crime in order to identify and catch criminals. Stings tend to have

> four basic elements: (1) an opportunity or enticement to commit a crime, either created or exploited by police; (2) a targeted likely offender or group of offenders for a particular crime type; (3) an undercover or hidden police officer or surrogate, or some form of deception; and (4) a "gotcha" climax when the operation ends with arrests.[12]

These operations often implicate cybergangs with members based in several countries. For instance, in 2012, the Federal Bureau of Investigation arrested twenty-four hackers in a sting spanning thirteen countries in North America, Asia, and Europe.[13]

Cyber stings, while imperative in the response to cybercrime, call into question the degree to which individuals are protected by the entrapment defense. Entrapment occurs when "a government agent induc[es] a person to commit an offense that the person would otherwise have been unlikely to commit."[14] There are several methods that law enforcement agencies can use to catch cybercriminals. Law enforcement often implements "honeypots," which are security mechanisms created by police to lure cybercriminals to attack what appears to be a legitimate digital target.[15] For example, a honeypot might mimic a company's online storage system with sensitive financial information. The honeypot then earns its name by being an attractive target for criminals, who then attack the system via its security vulnerabilities. Once the criminals attack the illegitimate system, honeypots can enable law enforcement to collect information about the identities, methods, and motivations of adversaries.[16] Honeypots are generally not a form of problematic entrapment, as they do not

---

9 ANA I. CEREZO ET AL., INTERNATIONAL COOPERATION TO FIGHT TRANSNATIONAL CYBERCRIME 1 (Second Int'l Workshop on Digit. Forensics & Incident Analysis, 2007).

10 *Id.*

11 *See* Thomas T. Kubic, *Deputy Assistant Director, FBI, Before the House Committee on the Judiciary, Subcommittee on Crime*, FBI (June 12, 2001), https://perma.cc/ARK6-FE9D.

12 GRAEME R. NEWMAN, PROBLEM-ORIENTED GUIDE FOR POLICE RESPONSE GUIDES SERIES: STING OPERATIONS 3 (U.S. Dep't of Just. Cmty. Oriented Policing Servs., No. 6, 2007).

13 Robert N. Charette, *This Week in Cybercrime: FBI Sting, RBS Phish*, IEEE SPECTRUM (June 27, 2012), https://perma.cc/7DH4-E766.

14 *Entrapment*, IBJ CRIM. DEFENSE WIKI (Nov. 12, 2010), https://perma.cc/EX8Z-UF33.

15 *See Honeypots in Cybersecurity Explained*, CROWDSTRIKE (Mar. 9, 2022), https://perma.cc/H4HR-SKKU.

16 *See id.*

persuade individuals to commit the crime.[17] Other forms of cyber stings, however, can cause entrapment concerns. For example, the risk of police entrapping individuals arises in cyberspace when users are on dark web marketplaces controlled by law enforcement who work to establish trust with criminals using these spaces.[18] Entrapment is a complete defense to criminal charges on the theory that law enforcement should not be manufacturing crime.[19] A defendant must show that a government agent induced the crime and that the defendant was not predisposed to commit the crime.

There is no global consensus about the extent to which defendants can claim the entrapment defense. In some countries, like South Africa, the concept of entrapment is codified in legislation.[20] More typically, entrapment rights are embodied in case law. [21] Criminal courts around the globe recognize varied models of the entrapment defense.[22] For example, in the U.S., entrapment is a substantive defense.[23] In Singapore, entrapment is a mitigating circumstance in sentencing.[24] In Australia, New Zealand, South Africa, England, Wales, and Scotland, entrapment is grounds for the discretionary exclusion of evidence.[25] In Canada, entrapment can cause the court to impose a permanent stay in proceedings.[26]

The lack of consensus regarding a defendant's right to the entrapment defense is an impediment to international collaboration among law enforcement. To promote international security and ease cooperation, a common agreement acknowledging the rights associated with the entrapment defense should be reached. According to Paul Valentine, "[g]iven the emergence of internet sting operations and covert government investigations, it is now more important than

---

17 *See Are Honeypots Illegal?*, NETSURION (2023), https://perma.cc/HL85-59BT.

18 *Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs*, NAT'L INST. OF JUST. (June 15, 2020), https://perma.cc/A3EL-ESPY. Child pornography presents another area in which entrapment presents a concern for law enforcement stings. In *Jacobson v. United States*, "[u]ndercover agents spent two years corresponding with Jacobson about sex, sending him many letters advocating sexual liberty with minors and the right to child pornography. When solicited, Jacobson promptly ordered such pornography, but when police searched his home, they found only the material they had sent him . . . the Court found insufficient evidence of predisposition (prior to the government's communications)." Richard H. McAdams, *The Political Economy of Entrapment*, 96 J. CRIM. L. & CRIMINOLOGY 107, 117–18 (2005).

19 U.S. Dep't of Just., Criminal Resource Manual § 645 (2020).

20 Daniel Hill et al., *Entrapment*, ELGAR ENCYC. CRIME & CRIM. JUST. (forthcoming Feb. 2024) (manuscript at 1, 3), https://perma.cc/QXT9-L3GA.

21 *Id.* This is the case in the U.S., Canada, England, Wales, Germany, Scotland, and Singapore. *Id.*

22 *See id.*

23 *Id.*

24 *Id.*

25 Hill et al., *supra* note 20.

26 *Id.*

ever that the [entrapment] defense be given some credence by courts throughout the world."[27] The transnational nature of cybercrime has rendered traditional domestic policing methods obsolete.[28]

To adequately respond to the threat of cybercrime, it is crucial that countries have the means to coordinate their responses through international cooperation.[29] Giulio Calcara, a transnational criminal law scholar, argues that "[p]olice services might decide to desist on activating cooperation processes if differences in substantive criminal law are significant. In general, police cooperation is firmly grounded on the premise of an equivalent criminalization of specific acts or omissions."[30] It is rare for law enforcement to catch cybercriminals, since "[c]atching cyber criminals often requires cooperation between several law enforcement agencies, but so far a limited international legal framework has hampered their efforts."[31] A lack of a common framework on entrapment poses a problem because countries that are beholden to entrapment protections will not want to collaborate in investigations with countries that do not have similar protections.

In 2014, the Council of Europe assessed why requests for cooperation and mutual legal assistance between countries were failing in the context of cybercrime.[32] Specifically, it asked States Parties and observer states to the Budapest Convention why their requests to cooperate with other countries to combat cybercrime had been unsuccessful.[33] Albania, Moldova, Norway, Romania, Serbia, and Ukraine each reported that they had experienced failed attempts of mutual legal assistance due to "[d]iscrepencies between legal systems, such as regarding investigative powers."[34] The lack of consensus regarding international cooperation, specifically in the investigatory phase, poses a significant threat to global security if the international community cannot effectively collaborate and respond to cybercrime threats. Such need for cooperation has prompted the creation of international instruments to "offer

---

27 Paul W. Valentine, *To Catch an Entrapper: The Inadequacy of the Entrapment Defense Globally and the Need to Reevaluate Our Current Legal Rubric*, 1 PACE INT'L L. REV. 22, 22 (2009).

28 *See* Giulio Calcara, *Rethinking Legal Research on Matters of International Police Cooperation: Issues, Methods and Raison d'Être*, 40 LIVERPOOL L. REV. 95, 96 (2019).

29 *Id.*

30 *Id.* at 98.

31 Joao Paulo de Mello Barreto, *Global Cyber Crime: Catching Overseas Hackers*, COLUM. UNDERGRADUATE L. REV. (Apr. 28, 2015), https://perma.cc/7HVE-6KCJ.

32 *See* COUNCIL OF EUR., CYBERCRIME CONVENTION COMM., T-CY ASSESSMENT REPORT: THE MUTUAL LEGAL ASSISTANCE PROVISIONS OF THE BUDAPEST CONVENTION ON CYBERCRIME (2014).

33 *Id.* at 3–4.

34 *Id.* at 38.

parties a legal basis for judicial and law enforcement cooperation on extradition, mutual legal assistance, asset recovery and joint investigations."[35]

International agreements have yet to establish a common entrapment defense. The Budapest Convention, signed in 2001, was the first international agreement to combat cybercrime.[36] While the agreement sought to standardize national laws and improve international cooperation, it did not mention entrapment. Current scholarship has explored the disparities between the various models of cybercrime internationally, but it has not addressed how a lack of consensus regarding entrapment impacts international cooperation, particularly in the context of cybercrime.[37]

The interest of international security is undeniably important in addressing cybercrime. Negative ramifications of cybercrime include economic instability, political unrest, and social vulnerability from data exposure and loss of intellectual property. This Comment makes two arguments. First, the lack of agreement about entrapment is undermining international cooperation in combating cybercrime and is impeding efficient partnerships between countries. A mutual agreement would ease cooperation between international law enforcement groups by defining the parameters of their operations. Second, the lack of agreement about entrapment is resulting in law enforcement abuse in the cybersphere. This Comment argues that establishing a common framework of entrapment rights will safeguard the legitimacy of government institutions and protect individuals from targeted incrimination. Individuals should, as a normative matter, have entrapment rights because police should not intrude on the lives of innocent individuals or entice them to commit crimes. When countries with dissimilar entrapment rights cooperate to share data and carry out cyber stings, there is a heightened risk of diluting the rights of private citizens.[38] As responses to cybercrime grow and adapt, government operations have begun to seep into the lives of everyday citizens without sufficient restraints. This Comment will consider the risk of governments continuing to expand the definition of cybercrime in order to justify government intervention, injuring the legitimacy of government institutions and threatening freedom of expression. The increasingly intrusive nature of government operations in response to

---

35 *International Cooperation Vital to Address All Forms of Crime, Terrorism & New & Emerging Forms of Crime*, U.N. OFF. ON DRUGS & CRIME (2022), https://perma.cc/UXK7-CXE8.

36 *Treaties & International Agreements on Cyber Crime*, GEORGETOWN L. LIBR. (Sept. 6, 2022), https://perma.cc/A8X6-D9FN.

37 *See* Calcara, *supra* note 28, at 99 (arguing that "international police cooperation is a topic of legal research that has been largely neglected").

38 *See Cybercrime Treaty Negotiations at the United Nations*, U.S. DEP'T OF STATE (Aug. 30, 2022), https://perma.cc/K3QK-PLWC; *see also* U.N. SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE, THE STATE OF INTERNATIONAL COOPERATION FOR LAWFUL ACCESS TO DIGITAL EVIDENCE: RESEARCH PERSPECTIVES 26 (2022).

cybercrime calls for a system of restraint—one that involves a consensus in favor of the entrapment defense—to protect fundamental human rights.

This Comment's scope is limited to cybercrime entrapment. Cybercrime presents a worthwhile opportunity to pursue an agreement about entrapment due to its transnational nature, requiring a coordinated international response to share information and resources. In struggling to apply our existing legal framework to cyberspace, cybercrime reveals specific outdated legal mechanisms that demand attention. There is a greater likelihood of success in proposing common entrapment rights within the sphere of cybercrime, rather than in general criminal procedure, given the disparity in judicial structures around the globe. For example, many countries follow the common law tradition that considers the way evidence was obtained to be irrelevant.[39] These countries would be hesitant to sign an agreement requiring a complete overhaul of their criminal justice system. By limiting the scope of an agreement to the pressing concern of cybercrime, the proposal would likely generate support from more countries.

This Comment reviews existing international agreements before proposing to establish a common degree of protection afforded by the entrapment defense. Three models of entrapment are considered as possible pathways forward: (1) subjective, (2) objective, or (3) a "minimum floor." The minimum floor approach is ultimately chosen as the most favorable model. The floor would require countries, at a minimum, to consider entrapment as grounds for mitigation at sentencing or discretionary exclusion of evidence. This Comment argues that the best means to integrate the minimum floor requirement into the international community is to modify Article 15 of the Budapest Convention. Given that the Convention has been supplemented before, it is plausible that the international community would be willing to adopt another change. Supplementing the Budapest Convention with the minimum floor model would codify what Part II identifies as a gradual global shift toward entrapment-based rights. States parties to the Convention have begun to accept entrapment rights in practice, even if they have not been officially codified in legislation. The minimum floor approach also represents a realistic step forward as a remedy that respects the ideals of entrapment. Part II's analysis suggests that any attempts to explicitly codify "entrapment" would prevent ratification of the amendment or would otherwise risk losing current signatories to the Budapest Convention itself. While the minimums are imperfect, constraining law enforcement would hopefully spur further regulation of undercover operations and nudge the prosecution of cybercriminals toward a greater standard of due process.

---

[39] *See* Tom Obokata, *The Value of International law in Combating Transnational Organized Crime in the Asia-Pacific*, 7 ASIAN J. INT'L L. 39, 55 (2015).

Part II explores the varied approaches to the entrapment defense on a global scale, discussing countries that have begun to adopt entrapment-based ideals in practice as well as weak models of the defense. In Part III, this Comment discusses how the lack of international consensus about the entrapment defense impacts international cooperation and has global security ramifications. Part III also reviews existing international agreements concerning international cooperation related to organized crime and cybercrime. It then describes recent negotiations by the United Nations (U.N.) about the evolving threat of cybercrime and considers widespread critiques of the proposed treaty. In Part IV, this Comment proposes a new pathway forward and recommends modifying an existing international agreement. The Budapest Convention should be amended to adopt a minimum floor model that respects entrapment rights and ultimately improves the ability for countries to cooperate. The likelihood of such an agreement being adopted is then assessed. Part V concludes and reviews unanswered questions, recommendations, and predictions.

II. ENTRAPMENT MODELS BY COUNTRY

A. Methodology

This section evaluates diverging models of entrapment internationally. First, it considers countries that explicitly recognize entrapment or offer remedies to individuals who have been entrapped. Then, countries that do not recognize entrapment or have weak models of the defense are discussed. The countries in this analysis were selected based on geographical diversity, diverging structures of government, and varied legal systems. The discussion is comprised of countries that had entrapment information available, following a comprehensive search of the most promising case studies of the defense internationally.

B. Countries with the Entrapment Defense or Related Remedies

The following discussion reviews the countries that acknowledge some degree of protection from entrapment. Many of the countries below have not codified the defense, but courts have evolved to recognize it in practice. Law enforcement tactics have adapted to modern threats like cybercrime, and have become more intrusive. While the concept of entrapment is American-born, the concern about protecting the accused from a crime manufactured by the police has permeated the international community.[40]

---

40 *See* McAdams, *supra* note 18, at 110.

1. United States

While American law is derived from English law, the entrapment defense does not have roots in the English common law system. The entrapment defense gained acceptance in the U.S. in the early 20th century.[41] There were two shifts in the American landscape that contributed to the development of the defense.[42] First, following the Civil War, the federal government began to grow its law enforcement systems.[43] The people sought protection from the courts in response to this "law enforcement leviathan."[44] Second, courts began to respond to the rising concern that government agents were creating crime, particularly during Prohibition in the 1920s.[45] Law enforcement became "heavily involved in setting up alcohol operations essentially so that they could then bust those same alcohol operations."[46] In 1928, Justice Brandeis wrote that government agents

> may set decoys to entrap criminals. But [they] may not provoke or create a crime and then punish the criminal . . . not because some right of [the defendant's] has been denied, but in order to protect the Government. To protect it from illegal conduct of its officers. To preserve the purity of its courts.[47]

In *Sherman v. United States*, the Supreme Court recognized that American entrapment is based on the presumption that Congress did not want its statutes to be enforced by the government tempting innocent citizens to commit violations.[48]

In the U.S., three actions must generally occur for the defendant to successfully claim entrapment:

> (1) the idea for committing the crime came from the government agent and not the accused, (2) the government agent persuaded the accused into committing the crime and did not provide a mere opportunity to act, and (3) the accused was not predisposed to committing the crime before interacting with the government agents.[49]

---

41 Paul Marcus, *The Development of Entrapment Law*, 33 WAYNE L. REV. 5, 9 (1986).

42 *See* Rebecca Roiphe, *The Serpent Beguiled Me: A History of the Entrapment Defense*, 33 SETON HALL L. REV. 257, 258 (2003); *see also* Paul Marcus, *The Entrapment Defense: An Interview*, 30 OHIO N.U. L. REV. 211, 216 (2004).

43 Roiphe, *supra* note 42, at 258.

44 *Id.*

45 *See* Marcus, *supra* note 42, at 216.

46 *Id.*

47 Casey v. United States, 276 U.S. 413, 425 (1928); *see also* Marcus, *supra* note 41, at 15.

48 356 U.S. 369 (1958); *see also* Carissa Prevratil, *Creating Terrorists: Issues with Counterterrorism Tactics and the Entrapment Defense*, RAMAPO COLL. OF N.J. (Sept. 17, 2020), https://perma.cc/X4ZT-7RKY.

49 *Entrapment*, IBJ CRIM. DEFENSE WIKI, *supra* note 14.

Federal courts in the U.S. have evolved the entrapment defense into two forms: subjective and objective.[50] The subjective model "focuses on the defendant's individual characteristics more than on law enforcement's behavior."[51] The defendant will not prevail on the defense if the facts indicate that they were predisposed to commit the crime.[52] Federal courts and two-thirds of U.S. state courts have adopted this subjective model.[53]

The objective model focuses on law enforcement behavior, rather than on the defendant's characteristics.[54] "If law enforcement uses tactics that would induce a reasonable, law-abiding person to commit the crime, the defendant can successfully assert the entrapment defense in an objective entrapment jurisdiction."[55] The objective model focuses on the actions of a reasonable person, not the particular defendant.[56] The defendant's predisposition to commit the crime is not considered.[57]

While entrapment originated in the U.S., the theory that courts should regulate undercover government operations has been "exported" to the rest of the international community.[58] In response to international drug enforcement challenges, the U.S. has successfully persuaded other countries to use undercover operations more aggressively.[59] According to Richard McAdams, a criminal law scholar, the rise in undercover operations has prompted several nations to embrace the regulation of these activities.[60] "These nations recognize not a criminal 'defense' but the judicial power to stay prosecutions or exclude evidence as a remedy to unlawful operations."[61] While such nations have not explicitly recognized entrapment rights in legislation, courts have recognized the shift in police responses to crime and modified their procedures.

Research on international judicial systems supports McAdams's theory that courts have gradually adapted the remedies available to defendants in response to the rising use of entrapment. Some scholars note that many courts avoid the

---

50 Chandrika Bothra, *Rethinking the Traditional Approaches to the Defence of Entrapment in Indian Law and Society: Lessons from America (Part II)*, J. INDIAN L. & SOC'Y BLOG (Oct. 23, 2019), https://perma.cc/J2TU-YXFN.

51 *Entrapment*, UNIV. OF MINN. (2010), https://perma.cc/E3VJ-GA85.

52 *Id.*

53 *Entrapment*, IBJ CRIM. DEFENSE WIKI, *supra* note 14.

54 *Entrapment*, UNIV. OF MINN., *supra* note 51.

55 *Id.*

56 *Id.*

57 *Id.*

58 *See* McAdams, *supra* note 18, at 110.

59 *Id.*

60 *Id.*

61 *Id.*

issue of explicitly recognizing entrapment.[62] Nevertheless, "if a person is accused of a crime obviously manufactured by the police with only the prosecution motive in mind, that person will probably be acquitted in the U.S., England, and Canada."[63] The defense of entrapment is "no longer peculiarly American."[64] England, Wales, Canada, and the European Court of Human Rights have recognized the defense.[65]

2. England

In England, there is no explicit entrapment defense, but remedies have gradually become available to defendants who have been entrapped. In the 2001 case of *Regina v. Looseley*, Lord Nicholls of Birkenhead wrote that "although entrapment is not a substantive defence, English law has now developed remedies in respect of entrapment: the court may stay the relevant criminal proceedings, and the court may exclude evidence pursuant to section 78."[66] Section 78, governing the "Exclusion of Unfair Evidence," reads that

> the court may refuse to allow evidence on which the prosecution proposes to rely . . . if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.[67]

Additionally, if the defendant was deceived into committing an offense, this fact may be considered in sentencing.[68] Incitement also permits the court to exercise discretion to "suppress the prosecution as an abuse of process."[69] While English courts consider entrapment to be a trigger for certain remedies, the judiciary has proven hesitant to exercise this discretion.[70]

English courts have demonstrated great reluctance in becoming involved with police detection methods.[71] Although English judges may exercise discretion in sentencing, it is extremely rare that this discretion is applied.[72]

---

62 *See* Joel Shafer & William J. Sheridan, *The Defence of Entrapment*, 8 OSGOODE HALL L.J. 277, 277 (1970).

63 *Id.*

64 Kent Roach, *Entrapment and Equality in Terrorism Prosecutions: A Comparative Examination of North American and European Approaches*, 80 MISS. L.J. 1455, 1455 (2010).

65 *Id.*

66 [2001] UKHL 53, [3] (appeal taken from Eng.).

67 Police and Criminal Evidence Act 1984, c. 60 (UK), https://perma.cc/LN85-EFDU.

68 *See* J.R. Spencer, *Entrapment and the European Convention on Human Rights*, 60 CAMBRIDGE L.J. 30, 31 (2001).

69 *See id.*

70 *See* Andrew Choo, *A Defence of Entrapment*, 53 MOD. L. REV. 453, 471 (1990).

71 *See id.*

72 *See id.*

Given that there have been so few instances where the judiciary has exercised such discretion, there are no clear principles about when discretion should be exercised.[73] Defendants would benefit from a more consistent application of judicial discretion or defined principles about when remedies would apply.

3. Canada

Canada has adopted the objective approach to entrapment, focusing on an abuse of process by the police. This understanding of entrapment stands in contrast to the subjective model widely used in the U.S. that considers the accused's predisposition to commit the crime.[74] In the 1988 case of *R v. Mack*, the Supreme Court of Canada found that objective entrapment "is a question to be decided by the trial judge, and the proper remedy is a stay of proceedings."[75] The Canadian legal system views a finding of entrapment as a judicial disapproval of law enforcement investigatory tactics.[76] Courts should "direct their attention away from the offender and remember that the 'exclusive rationale [of the doctrine] is seen to lie in the need to control police conduct.'"[77] The Canadian model focuses on reducing the potential for a law enforcement leviathan that induces crime by innocent citizens.

4. European Court of Human Rights

The European Court of Human Rights (ECtHR), established in 1953 by the European Convention on Human Rights (ECHR), has had considerable influence on the entrapment positions of European countries. Article 6, Section 1 of the ECHR entitles each person to a fair and public hearing by an impartial tribunal. Section 1 suggests that unlawful police incitement could be an infringement of this right.[78] Article 8, Section 1 refers to the guarantees that citizens have regarding privacy and family life. Article 8 has been understood as particularly relevant to police investigation tactics such as entrapment and surveillance. However, "interference with exercise of the right is permitted, provided that it is in accordance with the law and is necessary in a democratic society, *inter alia*, in the interests of national security, public safety or the

---

73 *See id.* at 456.

74 *See* R v. Mack, [1988] 2 S.C.R. 903 (Can.).

75 *Id.*

76 Matthew Zaia, *Scraping in Cyberspace: Police Entrapment in the Virtual World*, 26 CAN. CRIM. L. REV. 203, 206 (2022) (citing E.G. EWASCHUK, CRIMINAL PLEADINGS & PRACTICE IN CANADA (2d ed. 2021)).

77 *Id.* (citing DON STUART, AMATO: WATERSHEDS IN ENTRAPMENT AND ABUSE OF PROCESS (1982)).

78 *See* Franziska Görlitz et al., *"Tatprovokation": The Legal Issue of Entrapment in Germany and Possible Solutions*, 20 GER. L.J. 496, 498 (2019).

prevention of disorder or crime."[79] In the context of cyberspace, law enforcement could readily justify intrusive cyber stings by relying upon this national security and public safety exception. Particularly regarding cybercrime, a more consistent and agreed upon minimum floor would benefit defendants.

5. Germany

The ECtHR has influenced how German courts review incidents of entrapment. German jurisprudence insists on the legitimacy of entrapment, but the law does not delineate what constitutes the defense. The decisions of the ECtHR have shifted German case law, and the country "now distinguishes between admissible and inadmissible entrapment, linking different consequences to each."[80] In deciding whether the entrapment is admissible, the German Federal Constitutional Court (*Bundesverfassungsgericht*) considers the fair trial principles laid out in Article 6 of the ECHR, as well as the public interest in the criminal prosecution.[81] Entrapment is considered admissible when the defendant has previously been suspected of committing similar, serious offenses to those involved in the entrapment operation.[82] A 2015 commission of German criminal law experts recommended that unlawful police incitement and legal consequences should be codified. These German law scholars have argued that a "legislative intervention is indeed long overdue."[83]

6. Brazil

In Brazil, there are statutory limits on deception. The use of undercover agents by law enforcement "requires a judicial warrant authorizing the infiltration of a criminal organization."[84] There is also a general protection against entrapment—with a caveat.[85] Article 17 of the Brazilian Criminal Code provides a defense against entrapment.[86] A defendant will not be held liable for possession of child pornography sent by law enforcement if the court

---

79 ED CAPE & ZAZA NAMORADZE, EFFECTIVE CRIMINAL DEFENCE IN EASTERN EUROPE 16 (U.N. Off. on Drugs & Crime, 2012).

80 Görlitz et al., *supra* note 78.

81 *See id.*

82 *See id.*

83 *Id.*

84 Lissa Griffin & Rafael Wolff, *Undercover Practices: A Comparison*, PACE CRIM. JUST. BLOG (Dec. 18, 2014), https://perma.cc/T39J-5QCN.

85 *See id.*

86 *See id.*

determines the defendant was entrapped.[87] If the defendant possesses other similarly illicit photos, they are not eligible to claim the defense.[88]

7. South Africa

In South Africa, entrapment has emerged in response to the constitutional movement that produced a Bill of Rights and the Criminal Procedure Second Amendment of 1996. Section 252A of the Criminal Procedure Second Amendment details the unfairness of government traps and the admissibility of evidence obtained using this method: The court should contemplate, "in considering the question whether the conduct goes beyond providing an opportunity to commit an offence . . . the type of inducement used, including the degree of deceit, trickery, misrepresentation or reward."[89] If the court finds that "in the setting of a trap or [by] engaging in an undercover operation the conduct goes beyond providing an opportunity to commit an offence, the court may refuse to allow such evidence to be tendered . . . if the evidence was obtained in an improper or unfair manner."[90] Rowland Cole, a South African legal scholar, suggests recent "constitutional dispensations" are a reflection of a national and global focus on human rights.[91] These shifts in South Africa have had a strong doctrinal influence on the country's criminal justice system.[92]

8. Synthesis

While the entrapment defense arose in the U.S., a general recognition that law enforcement should not be enticing innocent individuals to commit crime has spread around the globe. Establishing entrapment-based rights requires police to focus their operations on individuals who have displayed behavior that signals they are predisposed to committing the crime. While several nations have recognized the values of fairness and personal liberty associated with entrapment, many countries have rejected the defense.

C. Weak Models of the Entrapment Defense

This section reviews the countries where defendants have notably weak entrapment rights: Singapore, Australia, India, China, and Botswana.

---

87 *Id.*

88 *Id.*

89 Criminal Procedure Second Amendment Act of 1996 § 252A(3)(a).

90 *Id.*

91 *See* Roland James Victor Cole, Equality of Arms and Aspects of the Right to a Fair Criminal Trial in Botswana 173–76 (Mar. 2010) (Doctor of Law thesis, Stellenbosch University) (on file with author).

92 *See id.*

1. Singapore

In Singapore entrapment is legal. Evidence obtained through entrapment is admissible and accepted by courts if it is relevant to the case at hand.[93] The Court of Appeal has continually rejected the entrapment defense on the basis that courts should not be concerned with how evidence was gathered, but only how the evidence was presented.[94] The Singaporean legal system is based on the English common law due to its history as a former British colony. Nevertheless, the Court of Appeal has said that the previously discussed English case, *Regina v. Looseley*, has no authority in Singapore.[95] The court does not view entrapment to be an abuse of process.[96] In *PP v. Rozman bin Jusoh*, it stated that "[i]f entrapment can be considered at all, it is relevant only insofar as mitigation of the sentence is concerned."[97] The court is permitted to deny evidence obtained through entrapment if it determines that the harm it causes to the parties of the case is greater than its usefulness.[98]

2. Australia

There is currently no legal defense for entrapment in Australia.[99] A foundational tenet of the Australian criminal justice system is that individuals who voluntarily commit a crime should be held liable.[100] In *Ridgeway v. The Queen*, the High Court of Australia rejected the notion that entrapment should be grounds for a permanent stay of proceedings.[101] The court said that Australian courts already held the power to exclude evidence obtained in an improper manner.[102] "In some very limited cases, being induced to commit an offence can amount to a defence. However, entrapment does not provide a full substantive defence in Australia."[103] Legislatures in New South Wales, Queensland, and South Australia subsequently passed legislation making it permissible for law enforcement to carry out operations and collect evidence through illegal

---

93 *What is Entrapment and Is It Legal in Singapore?*, SING. LEGAL ADVICE (Feb. 17, 2021), https://perma.cc/X9FX-ZYNF.

94 *See* HILL ET AL., *supra* note 20, at 20.

95 *See id.*

96 *Id.*

97 *Id.*

98 *What is Entrapment and Is It Legal in Singapore?*, *supra* note 93.

99 Ugur Nedim, *Should Entrapment Be a Defence in Australia?* SYDNEY CRIM. LAW. (Apr. 6, 2014), https://perma.cc/8GXP-9FVN.

100 *See* HILL ET AL., *supra* note 20, at 10–11.

101 *See id.*

102 *See id.*

103 Michelle Makela, *Entrapment in Australia*, GO TO COURT (Sept. 22, 2016), https://perma.cc/535S-KRVS.

activity.[104] The court is only to exclude evidence when law enforcement actions are so severe that protecting the public interest outweighs securing a conviction.[105] Australia's reluctance to interfere with police detection methods is comparable to England's approach, although England has developed entrapment-based remedies. Paul Marcus, a criminal law scholar, considers Australia's understanding of entrapment to be a "mini-exclusionary rule."[106] Although the judge theoretically has discretion to exclude entrapment evidence, this "is not a very real possibility or, at least, not a possibility seen often."[107]

3. India

India's jurisprudence does not reveal an explicit stance on the state entrapment defense.[108] It is generally understood that if evidence is relevant and genuine, it is admissible regardless of how it was obtained.[109] The court may exercise some discretion in excluding evidence in cases where the accused person was treated tremendously unfairly.[110] In both India and Australia, the discretion afforded to judges relates to the exclusion of evidence. These approaches contrast sharply with Brazil, where there are statutory limits on deception and a defense against entrapment in the criminal code.

4. China

In China, there are "no laws or regulations on the evidentiary effect of entrapment."[111] Neither the law nor law enforcement agencies consider entrapment to be a violation of conduct.[112] Rather than excluding evidence, the court can reduce the sentence of the convicted when they were entrapped.[113] The Chinese government gives the police wide discretion to carry out operations and considers their sting operations to be a form of virtue testing.[114] The

---

104 *See* HILL ET AL., *supra* note 20, at 11.

105 *See id.*

106 Marcus, *supra* note 42, at 226.

107 *Id.*

108 Chandrika Bothra, *Rethinking the Traditional Approaches to the Defence of Entrapment in Indian Law and Society: Lessons from America (Part I)*, J. INDIAN L. & SOC'Y BLOG (Oct. 23, 2019), https://perma.cc/26B9-2J2H.

109 *See* HILL ET AL., *supra* note 20, at 16–17.

110 *See id.*

111 Dun Mingyue, *Entrapment Evidence for IP Protection: Admissible or Not?*, CHINA INTELL. PROP. (June 1, 2007), https://perma.cc/926J-2QSL.

112 *See* Daniel J. Hill et al., *What is the Incoherence Objection to Legal Entrapment?*, 21 J. ETHICS & SOC. PHIL. 47, 61(2022).

113 *See* Obokata, *supra* note 39.

114 *See* Sijia Zhou, Research on Entrapment in China with Reference to the Experience in Canada 37 (2013) (L.L.M thesis, McGill University) (on file with author).

excessive scope of power that Chinese police possess is reflective of the country's reputation as a surveillance state that analyzes and tracks human behavior.

> [China] uses vast quantities of data and cutting-edge artificial intelligence to build a nimbler form of authoritarianism that's capable of exercising unprecedented social control . . . The ultimate goal is a perfectly engineered society that automatically neutralizes dissidents while rewarding those who comply with lives of convenience, safety, and predictability.[115]

The ability for police to entrap dissidents into crime is critical to the health of the Chinese authoritarian state.

5. Botswana

Entrapment is not a defense in Botswana, but courts have expressed their displeasure with this practice.[116] Entrapment is used as a mitigating factor in sentencing[117] but has not been codified.[118] This may be because the defense has not been a frequent issue before the courts and has not undergone comprehensive review or been challenged constitutionally.[119] Rowland Cole, a South African legal scholar, points to the influence of the common law tradition on Botswana's legal structure.[120] The common law tradition considers the way evidence was obtained to be irrelevant.[121] Botswana has not undergone the doctrinal shift that South Africa experienced with the bolstering of constitutional rights.[122]

6. Synthesis

As Part II has identified, there is a lack of consensus in the international community about the extent to which defendants can claim the entrapment defense.[123] The countries with weak entrapment defenses consider the manner in which evidence was collected to be irrelevant; entrapment is only significant in a sentencing context.[124] These courts reject the notion that the state's capacity to

---

115 Mercy A. Kuo, *Surveillance State: Social Control in China*, DIPLOMAT (Oct. 3, 2022), https://perma.cc/J4HB-YBDD.

116 *See* Cole, *supra* note 91, at 174 ("The courts in Botswana have maintained that entrapment is not a defence even though they have expressed their displeasure with the practice.").

117 *Id.*

118 *See id* at 175.

119 *Id.*

120 *See id.*

121 Obokata, *supra* note 39, at 55.

122 *See id.*

123 *See supra* Part II.C.

124 *Id.*

incite crime is procedurally unfair to the defendant.[125] Reserving considerations of entrapment for sentencing leaves defendants in these countries vulnerable to unrestrained police operations. Differences in the entrapment defense internationally may be attributable to variances in how countries evaluate the risk of supporting an unrestrained, powerful government.[126] The U.S., for example, is much more fearful of arbitrary and discriminatory law enforcement investigations than Australia.[127] The French judiciary has also acknowledged that agents sometimes go beyond their prescribed duties in investigations, but there exists no affirmative entrapment defense, exclusion of evidence, or fines against police.[128] Countries like the U.S. that protect entrapment rights tend to be much more distrustful and cynical about large public institutions.[129]

III. LACK OF GLOBAL CONSENSUS & CURRENT INTERNATIONAL AGREEMENTS

Given the extent to which law enforcement relies on undercover operations to combat cybercrime, the importance of addressing the controversy regarding entrapment is salient.[130] Giulio Calcara, a scholar of transnational criminal law, argues that law enforcement cooperation is dependent upon equivalent criminalization of specific acts.[131] Cybercrime is considered the most transnational crime.[132] Due to the cross-border nature of cybercriminal networks, it is likely that multiple countries will have jurisdiction over any particular cybercrime.[133] Disagreement about standards of law enforcement conduct is a serious impediment to efficient and effective international cooperation. The following section reviews various international treaties that have addressed transnational crime and cybercrime, including the International Covenant on Civil and Political Rights, the U.N. Convention on the Rights of the Child, the U.N. Convention Against Transnational Organized Crime, and the Convention on Cybercrime (Budapest Convention). The potential of recent 2022 Cybercrime Treaty negotiations will also be discussed. No international treaties have codified entrapment.

---

125 *Id.*

126 *See* Marcus, *supra* note 42, at 226–28.

127 *See id.* at 227.

128 *See id.* at 226–27.

129 *Id.*

130 *See* McAdams, *supra* note 18, at 110.

131 *See* Calcara, *supra* note 28.

132 Verdelho, *supra* note 1.

133 *Id.*

A. Existing International Agreements Related to Crime & Their Shortfalls

The International Covenant on Civil and Political Rights (ICCPR) was adopted in 1966 and sets a minimum baseline for human rights.[134] The ICCPR "has become the primary place of reference for the universal standard of civil and political rights . . . [and] retains pride of place as the seminal source of international human rights law."[135] While the ICCPR does not mention cybercrime or entrapment, it does establish a right to personal liberty, a fair trial, and privacy. For example, Articles 9 through 11 discuss liberty and security of the person, in the form of freedom from arbitrary arrest and detention, and the right to habeas corpus.[136] Articles 14 through 16 discuss procedural fairness in the law through a fair and impartial trial and a presumption of innocence.[137] Additionally, the 173 parties to the ICCPR have generally recognized a common understanding that individuals have a right to privacy and due process.[138] Although the ICCPR does not include the entrapment defense, it established an important and widely-accepted baseline of human rights.

Unfortunately, many countries have reduced the effectiveness of the ICCPR by making reservations upon signing the treaty. The Bahamas and Belize, for example, do not compensate for "miscarriages" of justice, such as wrongful convictions.[139] Denmark reserves the right to exclude the public from its trials.[140] The U.S. reserves the right to impose capital punishment.[141] Although States Parties have altered their obligations, they must still abide by the object and purpose of the ICCPR. Article 19(c) of the Vienna Convention states that even if reservations "are not expressly prohibited [they] may still be invalidated if they are incompatible with a treaty's object and purpose.[142] While the ICCPR has

---

134 International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; *see also* DAVID HARRIS, A COMMENTARY ON THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS: THE U.N. HUMAN RIGHTS COMMITTEE'S MONITORING OF ICCPR xxv (Cambridge Univ. Press, 2020).

135 HARRIS, *supra* note 134, at xxv.

136 ICCPR arts. 9–11.

137 *Id.* arts. 14–16.

138 *See id.* art. 17.

139 *International Covenant on Civil and Political Rights*, U.N. TREATY COLLECTION (Nov. 13, 2022), https://perma.cc/QW3J-NQ6N.

140 *Id.*

141 *Id.*

142 D. Kirk Morgan II, *International Covenant on Civil and Political Rights: A New Challenge to the Legality of the Juvenile Death Penalty in the United States?*, 50 CATH. U. L. REV. 144, 158 n.93 (2000) (discussing Vienna Convention on the Law of Treaties art. 19(c), May 23, 1969, 1155 U.N.T.S. 331).

been criticized for the amount of signatories' reservations,[143] it nevertheless established an important standard of human rights that the international community agreed upon.

The U.N. Convention on the Rights of the Child (1989) protects children from exploitation and abuse, including pornography.[144] The agreement first referred to cyberspace when it was updated in 2000 by the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.[145] The Protocol represents the earliest international response to the internet's globalization of certain crimes. Article 2(3) of the Protocol establishes a definition of child pornography that is considered broad enough to encompass virtual images of children on the internet.[146] Article 3(1)(c) prohibits the distribution of child pornography and considers the internet to be a means of distribution.[147] Although the Protocol was an early effort by the international community to police cyberspace, it does not provide guidelines for international law enforcement cooperation or mention the entrapment defense.[148]

The U.N. Convention on the Rights of the Child suggested that the international community was adapting its criminal law to respond to the growing risks of the internet. Cyber stings are commonly used in law enforcement to proactively police the online sexual exploitation of children.[149] Police might pose as a potential customer of illegal content or as a child in a chat room to lure and identify criminals. An American study found that " in 13% of cases an offender caught in a sting operation was also concurrently talking to a real child and in 41% of the cases the offenders were found to have child pornography on their computer."[150] But the statistics regarding the success of sex cyber stings are contested.[151] While the ability of police to proactively catch criminals is critical to public safety, there is a limited understanding about the extent to which police are truly targeting individuals who would have otherwise committed the crime if

---

143 *See* Michael Da Silva, *International "Constitutions" and Comparative Constitutional Law*, 10 NOTRE DAME J. INT'L & COMP. L. 139, 168 n.164 (2020).

144 Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3 [hereinafter CRC]; *see also Treaties & International Agreements on Cyber Crime*, *supra* note 36.

145 *See Treaties & International Agreements on Cyber Crime*, *supra* note 36; G.A Res. A/RES/54/264, The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (May 25, 2000) [hereinafter CRC Optional Protocol].

146 *Id.*; *Treaties & International Agreements on Cyber Crime*, *supra* note 36.

147 CRC art. 3(1)(c).

148 *See generally* CRC Optional Protocol.

149 *See* Kimberly J. Mitchell et al., *Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?*, 17 SEXUAL ABUSE 241 (2005),

150 Alisdair A. Gillepsie, *Cyber-Stings: Policing Sex Offences on the Internet*, 81 POLICE J. 196, 199 (2008) (citing *id.* at 260).

151 *Id.*

not for the cyber sting.[152] As the international community began to respond to the changing landscape of cybercrime, it failed to include guidelines for police pursuit of online predators.[153]

In 2000, the U.N. Convention Against Transnational Organized Crime (UNTOC) established a framework that governs international cooperation between judicial authorities and law enforcement.[154] With 190 parties, UTOC is almost universally ratified.[155] UNTOC stipulates how countries are to pursue criminals and share evidence.[156] It is "the main international instrument in the fight against transnational organized crime."[157] UNTOC defines an organized criminal group as a structured organization that has at least three members.[158] It also includes legislative standards for nations to implement domestically.[159]

UNTOC has proven difficult to execute, likely due to a lack of political will.[160] For example, "the governments of Russia and other Eurasian countries are known to benefit from ties between [transnational organized crime] and . . . cybercrime."[161] UNTOC does not mention entrapment rights or discuss operational practices related to the growing "nexus" between organized crime and modern technology.[162] State Parties "remain wary of using the [treaty] as it does not provide a clear, elaborate concept upon which states may rely, legislate and train around."[163] While UNTOC is widely adopted, this may be because it "imposes few specific obligations" on States Parties, and mandatory obligations are phrased to allow countries great discretion.[164] The textual weaknesses of UNTOC do not make it an ideal vehicle to implement entrapment based rights because many countries would likely exercise discretion and opt out of the base-line standards.

---

152 *See id.* at 200.

153 *See generally* CRC.

154 *See* Ian Tennant, *Fulfilling the Promise of Palermo? A Political History of the U.N. Convention Against Transnational Organized Crime*, 2 J. ILLICIT ECONS. & DEV. 53, 55 (2001).

155 *Id.*

156 *Id.*

157 *Background Information: United Nations Convention Against Transnational Organized Crime and the Protocols Thereto*, U.N OFF. ON DRUGS & CRIME (2023), https://perma.cc/7NJY-EDD5.

158 U.N. Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.

159 *See id.*

160 *Issue Brief: Global Governance Monitor*, COUNCIL ON FOREIGN RELS. (2021), https://perma.cc/5K6E-6KJM.

161 *Id.*

162 *See id.*

163 Fiona Rebecca Livey, International Legal Framework for Combating Transnational Organised Crime (2017) (LL.M. thesis, University of Glasgow School of Law) https://perma.cc/9ASQ-937T.

164 *See id.*

The Convention on Cybercrime, also known as the Budapest Convention, was ratified by the Council of Europe in 2001.[165] Notably, most treaties drafted by the Council of Europe are open to signature by any country, regardless of whether they are a member of the Council.[166] As such, sixty-eight States Parties have ratified the Budapest Convention, even though there are forty-six member states in the Council of Europe.[167] For example, Argentina, Israel, and Nigeria, are among the countries that have ratified the agreement.[168]

The Convention is the first international agreement aimed at reducing cybercrime.[169] It attempts to increase international cooperation, harmonize national laws, and improve investigation methods.[170] Specifically, the agreement "provides for (i) the criminalisation of conduct ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (ii) procedural law tools to investigate cybercrime and secure electronic evidence in relation to any crime; and (iii) efficient international cooperation."[171] The notable articles of the agreement are discussed below.

Article 15 details "[c]onditions and safeguards."[172] It requires each party to "ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties."[173] Safeguards refer to judicial or other independent supervision, limitation of the scope and duration of a power, and grounds justifying the application of a power.[174]

Article 15 also explicitly refers to the obligations that countries have to respect human rights under the ICCPR.[175] While the Convention is the most comprehensive multilateral cybercrime treaty, it has been criticized for lacking stronger human rights safeguards.[176] The Convention expresses a concern about

---

165 Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167.

166 *Participation of Non-Member States*, COUNCIL OF EUR. (2023), https://perma.cc/4YUN-ZBL5.

167 *Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY*, COUNCIL OF EUR. (2023), https://perma.cc/998Q-RJDN.

168 *Id.*

169 *Treaties & International Agreements on Cyber Crime*, *supra* note 36.

170 *Id.*

171 COUNCIL OF EUR., THE BUDAPEST CONVENTION ON CYBERCRIME: BENEFITS AND IMPACT IN PRACTICE 4 (2020), https://perma.cc/YU9G-9HMU.

172 Convention on Cybercrime art. 15.

173 *Id.* art. 15(1).

174 *Id.* art. 15(2).

175 *Id.* art. 15(1).

176 *See, e.g.*, Deborah Brown, *Cybercrime is Dangerous, but a New U.N. Treaty Could Be Worse for Rights*, HUM. RTS. WATCH (Aug. 13, 2021), https://perma.cc/2JKN-8LAL.

international cooperation and protections of human liberty involved in cyber investigations, but it does not set parameters for law enforcement operations.[177] Perhaps the omission of an entrapment defense as a "safeguard" in the Convention is attributable to the lack of consensus among States Parties in their application of the defense, as discussed in Part II.[178] For example, Australia, Canada, the U.K., and the U.S. have ratified the Convention and have disparities in entrapment-based rights.[179] Articles 27 through 34 of the Convention detail the procedures for requesting mutual assistance from one Party to another Party regarding an investigation.[180] Article 35 established a 24/7 point of contact for each Party to contact and request assistance in an investigation or proceeding.[181]

Two additional protocols have supplemented the Budapest Convention since its ratification. First, in 2003, an additional protocol obligating States Parties to enact laws that would criminalize racist and xenophobic acts expressed online was added.[182] Thirty-three countries have ratified this supplemental protocol.[183] The second addition to the Convention pertains to enhanced cooperation and disclosure of electronic evidence.[184] It states that "effective cross-border co-operation for criminal justice purposes, including between public and private sectors, benefits from effective conditions and safeguards for the protection of human rights and fundamental freedoms."[185] The protocol does not mention entrapment but rather focuses on a system of cooperatively sharing evidence between countries.[186] In May 2022, this supplemental protocol became open for signature, and has not entered into force.[187] As of June 2023, there are thirty-eight signatories.[188]

---

177 Convention on Cybercrime arts. 14(1), 23.

178 *See supra* Part II.

179 *See id.*; *Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY*, *supra* note 167.

180 Convention on Cybercrime arts. 27–34.

181 *Id.* art. 35.

182 *See Treaties & International Agreements on Cyber Crime*, *supra* note 36.

183 C.E.T.S. No. 189.

184 C.E.T.S. No. 224.

185 *Id.*

186 *See id.*

187 *Treaties & International Agreements on Cyber Crime*, *supra* note 36.

188 *Chart of Signatures and Ratifications of Treaty 224*, COUNCIL OF EUR. (Oct. 9, 2022), https://perma.cc/MGK2-KAVT.

B. 2022 U.N. Cybercrime Treaty Negotiations

In February 2022, negotiations began for a new U.N. cybercrime treaty to respond to cybercrime threats.[189] Ironically, the treaty was proposed by Russia, a country that has been criticized for turning a "blind eye" to cybercriminals.[190] The proposed treaty is modeled after Russian domestic cyber laws and is expected to "bolster cross-border police surveillance powers to access and share user data, implicating the privacy and human rights of billions of people worldwide."[191] While it aims to improve international cooperation and enable countries to effectively share data, the proposal has sounded human rights alarm bells: "Russia and China seek to legitimize authoritarian internet control and undermine digital human rights."[192] The Budapest Convention, in contrast, "reconciles the vision of a free Internet, where information can freely flow and be accessed and shared."[193] The potential treaty proposed by Russia would broaden the definition of cybercrime, and risks empowering a "free speech witch-hunt."[194] Brazil, the Dominican Republic, the E.U., Liechtenstein, Norway, Switzerland, the U.K., and the U.S. have advocated for focusing the negotiations on reducing cybercrime, rather than imposing broad internet controls.[195] These negotiations shed light on the need for precise human rights safeguards to be adopted, including entrapment-based rights.

The Budapest Convention, although flawed, is a more suitable mechanism than the 2022 Cybercrime Treaty for protecting human rights in cyberspace.[196] "Ideally, treaty negotiations would enhance the safeguards of the Budapest Convention. But the dynamics at the U.N. and around this treaty in particular threaten to erode human rights protections, because many of the governments leading the initiative use cybercrime as a cover to crack down on rights . . . ."[197]

---

189 *See* Joyce Hakmeh, *Can a Cybercrime Convention for All Be Achieved?*, CHATHAM HOUSE (Mar. 31, 2022), https://perma.cc/7BRH-XG6B.

190 Brown, *supra* note 176.

191 Katitza Rodriguez & Karen Gullo, *Negotiations Over U.N. Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights*, ELEC. FRONTIER FOUND. (Mar. 3, 2022), https://perma.cc/4C6B-N4LP; *see also* Ivana Stradner, *Biden Must Rally Against a Russia-Led U.N. 'Cybercrime Treaty'*, THE HILL (June 28, 2022), https://perma.cc/5DEW-JZXZ.

192 Stradner, *supra* note 191.

193 COUNCIL OF EUR., *supra* note 171, at 4.

194 Stradner, *supra* note 191.

195 Katitza Rodriguez & Meri Baghdasaryan, *U.N. Committee to Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope*, ELEC. FRONTIER FOUND. (Feb. 15, 2022), https://perma.cc/8DW2-XW5J.

196 *See* Stradner, *supra* note 191.

197 Brown, *supra* note 176.

Notably, China and Russia are not parties to the Budapest Convention due to concerns about protecting digital sovereignty.[198]

Former Ambassador Deborah McCarthy is the U.S. Lead Negotiator for a potential U.N. cybercrime treaty.[199] In August 2022, she acknowledged that it can be difficult to establish criminal justice instruments when countries have disparate human rights obligations.[200] "As with every criminal justice treaty, we will be dealing with authorities that restrain freedoms for the sake of public safety in these discussions, and we must be very careful on how we exercise those powers."[201] There is a risk that countries with strong human rights protections will have these guarantees diluted if they cooperate and share data with countries that do not protect these liberties.[202] Negotiations are expected to conclude in 2023.[203]

The proposed treaty would likely expand law enforcement powers by increasing data sharing. "Broadly scoped investigative powers should not transform this instrument into a general-purpose vehicle for digital evidence gathering. Any cross-border investigative powers, in particular, should be carefully and narrowly crafted and remain closely linked to investigations of a specific, precisely worded criminal conduct."[204] The global community seems to agree that cybercrime is an international security threat that requires a common playbook among law enforcement to catch cybercriminals.[205] There is disagreement, however, about whether countries are willing to sacrifice the personal liberties of citizens to achieve unassailable cyber security.[206]

IV. A PROPOSED PATHWAY FORWARD: AMENDING THE BUDAPEST CONVENTION

The codification of entrapment-based rights is more likely to be successful if it is proposed as an amendment to the Budapest Convention, rather than a new treaty. Substantively, this amendment should allow for appropriate levels of law enforcement discretion and include enticements to appeal to as many countries as possible.

---

198 *See* Stradner, *supra* note 191.

199 *See Cybercrime Treaty Negotiations at the United Nations*, *supra* note 38.

200 *Id.*

201 *Id.*

202 *See id.*; *see also* U.N. SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE, *supra* note 38.

203 Brown, *supra* note 176.

204 Rodriguez & Gullo, *supra* note 191.

205 As evidenced by widespread agreement to the Convention on Cybercrime.

206 *See supra* Part II.

A. Contents of a Successful Amendment

An effective amendment to the Budapest Convention would balance the need for law enforcement's discretion with the risk of arbitrary enforcement. To effectively combat cyber criminals, law enforcement agencies need a certain degree of discretion. Police must be able to cooperate and adapt their operations to a constantly shifting threat landscape. Law enforcement require the capability to respond quickly to cyber threats and identify individuals who pose a credible threat to public safety or national security.

However, wide discretion to pursue potential cybercriminals poses the risk that a government will target dissidents. There are concerns that cybercrime laws will intentionally be expanded to justify operations that single out certain groups and facilitate large scale government surveillance.[207] Governments have used cybercrime as validation for targeting journalists, opposition politicians, religious reformers, artists, and human rights defenders.[208] For example, in 2019, the U.N. Human Rights Council Special Rapporteur reported that there were "fake accounts on LGBTI dating apps and other social media platforms . . . being used by State and non-State actors to entrap gay men and arrest or subject them to cruel and degrading treatment, or for blackmail."[209]

Additionally, certain countries seek to expand the definition of cybercrime to justify implementing sting operations to catch these newfound "criminals." This is especially plausible given that there are disputes within the international community about what constitutes cybercrime which could be exploited.[210] For example, as a complement to the recent U.N. cybercrime treaty negotiations, Russia submitted a draft treaty that would "greatly expand the scope of cybercrime, to include expression and online activity that is protected by international human rights standards."[211] Expanding the scope of cybercrime necessarily involves expanding the use of sting operations, prompting more entrapment concerns. Given both this attempt to broaden the definition of cybercrime and the 2022 cybercrime treaty negotiations, it is critical that entrapment rights are established going forward.

Historically, there has been limited scrutiny of how countries' methods to combat cybercrime threaten human rights.[212] But the laws expanding cybercrime to target gay dissidents are beyond the scope of entrapment-based rights; they

---

207 *See id.*

208 *See id.*; Brown, *supra* note 176.

209 Rep. of the Special Rapporteur on the Right to Privacy, U.N. Doc A/HRC/40/63 (Feb. 27, 2019).

210 *See* Rodriguez & Gullo, *supra* note 191.

211 Brown, *supra* note 176.

212 *See id.*

are simply unjust laws. This issue underscores the fact that a common protection against government intrusion is sorely needed, and the most promising pathway forward that protects human rights is not likely to be found in Russia's proposed treaty.

An ideal pathway forward would prioritize global cooperation by enlisting the support of states that did not initially sign the Budapest Convention. Perhaps some states did not sign the Budapest Convention because they did not perceive cybercrime to be a large enough threat to warrant an international agreement that reduces their digital sovereignty. Indeed, developed nations are more likely to experience cybercrime due to their higher-income economies, advanced technological infrastructure, digitalization, and urbanization.[213] Cyberthreats differ across the globe, and the risk of cybercrime is not spread equally.[214]

For example, vulnerabilities in a county's cybersecurity structure may make it more vulnerable to certain threats like malware and ransomware.[215] This is the case for Belarus, which is not a party to the Budapest Convention. Although Belarus is a developed country, it has poor cybersecurity infrastructure.[216] While Belarus has minimal cybersecurity, the rate of "infection" by cybercriminals on mobile phones remains low.[217] The Belarusian government has not made cybersecurity legislation a priority.[218] Furthermore, Belarusian law enforcement has been accused of supporting an authoritarian police state within the country.[219] Therefore, Belarus would likely need some sort of incentive to be willing to enter the Convention as it would likely be hesitant to place safeguards on police activity.[220] In these scenarios, existing States Parties should consider structuring an amendment to the Convention to include a benefit or "reward" to further entice new States Parties to ratify the treaty.

Anne van Aaken and Betül Simsek, German scholars of law and economics, define a reward as a transfer "of positively valued material or immaterial goods, such as opportunities for and benefits of cooperation, money,

---

213 Paul Bischoff, *Which Countries Have the Worst (and Best) Cybersecurity?*, COMPARITECH (Sept. 26, 2022), https://perma.cc/R4WZ-2WTF; Lance Whitney, *Why Developed Countries Are More Vulnerable to Cybercrime*, TECHREPUBLIC (May 27, 2020), https://perma.cc/ZJA2-P7AZ.

214 Shweta Sharma, *Which Countries are Most (and Least) at Risk for Cybercrime?*, CSO (Nov. 12, 2021), https://perma.cc/HF9V-AWP3.

215 *See generally Know the Types of Cyber Threats*, MASS. DIV. OF BANKS, https://perma.cc/7J2M-EHK4.

216 *Know the Risk: The Best and Worst Countries for Cybersecurity*, BROADBAND SEARCH (2022), https://perma.cc/52U4-R3TX.

217 *Id.*

218 Bischoff, *supra* note 213.

219 Piotr Żochowski, *Lukashenka's Last Line of Defence: The Belarusian Security Apparatus in a Time of Crisis*, CTR. FOR E. STUD. (Aug. 5, 2021), https://perma.cc/9ABC-TMLB.

220 *Id.*

technology, or social approval/good reputation."[221] They additionally distinguish between internal and external awards. Internal rewards are the benefits of cooperation that States Parties gain from participating in the treaty itself. External rewards are benefits "*outside* the bargain of the base treaty . . . [and] may be needed to induce entry/compliance if the cooperative gain of the treaty is insufficient or suffers from social dilemma problems"[222] Examples of external rewards for entering a treaty include receipt of development aid, an advantage in another treaty, a positive international reputation for cooperating, and access to resources or financial assistance to promote objectives beyond the treaty.[223] States Parties with high rates of cybercrime have a stronger interest in law enforcement cooperation; these parties may find it worthwhile to attract countries with differing cyberthreats through external rewards.

Japan, a party to the Convention, is an example of a country that would benefit from providing an external reward. Japan is ranked the highest globally for the percentage of online banking users who have been attacked by mobile banking trojans.[224] Trojans lure users to install malware on their phones, which enables cybercriminals to steal money from bank accounts.[225] Japan could offer an external reward, such as a state visit or funding for programs unrelated to the treaty, to incentivize additional countries to sign the Convention. This could attract countries that are not interested in an overall benefit from cooperation. An ideal amendment to the Convention would include greater incentives for countries to consent to a common framework of cooperation without overly expanding law enforcement discretion and raising potential human rights concerns.

B. Considerations: Proposing an Amendment or a New Treaty

A codification of entrapment-based rights is most likely to be successful if it is written as an amendment to Article 15 of the Budapest Convention, which provides "safeguards" of human rights in the fight against cybercrime. Compared to previously discussed treaties, the Convention has the most potential to adopt a supplementary provision due to its recent revisions and the lower number of necessary signatories. As discussed in Part III, the existing text of Article 15 has received extensive criticism due to its lack of specificity. The current text of the Convention leaves citizens at the whim of law enforcement

---

221 Anne van Aaken & Betül Simsek, *Rewarding in International Law*, 115 AM. J. INT'L L. 195, 196 (2021).

222 *Id.* at 196–97.

223 *See id.* at 206.

224 Bischoff, *supra* note 213.

225 *See* Kate Kochetkova, *Mobile Banking Trojans, Explained*, KASPERSKY DAILY (Oct. 14, 2016), https://perma.cc/NUE4-LAKF.

operations that violate human rights, like freedom of expression, but are justified as counter-cybercrime tactics.[226] These shortcomings provide a ripe opportunity to propose an amendment that would update Article 15 and incorporate entrapment-based rights.

The Convention's two recent additions in 2003 and 2022 suggest that the agreement is relatively fluid and that there is the potential for a successful amendment. It is worth noting that the Convention has only sixty-eight party countries, compared to some U.N. agreements that have around 170 parties. Indeed, the lower number of signatories suggests that the overall agreement would be less influential. Ideally, more countries would adopt proposed entrapment protections in a widely accepted treaty such as the ICCPR, which guarantees a right to a fair trial. Still, targeting the Budapest Convention, at least initially, presents the best opportunity to efficiently implement entrapment-based rights.

The countries that signed the Budapest Convention have self-selected themselves into a group of leaders that are willing to safeguard personal liberties in cyberspace. Even if the first attempt to establish precautions in the Convention was imperfect, these signatories are the most likely to support an amendment that provides an entrapment-based solution. Improving the global response to cybercrime is a time-sensitive effort and a proposed amendment to the Convention would encourage the greater international community to additionally implement these rights. It could spur global discussion, entrench entrapment protections as an international norm, or inspire its acceptance in more widely adopted treaties.

In order to amend the Convention, the parties will need to present a proposal to the Council of Europe's Cybercrime Convention Committee (T-CY), which represents the parties to the Convention.[227] When the most recent amendment to the Convention was proposed, the Committee took four years to prepare the Protocol.[228] A proposed amendment to Article 15 will likely undergo lengthy negotiations and drafting, especially given the different approaches to entrapment discussed in Part II. This Comment recognizes three possible ways to incorporate entrapment rights into international law.

C. Pathways 1 & 2: Explicit Standard Codification

1. Pathway 1: The Subjective Model of Entrapment

The first potential pathway towards a common understanding of the entrapment defense is an amendment to the Budapest Convention that explicitly

---

226 *See id.*

227 *See Protocol Negotiations*, COUNCIL OF EUR. (2023), https://perma.cc/WU65-UPAV.

228 *Id.*

codifies the entrapment right under the subjective model. As discussed in Part II, the subjective approach concentrates on the state of mind of the accused and examines the predisposition of the defendant.[229]

There are downsides to this pathway that would make it difficult to codify. First, because the subjective approach relies on the defendant's prior behavior, it does not easily transfer to cybersphere applications.[230] Cybercriminals often operate via proxy IP addresses, making it time-consuming and difficult for law enforcement to trace crimes to certain individuals.[231]

Second, countries that already recognize the entrapment defense, either in legislation or in practice, more commonly use the objective approach. Attempts to convince these countries to fundamentally reframe their existing legal systems would most certainly fail.

Third, the subjective test will likely exert little control over government agents.[232] The nature of cyberspace makes it easier for governments to collect information, such as websites visited, about individuals who they suspect could be dangerous.[233] "Law enforcement might use information of this nature to prove predisposition before government contact. If the use of such information is accepted, law enforcement actions will be unrestrained as courts will not place their activities under scrutiny."[234] The subjective model would further pressure law enforcement to adopt invasive methods of monitoring to prosecute individuals. It would justify additional government intrusion into everyday life and likely lose the support of countries with strong civil liberties.

2. Pathway 2: The Objective Model of Entrapment

A second pathway is an amendment to the Budapest Convention that codifies the objective model. As Part II described, the objective model focuses on government agents' roles in the commission of the crime.[235] A defendant can raise the entrapment defense if an "ordinary person" would commit the crime.[236]

The objective approach is not an ideal model to protect the rights of citizens in cyberspace because it is difficult to determine how a "reasonable person" would behave in the cybersphere.[237]

---

229 *See supra* Part II.B.

230 *See* Valentine, *supra* note 27, at 23.

231 *See* Woodward, *supra* note 6; *see also* Fox, *supra* note 6.

232 *See* Jarrod S. Hanson, *Entrapment in Cyberspace: A Renewed Call for Reasonable Suspicion*, 1996 U. CHI. LEGAL F. 535, 542 (1996).

233 *See id.* at 542–43.

234 *See id.* at 543.

235 *See supra*, Part II.B.

236 Hanson, *supra* note 232, at 544.

237 *See id.*; Valentine, *supra* note 27, at 30–31.

Paul Valentine argues that the objective model is especially weak when applied to terrorism.[238] If an individual commits cyberterrorism, the objective model asks the court to consider what a reasonable person would do in that situation.[239] The objective logic fails to consider that no reasonable person would commit an act of cyberterrorism.[240] In several countries, a defendant would find it exceedingly difficult to raise the entrapment defense in a terrorism case. In applying the objective model, no judge in the U.S. would find that a reasonable citizen would engage in terrorism.[241] "In Germany, the court would consider the difficulty in detection of terrorism and would give great deference to law enforcement agents."[242] In the U.K., the court would apply *Regina v. Looseley* and find that the "type of crime being investigated . . . would work heavily against the defendant."[243] Valentine argues that "Australia and Singapore and many other nations would give absolutely no credence to this defense whatsoever."[244] According to Valentine, the objective model of entrapment only provides an "escape hatch" to defendants committing less serious crimes.[245] The objective model would not provide an all-inclusive defense that is readily transferable to the cybersphere.

As was the case with the subjective approach, an amendment codifying the objective approach would be unlikely to succeed. A proposal overtly constraining law enforcement discretion would likely receive only a fraction of support from the current sixty-eight signatories.

3. Likelihood of Success

Requiring countries to adopt the subjective or objective models would receive minimal support or fail to be implemented. Many countries follow the common law tradition that considers the way evidence was obtained to be irrelevant.[246] Codifying the subjective or objective models would demand an overhaul of many signatories' criminal justice systems. A strict subjective or objective approach would risk alienating existing parties to the Convention, like Australia. Australia's reluctance to interfere with police detection methods and "mini-exclusionary rule" suggest that it would not support an amendment that

---

238 Valentine, *supra* note 27, at 30–31.

239 *See id.*

240 *See id.*

241 *Id.* at 31.

242 *Id.*

243 *Id.*

244 *Id.*

245 *Id.* at 32.

246 *See* Obokata, *supra* note 39, at 55.

imposes a rigid model of the entrapment defense.[247] A strict entrapment model also risks prompting countries to withdraw from the Convention entirely. Countries may view a proposal that adopts the subjective or objective model as fundamentally offensive to their government institutions, as they would need to restructure their judicial systems.

There is also a potential concern that attempting to explicitly codify a standard of entrapment will ultimately dilute the already existing rights for individuals in countries that have comparatively strong entrapment rights. The UN Security Council's Counter-Terrorism Committee Executive Directorate (CTED) has argued that:

> Agreeing on a common standard across States will almost certainly lead to a lower standard than one that would be achieved by identifying a high universal standard and asking States to 'level up'. The concern is that, in order to address law enforcement's jurisdictional problems, the substantive law will become weakened, giving law enforcement too-quick access with too-little due process. The trend towards universalization, in other words, could lead to a lowest common denominator in terms of due process.[248]

Proposing the codification of the subjective or objective models of entrapment has a slim likelihood of success and risks the withdrawal of current signatories. A loss of Convention signatories would reduce law enforcement cooperation related to cybercrime, acting contrary to the goals of the amendment itself.

D. Pathway 3: The Minimum Floor Approach

Article 15 of the Budapest Convention should be modified to establish a minimum floor for entrapment rights. This novel pathway is preferrable to the explicit codifications of the entrapment defense because it instead codifies the observed movement towards recognizing entrapment-based rights.[249] This floor would require countries, at a minimum, to consider entrapment as grounds for mitigation at sentencing or discretionary exclusion of evidence. The proposed amendment would enable countries with strong entrapment rights to maintain their protections while offering an achievable compromise to countries that have informally developed remedies for entrapment. These minimums would codify the informal existing practices of some states while challenging countries that have yet to take a stance on the. Common minimums will streamline current law

---

247 *See* Marcus, *supra* note 42, at 226.

248 U.N. SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE, *supra* note 38.

249 *See supra* Part II.

enforcement cooperation and provide a framework that may be adjusted as cyberthreats continue to shift.[250]

Admittedly, countries would ideally agree to a common model of entrapment in cyberspace. The minimums would be an attempt to propose constraints on governments that have a realistic opportunity to be ratified. The gradual acceptance of entrapment-based rights in practice suggests that there would be a lower risk of States Parties refusing to support the minimum floor or ultimately withdrawing from the agreement.

Countries that have already codified entrapment, such as the U.S., can be expected to support minimums because the amendment would not lower its existing standard by requiring States Parties to meet the proposed baseline. The minimums would be most impactful in States Parties like Germany, where jurisprudence has begun to acknowledge and express displeasure with entrapment, but legislation has failed to delineate what constitutes the defense or provide guidance to judges. In Germany in particular, scholars have observed a need for legislation to guide judge discretion in the realm of entrapment cases. The minimums would encourage countries to synchronize legislation with an identified shift towards entrapment rights in the legal system, while still leaving countries with the discretion to implement such rights.

While the minimums are imperfect, constraining government operations would hopefully spur further regulation of undercover activity and nudge the prosecution of cybercriminals towards a higher standard of due process. Rather than proposing a standard of entrapment that would lead a series of countries to step away from the negotiating table, this type of amendment could prompt meaningful discussion among world leaders. By establishing a minimum floor, countries could cooperate effectively while respecting human rights.

V. CONCLUSION

A global lack of consistency regarding the entrapment defense impacts the extent to which law enforcement can cooperate and effectively address cybercrime. Unrestrained police operations to carry out cyber stings also pose the risk that governments will manufacture crime to target certain citizens. This Comment recommends that the international community adopt a "minimum floor" that would require countries to consider entrapment to be grounds for mitigation at sentencing or discretionary exclusion of evidence. The number of cyber stings that are executed by law enforcement remains unanswered, due to the absence of available data. The extent to which cyber stings truly transform

---

250 *See* Dina Kartit & Elizabeth Howcroft, *Interpol Says Metaverse Opens Up New World of Cybercrime*, REUTERS (Oct. 27, 2022), https://perma.cc/N9LU-Z6MC (explaining how Interpol, an international police organization that facilitates global cooperation, has warned that the metaverse will breed new kinds of crime and enable existing crime to exist on a larger scale).

innocent citizens into criminals is also difficult to determine. Regardless of available information, the rise of cyberattacks and other cybercrimes suggests that setting a minimum floor will provide common guidance to law enforcement to encourage collaboration and protect civil liberties.

The emergence of new technologies will only affirm the sore need for a common playbook that enables law enforcement to adapt to shifting virtual environments. Crime in the cybersphere will continue to grow and transform, revealing outdated legal mechanisms that demand attention by the international community. This Comment has proposed a new framework to adapt to the modern challenge of applying our legal system to the cybersphere, but a more detailed analysis will be required as emerging technologies materialize over time.