UNCAC

UPDATE PAPER

NHSMUN
National High School Model United Nations

Email: info@imuna.org
Phone: +1 (212) 652-9992
Web: www.nhsmun.nyc

Hello Delegates!

It is a great pleasure for me to welcome you all to NHSMUN 2025 as well as to the UNCAC committee! My name is Joshua Labrin, I´m 19 years old, I was born and raised in Peru and on this occasion, I have the honor of being your Chair Director. I'm also finding myself super excited about starting my journey as staff alongside this wonderful people and this amazing conference. I'm currently a first-year student in Constructor University, Bremen, majoring in Global Economics and Management, with a minor in Industrial Engineering and Management.

I started my MUN career back in 2020 and I couldn't be happier for making the decision to enter this wonderful world. I have had the opportunity to participate in many conferences since then and 2024 was especially important for me, since I had the honor of representing my country at both HarvardWorldMUN (Taiwan) and HarvardNationalMUN-LA (Panama). I am very happy to have had the opportunity of coaching my school's MUN delegation and to be considered as a respected member of the Peruvian MUN circuit. For me, Model United Nations is more than just a debate. It is a great opportunity to challenge ourselves and push our limits, helping us become better students, friends, and people..

I consider myself someone who is super reasonable with people, so if you have any complications, questions or concerns, do not hesitate to contact me and I will be more than happy to support you. I am a huge fan of Formula 1 (Essere Ferrari!) and Star Wars. I have read many novels, mainly classics, and I have a lot of interest in sports, such as football, surfing and rowing, being the last one the one that gave me the opportunity to represent the city I live in (Bremen) in huge races around Germany and Europe alongside classmates of my university.

I could spend hours telling you about so many experiences and lessons that MUN gave me but the most important thing I can say about having the chance of participating in conferences like this one is that having fun is the only thing that should matter the most to you. You must live the MUN experience to the fullest. Make friends, learn, grow and above all, remember that a prize and the people around you do not define your limits and capabilities, but yourself. You oversee your happiness, your growth and especially, the benefit you get from this opportunity. So, just enjoy the experience, give 110 percent of yourselves to the conference and most importantly, be yourselves.

See you at the conference!

Yours in diplomacy

Joshua Labrin

United Nations Convention Against Corruption

Session II

nhsmun.uncac@imuna.org

NHSMUN
National High School Model United Nations

Email: info@imuna.org
Phone: +1 (212) 652-9992
Web: www.nhsmun.nyc

Dear Delegates,

Welcome to The United Nations Convention Against Corruption (UNCAC)! My name is Shruthi Nadathur, and I will be your Assistant Director for Session II for NHSMUN 2025! This is my first year on staff for NHSMUN, and I am so excited to see what you all accomplish at our conference.

I am currently a freshman at the University of Southern California, studying Political Economy & Law, History, and Culture with a minor in News Media and Society. I plan on working towards becoming either a constitutional or public interest lawyer while concurrently working as an election campaign manager. My number one goal is to make an impact in our society, whether through legal assistance or political influence.

I've spent my entire life in Plano, Texas, a large suburb in the Dallas-Fort-Worth metropolitan area. Many of my hobbies and personal passions have revolved around music and the performing arts. I've played the piano for almost twelve years, the violin for eight, and self-learned both the guitar and viola during the COVID-19 Pandemic. I've been active in theatre in the past, and I was trained as an Indian Carnatic Classical singer for eight years. A fun fact about me is that I used to compose music as a distraction when I was overwhelmed with school! Other than these, you'll find me reading (my favorite genre is a tie between psychological thrillers and political memoirs), crocheting, or catching up on the most recent edition of *Vogue*.

I began participating in MUN in high school and have continued as a member of the University of Southern California's Model United Nations team. I appreciated the way MUN combined my love for international affairs with my experience in public speaking, and as a result, I have a deeper understanding of diverse perspectives and diplomacy. NHSMUN may seem daunting but focus on learning from your experience here: through researching and discussing our topics, you will gain insights into perspectives you've never considered before. At the end of the day, you will grow and prosper in the field of global diplomacy and multi-perspective thinking.

My Director and I are pleased to bring you an Update Paper that contains recent information relevant to the topics in UNCAC. Make sure to consider the research obtained here along with your Background Guide as you prepare for your conference.

I wish you the best of luck at this year's conference, and I look forward to meeting you all very soon!

Best,

Shruthi Nadathur

United Nations Convention Against Corruption

Session II

nhsmun.uncac@imuna.org

UNCAC

NHSMUN 2025

TOPIC A:
CORRUPTION AND PRESS FREEDOM

Photo Credit: Muhammad Mahdi Karim

Introduction

Corruption and press freedom are deeply connected. This issue has existed for years worldwide. Journalists covering politics, conflicts, or other topics face dangerous and terrifying risks. Journalists in 2024 face risks, such as financial or legal pressures. In addition, reporters also face physical threats, such as reporting from conflict zones or risking their lives depending on the topics they cover. UNESCO reported that between 2019 and 2024 attacks on environmental journalists increased 42 percent.[1] According to the latest Corruption Perception Index (CPI), the majority of countries have made no progress on overcoming corruption in the last decade.[2] Nevertheless, the Committee to Protect Journalists (CPJ) reported that 2024 was one of the worst years for journalists.[3] In 2024 the number of media professionals detained increased. By December of 2024 the CPJ reported 361 journalists behind bars due to their job.[4] The main reason was censorship topics such as authoritarian repression, war, and political or economic instability. Journalist deaths also increased in 2024, mainly due to conflict zones around the world. Different organizations estimate that 101 journalists were killed in 2024, 31 of which were in conflict zones.[5] Journalists face imprisonment, kidnapping, murder, and enforced disappearances for exercising their rights to information and freedom of expression.

Meanwhile, the digital age has reshaped the fight between corruption and press freedom. News is now accessible in seconds via phones, tablets, or computers. Digital tools have boosted investigative and independent journalism. This has helped journalists uncover and share information quickly in new and different formats. However, these same tools can be used to suppress freedom. Corrupt governments use technology to surveil, manipulate, hack, harass, and threaten journalists. Without safeguards, digital technology is a double-edged sword. It can expose corruption but also silence dissent and control narratives. It is important to understand the challenges facing reporters in 2024. Some of these include the increase in conflict zones and new technologies as a means of information, to ensure their safety and freedom of expression. Is important to ensure press freedom as attacking this right will evolve to attacks on other freedoms.

The Impact of Digital Media on Press Freedom

Newspapers and magazines are declining day by day and are among the least used methods of communication. Local newspapers are being the most affected, with 127 newspapers being closed in 2024 in the U.S.[6] The decline of traditional journalism and newspapers has led to other sources of information. For instance, social media has become a common news source. Social media is at least one of the information sources for 72 percent of Americans.[7] On the other hand, independent journalism has grown worldwide and increased access to information. Independent journalism is journalism

1 "At least 68 journalist killings in 2024, UNESCO reports," United Nations, last edited December 12, 2024, https://news.un.org/en/story/2024/12/1158141."At least 68 journalist killings in 2024, UNESCO reports," United Nations, last edited December 12, 2024, https://news.un.org/en/story/2024/12/1158141.
2 "Corruption Perceptions Index," Transparency International, accessed January, 2025, https://www.transparency.org/en/cpi/2023?gad_source=1&gclid=Cj0KCQiAhbi8BhDIARIsAJLOluek_iZptCheNpRJQV0qMCmrVX8cy2bdy32BWhVnB9YmMVueabkZMYsaAun5EALw_wcB.
3 "Journalist jailings near record high in 2024 as crackdown on press freedom grows," Committee to Protect Journalists, last edited January 16, 2025, https://cpj.org/2025/01/journalist-jailings-near-record-high-in-2024-as-crackdown-on-press-freedom-grows/.
4 Committee to Protect Journalists, "Journalist jailings near record high in 2024 as crackdown on press freedom grows."
5 "Explore CPJ's Database of Attacks on the Press," Committee to Protect Journalists, accessed January, 2025, https://cpj.org/data/killed/2024/?status=Killed&motiveConfirmed%5B%5D=Confirmed&type%5B%5D=Journalist&start_year=2024&end_year=2024&group_by=location; "RSF's 2024 Round-up: journalism suffers exorbitant human cost due to conflicts and repressive regimes," Reporters Without Borders, accessed January, 2025, https://rsf.org/en/rsf-s-2024-round-journalism-suffers-exorbitant-human-cost-due-conflicts-and-repressive-regimes.
6 "State of the News Media 2024: It's Bad," Dreier RoundTable - Claremont McKenna College, last edited October 24, 2024, https://drt.cmc.edu/2024/10/24/state-of-the-news-media-2024-its-bad/.
7 Matt Purdue, "The rise of independent journalists and tips for engaging with them," PR Daily, last edited November 11, 2024, https://www.prdaily.com/the-rise-of-independent-journalists-and-tips-for-engaging-with-them/.

that doesn't belong to governments, corporations, or other outside influences. This allows for a more impartial reportage. Since independent journalism is more transparent, many people have started to prefer this news source. The Free Press Survey revealed that 51 percent of people think that these independent journalists are combating misinformation. Independent journalism secures journalistic objectivity too. This has caused distrust in traditional media and the reliability of the news. Only 32 percent of Americans feel "a fair amount" of confidence that the traditional media is reporting the news fairly and accurately.[8] This shows how traditional journalism is being used as a tool to manipulate society and respond to political and economic interests.

This new era of information and easy diffusion has allowed the growth of "fake news". Fake news are false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke.[9] They spread easily with digital media and freedom of speech agenda. This news is presented to society seeking to deceive or influence people through misleading information. These include manipulated and fabricated stories, edited images or images taken out of context that aim to create a false impression in the reader. Social media and its increased use throughout the world, along with online platforms have allowed the spread of these to be much easier. These media allow anyone to share information without their facts verified. This has caused many problems within societies that maintain a reputation for corrupt governments. In many cases, fake news can cast doubt on the integrity of people or institutions who are targeted by a particular fake news story. The 2024 US presidential election brought to light the great influence of social media and fake news. Both candidates were subject to false accusations, as well as international actors spreading false information about the legitimacy of the election.[10] Other actors, like Elon Musk, proved to be key to information during the elections. The Center for Countering Digital Hate studied Musk's posts during the campaign. Researchers identified at least 746 posts on X (former twitter) related to the elections, in which at least 87 were proven to have false or misleading information.[11] It is estimated that those posts with fake news were viewed 2 billion times.[12]

Fake news tends to confuse readers by providing information

8 Purdue, "The rise of independent journalists and tips for engaging with them."
9 "Fake News," Cambridge, accessed January 10, 2025, https://dictionary.cambridge.org/dictionary/english/fake-news.
10 Sarah Steffen, "Fact check: Disinformation's impact on the US election," *DW*, November 7, 2024, https://www.dw.com/en/fact-check-what-role-did-disinformation-play-in-the-us-election/a-70729575.
11 *Musk's Political Posts: How Elon Musk's political posts amass more views than all U.S. political campaign ads on X's disclosure dataset* (London: Center for Countering Digital Hate, November 11, 2024), https://counterhate.com/research/musk-political-posts-x/.
12 *Musk's Political Posts: How Elon Musk's political posts amass more views than all U.S. political campaign ads on X's disclosure dataset.*

Press conference regarding the Lava Jato incident, demonstrating the influence of the digital media

Credit: Coletiva do dep. Deltan Dallagnol

that makes it difficult for them to know whether what they are reading is real or not. Social media platforms have become spaces to share comments, usually misrepresented, about events, politics or influential public figures. This affects the trust and weakens real journalism as people doubt truthful news due to the information they access online. This is highly due to "echo chambers". As social media wants to keep us engaged, they give users personalized contents based on their preferences and ideologies.[13] This causes users to only see news that they are in favor of in their algorithm. It makes readers believe in stories that relate to their own beliefs and opinions. As people are only exposed to opinions of one type that a productive debate is eliminated and polarization increases.[14] Being exposed to a single opinion also makes them more secure in their beliefs and seeing more support leads to more radicalization.

Media literacy has proven to be important during election seasons worldwide. 2024 was the world's biggest election year in human history with 70 elections throughout the year across the globe.[15] With new tools like AI, misinformation and fake news were a main concern for most countries. This year showed the relation between strong democracies and strong protections against fake news. The more fragile and corrupt democracies had higher rates of misinformation throughout the election year.[16] For example, even though Finland had accusations around fake news during elections different NGOs confirm it did not affect the results.[17] In 2014, the Finnish government launched a strong anti-fake news program in schools, as a consequence it is the country with the best media literacy.[18] On another hand, Romania's elections were cancelled after the first round. Intelligence reports Moscow's intervention through an anti-Western propaganda campaign, mainly on TikTok, to change the vote.[19]

Misinformation needs to be addressed as it is the most pressing short-term global risk, according to the Global Risks Report 2024.[20] Fake news and misinformation can be resolved in different ways. It is important to promote media literacy education through critical thinking among readers. The Organization for Economic Cooperation and Development (OECD) is encouraging their member states to include media literacy in their high school curriculum.[21] This would help users recognize and differentiate true from false information. In addition, it is urgent that social networks and media platforms assume responsibility for better filtering information and verifying its veracity, reducing the spread of misleading news.[22] Access to unverified news is easier than ever. Traditional news has failed to satisfy people's need for researchers and accessibility of information. A study carried out by Reuters institute revealed that 31 percent of people turn to YouTube for news each week, 21 percent for WhatsApp, 13 percent use TikTok and X 10 percent.[23]

Currently, digital media is both a tool and a threat to press freedom. It helps journalists report and work together more easily. It also increased the access of information to people and allowed them to share news quickly. However, it also creates new dangers, such as prioritizing speed over information quality and fake news being easily spread. To protect press freedom, we need better laws, stronger technology, and global teamwork. Journalists must be able to work safely and freely.

13 Frances Crinnion, Natalia Yannopoulou, Saurabh Bhattacharya, "Chapter eight - Fake news inside ideological social media echo chambers," Handbook of Social Media in Education Consumer Behavior and Politics 1, (2024: 139-187, https://doi.org/10.1016/B978-0-323-90237-3.00008-4.
14 Catherine McCarthy, "Political echo chambers are dangerous to democracy", *The Miscellany News*, November 13, 2024, https://miscellanynews.org/2024/11/13/opinions/political-echo-chambers-are-dangerous-to-democracy/.
15 Niranjan Sahoo, "How 2024's elections redefined political landscapes across the world," Democracy Without Borders, January 15, 2025, https://www.democracywithoutborders.org/34695/how-2024s-elections-redefined-political-landscapes-across-the-world/.
16 Anna Desmarais, "Which countries fared best against disinformation during major 2024 election year?," *Euro News*, January 3, 2025, https://www.euronews.com/next/2025/01/03/which-countries-fared-best-against-disinformation-during-major-2024-election-year.
17 Anna Desmarais, "Which countries fared best against disinformation during major 2024 election year?"
18 Anna Desmarais, "Which countries fared best against disinformation during major 2024 election year?"
19 Anna Desmarais, "Which countries fared best against disinformation during major 2024 election year?"
20 C.M. Rubin, "Combating Misinformation: AI, Media Literacy, And Psychological Resilience For Business Leaders And Educators," *Forbes*, last updated December 2, 2024, https://www.forbes.com/sites/cathyrubin/2024/12/02/combatting-misinformation-ai-media-literacy-and-psychological-resilience-for-business-leaders-and-educators/.
21 Rubin, "Combating Misinformation: AI, Media Literacy, And Psychological Resilience For Business Leaders And Educators."
22 Jocelyn Maclure, "Overcoming online echo chambers requires institutional and individual commitment," Policy Options - Institute for Research on Public Policy, December 19, 2024, https://policyoptions.irpp.org/magazines/december-2024/online-echo-chambers/.
23 Nic Newman, "Resumen Ejecutivo y Hallazgos Clave Del Informe de 2024," Reuters Institute for the Study of Journalism, June 17, 2024, https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2024/dnr-resumen-ejecutivo.

The Israel/Gaza Conflict

The conflict between Israel and Gaza is not new. It started around 1948, nevertheless, recently we have seen it intensified by the growing political and religious tensions. Since the attacks of October 7, 2023, at least 217 journalists and media workers had been killed in Gaza.[24] Palestine is the most dangerous country for journalists. Journalists in this zone today face multiple dangers. These arise not only from the violent nature of the crisis, but also from the complex dynamics between politics involved in the conflict. The most easily encountered danger is that journalists are direct, intentional or unintentional targets of military forces on both sides. Reporters without Borders (RSF) has identified at least 35 cases with enough information to confirm the journalists were directly targeted because of their profession.[25] For example, airstrikes in the region hit buildings occupying communication networks, where journalists often find themselves caught in the crossfire. A clear example of this is the case of Hamza al-Dahdouh, a journalist and cameraman for Al-Aqsa TV and son of Wael al-Dahdouh, Bureau Chief of the well-known Al Jazeera news network. It occurred on January 7, 2024, during an Israeli airstrike. Witnesses reported that al-Dahdouh was wearing distinctive clothing with markings that allowed him to be identified as a member of the press, but despite this, after an unfortunate event he became one of the victims of an attack in an area entirely populated by civilians and reporters, in other words "a peace zone."[26] This shows how even when recognized as press, journalists keep being targeted and affected by the conflict.

This event has led to widespread condemnation by international human rights organizations such as the Reporters without Borders (RSF) organization. RSF stated that the Israeli army repeatedly shows disregard for international laws that are responsible for protecting the safety of journalists and protecting their rights of expression.[27] RSF mentioned severe conventions and international laws that protect journalists that are being broken in Gaza. For example, the UN Security Council (UNSC) Resolution 2222 from 2015: On protection of journalists and associated media personnel in armed conflict or Article 79 of The Geneva Conventions.[28] Both of these documents assure that journalists should be treated and protected as civilians during the war. Nevertheless, this unfortunate death and severe other cases proves that journalists are not being seen as civilians seeking to provide information to the public in Gaza. Therefore, RSF completed multiple complaints and petitions to the International Criminal Court to prioritize the investigation into the IDF's crimes against journalists in Gaza since 7 October.[29] Hamza's case highlights the challenges faced by journalists not only in Gaza, but in general, where airstrikes, strict movement restrictions, kidnappings, rape, abuse, violence and more act as obstacles to the main objective of journalists, which is to freely and safely inform their target audiences.[30] Since al-Dahdouh's death, journalists have found themselves facing increasing hostility ranging from physical attacks and arrests to smear campaigns, where high-profile cases like this have escalated, leading to the so-called accountability cases of journalist murders.

On another hand, Israel's Press Freedom Index decreased to a score of 53. The media landscape was affected in 2022 with the new government, however it decreased significantly.[31] It was also reported that critical debate and objective content is harder to find since October 7.[32] Reports related to the war on Gaza face multiple obstacles, as only journalists

24 Mohamed A. Hussein and Hanna Duggal, "Know their names: Palestinian journalists killed by Israel in Gaza," *Al Jazeera*, December 31, 2024, https://www.aljazeera.com/features/longform/2024/12/31/know-their-names-the-palestinian-journalists-killed-by-israel-in-gaza.
25 Reporters Without Border, "RSF's 2024 Round-up: journalism suffers exorbitant human cost due to conflicts and repressive regimes."
26 Shaimaa Khalil, "Al Jazeera bureau chief's son Hamza al-Dahdouh among journalists killed in Gaza," *BBC*, January, 2024, https://www.bbc.com/news/world-middle-east-67905566.
27 "RSF files third complaint with ICC about Israeli war crimes against journalists in Gaza," Reporters Without Borders, May, 2024, https://rsf.org/en/rsf-files-third-complaint-icc-about-israeli-war-crimes-against-journalists-gaza.
28 "International Day to End Impunity for Crimes against Journalists, 2 November," United Nations, November, 2024, https://www.un.org/en/observances/end-impunity-crimes-against-journalists; Daoud Kuttab, "Silence on Israel's massacres of journalists is dangerous to all," *Al Jazeera*, January 4, 2025, https://www.aljazeera.com/opinions/2025/1/4/silence-on-israels-massacres-of-journalists-is-dangerous-to-all.
29 Reporters Without Borders, "RSF files third complaint with ICC about Israeli war crimes against journalists in Gaza."
30 Khalil, "Al Jazeera bureau chief's son Hamza al-Dahdouh among journalists killed in Gaza."
31 "Israel," Reporters Without Borders, accessed January, 2025, https://rsf.org/en/country/israel.
32 Reporters Without Borders, "Israel."

History is Watching (Israel conflict)
Credit: Alisdare Hickson

associated with The Israel Defense Forces (IDF) are allowed to report.[33] Furthermore, the press landscape in Israel became more complicated when in April 2024 the parliament approved a bill that allows the government to temporarily close international news channels in Israeli territory.[34] For example, on November 24, 2024, the Haaretz, Israel's oldest newspaper, was sanctioned.[35] These sanctions were proposed by Communications Minister Shlomo Karhi and unanimously approved by Israel's far-right Cabinet. The sanctions and boycott were proposed following critical content about the war in Gaza and posts suggesting sanctions on high government officials for violating international law.[36] Noa Landau, deputy editor-in-chief of the paper, stated that this boycott was another step in Netanyahu's journey to dismantle Israeli democracy.[37] Another case in 2024 was Al Jazeera. Al Jazeera's office in Ramallah was raided in August 2024 and ordered to shut down for 45 days by a Court Order.[38]

Addiotionally, the conflict between Israel and Palestine is challenging press freedom worldwide. Irene Khan, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, reported that the conflict is increasing global polarization.[39] Also, few conflicts have tested freedom of opinion and expression so widely within countries not involved in it. All kinds of demonstrations in support of Palestine have been seen around the world, however most of them have been brutally dismantled. It highlighted how private institutions, such as universities and companies, had a big role in intimidating, isolating and silencing voices that differ from theirs.[40] Irene Khan also reported that other rights were being violated, such as education and academic freedom, because people were

33 Reporters Without Borders, "Israel."
34 "Israel: New law allows government to temporarily shut down Al Jazeera," International Federation of Journalists, April 2, 2024, https://www.ifj.org/media-centre/news/detail/category/middle-east-arab-world/article/israel-new-law-allows-government-to-temporarily-shut-down-al-jazeera.
35 Tania Krämer, "Israel's media crackdown is bad news for press freedom," *DW*, last edited November 28, 2024, https://www.dw.com/en/israels-media-crackdown-is-bad-news-for-press-freedom/a-70894536.
36 Krämer, "Israel's media crackdown is bad news for press freedom."
37 Krämer, "Israel's media crackdown is bad news for press freedom."
38 "Journalists are not targets: Israel's shutdown of Al Jazeera's Ramallah office threatens press freedom," Amnesty International, September 25, 2024, https://www.amnesty.org.au/israels-shutdown-of-al-jazeeras-ramallah-office/.
39 "Global threats to freedom of expression arising from the conflict in Gaza – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan (A/79/319)," United Nations, August 23, 2024, https://www.un.org/unispal/document/report-special-rapporteur-23aug24/#_ftn25.
40 United Nations, "Global threats to freedom of expression arising from the conflict in Gaza – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan (A/79/319)."

practicing their right to protest and freedom of speech.[41] For example, during the nationwide students protests in May 2024 in the U.S, it was proved that different universities were linked to companies that were profiting from the war in Gaza.[42] Therefore, one of the main demands on the different campuses was to divest from these companies. Divestment from Israel was more complex than it seems, since several universities have high-value investments that could result in great penalties if they were to be abandoned.[43]

Maintaining the right to free expression is necessary during times of conflict. The right of freedom of expression includes access to quality and objective information, without censorship. However, three big challenges that have worsened in the past year were identified in the war in Gaza. First, attacks on journalists and media have put global access information about the conflict at risk. Second, Palestinian voices are being silenced unfairly, harming academic, artistic, and overall freedom of expression. Third, the line between allowed and banned speech is becoming unclear.[44] It is important to understand that all human rights are based on no discrimination. Therefore, freedom of expression cannot be used as an excuse to promote discrimination, violence and hate speech. The right to practice and enjoy freedom of expression without discrimination should be secure on an equal basis by all sides. After October 7, 2023, both Muslims and Jews have experienced an increase of islamophobia and antisemitism and overall discrimination at work.[45] Confusion about what counts as antisemitism has made fighting hate speech harder. Weak laws, social media, and political agendas add to the problem.[46] These issues have been used to undermine and misuse efforts against hate speech. Freedom of expression is necessary to democracy, conflict resolution and peace building. Without freedom of expression, other rights are at risk. Ensuring the lives of journalists in conflict zones, objective reporting and non-discrimination is key to resolving the conflict.

Conclusion

The relationship between corruption and press freedom shows that journalism is being used as a political tool. Media sources are no longer transparent, but instead often alter information. This allows for the spread of manipulation and fake news. Along with a mistrust to journalism and a decrease in press freedom, recent years have shown an alarming increase in threats against journalists. Many journalists are currently facing violence, surveillance, harassment and even murder for trying to shed light on pressing news. Digital media has introduced a double-edged sword into the world. On one hand, there is more access to information than ever, allowing easier investigation and presentation of cases. On the other hand, these same tools are used to oppress and influence people's perspectives. As a result, introducing disinformation into society and censoring journalists.

This situation is especially alarming because it has spread around the world and it is not restricted to a single country or region.[47] Traditional journalism is decreasing every day, with more newspapers closing constantly. They are being replaced by independent journalism or in many cases social media. This allows for fake stories to travel faster. Many people are often unsure on what to believe, which makes taking informed decisions almost impossible. For example, a study by Pew Research showed that 64 percent of Americans believed that fake news confused the public during political campaigns.[48] This shows how easily the media can influence people's way of thinking and as a result it can have a direct impact on pivotal political decisions, such as an election.

41 "Amid campus crackdowns, Gaza war triggers freedom of expression crisis," United Nations, April 25, 2024, https://news.un.org/en/story/2024/04/1149001.
42 Zachary Folk, "College Protesters Want Divestment From Israel: Here's Why That's So Difficult," *Forbes*, May 15, 2024, https://www.forbes.com/sites/zacharyfolk/2024/05/15/college-protesters-want-divestment-from-israel-heres-why-thats-so-difficult/.
43 Folk, "College Protesters Want Divestment From Israel: Here's Why That's So Difficult."
44 United Nations, "Global threats to freedom of expression arising from the conflict in Gaza – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan (A/79/319)."
45 "A Summary Of Our Latest Research: Antisemitism and Islamophobia In The Workplace," Pearn Kandola, October 1, 2024, https://pearnkandola.com/insights/a-summary-of-our-latest-research-antisemitism-and-islamophobia-in-the-workplace.
46 United Nations, "Global threats to freedom of expression arising from the conflict in Gaza – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan (A/79/319)."
47 Nazish Mehmood,"The Global Crisis of Bullshit Culture and Media Manipulation," *Modern Diplomacy,* January 3, 2025, moderndiplomacy.eu/2025/01/03/the-global-crisis-of-bullshit-culture-and-media-manipulation/.
48 Nazish,"The Global Crisis of Bullshit Culture and Media Manipulation."

The protection of journalists needs to be addressed to ensure people have access to truthful and transparent information. This will allow for more clear perspectives on global issues and hence a better-informed decision making. To achieve this, it is necessary to protect journalists and increase media literacy through education. Delegates need to come together to find solutions for this global problem. It's necessary to ensure journalists can work without fear, so that the truth prevails. This way, corruption and manipulation can be exposed instead of being hidden.

UNCAC

NHSMUN 2025

TOPIC B:
CYBERCRIME AND CORRUPTION

Photo Credit: Navy Petty Officer 1st Class Tim D. Godbee

Introduction

Cybercrime and corruption have created significant problems around the world. As technology changes, cybercriminals find new ways to cause harm and make money. According to Cybersecurity Ventures, the global cost of cybercrime was expected to reach USD 9.5 trillion in 2024.[1] If cybercrime was measured as a country, it would currently have the third-largest economy in the world.[2] Many countries do not have strong rules to stop these crimes, leaving them open to attacks. Canada, Russia, the United States, and Malaysia all invested in resources for cybersecurity protections due to the large number of attacks they experience.[3] Governments are not technologically prepared to handle these new cyber threats. Some countries in the Global South do not have the resources or workers to build cybersecurity systems. This makes them easy targets for cybercrime and increased corruption, which hurts governments and the economy. A strong international effort is required to uphold accountability in our growing digital era. Targeting supply chains was an increasing concern in 2024, when hackers used third-party vulnerabilities to compromise many companies at once.[4] Data theft, service interruptions, and financial losses were caused by ransomware organizations like Termite and Salt Typhoon. No organization is immune to the tactics of threat actors in the world of cybercrime. This is shown by the fact that even prominent government agencies, such as the U.S. Securities and Exchange Commission (SEC), were the targets of credential theft and SIM-swapping attacks.[5]

This update paper will discuss a series of recent attacks in 2024 within the realm of cryptocurrency and media platforms. In 2024, healthcare institutions and social media were two of the main targets of cybercrime. Major corporations like AT&T and Ticketmaster have also suffered major attacks on users' personal data.[6] Cybercriminals targeted weaknesses in a variety of businesses in 2024, posing several serious cybersecurity issues. The threats range from high-level ransomware attacks to the creation of advanced supply chain and phishing tactics. Delegates of the United Nations Convention Against Corruption (UNCAC) must debate the best course of action to counter the rise of these new and improved cybercrime tactics. As a committee, delegates must investigate solutions that will decrease the cyberattacks around the world. As our society becomes more and more reliant on the internet, it is important that we take steps to make sure people do not use it for crime. However, many companies and organizations also need to work together on making sure these types of attacks do not happen. Delegates will need to look at both government-led and private sector-led solutions. Doing so will help governments and organizations be able to take on this issue where they have difficulty directly enforcing.

Recent Global Cyberattacks

There have been several recent cases of hackers in the cryptocurrency sector. Recently, cryptocurrencies have become more popular and valuable. What makes cryptocurrency a big target for hackers is their blockchain technology. The blockchain technology helps disguise the origin and destination of transactions. As a result, most of the cryptocurrency that is used in transactions or stolen is untraceable. To get cryptocurrency, criminals have looked at ways to steal them from where they are traded. Cryptocurrency

1 Steve Morgan, "Boardroom Cybersecurity Report 2024," Secureworks, November 5, 2024, https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024#.
2 Morgan, "Boardroom Cybersecurity Report 2024."
3 "BlackBerry Quarterly Global Threat Report," www.blackberry.com (BlackBerry, November 1, 2024), https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report.
4 "Cybersecurity in 2025: A Look Back at 2024'S Biggest Cyber Attacks & Lessons for the Future - SOCRadar® Cyber Intelligence Inc.," SOCRadar Your Eyes Beyond (SOCRadar Cyber Intelligence Inc., January 6, 2025), https://socradar.io/cybersecurity-in-2025-2024s-biggest-cyber-attacks-lessons-for-future/.
5 "Cybersecurity in 2025."
6 "Cybersecurity in 2025."

is often traded on digital marketplaces called exchanges. These exchanges help manage and carry out transactions and trades of cryptocurrency between buyers and sellers. This is a rapidly growing industry which means that many exchanges are not well protected by cybersecurity measures. This has led to many high-level scandals of hackers stealing cryptocurrency from exchanges.

In September 2024, Indodax was hacked and lost over USD 22 million.[7] Indodax happens to be Indonesia's largest cryptocurrency exchange. The company temporarily shut down to address the issue and promised to refund around 6.8 million users.[8] This incident revealed a large flaw in mainstream cryptocurrency platforms. They were decidedly not immune to cybercrime and the influence of hackers. In October 2024, North Korean hackers successfully attacked the DeFi project Radiant Capital and stole USD 50 million[9] through fake transactions using malware-infected devices. The operation was highly complex, using the new skills of state-sponsored cyber criminals. The bad actors, also known as the UNC4736 group and operating as AppleJeus or Citrine Sleet, performed their attack in multiple steps using a normal-looking PDF file. By communicating through Telegram, the hackers were able to stay hidden since September 14. In September 2024, the Singaporean-based cryptocurrency exchange BingX suffered a major hack. Over USD 50 million in assets were stolen.[10] The attack targeted digital "hot" wallets across several blockchain networks. Including Ethereum, Binance Smart Chain, Base, Optimism, Polygon, Arbitrum, and Avalanche.[11] BingX promised to fully compensate users. They noted most funds remained safe in "cold" wallets. After the breach, BingX began an investigation with cybersecurity experts. They also partnered with blockchain security firms like SlowMist and Chainalysis to study the attack.[12] While the number of users affected was not stated, the exchange affected millions of customers worldwide. BingX recovered about USD 10 million through freezing stolen assets.

North Korean hackers have become very active in cryptocurrency-related cybercrime. Reports from December 2024 claimed that North Korean hackers stole around USD 1.34 billion. This makes up around 60 percent of all crypto stolen in 2024.[13] The money was used to finance ballistic missile and nuclear programs throughout the country. This sets off alarms and creates more problems for international security. North Korea has a large number of cybercrime hackers, falling just behind Russia and Ukraine.[14] A large portion of cyber operations in North Korea produce foreign currency income, which allow North Korea to fund these weapons programs.[15] Among the increasing risks, the European Securities and Markets Authority (ESMA) has urged strong cybersecurity measures for digital asset firms.[16] These firms include Byte Federal and WazirX, which have lost millions of cryptocurrency.[17] ESMA specifically urged the inclusion of third-party audits of cyber defenses for the new cryptocurrency laws in the European Union. This effort aims to provide more protection to consumers from the threat of a cyber-attack. The rise in cryptocurrency threats has led to

7 "Largest Crypto Exchange in Indonesia Pledges to Reimburse Users after $22 Million Theft," Cyber Security News | The Record, September 13, 2024, therecord.media/indodax-crypto-exchange-pledges-to-reimburse-after-theft.
8 "Indonesian Crypto Exchange Indodax Allegedly Hacked, but Claims User Funds Are Safe," The Hindu, September 12, 2024, www.thehindu.com/sci-tech/technology/indonesian-crypto-exchange-indodax-allegedly-hacked-but-claims-user-funds-are-safe/article68633519.ece.
9 Ionut Arghire, "$50 Million Radiant Capital Heist Blamed on North Korean Hackers," SecurityWeek, December 10, 2024, www.securityweek.com/radiant-capital-50-million-heist-blamed-on-north-korean-hackers/.
10 Dishita Malvania, et al, "Singapore's BINGX Exchange Suffers over $50 Million Hack," The Crypto Times, September 20, 2024, www.cryptotimes.io/2024/09/20/singapores-bingx-crypto-exchange-suffers-50-million-hack/.
11 "Crypto Security Incidents September 2024," Nominis, December 2, 2024, www.nominis.io/post/crypto-security-incidents-september-2024.
12 Kyle Baird, "BingX Dismisses $45m Hack Cover-up Claims, Restores Deposits and Withdrawals," DL News, September 22, 2024, www.dlnews.com/articles/markets/bingx-dismiss-hack-cover-up-restore-deposit-withdrawal/.
13 João da Silva, "North Korean Hackers Stole $1.3bn in Crypto This Year, Report Says," BBC News, December 20, 2024. www.bbc.com/news/articles/cwy3dz0614jo.
14 "Where Do Cyber Threats Come From?" Website News RSS, www.sciencespo.fr/centre-etudes-europeennes/en/news/where-do-cyber-threats-come-from/.
15 Sebastian Garcia, et al, "Facing the North Korean Cyber Threat: United States-South Korea Coordination in Cyberspace," Wilson Center, www.wilsoncenter.org/blog-post/facing-north-korean-cyber-threat-united-states-south-korea-coordination-cyberspace.
16 JD Supra, "EU Adopts ESG Ratings Regulation: Strengthening Transparency and Reliability in Sustainable Finance," www.jdsupra.com/legalnews/eu-adopts-esg-ratings-regulation-2919006/.
17 "Indian Crypto Platform Wazirx Confirms $230 Million Stolen during Cyberattack," Cyber Security News | The Record, 18 July 2024, therecord.media/wazirx-crypto-platform-confirms-230-million-heist.

more interest in government regulation.[18] These threats could have a great impact on global economies and policies. Thus, international cooperation is key to creating cybersecurity regulations.

Cyber-attacks have also affected people by exposing their information. These attacks have targeted platforms like Instagram, VK (a Russian social media platform), or the Internet Archive. These sites have seen millions of users worldwide lose personal data to hackers. This is primarily because governments have been slow with combating cyberattacks. There has not been significant regulation on making sure websites and companies protect user data. Additionally, no widely adopted law sets a specific minimum of protection that is expected of user data. As a result, many websites and internet companies have allowed their cybersecurity to become a second thought. Only large corporations have been able to invest in building up their cyber protections. Without proper regulations, hackers will keep being a threat to personal information worldwide.

In September 2024, VK, Russia's largest social networking website, suffered a large data leak.[19] A hacker by the name "Hikkl-Chan" had leaked the personal information of over 390 million VK users on a cybercrime forum.[20] Over 27 GB of leaked data included users' full names, city, country, and profile image URLS. However, the breach did not compromise any phone numbers or passwords. He described the data as a "second order" breach, since it had been sourced indirectly through the compromise of a third party rather than directly from VK's servers.[21] A second-order breach means that the data is accessed indirectly by a third party that has access to information of the primary organization without directly attacking the primary organization itself. A first-order breach, in contrast, is a direct breach where attackers compromise an organization's systems to steal data. For example, if hackers had directly breached VK's servers to obtain user information, this would be considered a first-order breach.[22] VK responded quickly and securely to the incident. The company denied any security breach, stating, "we can confirm that there have been no security breaches of any kind, including those involving personal information. VK user data is securely protected, and the content in question was collected solely from publicly available sources. This information does not contain any confidential data but consists of details that our users have voluntarily shared on their profiles".[23]

In October 2024, Internet Archive, known for its "Wayback Machine," suffered a data breach affecting 31 million users.[24] Hackers stole an authentication database with email addresses, usernames, and passwords. The breach came to public eye when a JavaScript alert showed up on a website owned by Archive asking users to check from compromised data using "Have I Been Pwned". Since this data breach, the Internet Archive has moved to contain the breach. In addition, several companies have begun to take similar measures for cybersecurity regulations. Companies are following new cybersecurity rules starting in 2024.[25] These require major incidents to be reported within four business days.[26] Cybersecurity has become a key part of corporate planning. Businesses are now managing risks and sharing updates in their annual reports.

Many companies are including third-party vendors in their cybersecurity policies. Regular training for employees, company testing, and systems to monitor threats in real-time

18 "Cryptocurrency – Regulatory Crackdowns and Inflation Risks," Infortal, June 27, 2023, infortal.com/cryptocurrency-crackdowns-and-inflation-risks/.
19 SC Staff, "Over 390m Impacted by Russian Social Network Breach," SC Media, October 9, 2024, www.scworld.com/brief/over-390m-impacted-by-russian-social-network-breach.
20 Mitchell Langley, and Gabby Lee, "This Week in Cybersecurity: 02nd September to 06th September, VK Data Leak Exposes 390 Million Users," Daily Security Review, November 21, 2024, dailysecurityreview.com/cyber-security/this-week-in-cybersecurity-02nd-september-to-06th-september-vk-data-leak-exposes-390-million-users/.
21 "Third-Party Data Breaches: What You Need to Know," *Prevalent*, www.prevalent.net/blog/third-party-data-breaches/.
22 "Third-Party Data Breaches: What You Need to Know," *Prevalent*,
23 WAQAS, "Hacker Leaks Data of 390 Million Users from VK, a Russian Social Network," Hackread - Latest Cybersecurity, Tech, Crypto & Hacking News, September 3, 2024, https://hackread.com/hacker-leaks-data-of-vk-users-russian-social-network/.
24 Abrams Lawrence, "Internet Archive Hacked, Data Breach Impacts 31 Million Users," BleepingComputer, October 20, 2024, www.bleepingcomputer.com/news/security/internet-archive-hacked-data-breach-impacts-31-million-users/.
25 "SEC Cybersecurity Rules 2024: Navigating New Regulations and Compliance Strategies," Metomic, www.metomic.io/resource-centre/sec-cybersecurity-rules.
26 David Jones, "In 2024, the Cybersecurity Industry Awaits More Regulation - and Enforcement," Cybersecurity Dive, January 31, 2024, www.cybersecuritydive.com/news/cyber-enforcement-regulation/706141/.

are now common. Companies are also looking at how these rules affect their work and are making plans to follow them. There have been several instances where main social media services have been affected. Reports came in December 2024 that data on around 500 million Instagram users had been stolen by hackers.[27] This is an instance of data scraping, which is the collection of public information, and raises concerns about privacy. Scraped data often is used with malicious intentions, such as phishing attacks and identity theft. The absence of privacy regulations has allowed for cybercrimes to continue throughout the globe.

After the data scraping, global privacy regulators acted. In January 2025, the United States began the 'U.S. Cyber trust Mark' program. [28] This program helps people find products that meet cybersecurity standards. Manufacturers can test their products using the rules from the National Institute of Standards and Technology. Americans can now safely use products knowing that they are cybersecure.

United Nations Cybercrime Convention

After two years of talks, the United Nations (UN) agreed to hold a conference dealing with cross-border cybercrime.[29] In August 2024, the UN Cybercrime Convention was finalized after three years of work by the Ad Hoc Committee. This is a major step in fighting cybercrime globally. The convention emphasizes the need for international cooperation in fighting online threats.[30] As the first global anti-crime treaty in twenty years, the approval of this agreement is historical in international cooperation. It targets important crimes like money laundering, online scams, and online child sexual abuse.[31] It has also become one of the first overarching agreements that have focused on cybersecurity. The convention has been finalized this past December and will now be adopted by the United Nations and ratified by its individual member states in 2025. After member states become signatories, each would need to go through its own internal ratification process. This means, each country must go through its own process of legally accepting to abide by the convention. In order for the Cybercrime Convention to go into effect, 40 countries need to ratify the convention.[32] Once the treaty passes the 40-member state ratification mark, countries can still ratify the treaty. However, this means that the treaty now becomes part of international agreements. Countries that ratify are expected to implement all parts of the convention. Many countries are expected to incorporate some of the content of the treaty into their national laws. The effectiveness of the convention will be tested in how the UN chooses to balance security with human rights protections.

One of the key points in the convention is the need for electronic evidence sharing between countries to prosecute cybercrime. The convention, for this reason, defined the process of collection and preservation of electronic evidence as an effective means to prosecute cyber criminals.[33] This helps combat cyber criminals since it unifies the world under a general standard on how to gather evidence on prosecuting criminals. Now, countries can look at other countries with similar legal systems to see how the criminal evidence can be used in a trial. It also makes it easier for countries to share information if the same cybercriminal attacks both countries. The convention also focused on the importance of cooperation to ensure all countries build stronger cybersecurity systems. The capacity-building programs would ensure that all member

27 "Almost 500 Million Instagram Users Had Their Data Scraped, Hackers Claim," Cybernews. cybernews.com/news/instagram-user-data-scraping/.
28 "White House Launches 'U.S. Cyber Trust Mark', Providing American Consumers an Easy Label to See If Connected Devices Are Cybersecure," The White House, January 7, 2025, www.whitehouse.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/.
29 "United Nations Convention against Cybercrime," United Nations : Office on Drugs and Crime, www.unodc.org/unodc/cybercrime/convention/home.html.
30 "United Nations: Member States Finalize a New Cybercrime Convention," United Nations: Office on Drugs and Crime, www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html.
31 "UN General Assembly Adopts Landmark Convention on Cybercrime," United Nations : Office on Drugs and Crime (UNODC, December 24, 2024), https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html
32 "UN General Assembly Adopts Landmark Convention on Cybercrime."
33 Anja P. Jakobi and Lena Herbst, "Between a Rock and a Hard Place: The UN Cybercrime Convention," PRIF BLOG, December 9, 2024, blog.prif.org/2024/12/09/between-a-rock-and-a-hard-place-the-un-cybercrime-convention/.

General Assembly of the UN - Foundations of the Cybersecurity Conference

Credit: azugaldia

states are better equipped with the necessary tools and skills to respond to cyber threats effectively.[34] This means pushing each country to have its own dedicated agency focused on combating cyber criminals. By doing so, countries will be able to develop their own methods for combating cyber criminals. A dedicated agency to fight cybercrime will allow for more resources to be focused on this effort. It would ultimately be more coordinated and effective at targeting criminals.

Capacity building is important because of the large gaps in cybersecurity capabilities between countries, especially between developed and developing nations. Many developing countries lack the tools, skills, and funding to tackle cyber risks. The ITU Global Cybersecurity Index shows that Least Developed Countries (LDCs) are improving slowly. Most of the LDCs have weaker defenses and outdated systems. To address these gaps between countries, several international programs are helping countries improve their cybersecurity capabilities. The World Bank's Cybersecurity Multi-Donor Trust Fund supports global cybersecurity development. The World Bank recognizes the importance of knowledge sharing and country assessments.[35] Furthermore, the Carnegie Endowment for International Peace's FinCyber project suggests creating a global foundation to strengthen cybersecurity and support financial inclusion, especially in developing countries. The United States and other countries have emphasized the importance of the convention as a tool in the global fight against cybercrime. U.S. officials have specifically emphasized the need to work with allies to positively shape the treaty and mitigate risks of some of the provisions. However, digital rights groups have voiced concerns about the convention. They pose scenarios like authoritarian regimes misusing the convention. For instance, there are fears that some provisions could justify surveillance by disguising it as combating cybercrime.[36] The convention has several flaws: vague and expansive wording that might hurt valid security research, weak human rights protections, abuse of the convention to target dissidents, worries about data privacy violations, and insufficient safeguards for ethical hacking.[37]

The convention also formalized the definition of various cybercrimes. Under the criminalization chapters of the convention, the treaty mandates that certain types of illegal hacking were to be criminalized.[38] This includes illegal

34 Jakobi and Herbst, "Between a Rock and a Hard Place."
35 "Cybersecurity Multi-Donor Trust Fund," World Bank. www.worldbank.org/en/programs/cybersecurity-trust-fund.
36 "The Final Call: UN Member States Adopt a New Cybercrime Treaty," Global Initiative, September 12, 2024, globalinitiative.net/analysis/the-final-call-un-member-states-adopt-a-new-cybercrime-treaty/.
37 "UN General Assembly Adopts Landmark Convention on Cybercrime."
38 United Nations Office on Drugs and Crime, "Chapters of the United Nations Convention against Cybercrime," United Nations: Office on Drugs and Crime, accessed February 9, 2025, https://www.unodc.org/unodc/en/cybercrime/convention/chapters.html.

interference, access, and misuse of electronic devices. While broad, it sets a baseline for how to define cybercrimes. With this wording adopted, there would be a common definition to make prosecutions around the world become more consistent. The new legal definitions also included criminalizing something called "cyber-enabled crimes".[39] These types of crimes are often regular crimes that can be committed or assisted by the internet. These crimes include forgery, theft, money laundering, and blackmailing. By defining these crimes, the convention broadened the scope of cybercrimes. Doing so has expanded the scope of the treaty to also apply to use the internet to conduct crime. It has also pushed countries to expand enforcement to protect those who may have been affected by cyber-enabled crimes. This paves the way to help give them some much needed justice and support. Children are especially noted as a group that needs to be protected from online exploitation. Overall, these legal definitions are necessary and beneficial to coordinating efforts to counter cybercrime. By harmonizing legal definitions, there is a basic standard to consider when it comes to prosecuting cyber criminals. Some cyber criminals operate across borders and target multiple countries. Harmonized legal language allows countries to coordinate on evidence sharing and build a case to prosecute the criminal.

Article 6.2 of the convention states that "nothing in this Convention shall be interpreted as permitting the suppression of human rights or fundamental freedoms."[40] Article 6.2 is intended to stop the convention from expressly permitting the use of its provisions and powers to repress human rights, particularly among governments that have not ratified pertinent human rights treaties. In principle, this is a necessary safeguard for the convention. The convention does not, however, include certain protections that are required to adequately uphold human rights. In fact, several governments still maintain that this clause gives considerable weight to national preferences and sovereignty. One country even contends that Article 6.2 places no duties on countries that have not ratified a human rights treaty on their own. Therefore, those that currently exhibit the least observance of human rights are already able to abuse the treaty in order to further repress human rights.[41] This remains a core weakness of the convention and would need to be further clarified and defined by subsequent meetings of the parties of the treaty. However, the treaty overall still makes a significant contribution towards addressing cybercrime. More needs to be done and cybercrimes are constantly evolving. As technology changes, the convention would need to be updated with new technological developments. The need for future updates led to the treaty outlining an implementation mechanism called the Conference of the Parties to the Convention.[42] This conference is the main body that meets on a regular basis to discuss how the treaty is being implemented. Additionally, the body looks at ways to update the treaty if it needs to be. This ensures that the treaty has a way to be updated when new technological developments happen. However, the slower pace of the body compared to the fast development of technology will test that assumption.

Conclusion

The world of cybercrime evolves quickly. Complex and connected cyber threats demand a united international response. Large breaches in the cryptocurrency and social media sectors shows that no corporation or country is safe from advanced cybercriminals. These incidents reveal vulnerabilities in both advanced and developing countries. This especially highlights the need for strong cybersecurity frameworks, global cooperation, and capability building. There is a lot that needs to be done to bring the entire world to the same level of security as some of the most developed countries. However, steps can be taken to set a bare minimum level of enforcement and monitoring.

To achieve that, the UN Cybercrime Convention has been created to establish the basic framework for cybercrime enforcement. It is a key step toward fostering global collaboration. One of the core parts of this treaty is the

39 United Nations Office on Drugs and Crime, "Chapters of the United Nations Convention against Cybercrime,"
40 Katitza Rodriguez, "The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy," Just Security, August 27, 2024, https://www.justsecurity.org/98738/cybercrime-convention-human-rights/.
41 Rodriguez, "The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy."
42 United Nations Office on Drugs and Crime, "Chapters of the United Nations Convention against Cybercrime,"

establishment of a common standard for cybercrimes. It creates a basis for countries to follow. Additionally, countries can extend a basic level of protection for its citizens and businesses. Enabling records sharing and reducing cybersecurity gaps are among the first steps for a solid framework. However, its success depends on balancing security with digital rights to avoid misuse from authoritarian regimes. Governments, businesses, and international bodies must adopt the convention but also invest on technological improvements, regulatory measures, and public awareness. By doing so, the international community can protect economies, safeguard privacy, and create a secure digital future.

Delegates must consider many risks and challenges when crafting their resolutions. The privacy of a country's citizens can be easily infringed upon for the sake of enforcement. This same ethical question was asked in the United States when its government was found to be spying on people's communications. Additionally, technology is still developing at a rapid pace. New technology like artificial intelligence and advanced computing has increased the risk of new ways to commit cybercrimes. The parties within the treaty now need to create policies and ways to anticipate these technological advancements. Additionally, standards will need to be updated at a quick pace to stay updated with how cybercrime evolves. However, it is up to the parties of the treaty to decide how quickly they want to update it. Lastly, it is important that delegates consider how to ensure the wide adoption of the treaty. Enforcement is only possible if most countries have a similar level of commitment to the treaty. If some countries fail to implement the treaty, then this opens more opportunities for criminals to exploit weaknesses. Delegates must find a way to balance all these issues and create encompassing resolutions that aim to keep pace with the changes of cybersecurity.

Works Cited

Topic A

UN Sources

United Nations. "Amid campus crackdowns, Gaza war triggers freedom of expression crisis." April 25, 2024. https://news.un.org/en/story/2024/04/1149001.

United Nations. "At least 68 journalist killings in 2024, UNESCO reports." Last edited December 12, 2024. https://news.un.org/en/story/2024/12/1158141.

United Nations. "Global threats to freedom of expression arising from the conflict in Gaza – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan (A/79/319)." August 23, 2024. https://www.un.org/unispal/document/report-special-rapporteur-23aug24/#_ftn25.

United Nations. "International Day to End Impunity for Crimes against Journalists, 2 November." November, 2024. https://www.un.org/en/observances/end-impunity-crimes-against-journalists

Non-UN Sources

A. Hussein, Mohamed and Hanna Duggal. "Know their names: Palestinian journalists killed by Israel in Gaza." *Al Jazeera*. December 31, 2024. https://www.aljazeera.com/features/longform/2024/12/31/know-their-names-the-palestinian-journalists-killed-by-israel-in-gaza.

Amnesty International. "Journalists are not targets: Israel's shutdown of Al Jazeera's Ramallah office threatens press freedom." September 25, 2024. https://www.amnesty.org.au/israels-shutdown-of-al-jazeeras-ramallah-office/.

Cambridge. "Fake News," Accessed January 10, 2025. https://dictionary.cambridge.org/dictionary/english/fake-news.

Center for News, Technology & Innovation. "Journalists & Cyber Threats." Last updated October 11, 2024. https://innovating.news/article/journalists-cyber-threats/.

Committee to Protect Journalists. "Explore CPJ's Database of Attacks on the Press." Accessed January, 2025. https://cpj.org/data/killed/2024/?status=Killed&motiveConfirmed%5B%5D=Confirmed&type%5B%5D=Journalist&start_year=2024&end_year=2024&group_by=location.

Committee to Protect Journalists. "Journalist jailings near record high in 2024 as crackdown on press freedom grows." Last edited January 16, 2025. https://cpj.org/2025/01/journalist-jailings-near-record-high-in-2024-as-crackdown-on-press-freedom-grows/.

Crinnion, Frances, Natalia Yannopoulou, and Saurabh Bhattacharya. "Chapter eight - Fake news inside ideological social media echo chambers." *Handbook of Social Media in Education Consumer Behavior and Politics* 1 (2024): 139-187. https://doi.org/10.1016/B978-0-323-90237-3.00008-4.

Desmarais, Anna. "Which countries fared best against disinformation during major 2024 election year?" *Euro News*. January 3, 2025. https://www.euronews.com/next/2025/01/03/which-countries-fared-best-against-disinformation-during-major-2024-election-year.

Dreier RoundTable - Claremont McKenna College. "State of the News Media 2024: It's Bad." Last edited October 24, 2024. https://drt.cmc.edu/2024/10/24/state-of-the-news-media-2024-its-bad/.

Folk, Zachary. "College Protesters Want Divestment From Israel: Here's Why That's So Difficult." *Forbes*. May 15, 2024. https://www.forbes.com/sites/zacharyfolk/2024/05/15/college-protesters-want-divestment-from-israel-heres-why-thats-so-difficult/.

International Federation of Journalists. "Israel: New law allows government to temporarily shut down Al Jazeera." April 2,

2024. https://www.ifj.org/media-centre/news/detail/category/middle-east-arab-world/article/israel-new-law-allows-government-to-temporarily-shut-down-al-jazeera.

Khalil, Shaimaa. "Al Jazeera bureau chief's son Hamza al-Dahdouh among journalists killed in Gaza." *BBC*. January, 2024. https://www.bbc.com/news/world-middle-east-67905566.

Krämer, Tania. "Israel's media crackdown is bad news for press freedom." *DW*. Last edited November 28, 2024. https://www.dw.com/en/israels-media-crackdown-is-bad-news-for-press-freedom/a-70894536.

Kuttab, Daoud. "Silence on Israel's massacres of journalists is dangerous to all." *Al Jazeera*. January 4, 2025. https://www.aljazeera.com/opinions/2025/1/4/silence-on-israels-massacres-of-journalists-is-dangerous-to-all.

Maclure, Jocelyn. "Overcoming online echo chambers requires institutional and individual commitment." *Policy Options - Institute for Research on Public Policy*. December 19, 2024. https://policyoptions.irpp.org/magazines/december-2024/online-echo-chambers/.

McCarthy, Catherine. "Political echo chambers are dangerous to democracy." *The Miscellany News*. November 13, 2024. https://miscellanynews.org/2024/11/13/opinions/political-echo-chambers-are-dangerous-to-democracy/.

Mehmood, Nazish. "The Global Crisis of Bullshit Culture and Media Manipulation." *Modern Diplomacy*. January 3, 2025. moderndiplomacy.eu/2025/01/03/the-global-crisis-of-bullshit-culture-and-media-manipulation/.

Musk's Political Posts: How Elon Musk's political posts amass more views than all U.S. political campaign ads on X's disclosure dataset. *London: Center for Countering Digital Hate*. November 11, 2024. https://counterhate.com/research/musk-political-posts-x/.

Newman, Nic. "Resumen Ejecutivo y Hallazgos Clave Del Informe de 2024." *Reuters Institute for the Study of Journalism*. June 17, 2024. https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2024/dnr-resumen-ejecutivo.

Nieman Lab. "Predictions for Journalism, 2024." Accessed January, 2025. https://www.niemanlab.org/2023/12/investigative-reporting-will-experiment-with-new-forms/.

Pearn Kandola. "A Summary Of Our Latest Research: Antisemitism and Islamophobia In The Workplace." October 1, 2024. https://pearnkandola.com/insights/a-summary-of-our-latest-research-antisemitism-and-islamophobia-in-the-workplace.

Purdue, Matt. "The rise of independent journalists and tips for engaging with them." *PR Daily*. Last edited November 11, 2024. https://www.prdaily.com/the-rise-of-independent-journalists-and-tips-for-engaging-with-them/.

Reporters Without Borders. "RSF files third complaint with ICC about Israeli war crimes against journalists in Gaza." May, 2024. https://rsf.org/en/rsf-files-third-complaint-icc-about-israeli-war-crimes-against-journalists-gaza.

Reporters Without Borders. "RSF's 2024 Round-up: journalism suffers exorbitant human cost due to conflicts and repressive regimes." Accessed January, 2025. https://rsf.org/en/rsf-s-2024-round-journalism-suffers-exorbitant-human-cost-due-conflicts-and-repressive-regimes.

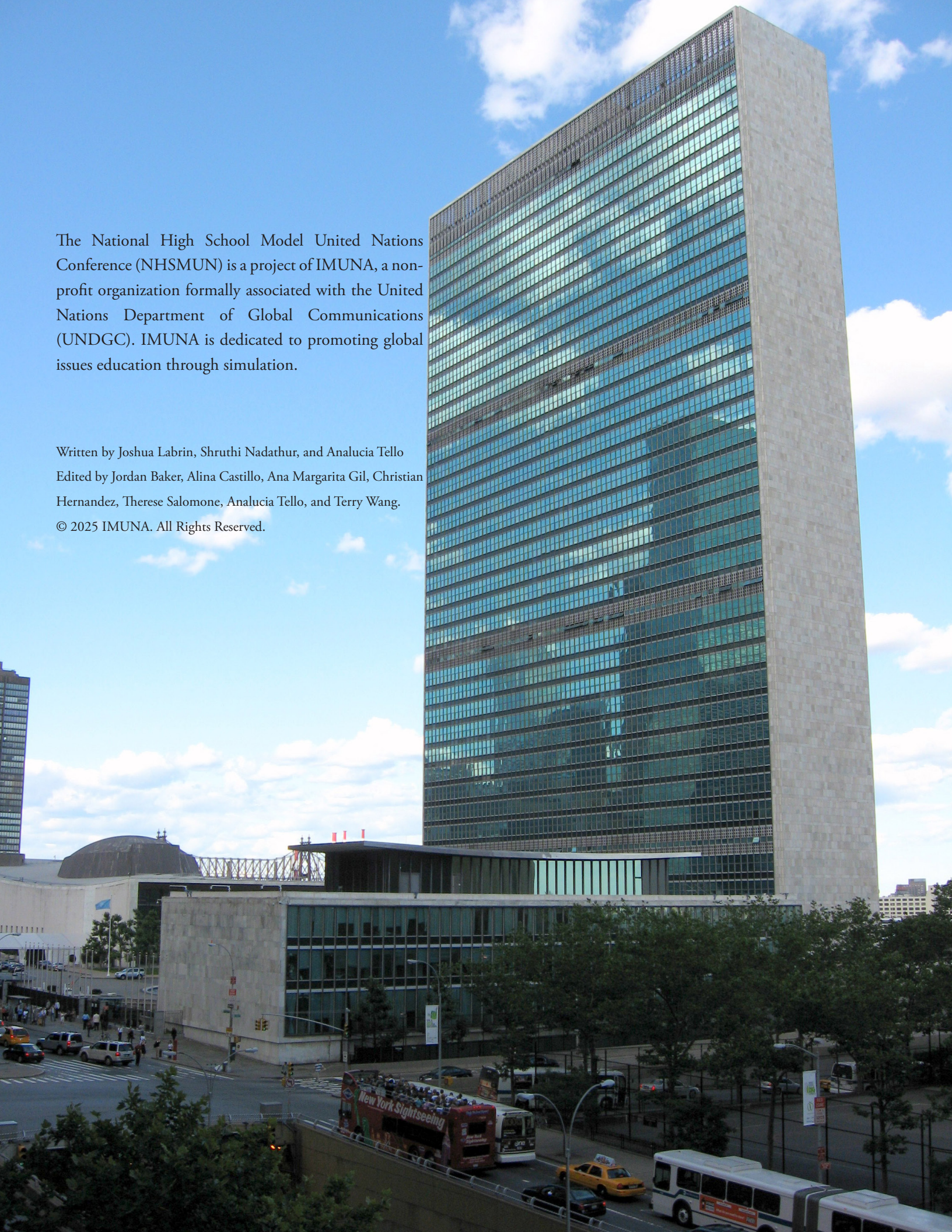
Rubin, C.M. "Combating Misinformation: AI, Media Literacy, And Psychological Resilience For Business Leaders And Educators." *Forbes*. Last updated December 2, 2024. https://www.forbes.com/sites/cathyrubin/2024/12/02/combatting-misinformation-ai-media-literacy-and-psychological-resilience-for-business-leaders-and-educators/.

Sahoo, Niranjan. "How 2024's elections redefined political landscapes across the world." *Democracy Without Borders*. January 15, 2025. https://www.democracywithoutborders.org/34695/how-2024s-elections-redefined-political-landscapes-across-the-world/.

Steffen, Sarah. "Fact check: Disinformation's impact on the US election." *DW*. November 7, 2024. https://www.dw.com/en/fact-check-what-role-did-disinformation-play-in-the-us-election/a-70729575.

Transparency International. "Corruption Perceptions Index." Accessed January, 2025. https://www.transparency.org/en/cpi/2023?gad_source=1&gclid=Cj0KCQiAhbi8BhDIARIsAJLOluek_

iZptCheNpRJQV0qMCmrVX8cy2bdy32BWhVnB9YmMVueabkZMYsaAun5EALw_wcB.



The National High School Model United Nations Conference (NHSMUN) is a project of IMUNA, a non-profit organization formally associated with the United Nations Department of Global Communications (UNDGC). IMUNA is dedicated to promoting global issues education through simulation.

Written by Joshua Labrin, Shruthi Nadathur, and Analucia Tello
Edited by Jordan Baker, Alina Castillo, Ana Margarita Gil, Christian Hernandez, Therese Salomone, Analucia Tello, and Terry Wang.