NHSMUN

National High School Model United Nations

2023

BACKGROUND GUIDE: UNCAC

Topic A: Corruption and Press Freedom

Topic B: Cybercrime and Corruption

NHSMUN
National High School Model United Nations

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

Hello Delegates!

My name is Renan Rocha, and I am a Senior at American University, currently studying political science and business & entertainment while focusing on the music industry. I am from NYC, the exact place where this conference is being held! I grew up in Queens, New York, and I am currently into things that have to do with politics and music. Fun fact, I spent seven years of my life while in high school and middle school playing the cello.

This is my second year doing NHSMUN. Last year, I was an Assistant Director for DISEC in the first session. I have been doing Model UN since my Sophomore year at American University. I am currently on the collegiate team, so I am doing exactly what all of you are doing, just while in college and competing more competitively. I have always done some type of debate activity while in high school. My high school did not have a Model UN team, so I was on the Speech and Debate team for all four years. I did Extemporaneous Speaking for most of my four years, and I dabbled in Student Congress during my Senior year. I've always had a sense of a debate edge when it comes to my character, and that is why I am extremely excited to chair this committee session for you all!

Being able to write about the topic of Cybercrimes and Cybersecurity has been such a pleasure, and I am extremely grateful and excited to hear all of what you have to say when it comes to all things Cybersecurity. I picked this topic because of how relevant it is to the world we live in today. Technology has changed over the past decades, more people have more access to the internet, and more people are taking advantage of others when it comes to anything digital. The awareness, and the topic itself, bring to light issues that many politicians, presidents, and leaders are struggling to deal with today.

While I am not expecting you all to have the answers to the questions presented, I want you all to think outside the box when it comes to certain solutions, resolutions, and connections that you all can make for combating cyber crimes and protecting cyber security. Do your research and come prepared to ask things that your country wants. Research on this topic is extremely important because the more information and knowledge you have about certain topics, the more ideas you can create for yourselves when it comes to solving these issues.

Regardless of that, I want everyone to have fun and remember that this is a learning experience for all. This committee is meant to teach new ways of thinking and how to become diplomatic with each other and create meaningful connections moving forward. You all are going to do amazing, and I cannot wait to see all of you in NYC! Be excited and curious. I wish you all the best of luck, and I will see all of you soon.

All the best,

Renan Rocha
United Nations Convention Against Corruption
Session I
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,

My name is Cayetana Rodriguez, and I am thrilled to welcome you to the UN Convention Against Corruption (UNCAC) Committee for the 2023 National High School Model United Nations Conference! Alongside my Co-Director, Renan Rocha, we are excited to see what delegates bring to the table to have fruitful discussions and conversations.

My Model UN journey has been an essential part of my life for the last four years. I was Head Delegate for my high school team in 2020 and Secretary-General for my high school's Model UN conference. I came to NHSMUN 2020 as a delegate. After having one of the most memorable experiences, I decided to come back and provide delegates with the same experience and opportunities I gained as a delegate. Last year, I was the Assistant Director for the United Nations Commission on Narcotic Drugs (CND). I truly enjoyed being an AD and being a support for delegates, which is why I decided to be a Committee Director for NHSMUN 2023. Model UN has helped me gain self-confidence, improved my English skills, allowed me to meet friends from all over the world, and made me aware of how ongoing world issues impact our lives.

Currently, I am a sophomore at Clark University, where I am double majoring in management and political science. Some of my professional interests include law, social impact, corporate social responsibility, and environmental, social, and corporate governance. I enjoy entrepreneurship, marketing, social media management, and higher education as well. I am involved in the Clark Model UN Club as Director-General on campus for the high school conference. Furthermore, I have two jobs. I work as a Peer Mentor for the first-year class and as a Student Ambassador for Clark Undergraduate Admissions (as well as for Clark Admissions' marketing team!). I love listening to Broadway soundtracks, dancing, singing, and exploring new places in my free time.

I am eager to hear your proposals for both Topic A, "Press and Corruption," and Topic B, "Cybercrime and Corruption." Our selected topics touch on important issues such as government transparency and regulations, which are extremely important when eliminating corruption. Corruption is a considerable barrier to democracy, and I am excited to see your actions to preserve it around the globe.

I cannot wait to hear your ideas and meet you in March. I hope this Background Guide serves as a map to navigate these crucial topics, but if you have any questions or concerns, do not hesitate to contact Renan or me.

Sincerely,

Cayetana Rodriguez
United Nations Convention Against Corruption
Session II
nhsmun.uncac@imuna.org

Table of Contents

A Note on the NHSMUN Difference

Esteemed Faculty and Delegates,

Welcome to NHSMUN 2023! We are Ming-May Hu and Ana Margarita Gil, and we are this year's Secretary-General and Director-General. Thank you for choosing to attend NHSMUN, the world's largest and most diverse Model United Nations conference for secondary school students. We are thrilled to welcome you to New York City in March!

As a space for collaboration, consensus, and compromise, NHSMUN strives to transform today's brightest thinkers into tomorrow's leaders. Our organization provides a uniquely tailored experience for all in attendance through innovative and accessible programming. We believe that an emphasis on education through simulation is paramount to the Model UN experience, and this idea permeates throughout NHSMUN.

Realism and accuracy: Although a perfect simulation of the UN is never possible, we believe that one of the core educational responsibilities of MUN conferences is to educate students about how the UN System works. Each NHSMUN committee is a simulation of a real deliberative body so that delegates can research what their country has said in the committee. Our topics are chosen from the issues currently on the agenda of that committee (except historical committees, which take topics from the appropriate time period). This creates incredible opportunities for our delegates to conduct first-hand research by reading the actual statements their country has made and the resolutions they have supported. We also strive to invite real UN, NGO, and field experts into each committee through our committee speakers program. Moreover, we arrange meetings between students and the actual UN Permanent Mission of the country they are representing. No other conference goes so far to deeply immerse students into the UN System.

Educational emphasis, even for awards: At the heart of NHSMUN lies education and compromise. Part of what makes NHSMUN so special is its diverse delegate base. As such, when NHSMUN distributes awards, we de-emphasize their importance in comparison to the educational value of Model UN as an activity. NHSMUN seeks to reward students who excel in the arts of compromise and diplomacy. More importantly, we seek to develop an environment in which delegates can employ their critical thought processes and share ideas with their counterparts from around the world. Given our delegates' plurality of perspectives and experiences, we center our programming around the values of diplomacy and teamwork. In particular, our daises look for and promote constructive leadership that strives towards consensus, as real ambassadors do in the United Nations.

Debate founded on strong knowledge and accessibility: With knowledgeable staff members and delegates from over 70 countries, NHSMUN can facilitate an enriching experience reliant on substantively rigorous debate. To ensure this high quality of debate, our staff members produce detailed, accessible, and comprehensive topic guides (like the one below) to prepare delegates for the nuances inherent in each global issue. This process takes over six months, during which the Directors who lead our committees develop their topics with the valuable input of expert contributors. Because these topics are always changing and evolving, NHSMUN also produces update papers intended to bridge the gap of time between when the background guides are published and when committee starts in March. As such, this guide is designed to be a launching point from which delegates should delve further into their topics. The detailed knowledge that our Directors provide in this background guide through diligent research aims to increase critical thinking within delegates at NHSMUN.

Extremely engaged staff: At NHSMUN, our staffers care deeply about delegates' experiences and what they take away from their time at NHSMUN. Before the conference, our Directors and Assistant Directors are trained rigorously through hours of workshops and exercises both virtual and in-person to provide the best conference experience possible. At the conference, delegates will have the opportunity to meet their dais members prior to the first committee session, where they may engage

one-on-one to discuss their committees and topics. Our Directors and Assistant Directors are trained and empowered to be experts on their topics and they are always available to rapidly answer any questions delegates may have prior to the conference. Our Directors and Assistant Directors read every position paper submitted to NHSMUN and provide thoughtful comments on those submitted by the feedback deadline. Our staff aims not only to tailor the committee experience to delegates' reflections and research but also to facilitate an environment where all delegates' thoughts can be heard.

Empowering participation: The UN relies on the voices of all of its member states to create resolutions most likely to make a meaningful impact on the world. That is our philosophy at NHSMUN too. We believe that to properly delve into an issue and produce fruitful debate, it is crucial to focus the entire energy and attention of the room on the topic at hand. Our Rules of Procedure and our staff focus on making every voice in the committee heard, regardless of each delegate's country assignment or skill level. Additionally, unlike many other conferences, we also emphasize delegate participation after the conference. MUN delegates are well researched and aware of the UN's priorities, and they can serve as the vanguard for action on the Sustainable Development Goals (SDGs). Therefore, we are proud to connect students with other action-oriented organizations to encourage further work on the topics.

Focused committee time: We feel strongly that face-to-face interpersonal connections during debate are critical to producing superior committee experiences and allow for the free flow of ideas. Ensuring policies based on equality and inclusion is one way in which NHSMUN guarantees that every delegate has an equal opportunity to succeed in committee. In order to allow communication and collaboration to be maximized during committee, we have a very dedicated administrative team who work throughout the conference to type up, format, and print draft resolutions and working papers.

As always, we welcome any questions or concerns about the substantive program at NHSMUN 2023 and would be happy to discuss NHSMUN pedagogy with faculty or delegates.

Delegates, it is our sincerest hope that your time at NHSMUN will be thought-provoking and stimulating. NHSMUN is an incredible time to learn, grow, and embrace new opportunities. We look forward to seeing you work both as students and global citizens at the conference.

Best,

Ming-May Hu
Secretary-General

Ana Margarita Gil
Director-General

A Note on Research and Preparation

Delegate research and preparation is a critical element of attending NHSMUN and enjoying the debate experience. We have provided this Background Guide to introduce the topics that will be discussed in your committee. We encourage and expect each of you to critically explore the selected topics and be able to identify and analyze their intricacies upon arrival to NHSMUN in March.

The task of preparing for the conference can be challenging, but to assist delegates, we have updated our **Beginner Delegate Guide** and **Advanced Delegate Guide**. In particular, these guides contain more detailed instructions on how to prepare a position paper and excellent sources that delegates can use for research. Use these resources to your advantage. They can help transform a sometimes overwhelming task into what it should be: an engaging, interesting, and rewarding experience.

To accurately represent a country, delegates must be able to articulate its policies. Accordingly, NHSMUN requires each delegation (the one or two delegates representing a country in a committee) to write a position paper for each topic on the committee's agenda. In delegations with two students, we strongly encourage each student to research each topic to ensure that they are prepared to debate no matter which topic is selected first. More information about how to write and format position papers can be found in the NHSMUN Research Guide. To summarize, position papers should be structured into three sections:

I: Topic Background – This section should describe the history of the topic as it would be described by the delegate's country. Delegates do not need to give an exhaustive account of the topic, but rather focus on the details that are most important to the delegation's policy and proposed solutions.

II: Country Policy – This section should discuss the delegation's policy regarding the topic. Each paper should state the policy in plain terms and include the relevant statements, statistics, and research that support the effectiveness of the policy. Comparisons with other global issues are also appropriate here.

III. Proposed Solutions – This section should detail the delegation's proposed solutions to address the topic. Descriptions of each solution should be thorough. Each idea should clearly connect to the specific problem it aims to solve and identify potential obstacles to implementation and how they can be avoided. The solution should be a natural extension of the country's policy.

Each topic's position paper should be **no more than 10 pages** long double-spaced with standard margins and font size. **We recommend 3–5 pages per topic as a suitable length**. The paper must be written from the perspective of your assigned country and should articulate the policies you will espouse at the conference.

Each delegation is responsible for sending a copy of its papers to their committee Directors via myDais on or before **February 24, 2023**. If a delegate wishes to receive detailed feedback from the committee's dais, a position must be submitted on or before **February 3, 2023**. The papers received by this earlier deadline will be reviewed by the dais of each committee and returned prior to your arrival at the conference.

Complete instructions for how to submit position papers will be sent to faculty advisers via email. If delegations are unable to submit their position papers on time, please contact us at info@imuna.org.

Delegations that do not submit position papers will be ineligible for awards.

Committee History

In the early 2000s, one pressing issue hindered the accomplishment of the Millennium Development Goals—corruption. The Ad Hoc Committee of the Negotiation against Corruption was the first body established to evaluate the scope of the problem, but it lacked a definitive mandate.[1] On October 31, 2003, the United Nations Convention Against Corruption (UNCAC) was adopted by the UN General Assembly under the scope of the UN Office on Drugs and Crimes (UNODC) as a multilateral treaty with the purpose of developing a thorough solution to a problem that happens anywhere and involves anyone: corruption.[2] The mandate of the convention covers three main points: the effective prevention of the issue, the enhancement of international cooperation, and the transparency and proper management of public affairs and public property, which by being achieved, will reduce corruption across the globe.[3]

The UNCAC mandate was divided into chapters. Chapter I states the Convention's mandate as well as what the Convention does not promote, endorse, or permit. Primarily, the Convention does not permit the upholding of state sovereignty, which means that each state has to act within its domestic laws. States are to act in a consistent manner with sovereign equality and should practice non-intervention in the domestic affairs of other states. Nor, according to the convention, should a member state prosecute corrupt officials from another state.[4] Under the UNCAC, change must come from within each country.

Chapters II–VI of the UNCAC mandate text each describe one of the five provisions of the Convention. First are the preventative measures, including enhancing political transparency, establishing frameworks to monitor public officials, and promoting judicial integrity. Second are the criminalization and law enforcement measures, requiring countries to criminalize certain corruption-related offenses. Third is international cooperation which promotes international assistance to counter the transnationality of corruption. Fourth are the asset recovery mechanisms that target the prevention and seizure of criminal assets, often transferred internationally. Finally, Chapter VI promotes the training of anti-corruption personnel and, when necessary, international assistance for states party to the Convention without the capacity for technical training.[5]

1 UN General Assembly, Resolution 58/4, United Nations Convention Against Corruption, A/RES/58/4, (September 18, 2022) https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.
2 "United Nations Convention against Corruption," United Nations Office on Drugs and Crimes, accessed September 18, 2022, https://www.unodc.org/unodc/en/corruption/uncac.html.
3 A/RES/58/4, 37.
4 A/RES/58/4, 23-25, 41-42.
5 A/RES/58/4.

UNCAC

NHSMUN 2023

TOPIC A:
CORRUPTION AND PRESS FREEDOM

Photo Credit: Muhammad Mahdi Karim

Introduction

The lack of freedom of expression is a threat to a country's democratic process. Over the last few decades, there has been alarming evidence of violence against journalists, which prevents them from exercising freedom of speech in their countries.[1] The Committee to Protect Journalists (CPJ), an independent nonprofit that fights for press freedom worldwide, has revealed that in 2021, at least 293 journalists were imprisoned across the world, compared to 280 journalists in 2020.[2]

Press censorship is a relevant issue for many countries because of corruption within the media by government officials and related agencies. Through coercion, many media agencies have transformed their content and information as politicians practicing bribery pressure the media to use uncertain facts, manipulate information, or oversimplify the news.[3] These practices are also consistent with violence against journalists and threats to their craft. Clearly, corruption within the press is a barrier to democracy, safety, and development. Without reliable and transparent media, a society cannot progress. Corruption in the media can also translate to distrust in the government, which can create a rift between the public and the government and deepen political divides and instability.

Issues related to this topic are the lack of protections for journalists, censorship, bribery, and press corruption. With these issues, journalists live with the fear of being attacked by government officials or imprisoned due to their work.[4] Journalists should be able to freely report any sort of bribery exposure or incentive. Censorship and limited access to information play an important role in the fight against press corruption. With technology accessible in most countries, online corruption in the media is also prevalent. In Azerbaijan, criminal defamation laws have been extended to what is posted on social media platforms, including opinions on governmental actions and decisions.[5] Lastly, press corruption restricts progress in developing countries. The lack of employment standards, resources, and legal mechanisms for reporting have made corruption in the media an ongoing problem.

A free press providing reliable information can endorse democracy, quality education, poverty reduction, and a culture of justice and human rights.[6] It also fosters a safer and more secure work environment for journalists. Through transparency policies, reporting mechanisms, and protection for journalists, corruption can be uncovered, and government officials can be held accountable for their actions.

History and Description of the Issue

Defining Corruption and Press Freedom

According to the 2000 World Bank Institute Report, corruption is "the abuse of public power for personal gain or the benefit of a group to which one owes allegiance."[7] Corruption is a social, political, economic, and legal issue that limits democratic advancement worldwide.[8] This issue manifests through altering electoral processes, perverting the law, or enabling bribery to take place.[9] Corruption is a severe challenge for development, as it undermines good governance

1 *UN Plan of Action on the Safety of Journalists and The Issue of Impunity*, (Paris: United Nations Educational, Scientific, and Cultural Organization, 2011), https://www.ohchr.org/sites/default/files/Documents/Issues/Journalists/UN_plan_on_Safety_Journalists_EN.pdf.
2 "What We Do," Committee to Protect Journalists, accessed July 14, 2022, https://cpj.org/about/; Arlene Getz, "Number of journalists behind bar reaches global high," Committee to Protect Journalists, last modified December 9, 2021, https://cpj.org/reports/2021/12/number-of-journalists-behind-bars-reaches-global-high/.
3 Peter Vanderwicken, "Why the News Is Not the Truth," Harvard Business Review, last modified June 1995, https://hbr.org/1995/05/why-the-news-is-not-the-truth.
4 "10 Most Censored Countries," Committee to Protect Journalists, accessed July 14, 2022, https://cpj.org/2015/04/10-most-censored-countries/.
5 Committee to Protect Journalists, "10 Most Censored Countries."
6 United Nations Educational, Scientific, and Cultural Organization, *UN Plan of Action on the Safety of Journalists and The Issue of Impunity*.
7 Lee B. Becker et al, "Measurement Issues and the Relationship Between Media Freedom and Corruption," *Grady College of Journalism & Mass Communication, University of Georgia,* (June 2013): 6-14, http://grady.uga.edu/coxcenter/Conference_Papers/Public_TCs/Becker_Naab%20_English_Vlad_IAMCR_5_22_2013.pdf.
8 "UNODC's Action against Corruption and Economic Crime," UN Office on Drugs and Crime, accessed July 13, 2022, https://www.unodc.org/unodc/en/corruption/index.html.
9 UN Office on Drugs and Crime, "UNODC's Action against Corruption and Economic Crime."

and reduces compromise with a country's legal system.[10]

Press freedom is a right, and it ensures that the media is independent, free, and plural. It is essential in a democracy as it ensures transparency, accountability, and the rule of law. Moreover, a country with press freedom allows civic participation in public and political discourse. It empowers the community to participate in the democratic process. Press freedom goes hand in hand with two rights: freedom of expression and freedom of information. The first is a human right stated in Article 19 of the Universal Declaration of Human Rights. It includes the freedom to hold opinions and to seek, receive, and impart information through any media. The second right, freedom of information, ensures the means by which information is made available. It has two aspects: the legal framework of the country regarding information and the circulation of information by the public and private sectors.[11]

There is a clear and direct relationship between press freedom and corruption. Former World Bank President, James Wolfensohn, established that government corruption is the primary barrier to development. He also stated that independent media and the press are essential tools to fight government corruption. For instance, it promotes reliable information with which a population can make informed decisions, such as voting.[12] Unbiased information, diverse opinions, and an empowered society are all key factors in the building and maintenance of a solid democracy.[13] Due to the press's influence, different governments have corrupted the media. According to Paul H. Weaver, a former political scientist at Harvard University, the government corrupts the media as a response to a "circle of mutual manipulation, mythmaking, and self-interest." If the media complies with government interests, the population will have a positive attitude toward the government. For example, journalists can dramatize news to show politicians responding to crises.[14]

Some of the most recent actions against corruption executed by the United Nations occurred in 2021, as several milestones were achieved.[15] One important step is the ninth session of the Conference of States Parties (CoSP) to the UNCAC.[16] The CoSP met from December 13–17, 2021, and developed several resolutions. One of the most relevant is Resolution 9/3, which talks about the relationship between fighting corruption, the use of information, and communication technologies. More specifically, it "encourages state parties… [to] utilize information and communications technologies to strengthen the implementation of the Convention…[and] promote transparency and public reporting in areas such as public procurement, management of public finances, and asset and interest disclosure."[17] In other words, Resolution 9/3 suggests employing communication measures to promote government transparency. One of these means of communication is the press. Unfortunately, the media and press do not enjoy the freedom of expression in every country. When there is more corruption in the press, there will be less freedom of expression.

Another advantageous step has been the International Country Risk Guide (ICRG). It is a dataset that provides information from 1984 onward on risk ratings of countries, which are updated annually. These ratings are produced by analyzing political, economic, and financial subcategories; each of these subcategories has its own index.[18] For UNCAC's purposes, the political index is most relevant, as it looks at government stability, socioeconomic conditions, internal and external

10 Becker et al, "Measurement Issues and the Relationship Between Media Freedom and Corruption."
11 "Press Freedom Day," United Nations, accessed October 3, 2022, https://www.un.org/en/observances/press-freedom-day/background.
12 Rafael Di Tella and Ignacio Franceschelli, *Government Advertising and Media Coverage of Corruption Scandals* (Boston: American Economic Journal, 2011), https://www.hbs.edu/ris/Publication%20Files/AEJ_Govt%20advertising%20and%20media%20coverage%20of%20corruption%20scandals_cbb969cd-4266-4818-8656-8d751e9b5b28.pdf.
13 United Nations, "Press Freedom Day."
14 Vanderwicken, "Why The News is Not The Truth."
15 "Corruption and Economic Crime 2021 Annual Report," UN Office on Drugs and Crime, accessed July 14, 2022, https://www.unodc.org/unodc/en/corruption/2021-annual-report.html.
16 UN Office on Drugs and Crime, "Corruption and Economic Crime 2021 Annual Report."
17 "Resolutions and decisions adopted by the Conference of the States Parties to the United Nations Convention against Corruption," UN Office on Drugs and Crime, accessed September 29, 2022, https://www.unodc.org/unodc/en/corruption/COSP/session9-resolutions.html.
18 "International Country Risk Guide (ICRG) Researchers Dataset," University of Toronto, accessed September 29, 2022, https://mdl.library.utoronto.ca/collections/numeric-data/statistics/international-country-risk-guide-icrg-researchers-dataset.

conflict, corruption, military in politics, religion in politics, democratic accountability, and bureaucratic quality.[19] High-risk scores are consistent with countries in more precarious political environments, whereas low-risk scores are associated with stable and safe political environments. The ICRG corruption indicator demonstrated that corruption decreases with more media freedom. An improvement in press freedom could reduce corruption indexes between 0.4–0.9 points (on a scale from 0–6). As stated, corruption is directly correlated with the media and press. Corruption perceptions are caused by what the media publicly exposes.[20] So, if controlled media produces fewer publications criticizing a corrupt government, the population will perceive the regime positively.

The Corruption Perceptions Index (CPI) measures global corruption by the non-governmental organization Transparency International.[21] CPI defines corruption as the "abuse of entrusted power for private gain."[22] To create this index, experts in the field analyzed 13 different resources related to corruption. Some of these resources include the African Development Bank Country Policy and Institutional Assessment, the World Bank Country Policy and Institutional Assessment, Varieties of Democracies, and more. Transparency International states that each country examined by the CPI has a score calculated by three data sources from thirteen corruption surveys.[23] Concerning public sector corruption, the CPI looks at instances of bribery, nepotism in civil service appointments, diversion of public funds, and access to information on public affairs and government activities. The data is collected by authorized institutions such as the World Bank. A country's score is the perceived corruption in the public sector on a scale from 0-100, where 0 is highly corrupt, and 100 is not corrupt.[24]

The Government's Power Over the Press

In 1883, Joseph Pulitzer bought the New York World and made it the largest newspaper in the United States. In the nineteenth century, almost every newspaper had an institutional format- very similar to the minutes of a board meeting. Pulitzer changed this and gave it a dramatic focus to increase the reader's interest. His strategy was simple: making news thought-provoking and sensationalized. Instead of just stating facts, he would turn news articles into stories with plots, actors, and many details. He added blasting headlines, large pictures, and impressive graphics. He also changed the tone of the news and switched from informative to emotional. This transformation made the press the perfect platform for the government to portray a series of dramatized events.[25]

The media, just like any other institution or business, is exposed to corruption and bribery. Besides ideological influences, government corruption over the press leads to biased journalism in exchange for financial benefits, transactions, or advertisements.[26] A government controlling the press permits censorship, enables a culture of self-censorship, and destroys the public's freedom of opinion.[27] Additionally, corruption attacks democracy, distorts the political processes, and slows development.

The influence exerted by a government on the press occurs because of how the press dramatically influences voters' perceptions. Consequently, politicians or government agencies will try to find a way for the press to showcase them beneficially. This has been reflected in the Venezuelan media. Several government policies have negatively impacted press freedom within this country. The monopoly on imports of paper and printing supplies led to the disappearance of printed editions of most newspapers. Moreover, a policy for granting

19 University of Toronto, "International Country Risk Guide (ICRG) Researchers Dataset."
20 Becker, "Measurement Issues and the Relationship Between Media Freedom and Corruption," 6-14.
21 "The ABCs of the CPI: How The Corruption Perceptions Index Is Calculated," Transparency International, accessed July 14, 2022, https://www.transparency.org/en/news/how-cpi-scores-are-calculated.
22 "What is Corruption?" Transparency International, accessed September 29, 2022, https://www.transparency.org/en/what-is-corruption.
23 Transparency International, "The ABCs of the CPI."
24 Transparency International, "The ABCs of the CPI."
25 Vanderwicken, "Why the News is Not the Truth."
26 Di Tella and Franceschelli, *Government Advertising and Media Coverage of Corruption Scandals.*
27 "Government Policy for the Internet Must Be Rights-Based and User-Centered," United Nations Chronicle, accessed July 15, 2022, https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred.

and recalling concessions for radio broadcasting led over 200 radio stations to close.[28] About three-fourths of Venezuelan newspapers have closed over the last few years, and the government fully owns the only running media outlet.[29] The NGO Reporters Without Borders has also documented multiple cases of arrests, expulsion, and libel lawsuits against Venezuelan journalists.[30]

Myanmar asserts a similar influence over the press. The country has suffered decades of repression, corruption, poverty, and wars with ethnic minority groups.[31] At the beginning of 2021, Myanmar's parliament was expected to legitimize the next government.[32] The military refused to accept the election results that showed the National League for Democracy as the dominant party and threatened to take action, which resulted in a coup.[33] Because of the 2021 coup, a total of 7,122 people are under detention.[34] A considerable number of these detained people are journalists. Over the last few months, activists and journalists have been threatened and criminalized for their work.[35] One arrested journalist is Danny Fenster, an American journalist arrested on May 24, 2021, by authorities at Yangon's Mingaladon Airport and taken to the Insein Prison.[36] According to Fenster, he was arrested because the government is trying to prevent the exposure of human rights violations in Myanmar.[37] Other journalists in the country were shot while covering protests.[38] Unfortunately, few journalists have been released, and the military convicted the ousted governor Aung San Suu Kyi on more corruption charges and added six more years to her previous 11-year sentence. The trial against her has been held behind closed doors and lacks media access.[39] Myanmar's government tried to legitimize itself by controlling the media and oppressing journalists. This is not unique.[40] Other examples of censorship enforced by corruption have taken place in Sub-Saharan Africa. Here, corruption is strongly linked to natural resource management and can strongly impede peoples' access to public services. To clean politicians' images and keep corruption out of the public eye, governments across the territory "have limited information and cracked down on independent voices calling out abuses of power."[41]

Another case of censorship is Bill 369, or the "Anti-Corruption Bill," passed by the Chamber of Representatives in Colombia on December 6, 2021. It included an article where judges are granted the right to "suspend or cancel the legal status of any organization whose members defame or slander any active or former government official."[42] The bill also modified article 221A of the Colombian penal code. This article criminalizes defamation and slander by empowering authorities to suspend or cancel the legal status of organizations where the victims are active or former public officials. This modification has broad implications for government trust and transparency. The reform hinders public debate and creates the perfect platform for corruption, as the press and other organizations are now fearful of reporting the truth. The stated reason for this censorship is to create laws against defamation, but the

28 "Venezuela," Reporters Without Borders, accessed August 28, 2022, https://rsf.org/en/country/venezuela.
29 "Maduro con el control casi absoluto de la prensa; sólo sobrevive," Radio Television Marti, last modified July 26, 2018, https://www.radiotelevisionmarti.com/a/cierre-de-medios-en-venezuela-deja-la-cobertura-en-manos-del-estado/190947.html.
30 Radio Television Martí, "Maduro con el control casi absoluto de la prensa."
31 Lindsay Maizland, "Myanmar's Troubled History: Coups, Military Rule, and Ethnic Conflict," Council on Foregin Relations, last modified January 31, 2022, https://www.cfr.org/backgrounder/myanmar-history-coup-military-rule-ethnic-conflict-rohingya.
32 Russell Goldman, "Myanmar's Coup, Explained," *The New York Times,* April 27, 2022, https://www.nytimes.com/article/myanmar-news-protests-coup.html.
33 Goldman, "Myanmar's Coup, Explained."
34 "Repression of activists and journalists persist in Myanmar despite Asean rebuke," CIVICUS, accessed July 16, 2022, https://monitor.civicus.org/updates/2021/11/09/repression-activists-and-journalists-persists-myanmar-despite-asean-rebuke/.
35 CIVICUS, "Repression of activists and journalists persist in Myanmar despite Asean rebuke."
36 "Myanmar: Cease persecution of journalists," Amnesty International, accessed July 16, 2022, https://www.amnesty.org/en/latest/press-release/2021/05/myanmar-cease-persecution-journalists/.
37 Amnesty International, "Myanmar: Cease persecution of journalists."
38 Amnesty International, "Myanmar: Cease persecution of journalists."
39 Frances Mao, "Aung San Suu Kyi: Myanmar sentences ex-leader to jail for corruption," *BBC News*, April 27, 2022, https://www.bbc.com/news/world-asia-61239881.
40 Mara Mendes, *Overview of corruption in the media in developing countries,* (Germany: Transparency International, 2013), https://assets.publishing.service.gov.uk/media/57a089fbe5274a27b2000367/expertanswer-368.pdf.
41 "CPI 2021 FOR SUB-SAHARAN AFRICA: AMID DEMOCRATIC TURBULENCE, DEEP-SEATED CORRUPTION EXACERBATES THREATS TO FREEDOMS," Transparency International, last modified January 25, 2022, https://www.transparency.org/en/news/cpi-2021-sub-saharan-africa-amid-democratic-turbulence-deep-seated-corruption.
42 "Colombian legislature passes anti-corruption bill that threatens press freedom," Committee to Protect Journalists, accessed July 14, 2022, https://cpj.org/2021/12/colombian-legislature-passes-anti-corruption-bill-that-threatens-press-freedom/.

real effect is that the Colombian people's freedom of speech is limited. As a result, this bill represents a major setback to the global fight against political corruption. In 2022, the Colombian Foundation for Press Freedom (FLIP) reported 47 attacks on journalists amid presidential elections. Attacks included harassment and false information through social media platforms.[43] While organizations such as FLIP act as a corruption and press censorship watchdog, the government still holds immense power over the information being spread, especially after Bill 369.

A country's legal framework directly influences journalists' ability to do work impartially. Article 19 of the Universal Declaration of Human Rights establishes that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Unfortunately, not all UN member states abide by this. States have limited press freedom in different forms. For instance, the Chinese government has a history of censorship by blocking certain websites and platforms in the country. North Korea and Cuba have dominated state control over the media. In Eritrea, Uzbekistan, and Syria, journalists have suffered violence and imprisonment at the hands of the government due to limitations and restrictions on the press. Jordan has codified specific legal provisions which limit press freedom. Its penal code states that "coverage on issues that could breach national unity, divide the population or damage the image and the reputation of the state will lead to prison sentences for journalists that breach this law."[44] This standard is open to interpretation and can lead to the imprisonment of many journalists. Moreover, there are states where freedom of the press is codified but not actively put into practice.

Media licensing is another crucial factor regarding press freedom and corruption. Governments use licenses to control the media. This is the case in Malaysia, where newspapers must renew their licenses yearly. As a result, editors and journalists who have reported unfavorable government views can have their licenses revoked or unrenewed. In some states, journalists' registration and licensing practices exist as barriers to freedom of the press. In Saudi Arabia, the government must approve who can work as a journalist and can dismiss editors-in-chief of newspapers.[45] This gives a platform for public officials to dismiss or reject journalists that have expressed criticism against them.

Media ownership is another factor that affects the integrity of the press. When any public institution owns the media, the government can exert control by censoring reports or posing barriers to investigations into essential cases.[46] This is especially true in many of the Balkan states, including Serbia and Bosnia and Herzegovina.[47] A 2011 report from the Anti-Corruption Council of Serbia states that over 25 percent of Serbian media revenues come from government institutions.[48] Maintaining this hold on the media helps the state strengthen political control while preventing rival parties from advertising to citizens. This is further proven by a 2013 report from the Croatian Chamber of Commerce, which revealed that almost 4.2 million euros were used for illicit marketing services.[49] This essentially signifies that large sums of money were utilized in political corruption, which indicates biased and unreliable media.

These cases showcase the power that government can hold over the media. As mentioned, strong governmental control has led to journalist oppression, shutdowns of newspapers, and the monopolization of media outlets, but there are some further solutions that can begin to fortify journalism.

Harm to Journalists

Journalists possess the crucial power to inform and influence

43 "Asociaciones que defienden la libertad de prensa en el continente pidieron parar el asedio a periodistas en medio de la campaña presidencial," Infobae, accessed July 14, 2022, https://www.infobae.com/america/colombia/2022/06/15/asociaciones-que-defienden-la-libertad-de-prensa-en-el-continente-pidieron-parar-el-asedio-a-periodistas-en-medio-de-la-campana-presidencial/.
44 Mendes, *Overview of corruption in the media in developing countries.*
45 Mendes, *Overview of corruption in the media in developing countries.*
46 Mariana Sosa Cordero, "Three ways to fight corruption in the media," Transparency International, last modified November 18, 2016, https://www.transparency.org/en/news/three-ways-to-fight-corruption-in-the-media.
47 *Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom*, (London: Ethical Journalism Network, 2015), https://dev.ethicaljournalismnetwork.org/wp-content/uploads/2016/08/untold-stories-full.pdf.
48 Ethical Journalism Network, *Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom.*
49 Ethical Journalism Network, *Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom.*

the public, and as a result, their work can be incredibly dangerous. Just for doing their jobs, journalists can face threats, attacks, and other forms of intimidation. In the last few years, there has been an increase in these attacks and threats toward journalists. Estimates also show that justice is rarely served in these instances, as nine of ten killings of journalists remain unpunished.[50] Even though journalists are legally never legitimate targets in a conflict zone, in at least 90 percent of cases when journalists are murdered, those responsible are not held to account.[51]

Sometimes, the persecution of journalists is related to political situations or unstable circumstances. In Ukraine in 2022, six out of every seven journalists killed while working were targeted deliberately by Russian forces. Actions like these could be construed as possible war crimes.[52] However, conflict does not always indicate journalist persecution. In fact, according to the United Nations Educational, Scientific and Cultural Organization (UNESCO), the number of journalists killed outside of conflict zones exceeds the number within them every year since 2016.[53] For example, in 2018, Jan Kuciak, a Slovak journalist, was murdered after he published his report about the misappropriation of EU funds and detailed how the government covered up years of organized crime. His murder led to massive protests, which forced the former Prime Minister, Roberto Fico, to resign.[54] Shireen Abu Akleh, a correspondent for Al Jazeera, was fatally shot in May 2022 while covering an Israeli military raid in the West Bank. Abu Akleh was killed while clad in a press vest, standing next to other reporters.[55] These attacks have affected journalists' ability to exercise their freedom of expression because of the danger to their life. Journalists are at high risk when working for corrupted media or exposing corrupt systems and may face other harms, too, such as imprisonment. In fact, the Committee to Protect Journalists shows that globally, journalist imprisonment is inversely related to journalist killings: even as journalist killings decline, imprisonments are on the rise.[56]

50 "Journalism: a dangerous profession," United Nations Educational, Scientific, and Cultural Organization, accessed September 29, 2022, https://en.unesco.org/courier/2021-4/journalism-dangerous-profession.
51 Sonya Diehn, "The unprecedented rise in journalist slayings — and what can be done to stop them," *DW,* May 11, 2022, https://www.dw.com/en/the-unprecedented-rise-in-journalist-slayings-and-what-can-be-done-to-stop-them/a-6176342.
52 Diehn, "The unprecedented rise in journalist slayings — and what can be done to stop them."
53 "Threats that Silence: Trends in the Safety of Journalists," United Nations Educational, Scientific and Cultural Organization, accessed October 21, 2022, https://unesdoc.unesco.org/ark:/48223/pf0000379589/PDF/379589eng.pdf.multi
54 Wasil Schauseil and David Jackson, *Media and anti-corruption,* (Norway: U4 Anti-Corruption, 2013), https://www.u4.no/publications/media-and-corruption.pdf.
55 "Abbas demands US seek justice over Shireen Abu Akleh's killing," *Aljazeera,* September 23, 2022, https://www.aljazeera.com/news/2022/9/23/abbas-slams-israels-impunity-over-shireen-abu-aklehs-killing.
56 UNESCO, "Threats that Silence."

Journalist Santiago O'Donnell and his book exposing chains of bribery within the Macri's government in Argentina.

Credit: PÁGINA 12

Delegates should note that declining journalist deaths in a region does not necessarily indicate journalist safety.

Journalists are threatened with other rights violations, like in the O'Donnell case in Argentina. The journalist Santiago O'Donnell published a book in February 2021 exposing secret financial agreements and expenses related to corruption within the Macri presidential family. It specifically discusses a secret agreement between five of the six Macri children to allocate their father's inheritance. Moreover, it gave insight into the former Argentine President Mauricio Macri's mysterious wealth.[57] Within two weeks of the book's release, an Argentinian judge requested O'Donnell to turn over his recordings of interviews between the journalist and Mariano Macri, the younger brother of former president Mauricio Macri. The presidential family expressed anger against the book, and Mauricio Macri did not let bookstores release the book to protect his own reputation, actively censoring this information.[58] O'Donnell was intimidated and economically pressured to comply, but he fought back, proclaiming that "every journalist has the right to protect their sources of information, notes and personal and professional archives." Unfortunately, this right is not always guaranteed by systems in power, and journalists around the world face threats.

Journalists are also not a homogenous group; different individuals face varying risks based on their specific roles and their personal demographics. Television journalists are the most attacked group, accounting for 134 journalist fatalities (34 percent) between 2016-2020, followed by print journalists (22 percent) and radio journalists (20 percent).[59] Most fatally-targeted journalists are killed in their home country; this may be connected to increasing reliance on local journalists to report for international outlets.[60] Female journalists are also disproportionately targeted; they face gender-based violence, including stigmatization, sexist hate speech, trolling, physical assault, rape, and murder. Female journalists have recently been increasingly the targets of online violence.[61] Irene Khan, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, stated that "while both male and female journalists are exposed to violence and threats to their safety in retaliation for their work, attacks on the women are gender-based and highly sexualized online and offline."[62] Both virtual and in-person harassment can impact journalists' productivity, wellbeing, and physical safety.

Online violence, often targeted at women, is organized and coordinated. These actions targeted at journalists can involve acts of trolling for supposed "patriotic" purposes and often extends beyond one victim; female journalists report that their families, sources, colleagues, and bystanders are also targets of hate speech and threats.[63] These threats of harm to those connected to female journalists are intended to slow down or prevent journalists from continuing their reporting. Alarmingly, nearly three-quarters (73 percent) of journalists identifying as women say that they experienced online abuse, harassment, threats, and attacks.[64] Beyond gender, many women journalists also face homophobia, racism, or faith-based discrimination, thus increasing the impact of their targeting.[65]

Specific threats to female journalists have strong misogynist tones, as women are attacked because of their gender. In one particularly striking example, Lebanese journalist Ghada Oueiss, Al Jazeera's principal Arabic presenter, reported the following:

"[Every day I went on air], I would receive on my Al Jazeera email - because somehow it was leaked - a death threat. One of them that I can never forget [said]: 'You will be looking at the camera to talk to your audience and you will start reading the bulletin and reading the autocue in front of you. You will

57 "Argentina's Latest Anti-Speech Scandal: Free Press on the Rocks?" Council on Foreign Relations, accessed August 3, 2022, https://www.cfr.org/blog/argentinas-latest-anti-speech-scandal-free-press-rocks.
58 Council on Foreign Relations, "Argentina's Latest Anti-Speech Scandal: Free Press on the Rocks?"
59 UNESCO, "Threats that Silence."
60 UNESCO, "Threats that Silence."
61 "The Chilling: Global trends in online violence against women journalists," United Nations Educational, Scientific and Cultural Organization, accessed October 21, 2022, https://unesdoc.unesco.org/ark:/48223/pf0000377223/PDF/377223eng.pdf.multi.
62 "Women journalists face violence and sexualized attacks - UN expert- #JournalistsToo – Women Journalists Speak Out," Office of the United Nations High Commissioner for Human Rights, accessed October 21, 2022, https://www.ohchr.org/en/press-releases/2021/11/women-journalists-face-violence-and-sexualized-attacks-un-expert.
63 UNESCO, "The Chilling: Global trends in online violence against women journalists."
64 UNESCO, "The Chilling: Global trends in online violence against women journalists."
65 OHCHR, "Women journalists face violence and sexualized attacks."

notice that there is a gun and [a] bullet, that bullet will go straight to your head.' Then I started getting emailed [sexually explicit] pictures… And then, they made another email in my name and they started sending to my colleagues pictures of [my] head [in sexually explicit] pictures."[66]

This example is a striking case of specific misogynist threats against a woman in the field of journalism who faces disproportionate vitriol on account of her gender. Sexually explicit images are a unique aspect of threats against women; men do not face such types of harassment at the same frequency as women.

This case is just one example of what women routinely face while working in media. Additionally, descriptive threats of violence do lead to complete acts of violence. In 2017, the celebrated Maltese investigative journalist Daphne Caruana Galizia and the prominent Indian journalist Gauri Lankesh, both of who had been targets of prolific, gendered online attacks, were murdered.[67] In the aftermath of the deaths, the targeted harassment was blamed for creating the conditions for murder.[68] International organizations, civil society, and researchers have given greater attention in recent years to threats, including various forms of online violence, that inordinately affect women journalists and those who represent minority groups in the profession.[69] There is still more to be done and as the landscape of the journalism profession continues to change with more women and minorities in the field, the need to protect journalists is paramount.

Protecting and Bolstering Journalism

Journalism should promote dignity and transparency. This can be achieved by establishing ethical standards through legislation that media outlets must follow. Effective measures to protect journalists' rights have been implemented in Norway. Their freedom of expression strategy is based on human rights compliance and dialogue, promoting partner organizations in the region, and ensuring ethical standards are followed by journalists.[70] Norway has also developed the Strategy for Promoting Freedom of Expression in Norwegian Foreign Policy and Development Policy.[71] This document describes actions that the country takes to ensure freedom of speech. Some of these include supporting the development of national and international institutions, enforcing self-regulatory agencies, protecting the confidentiality of sources, and more.[72] One of the bodies designated to fulfill these goals is the Norwegian Media Authority. The agency works alongside the government to provide financial support to media outlets, such as grants for local broadcasting or even minority-language publications. Moreover, Norway has developed strategic actions related to digital media and communications platforms. The country is conscious that online platforms can promote civil debate but can be a space for hate speech and disinformation.[73] Disinformation and hateful propaganda can threaten democracy in many countries. Norway is working on "promoting transparency and accountability" regarding social media or other online publications through the strategic plans mentioned previously.[74]

The UN has also taken important steps to ensure the protection of journalists. One clear action is the UN Plan of Action on the Safety of Journalists and the Issue of Impunity, which aims to "create a free and safe environment for journalists and media workers, both in conflict and non-conflict situations."[75] The plan brought together over 250 members of UN agencies, countries, regional intergovernmental organizations, media

66 UNESCO, "The Chilling: Global trends in online violence against women journalists."
67 Julie Posetti, Jackie Harrison, and Silvio Waisbord, *Online Attacks on Women Journalists Leading to 'Real World' Violence, New Research Shows,* (Washington: International Center for Journalists, 2022), https://docs.google.com/document/d/1k4sn6jl4gVc8GS4CAeRE53dntsjk9WUQy0SKURkVITs/edit.
68 Posetti, Harrison, and Waisbord, *Online Attacks on Women Journalists Leading to 'Real World' Violence.*
69 UNESCO, "Threats that Silence."
70 *Strategy for promoting freedom of expression in Norwegian foreign and development policy,* (Norway: Ministry of Foreign Affairs), https://www.regjeringen.no/globalassets/departementene/ud/vedlegg/mr/strategy_expression.pdf.
71 *Strategy for promoting freedom of expression in Norwegian foreign and development policy.*
72 *Strategy for promoting freedom of expression in Norwegian foreign and development policy.*
73 "New strategy for promoting freedom of expression in foreign and development policy," Norway in Saudi Arabia, accessed September 29, 2022, https://www.norway.no/en/saudi-arabia/norway-sa/news-events/new-strategy-for-promoting-freedom-of-expression-in-foreign-and-development-policy/.
74 Norway in Saudi Arabia, "New strategy for promoting freedom of expression in foreign and development policy."
75 "UN Plan of Action on the Safety of Journalists and the Issue of Impunity," United Nations Educational, Scientific, and Cultural Organization, accessed September 30, 2022, https://en.unesco.org/un-plan-action-safety-journalists.

outlets, and academia in 2014.[76] The most recent discussion was on June 29, 2017, when UNESCO and the Office of the UN Commissioner for Human Rights exchanged ideas on strengthening the UN Plan of Action on the Safety of Journalists.[77] A final draft was written, called "Strengthening the Implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity." The Plan is divided into strategic actions done by the United Nations, member states, regional intergovernmental organizations, civil society, the media, internet companies, and academia.[78] The draft recommends establishing reporting systems for attacks against journalists and considering gender-specific threats and violence, expanding media coverage of attacks towards journalists, and ensuring updated ethical standards and protocols for protecting journalists and media freelancers.[79] While this plan has not been officially published, it contains adequate suggestions for corruption and press freedom issues and serves as a starting point.

Journalists cannot practice civic engagement if they do not have the right to freedom of expression. In an environment where journalists are protected and democracy is ensured, citizens have quality and reliable information. Freedom of expression in journalism endorses quality education, democratic governance, poverty reduction, and a culture of justice and human rights.[80] Furthermore, under-resourced media leads to increased corruption. When journalists have low salaries and the economic needs of the press staff are not met, legitimate reporting will not be a priority. In these cases, journalists have more incentive to accept bribes from public officials in exchange for flattering reporting. A common form of corruption in these types of cases is media capture, which is when private or governmental entities utilize the media for their own interests.[81] In these scenarios, press corruption and bribery are frequent in countries with emerging economies. The media has a large role in fighting corruption. It helps curb corruption by increasing citizen access to information, which in turn keeps public officials in check. Press freedom can mobilize individuals and build pressure for reform.[82] However, in some countries, the press and media can be easily corrupted, as many countries lacking training and technical skills have limited financial resources for journalists, who face significant governmental opposition and the enforcement of undemocratic laws.[83] Developing countries are also at the risk of having government-owned media outlets, which are more prone to government influence.[84] Therefore, delegates should consider how providing resources and support to professionals can impact the integrity of the press.

Now more than ever, the press relies on non-traditional sources of revenue, which do not come from physical sales.[85] These include sponsored content, funding from advertisements, or crowd-sourced public funding. This sets a landscape where state subsidies, private contributions, or other funding means can present a challenge to neutrality in journalism.[86] This issue has been seen in countries such as Macedonia and Serbia, where the government uses taxpayer money to fund media outlets that showcase pro-government news. It is essential that media companies disclose financial information regarding their sources of income, as this expands transparency and press freedom.[87] The press can fight corruption through regulatory bodies created to ensure ethical and moral standards in the profession. These bodies are common in many countries and work independently from the government. In Rwanda, public officers often bribe journalists by giving them *giti* (gifts) for a specific news posting.[88] To safeguard against this, the Media High Council was created. It is a regulatory institution seeking to end media corruption through a code of ethics

76 *Strengthening the Implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity,* (Geneva: UNESCO and the UN Office of the High Commission on Human Rights, 2017), https://www.ohchr.org/sites/default/files/Documents/Issues/Journalists/OutcomeDocument.pdf.
77 *Strengthening the Implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity.*
78 *Strengthening the Implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity.*
79 *Strengthening the Implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity.*
80 *Strengthening the Implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity.*
81 Mendes, *Overview of corruption in the media in developing countries.*
82 Mendes, *Overview of corruption in the media in developing countries.*
83 Mendes, *Overview of corruption in the media in developing countries.*
84 Mendes, *Overview of corruption in the media in developing countries.*
85 Sosa Cordero, "Three ways to fight corruption in the media."
86 Sosa Cordero, "Three ways to fight corruption in the media."
87 Sosa Cordero, "Three ways to fight corruption in the media."
88 Mendes, *Overview of corruption in the media in developing countries.*

for journalists.[89] These bodies don't necessarily need to be councils; they can also be internal review systems or civil society organizations.[90] By providing investigative journalists with codes of conduct and constructive integrity training, media companies can drive transparency in journalism. Delegates should consider mechanisms for funding the media in transparent and unbiased ways to protect and support journalists.

The press can act as agenda setters; this means their work can make corruption a topic of public discourse. By discussing issues and drawing attention to such, the media can compel politicians to reconsider legislation or practices.[91] The creation of legal frameworks which promote transparency is necessary to fight corruption. NGO Reporters without Borders in Colombia has taken significant steps to achieve this.[92] The organization created a database available for the public to examine the concentration of media ownership. Reporters Without Borders publishes analyzed data about the media companies' holdings and the owners.[93] This allowed for more transparency in media, which strengthens public trust and can enhance political stability within a country. Another example of a notable practice is an Austrian law requiring media companies to disclose all financial stakeholders.[94] Requiring this transparency holds these companies accountable for their sources of funding and possible conflicts of interest. This improves the reliability of the information provided on these platforms and strengthens public trust in them as well.

Ideally, in the interest of limiting corruption and maximizing freedom of the press, laws and constitutional guarantees should prohibit any sort of censorship, government violence, and threats toward the media, ensure free access to valid information and news, and be transparent about the funds and administration behind any media outlet. Organs such as the UNCAC can ensure, through legal planning and enforcement, that the press can enjoy freedoms.

Impact of the Press on Corruption

Exposing corruption through journalism can be risky and challenging, resulting in legal issues or life-threatening situations for journalists.[95] The media can help ensure what is outlined in Article 19 of the UN Covenant of Civil and Political Rights, which is that everyone shall have the right to hold opinions without interference and that everyone shall have the right to freedom of expression.[96] Article 19. The press can raise awareness of moral standards, act as watchdogs against corruption, strengthen the media's independence, promote integrity and accountability, and encourage citizens to support anti-corruption efforts.[97]

Revealing corruption through journalism can lead to the resignation or impeachment of public officials.[98] In South Africa, thanks to massive press reports on government corruption, the Office of the Public Protector launched investigations. The Nkandla report in 2014 and the State Capture report in 2016 found illegal activity by the former president, Jacob Zuma. Consequently, Zuma resigned in 2018.[99] In general, the press can create a space for accountability, plurality, and legitimacy. This way, they are responsible for maximizing different societal perspectives, leading to increased public debate and policy discussions.

Investigative journalism has had a massive impact on corruption. This type of journalism involves interviews with politicians, in-depth research into government affairs, validating information, and intensive investigation. It requires financial resources, international and national networks, and working with researchers. It has led to positive outcomes, as the press can monitor the government and its actions by

89 Mendes, *Overview of corruption in the media in developing countries.*
90 Mendes, *Overview of corruption in the media in developing countries.*
91 Arnold and Lal, *Using Media to Fight Corruption.*
92 Sosa Cordero, "Three ways to fight corruption in the media."
93 Sosa Cordero, "Three ways to fight corruption in the media."
94 Sosa Cordero, "Three ways to fight corruption in the media."
95 "How to expose corruption, vice, and incompetence - by those who have," The Guardian, last modified October 14, 2021, https://www.theguardian.com/membership/2021/oct/14/laws-changed-around-the-world-why-investigative-journalism-matters.
96 "International Covenant on Civil and Political Rights," United Nations Human Rights, accessed August 14, 2022, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
97 Schauseil and Jackson, *Media and anti-corruption.*
98 "The role of the media in fighting corruption," UN Office on Drugs and Crime, accessed September 15, 2022, https://www.unodc.org/e4j/en/anti-corruption/module-10/key-issues/the-role-of-the-media-in-fighting-corruption.html.
99 UNODC, "The role of media in fighting corruption."

highlighting cases of maladministration and abuse of power. In India, the small and independent press organization Tehelka has been able to uncover corruption in defense deals. The organization started by releasing stories about match-fixing in cricket. It evolved and exposed defense deals and bribes that some public officials accepted or demanded. This caused the government to set up a commission of inquiry and the military to initiate proceedings against the personnel involved. Despite receiving threats and backlash from the government, the newsmagazine continues. What started as a small press company has evolved into a big news outlet that exposes corruption and gets tangible results.[100]

In other cases, after the media uncovered corrupt payments involving telecom contracts in Uzbekistan, Sweden's Telia Company agreed to pay penalties of at least USD 965 million to the United States and international authorities in 2017, and Russia's VimpelCom agreed to pay USD 835 million to settle a case following a media investigation of corrupt payments in 2016.[101] Exposing corrupt deeds can yield positive results and greater accountability. Also in Russia, the media generated much publicity around President Vladimir Putin's seaside estate, called "Putin's palace" on the Black Sea. This news story was reported on by individuals from various countries and crossed international boundaries to expose serious, long-term corruption; reports contain allegations of vast corruption schemes related to the USD 1.4 billion property cost.[102]

Additionally, the Pandora Papers, a leak of almost 12 million documents, which document the corrupt economics of the world's rich and powerful, required more than 600 journalists in 117 countries to sort through and interpret the files for months.[103] These types of international cooperation demonstrate how international collaboration can protect journalists and improves the coverage of corruption and bad actors across the globe.[104] Thus, it is unsurprising that studies show greater press freedom relates to significantly fewer instances of bribery involving public officials. Overall, businesses in freer-press countries report that corruption is not the biggest problem they face.[105]

Whistleblowing is reporting illegal activities done by a government or organization, mainly corruption-related.[106] Individuals who take the risk to blow the metaphorical whistle must be subsequently protected. This group especially needs special consideration, as they may become targets for retaliation. UNCAC has developed whistleblower projects and legal protections for whistleblowers. The Fast-Tracking UNCAC Implementation Project prioritizes ensuring identity protection for whistleblowers, dialogue with stakeholders, and the application of protective measures when carrying out investigations.[107] Through this, journalists can be protected to some extent from acts of violence.

UNCAC's whistleblower protection project includes providing a systematic assessment of the imminence of the risk and seriousness of the situation, legal support and service, and even medical and psychological support. These methods have been enforced among the G20 countries. The Protection of Whistleblowers legal framework ensures all services mentioned previously. The approved framework ensures protection against criminal charges, provides anonymity and confidentiality, and it even creates new reporting channels.[108] This last resource has benefited South Korea, which established a telephone hotline to receive whistleblowers' reports. In the United Kingdom, the UK Public Interest Disclosure Act ensures a safe channel of reports done by internal disclosures, regulatory disclosures, and broader disclosures to the police,

100 Anne-Katrin Arnold and Sumir Lal, *Using Media to Fight Corruption*, (Washington: Partnership for Transparency Fund, 2012), https://www.ptfund.org/wp-content/uploads/2018/07/WP01-Media-to-Fight-Corruption.pdf.
101 Nouf Binhadab, Michael Breen, and Robert Gillanders, "Press freedom and corruption in business-state interactions," *Economic Systems*, 45(4) (2021), https://www.sciencedirect.com/science/article/pii/S0939362521000704.
102 Mary Ilyushina, "Navalny releases investigation into decadent billion-dollar 'Putin palace'," *CNN*, last updated January 20, 2021, https://www.cnn.com/2021/01/20/europe/putin-palace-navalny-russia-intl/index.html.
103 Pandora Papers reporting team, "Pandora Papers: A simple guide to the Pandora Papers leak," *BBC News,* last updated 5 October 2021, https://www.bbc.com/news/world-58780561.
104 Binhadab, Breen, and Gillanders, "Press freedom and corruption in business-state interactions."
105 Binhadab, Breen, and Gillanders, "Press freedom and corruption in business-state interactions."
106 "Whistleblowing," UNCAC Coalition, accessed August 3, 2022, https://uncaccoalition.org/learn-more/whistleblowing/.
107 "FOCUS AREAS - WHISTLEBLOWER PROTECTION," United Nations Office on Drugs and Crime, accessed September 29, 2022, https://www.unodc.org/unodc/en/ft-uncac/focus-areas/whistleblower.html.
108 *Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation*, (Seoul: G20, 2010), https://www.oecd.org/g20/topics/anti-corruption/48972967.pdf.

media, and parliament members.[109]

Already, brave journalists have risked their personal safety for the sake of informing the public. Their coordinated and individual efforts have created tangible impacts on politics and society. They must be protected, as is their right, but also their work serves an essential function in the fight against corruption on global and local scales.

Current Status

Case Studies

A watchful media has the potential to impact political processes such as elections.[110] Government officials up for re-election aim to maximize their positive media coverage and are willing to bribe media outlets for more favorable coverage.[111] To maintain their power, some governments go to great lengths to silence the press.[112] Political and economic motives, combined with a lack of regulatory and transparency policies, make corruption and censorship a reality.

One recent case of press censorship is in Ghana. A study done by Dr. Joseph Yaw Asomah, a Ph.D. graduate in sociology from the University of Saskatchewan and a specialist in political sociology, human rights, and international development, revealed that different agents had different reasons and motivations to influence the media. These agents include journalists, politicians, and media owners.[113] Politicians have a strategic plan to silence journalists' voices. One of the journalists interviewed for the research—titled "What Motivates Some Ghanaian Private Media To Expose Political Corruption?"—confessed that he has received monetary compensation in exchange for silencing coverage about a politician.[114] There are also ongoing violent acts toward journalists in Ghana, which inhibit press freedom and security. In 2019, Ahmed Hussein-Suale, an investigative journalist, was murdered in Ghana, and police believe it was due to his career as a journalist.[115] Despite this, Ghana has improved conditions through fiscal programs and has achieved the country's personal highest rank in the history of the Press Freedom Index.[116] Though it has a long way to go, Ghana serves as an example that countries that rank low on the Press Freedom Index have the capacity to improve.

Colombia is considered one of the most dangerous countries for journalists.[117] Journalists in Colombia suffer different forms of corruption, such as manipulation by politicians, blackmailing, and irregular contractual relationships between journalists and companies.[118] Furthermore, there is no employment security for journalists, as only 51 percent of Colombian journalists have permanent contracts. This inhibits journalists from following a consistent career, as they can be frequently manipulated to comply in order to keep their job.[119] Many professionals have either a year-long contract or simply make their salary from advertisements.[120] Because of loose job security, they can be vulnerable to corruption tactics, especially since there are no good employment terms, protections, or rights for journalists in Colombia. To remediate this, Colombia and countries with similar press freedom circumstances should invest in career stability and security programs for journalists and prioritize their security and safety. These steps will help overall media transparency.

The media plays an important role in society by bringing governmental and private corruption to light, yet they

109 *Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation*
110 Jonathan A. Solis and Leonardo Antenangli, *Corruption is Bad News for Free Press: Reassessing the Relationship Between Media Freedom and Corruption*, (Wiley Online Library, August 2017), https://onlinelibrary.wiley.com/doi/pdf/10.1111/ssqu.12438.
111 Solis, *Corruption is Bad News for Free Press: Reassessing the Relationship Between Media Freedom and Corruption.*
112 Paul Glickman, *OFF LIMITS OFF LIMITS OFF LIMITS CENSORSHIP AND CORRUPTION CENSORSHIP AND CORRUPTION* (New York: Human Rights Watch, 1991), https://www.hrw.org/report/1991/07/01/limits/censorship-and-corruption.
113 Joseph Yaw Asomah, "Why some of Ghana's private media fight corruption: reasons, rules, and resources," The Conversation, last modified October 21, 2021, https://theconversation.com/why-some-of-ghanas-private-media-fight-corruption-reasons-rules-and-resources-169254.
114 Yaw Asomah, "Why some of Ghana's private media fight corruption.
115 Joel Gunter, "Murder in Accra: The life and death of Ahmed Hussein-Suale," *BBC Africa Eye*, January 30, 2019, https://www.bbc.com/news/world-africa-47002878.
116 Gunter, "Murder in Accra."
117 Ethical Journalism Network, *Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom.*
118 Ethical Journalism Network, *Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom.*
119 Ethical Journalism Network, *Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom.*
120 Ethical Journalism Network, *Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom.*

are consistently compelled to succumb to corruption themselves. The Organization for Economic Co-operation and Development (OECD) published the results of an investigative journalism survey, asking journalists to rate how safe they felt reporting on corruption cases.[121] Only 35 percent of journalists reported said they felt moderately safe, while most were concerned about actual legal action that could be taken against them.[122] These threats have escalated in some countries, especially for independent journalists not operating under a large corporation.[123] For example, on October 16, 2017, the Maltese anti-corruption journalist Daphne Caruana Galizia, mentioned earlier, was murdered after her many investigations into crime and corruption throughout Malta, specifically within their energy sector.[124] Her work as an investigative journalist and activist had broad economic and public image implications for Malta. This emphasizes that modern-day journalism is heavily impacted by corruption, and governments and anti-corruption agencies need to take substantive action to protect these journalists.

Exposing Corruption through Online Media

As the world becomes increasingly technology-driven, online press corruption is increasingly prevalent. The 2016 Panama Papers revealed corruption cases related to powerful politicians, tax evasion, and offshore companies.[125] Journalists involved in the investigation of these cases had access to databases and records, which simplified the whistleblowing process. Nevertheless, not all corruption was exposed. As journalists were looking for more information online, government officials were already hiding relevant information about their bribery schemes.[126]

China's "Great Firewall" is a prominent example of a government controlling what information is available to the public.[127] The Great Firewall routes all international internet traffic through strictly controlled access points that block a vast number of websites deemed unacceptable.[128] These are mostly websites used to search for information about what is happening outside of China or social media sites that contain critical reviews of the Chinese government. This method allows China to control what the public sees and forms opinions about. From Transparency International's Global Corruption Barometer, around 66 percent of people around the world think government corruption in China is a large issue that needs to be addressed.[129] That, combined with China's internet blockage, indicates major press corruption efforts within the country that aim to preserve China's image of power and stability for its citizens. China's citizens cannot speak poorly about the government anywhere online, or they will be harshly punished and arrested.[130]

The increasing complexity of technology helps governments hide corruption efforts. However, society's almost instantaneous and universal access to modern media plays a major role in holding government officials accountable for their actions.[131] As of this year, a total of 5 billion people use or have access to the Internet—63 percent of the world's population.[132] Today, social media also plays a large role in press freedom, as many turn to personal media platforms to expose injustice, corruption, and personal stories. There are around 4.7 billion social media users worldwide, showing the power civilian internet usage can have on world events and influencing public attitudes.[133] With society's ability to find and spread information, politicians are wary about records of past actions because social media can taint their public image considerably.

121 *The Role of the Media and Investigative Journalism in Combating Corruption*, (OECD, 2018), https://www.oecd.org/daf/anti-bribery/The-role-of-media-and-investigative-journalism-in-combating-corruption.pdf.
122 OECD, *The Role of the Media and Investigative Journalism in Combating Corruption*.
123 OECD, *The Role of the Media and Investigative Journalism in Combating Corruption*.
124 OECD, *The Role of the Media and Investigative Journalism in Combating Corruption*.
125 Nicholas Sorak, *Internet, Censorship, and Corruption* (University of Gothenburg, 2016), https://www.gu.se/sites/default/files/2020-05/QoGWP_2016_17_Sorak.pdf.
126 Sorak, *Internet, Censorship, and Corruption*.
127 Dennis Normile, "Science suffers as China's internet censors plug holes in Great Firewall," Science.org, last modified August 30, 2017, https://www.science.org/content/article/science-suffers-china-s-internet-censors-plug-holes-great-firewall?cookieSet=1.
128 Normile, "Science suffers as China's internet censors plug holes in Great Firewall."
129 "Country Data," Transparency International, accessed September 14, 2022, https://www.transparency.org/en/countries/china.
130 Normile, "Science suffers as China's internet censors plug holes in Great Firewall."
131 Sorak, *Internet, Censorship, and Corruption*.
132 "Digital Around the World," DATAREPORTAL, accessed September 14, 2022, https://datareportal.com/global-digital-overview.
133 "Digital Around the World," DATAREPORTAL

Turkish Journalists protesting imprisonment of their colleagues on Human Rights Day 2016.

Credit: Hilmi Hacaloğlu

There is an existing link between a population's level of education and corruption. If a population is more informed about the subject of corruption, they will most likely reject governmental corruption.[134] Nevertheless, governments and politicians often limit the population from being more educated about corruption so civilians do not reject measures taken by these officials. For instance, in 2016, the Turkish government shut off access to social media platforms such as Twitter, YouTube, and Facebook amid a coup attempt.[135] This was possible because a 2007 law permitted the government to ban or block websites.[136] The shutdown of popular sites led to large protests in Istanbul. Organizations such as AccessNow, a digital rights advocacy organization, began fighting against digital censorship.[137]

Free mass media can serve as a system to fight corruption. It allows society to keep a watch on all major political decisions, leaving input as they feel fit.[138] People have the ability to hold elected leaders accountable, which can manifest in public protests against government corruption and increased advocacy for important issues.[139] Even in countries with censorship of traditional media, major political and economic decisions throughout the country can be attributed to public participation in online media.[140] However, delegates should be aware that not all corruption can be exposed through online media and more solutions need to be discussed to address the issue of press corruption. These can include independent review bodies, oversight mechanisms, increased transparency initiatives, funding for career security and safety for journalists, and many more pathways.

Sustainable Development Goals

The 2030 Agenda for Sustainable Development was adopted by all UN member states in 2015. The agenda encompasses 17 Sustainable Development Goals (SGDs) and 169 target goals, all with the purpose of improving international development, strengthening global partnerships, and achieving world peace. The Sustainable Development Goals relevant to corruption

134 Sorak, *Internet, Censorship, and Corruption.*
135 Julia Carrie Wong, "Social media may have been blocked during Turkey coup attempt," *The Guardian*, July 15, 2015, https://www.theguardian.com/world/2016/jul/15/turkey-blocking-social-facebook-twitter-youtube.
136 Wong, "Social media may have been blocked during Turkey coup attempt."
137 Wong, "Social media may have been blocked during Turkey coup attempt."
138 Christopher Starke, Teresa K. Naab, and Helmut Scherer, "Free to Expose Corruption: The Impact of Media Freedom, Internet Access, and Governmental Online Service Delivery on Corruption," International Journal of Communication, 10, (2016), 4702-4722, https://ijoc.org/index.php/ijoc/article/view/5712/1793.
139 Starke, Naab, and Scherer, "Free to Expose Corruption."
140 Ruben Enikolopov, Maria Petrova, and Konstantin Sonin, "Social Media and Corruption," American Economic Journal, 10, no. 1, (Jan. 2019), 150-174, https://pubs.aeaweb.org/doi/pdfplus/10.1257/app.20160089.

Volunteer Katiuska Rodrigues from The Refugees' Voice interviews a prosecutor at their studio.

Credit: Allana Ferreira/UNHCR

are SDG 16: Peace, Justice and Strong Institutions and SDG 17: Partnerships for the Goals.[141] The SDGs serve as a guide for developing comprehensive and creative solutions.

The first SDG related to press corruption is SDG 16: Peace, Justice and Strong Institutions, which focuses on promoting peaceful societies and providing access to justice to build effective and accountable public and private institutions. This SDG advocates for global peace and ensures transparency among institutions. Some of its specific targets include significantly reducing all forms of violence, promoting the rule of law, reducing corruption and bribery in all forms, ensuring public access to information, and protecting fundamental freedoms.[142] Fundamental freedoms include the freedom of opinion and expression and the right to work and education.[143] Corruption "undermines democracy and the rule of law," which is a specific target that SDG 16 prioritizes.[144] One of the most recent but significant actions regarding SDG 16 is related to press freedom. The UN COVID-19 response has supported the project *La Voz de Los Refugiados* (The Refugees' Voice), a community radio program hosted in Brazil by Venezuelan refugees, which focuses on fighting disinformation about the Venezuelan political situation, as well as other topics.[145] In order to achieve peace and stronger institutions, it is important for journalists and information outlets to feel safe.

The second goal related to press corruption is SDG 17: Partnerships for the Goals. This SDG connects closely to all other SDGs. It seeks to encourage multiple groups to work together to achieve each of the other 16 goals.[146] The topic is strongly linked to Target 17.14, which states, "enhance policy coherence for sustainable development."[147] This means that countries should have a system to enforce policies and legislation to achieve set goals. This SDG is extremely relevant to this topic as it promotes partnerships between countries, which can improve transparency within government agencies.[148] Corruption is a major impediment

141 "Do you know all 17 SDGs?" UN Department of Economic and Social Affairs, accessed September 27, 2022, https://sdgs.un.org/goals.
142 "Goal 16," UN Department of Economic and Social Affairs, accessed September 27, 2022, https://sdgs.un.org/goals/goal16.
143 "Human Rights," United Nations, accessed September 27, 2022, https://www.un.org/en/global-issues/human-rights.
144 Matthew Jenkins, "TRACKING CORRUPTION ACROSS THE SUSTAINABLE DEVELOPMENT GOALS," Transparency International, last modified March 25, 2021, https://www.transparency.org/en/blog/tracking-corruption-across-the-sustainable-development-goals.
145 "Community radio fights misinformation for Venezuelan refugees and migrants in Brazil," United Nations, accessed September 27, 2022, https://www.un.org/en/coronavirus/community-radio-fights-misinformation-venezuelan-refugees-and-migrants.
146 "Goal 17," UN Department of Economic and Social Affairs, accessed September 27, 2022, https://sdgs.un.org/goals/goal17.
147 UN Department of Economic and Social Affairs, "Goal 17."
148 "Goal 17: Revitalize the global partnership for sustainable development," United Nations Sustainable Development Goals,

Committee to Protect Journalists (CPJ) having a virtual meeting with Secretary of State Antony Blinken, which enforces partnerships for the goals especially when it comes to protecting journalists.

Credit: U.S. Department of State

to development, so it should be considered a priority in the achievement of SDG 17.[149] Some examples of partnerships include the ones existing between the UN Economic and Social Council (ECOSOC) and other UN entities, where they host discussions with important leaders in public, private, and non-profit sectors to talk about how to achieve SDGs.[150]

Bloc Analysis

Points of Division

Press corruption involves both media and corrupt governments or agencies. It is relevant to include both press freedom and corruption measurements in order to understand how countries will approach corruption. When examining press freedom and corruption, it is important to understand all points of contention. For example, if a government holds enormous power over the press, it will focus on censorship strategies and limit transparency. Countries with a low corruption index and high press freedom will most likely defend freedom of expression. Some countries restrict freedom of the press, while others have little to no regulations on the media. Press corruption within a country can be measured by the amount of corruption, press freedom, and type of governance. For the purpose of analyzing blocs within the UNCAC committee, the Corruption Perceptions Index (CPI) and the World Press Freedom Index will be utilized.

The Corruption Perceptions Index (CPI) was developed in 1995 by the international non-governmental organization Transparency International as an indicator to measure perceptions of corruption among the public sector of countries.[151] The methodology for this report includes "selection of source data, rescaling source data, aggregating the rescaled data, and then reporting a measure for uncertainty."[152] In other words, the index is calculated through the research and analysis of diverse sources regarding bribery, diversion of public funds, or even nepotism within civil service.[153] It also utilizes sources such as the World Justice Project Rule of Law Index or the Political Risk Services International Country

accessed September 27, 2022, https://www.un.org/sustainabledevelopment/globalpartnerships/.
149 Mari Elka Pangestu, "Working in partnership is key to fighting corruption," World Bank Blogs, last modified September 23, 2020, https://blogs.worldbank.org/voices/working-partnership-key-fighting-corruption.
150 "ECOSOC Partnerships Forum," UN Economic and Social Council, accessed September 27, 2022, https://www.un.org/ecosoc/en/ecosoc-partnerships-forum.
151 "Corruption Perception Index," Transparency International, accessed September 30, 2022, https://www.transparency.org/en/cpi/2020.
152 Transparency International, "Corruption Perception Index."
153 Transparency International, "Corruption Perception Index."

Risk Guide.[154] Results are given on a scale from 0-100, 0 being highly corrupt and 100 corruption-free.[155]

The World Press Freedom Index is published every year by the international non-governmental organization Reporters Without Borders.[156] According to this organization, "press freedom is defined as the ability of journalists as individuals and collectives to select, produce, and disseminate news in the public interest independent of political, economic, legal, and social interference and in the absence of threats to their physical and mental safety."[157] The index measures freedom of the press in every country and demonstrates whether the media and journalists can exercise their freedom of speech. The Index scores range from 0-100, with 100 being the top score and 0 being the lowest.[158] The criteria used for the World Press Freedom Index is based on political, legal, economic, sociocultural, and safety contexts.[159] For example, political context involves how the government respects the media's right to freedom of expression. The legal aspect consists of analyzing the absence or presence of impunity for violence committed against journalists.[160]

Low Scoring Countries (0–30 points)

Countries in this bloc have a significant issue of corruption and press censorship within their territory. The majority of the countries within the lowest index ranking possess issues with their governments and experience economic instability. For example, one of the lowest-ranked countries is Venezuela, with a score of 14 in the CPI. Tulia Falleti, a political science professor and Director of Latin American and Latino Studies at the University of Pennsylvania, has analyzed Venezuelan politics under the authoritarianism exerted by President Nicolas Maduro and undemocratic electoral processes. Since 2017, the Venezuelan government has increased political repression against government opponents. The political situation generates barriers for the media to exercise freedom of speech. In this case, the political context is taken into consideration when researching countries and ranking them in the CPI.

A similar analysis goes into the Press Freedom Index. In this index, the Democratic People's Republic of Korea

154 Transparency International, "Corruption Perception Index."
155 Transparency International, "Corruption Perception Index."
156 "Detailed Methodology," Reporters Without Borders, accessed September 27, 2022, https://rsf.org/en/index-methodologie-2011-12.
157 "Methodology used for compiling the World Press Freedom Index," Reporters Without Borders, accessed September 27, 2022, https://rsf.org/en/index-methodologie-2022.
158 Reporters Without Borders, "Methodology used for compiling the World Press Freedom Index."
159 Reporters Without Borders, "Methodology used for compiling the World Press Freedom Index."
160 Reporters Without Borders, "Methodology used for compiling the World Press Freedom Index."

Protest banner in Venezuela, 2014, which states "Why do Venezuelans protest? Insecurity, injustice, shortages, censorship, violence and corruption. Protesting is not a crime, it is a right."

Credit: Jamez42

(DPRK) has the lowest ranking on the list. According to Reporters Without Borders, DPRK is one of the world's most authoritarian regimes, controlling information and prohibiting independent journalism.[161] North Korea's issues are tied to its own political, economic, and sociocultural history. North Korea is under a regime of heightened surveillance, censorship, and repression. Foreign media outlets are almost incapable of being transmitted in this country, and journalists are routinely put in danger.[162] Furthermore, internet technology in the country is meticulously filtered and surveilled by the government.[163]

It is of extreme importance to understand that a country can have a high corruption index and low press freedom due to its political, economic, legal, and sociocultural aspects. Unfortunately, it is the population that ends up being more affected by the situation. Nevertheless, other countries should be comprehensive and respectful in understanding how these low-ranked countries operate.

Finally, it is relevant to mention that while many countries in this bloc might have similar objectives and problems, there may be a few differences. Some countries may still want to maintain control over the press, while others are fighting to end this issue. For example, Sierra Leone is working diligently to improve press freedoms. The 2002 elections brought onto the table a dangerous law that endorsed media censorship. This was to preserve the government's image after the civil war in 1991.[164] Those in power continued to oppress the media and journalists for years. It was not until 2020 that a new presidential election brought an end to this censorship law, concluding the practice of criminalizing journalism in the country.[165] Some of the actions taken to improve press freedom were founding an independent media commission, creating a national fund for the media, and promoting transparent advertisements.[166] Sierra Leone's situation emphasizes the capacity of countries to improve their corrupt systems by expanding transparency, stability, and security for journalists, as well as the public.

Medium Scoring Countries (30–65 points)

Countries in this bloc have a moderate issue of corruption and press censorship within their territory. While it is not as detrimental as the previous bloc, they still have a long journey to achieve a high score in both indexes. Eastern Europe and Central Asia regions hold an average CPI score of 39.[167] Over the course of the COVID-19 pandemic, these regions have experienced attacks on freedom of expression, manifested through the dangerous and violent rhetoric of authoritarian regimes as well as a pattern of unjustified imprisonment of journalists.[168] Albania is one of the countries affected by corruption and press censorship in Eastern Europe and Central Asia. Albania suffered economically due to the COVID-19 pandemic as well as from earthquakes that took place in the country preceding the pandemic in 2019.[169] The Albanian government used this to restrict civil freedoms against non-governmental organizations.[170] As a result, a few economically and politically powerful individuals controlled the Albanian media. The government contracted a private business, Acromax Media GmbH, and filtered online media content on platforms such as Facebook.[171] Acromax Media is a company focused on "digital rights management," but they have banned online content in Albania related to certain politicians. The content banned was short clips criticizing politicians, political statements, scandals, and even music from local Albanian artists.[172] The reason for this was to censor

161 "North Korea," Reporters Without Borders, accessed September 27, 2022, https://rsf.org/en/country/north-korea.
162 Reporters Without Borders, "North Korea."
163 Reporters Without Borders, "North Korea."
164 Devin Windelspecht and Ume A Sarfaraz, "In Sierra Leone, a rare opening for press freedom," *International Journalists' Network,* July 8, 2022, https://ijnet.org/en/story/sierra-leone-rare-opening-press-freedom.
165 Windelspecht and Sarfaraz, "In Sierra Leone, a rare opening for press freedom."
166 Windelspecht and Sarfaraz, "In Sierra Leone, a rare opening for press freedom."
167 "CPI 2021 FOR EASTERN EUROPE & CENTRAL ASIA: DEMOCRATIC HOPES IN THE SHADOW OF GROWING AUTHORITARIANISM," Transparency International, last modified January 25, 2022, https://www.transparency.org/en/news/cpi-2021-eastern-europe-central-asia-democratic-hopes-growing-authoritarianism.
168 Transparency International, "CPI 2021 FOR EASTERN EUROPE & CENTRAL ASIA."
169 Gjergji Vurmo, "Nations in Transit 2021: Albania," Freedom House, accessed September 27, 2022, https://freedomhouse.org/country/albania/nations-transit/2021.
170 Vurmo, "Nations in Transit 2021: Albania."
171 Vurmo, "Nations in Transit 2021: Albania."
172 Johannes Estrada, "Acromax Media — Albanian Government's Tool for Online Political Censorship," *Exit News,* August 19, 2019, https://exit.al/en/2019/08/19/acromax-media-albanian-governments-tool-for-online-political-censorship/.

information that did not benefit Edi Rama and Erion Veliaj, Albanian politicians who ran a political campaign to gain mayoral positions.[173]

This problem in Eastern Europe and Central Asia is mostly caused by rising authoritarian governments. Corruption has allowed public figures to escape prosecution while still benefiting from government funding. There have been many cases of human rights abuses and freedom of the press violations against the general population, whereas political figures enjoy more freedom. For instance, Ilham Aliyev, Azerbaijan's President, had several journalists either imprisoned or tortured under his regime while he enjoyed a USD 650 million property in London, United Kingdom.[174] This scandal was exposed by the Pandora Papers, a set of documents that exposed politicians and other public figures and their ties with corruption and offshore shell companies.[175]

Countries in this bloc will focus on examining political, economic, legal, and sociocultural contexts regarding corruption and press freedom. While their situations might not be as extreme as the previous bloc category, they are at risk of falling under the rule of an authoritarian government. For this bloc, there should be an emphasis on reconstructing legal measures to ensure press freedom, especially after the COVID-19 pandemic. Delegates are encouraged to end corruption and press censorship by improving existing political, economic, and legal mechanisms.

High Scoring Countries (65–100)

Countries in this bloc have a handle on corruption and press censorship in their territory, meaning the press has more freedom of speech. Some countries include Denmark, Finland, New Zealand, Norway, Singapore, and the Netherlands. Denmark has the highest CPI score at 88. The country hosts eight national newspapers, five national radio channels, two public television stations, and eight regional television channels.[176] They are experiencing a growing market for online news outlets. In general, political institutions respect press freedom, but journalists can still be imprisoned for publishing information that threatens national security.[177] Another aspect that makes Denmark the highest ranked in the CPI is that media channels are self-governed. This independence ensures their freedom, as the government cannot interfere with their decisions on what to publish. There are existing media accountability systems with self and co-regulatory frameworks.[178] This means that workers and industry actors are responsible for monitoring and complying with relevant legislation. This shifts some of the burdens of oversight from the government to industry, which is often public-run in Denmark.[179]

While a country such as Denmark enjoys press freedom and little to no corruption, there is still a prevalent threat through digital misinformation and online content. As the UN Secretary-General, Antonio Guterres, quoted, "Digital technology has democratized access to information. But it has also created serious challenges."[180] Most of the goals of these online sources of information are purely to engage and entertain readers, which breeds misinformation and lies.[181] There is no regulation when it comes to what journalists or citizens can post online.

Press freedom is still relevant to maintain, even if journalists are employing online platforms to spread messages. Thus, it is important to find a balance between regulations and censorship, as digital journalism can be a starting point for misinformation and lies. Overall, countries of this bloc should act as an example for other members of UNCAC. By decreasing government-owned media outlets, enforcing press freedom agencies, and promoting transparency from

173 Estrada, "Acromax Media — Albanian Government's Tool for Online Political Censorship."
174 Margot Gibbs and Agustin Armendariz, "The Landlords," *International Consortium of Investigative Journalists,* November 3, 2021, https://www.icij.org/investigations/pandora-papers/the-land-lords/.
175 Gibbs and Armendariz, "The Landlords."
176 "Denmark," Reporters Without Borders, accessed September 27, 2022, https://rsf.org/en/country/denmark.
177 Reporters Without Borders, "Denmark."
178 "Nordic countries top 2021 World Press Freedom Index," Study in Denmark, accessed September 29, 2022, https://studyindenmark.dk/news/nordic-countries-top-2021-world-press-freedom-index.
179 "Definitions, concepts, and examples," European Economic and Social Committee, accessed September 29, 2022, https://www.eesc.europa.eu/en/definitions-concepts-and-examples.
180 "Focus on the digital challenge to journalism," UN in Western Europe, accessed September 29, 2022, https://unric.org/en/focus-on-the-digital-challenge-to-journalism/.
181 United Nations in Western Europe, "Focus on the digital challenge to journalism."

the government and their relations with the press, there is promise for the future.

Committee Mission

The purpose of the United Nations Convention Against Corruption is to fight against corruption through "prevention, criminalization and law enforcement measures, international cooperation, asset recovery, and technical assistance and information exchange."[182] One of the possible selected topics for this committee is "Corruption and Press Freedom," which can be tackled by the UNCAC mandate. The committee should focus on fighting against corruption and the power that governments and other related bodies exert over journalism. Delegates should aim to expose corruption, protect journalists and their freedom of expression, and develop ethical standards to ensure transparency between the governments and the press. In addition, the media can play an important role in preventing corruption by expanding oversight, promoting integrity, and engaging citizens with anti-corruption actions.[183]

Governments often pursue policies that do not take into consideration the perspectives and rights of individuals and instead focus more on the government's own benefit. Corruption and press censorship are clear examples of what a government is capable of doing regarding preserving its image and reputation.[184] Thus, delegates should not only focus on drafting frameworks to ensure media and governmental transparency but should also on strengthening relationships with media outlets and promoting integrity to citizens.

The main goal of the UNCAC is to prevent corruption at all costs across the international community by including preventing model policies, establishing anti-corruption bodies, and enhancing transparency in both government and the press.[185] Transparency and accountability are of extreme importance to this topic. Thus, in order to preserve global democracy, the UNCAC should incorporate solutions regarding transparency, accountability, policy, and restructuring of legal systems.

182 "The United Nations Convention against Corruption," UN Office on Drugs and Crime, accessed September 29, 2022, https://www.unodc.org/ropan/en/AntiCorruptionARAC/united-nations-convention-against-corruption.html.
183 Schauseil and Jackson, *Media and anti-corruption.*
184 Wafa Ben-Hassine, "Government Policy for the Internet Must Be Rights-Based and User-Centered," *UN Chronicle,* accessed September 27, 2022, https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred.
185 "UNCAC," Stolen Asset Recovery Initiative, accessed September 27, 2022, https://star.worldbank.org/focus-area/uncac.

UNCAC

NHSMUN 2023

TOPIC B:
CYBERCRIME AND CORRUPTION

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

Introduction

The world of digital technology is vastly new, so cybercrime and corruption still lack regulation. Cybercrimes are becoming more complex, and countries do not have the resources necessary to fight back against digital hackers. While some countries are familiar with the background of cybercrimes and cybersecurity, others lack the resources necessary for a working internet. Hackers with a wide range of intentions are either fueling the problem of cybersecurity or trying to make it better and improve the cybersecurity space for the greater good. Cyber security does not only affect countries but includes corporations, businesses, cyberterrorism, and more.

The importance of cybersecurity cannot be overlooked, as one of its many impacts is corruption. Issues such as internet fraud, digital awareness, national security, cyberterrorism, and the understanding of different types of hackers are all important to consider. A lack of digital awareness has led to a lack of resources to combat threats in the digital space. Without education, many countries do not know their next steps to combat cybercrimes and protect themselves from cyber-attacks. This can even place national security at risk. Terrorist organizations use the internet for recruitment and can hack into government organizations, banks, and other websites to gain advantages.

The severity of cyber attacks and crimes increases as time goes on. More countries are exposed to these attacks, and fewer know how to stop them from happening. Rather than working independently, there is a need to work together and collaborate to find different ways to combat the problem at hand. Cyber attacks cause billions of dollars in losses yearly, and the more time passes, the more vulnerable countries become.

Currently, there are few regulations on cybersecurity. The UN General Assembly recently voted to draft a "Cybercrime Treaty." However, there is disagreement on what the term "cybercrime" entails.[1] It can be defined as the use of digital devices to carry out a crime or illegal action.[2] Due to variations in laws around the world, what is illegal in one country may not be illegal in another, leading to difficulties in regulating cybercrime. In this committee, delegates will be tasked with finding common ground to combat corruption and how it manifests on the internet.

History and Description of the Issue

Internet Fraud

Internet fraud is a cybercrime involving software and online services to take advantage of victims. A common type of internet fraud is the denial of service (DoS) when traffic to a website is interrupted to cause a malfunction. Another common form of fraud is data breaches, in which criminals steal confidential information from individual users or organizations and move it to an untrusted location. This creates a higher risk of identity theft and the spread of sensitive personal information. These types of crimes account for millions of dollars in fraudulent activity every year. The amount will continue to increase as criminal techniques expand with internet advancements.[3]

A 2012 case in Nigeria emphasizes this point. Hope Olusegun Aroke is a convicted internet fraudster who scammed a maximum security prison worth at least USD one million and is currently serving a 24-year sentence. Nigeria's Economic and Financial Crimes Commission (EFCC) found that Olusegun Aroke was the leader of a network of fraud schemes across two continents. In prison, he managed to access the internet and a phone. He could also leave the prison to stay in hotels, meet with his family, and even attend social events. Aroke used a false name to open two bank accounts and buy a luxury car and multiple houses. He also possessed his wife's bank

1 Katitza Rodriguez and Meri Baghdasaryan, "UN Committee To Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope," *Electronic Frontier Foundation,* February 15, 2022, https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among.
2 Michael Aaron Dennis, "Cybercrime," accessed September 30, 2022, https://www.britannica.com/topic/cybercrime.
3 "What is internet fraud?" Fortinet, accessed August 26, 2022, https://www.fortinet.com/resources/cyberglossary/internet-fraud.

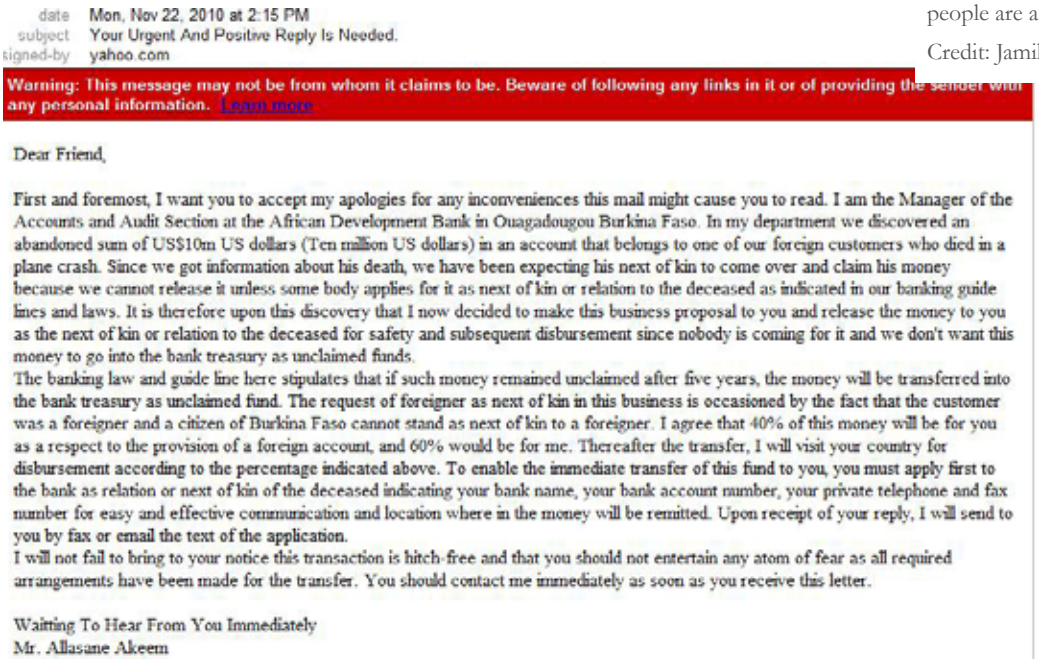
account token while in prison, which allowed him to carry out financial operations.[4]

It may seem shocking that a person can do all of the above in a maximum security prison. However, prison guards are often involved in corruption, as they are offered bribes to supplement their low salaries. In Aroke's case, there is an evident connection between corruption and cybercrime. However, hackers around the world have become more resourceful with their schemes to mishandle and gain private information. Their emails have become more believable, with information that looks like it is from a company. In the US, terms such as "wobblers" are used to categorize people who commit such acts. Their punishments may be consistent with a felony or misdemeanor standard. Therefore, a wobbler may be imprisoned, fined, or both.[5] The UK has specific laws against internet fraud as well. However, they are only punishable by a five-year prison sentence or a fine. Countries must work together to combat such crimes, as they rarely occur domestically. The internet's broad reach allows hackers to cause chaos wherever they choose.

Cybercrime is made up of 3 players: a victim, a motive, and an opportunity that enables the crime. With online services, victims and motives are more easily found. The third condition is met if the fraudster has the time, distraction, or need. In the past, natural disasters or social commotion have created a perfect landscape for internet fraud. This was the case during the Ebola virus outbreak in 2014. While it was not a worldwide pandemic, attackers took advantage of the upset it caused. Barracuda Networks, a company that provides security, networking, and storage products, reported 200,000 spam emails with Ebola news updates and 700,000 scam emails requesting donations to fake organizations. Largely, attackers will take advantage of people's fear and panic and exploit their empathy through internet fraud.[6]

Furthermore, the severity of internet fraud has increased drastically over the past years, especially during the COVID-19 pandemic. Businesses, citizens, and even agencies were targeted during the pandemic, tricked into sending large sums of money to hackers for various reasons. Unfortunately, most of the lost money is irretrievable, and many of these cases are still ongoing. Phishing websites reached their highest record levels in March and April 2020, as 2.2 times more users fell victim than the average. Increased use of online services and

4 "Internet fraud: Nigerian scammer 'pulls off $1m heist' from prison," *BBC News,* November 19, 2019, https://www.bbc.com/news/world-africa-50480495.
5 "Wobbler," Legal Information Institute, accessed July 15, 2022, https://www.law.cornell.edu/wex/wobbler.
6 Marzieh Bitaab, *Scam Pandemic: How Attackers Exploit Public Fear through Phishing,* (Arizona: Arizona State University), https://www.ftc.gov/system/files/documents/public_events/1582978/scam_pandemic_how_attackers_exploit_public_fear_through_phishing.pdf.



date Mon, Nov 22, 2010 at 2:15 PM
subject Your Urgent And Positive Reply Is Needed.
signed-by yahoo.com

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Dear Friend,

First and foremost, I want you to accept my apologies for any inconveniences this mail might cause you to read. I am the Manager of the Accounts and Audit Section at the African Development Bank in Ouagadougou Burkina Faso. In my department we discovered an abandoned sum of US$10m US dollars (Ten million US dollars) in an account that belongs to one of our foreign customers who died in a plane crash. Since we got information about his death, we have been expecting his next of kin to come over and claim his money because we cannot release it unless some body applies for it as next of kin or relation to the deceased as indicated in our banking guide lines and laws. It is therefore upon this discovery that I now decided to make this business proposal to you and release the money to you as the next of kin or relation to the deceased for safety and subsequent disbursement since nobody is coming for it and we don't want this money to go into the bank treasury as unclaimed funds.
The banking law and guide line here stipulates that if such money remained unclaimed after five years, the money will be transferred into the bank treasury as unclaimed fund. The request of foreigner as next of kin in this business is occasioned by the fact that the customer was a foreigner and a citizen of Burkina Faso cannot stand as next of kin to a foreigner. I agree that 40% of this money will be for you as a respect to the provision of a foreign account, and 60% would be for me. Thereafter the transfer, I will visit your country for disbursement according to the percentage indicated above. To enable the immediate transfer of this fund to you, you must apply first to the bank as relation or next of kin of the deceased indicating your bank name, your bank account number, your private telephone and fax number for easy and effective communication and location where in the money will be remitted. Upon receipt of your reply, I will send to you by fax or email the text of the application.
I will not fail to bring to your notice this transaction is hitch-free and that you should not entertain any atom of fear as all required arrangements have been made for the transfer. You should contact me immediately as soon as you receive this letter.

Waitting To Hear From You Immediately
Mr. Allasane Akeem

Email scams are exceedingly common, and millions of people are affected every year.

Credit: Jamil Velji

individuals' fear led to an escalation of internet engineering attacks.[7]

Some solutions have been put in place by the international community. Recently, 35 countries came together for three months to help combat organized crime groups that engaged in internet fraud. This process involved sharing information and data among the participating countries. This initiative allowed the International Criminal Police Organization (INTERPOL) to issue three Purple Notices, which are international requests for cooperation that allow police in different countries to share information. The Notices were on telephone scams, investment fraud, and social engineering schemes that were benefitting from the COVID-19 pandemic. The results were beneficial, as criminal techniques were uncovered, and INTERPOL arrested 20,000 individuals. Over 10,380 locations were raided, 21,549 operators, fraudsters, and money launderers were arrested, 310 bank accounts were frozen, and over USD 153,000,000 was intercepted.[8]

Internet fraud is an issue that needs to be addressed globally when it comes to combating hackers, "wobblers," or scammers. Hackers use tough times and personal hardships, such as natural disasters or global pandemics, to create deceiving messages. There is a need for more effective countermeasures concerning internet fraud and corruption. While many hackers believe they are untraceable due to the lack of resources, some countries may have to track down these people. The INTERPOL case shows that global cooperation and information-sharing between countries has proven successful.

Identity Theft and Invasion of Privacy

Identity theft is a type of fraud when someone maliciously obtains information and data to induce deception or for personal economic gains.[9] The primary goal of this type of attack is to gather as much information about the victim, assume their identity, and commit illicit activities. When criminals steal identity-related information, they use it to launder money, commit fraud, and engage in illicit activities related to organized crime, such as corruption, human trafficking, or terrorism.[10] In the United States alone, 33 percent of Americans have experienced some type of identity theft. The Federal Trade Commission, which deals with identity theft cases, handled 2.2 million cases in 2020, and every year, 15 million Americans experience and become victims of identity theft.[11] This can be seen from a worldwide perspective as well; 91 percent of consumers around the world have made online purchases, which puts individuals at risk. 40 percent of consumers worldwide have been victims of online identity theft.[12]

Despite the increase in cases of identity theft, there is no international organization that legislates or combats cyberspace identity theft.[13] However, there has been some progress in developing frameworks to combat cybercrime. The Council of Europe's Convention on Cybercrime created the first international treaty focusing on cybercrimes.[14] The treaty works by strengthening and unifying regional regulations, as well as "improving investigative techniques, and enhancing cooperation among European nations."[15] Improving investigative techniques is vital because as technology progresses, so do the techniques which hackers

7 Bitaab, *Scam Pandemic.*
8 "More than 20,000 Arrests in Year-Long Global Crackdown on Phone and Internet Scams," *INTERPOL*, December 9, 2020, https://www.interpol.int/en/News-and-Events/News/2020/More-than-20-000-arrests-in-year-long-global-crackdown-on-phone-and-Internet-scams.
9 "Identity Theft," The United States Department of Justice, last modified November 16, 2020, https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.
10 The United States Department of Justice,"Identity Theft."
11 Julija A., "20 Worrying Identity Theft Statistics for 2022," Fortunly, last modified February 17, 2022, https://fortunly.com/statistics/identity-theft-statistics/#gref.
12 Ivana Vojinovic, "Exploring Identity Theft Statistics in the Age of Data Breaches," *DataProt,* March 15, 2022, https://dataprot.net/statistics/identity-theft-statistics/.
13 Nazura Abdul Manap, Anita Abdul Rahim, and Hossein Taji, "Cyberspace Identity Theft: An Overview," *Mediterranean Journal of Social Sciences* 6, no. 4 (2015): 290, https://www.richtmann.org/journal/index.php/mjss/article/view/7290.
14 Manap, Abdul Rahim, and Taji, "Cyberspace Identity Theft."
15 Manap, Abdul Rahim, and Taji, "Cyberspace Identity Theft."

use to commit illicit activities. Digitalization has increased the use of automated systems to process data electronically. The information processed gets stored in databases, which are potential targets for offenders.[16]

Breaches of these databases cost companies millions of dollars annually. The United States ranks number one for the most expensive average data breach, followed by the Middle East, Canada, Germany, and Japan.[17] According to an IBM report studying 537 data breaches across 17 countries, 44 percent of data breaches include customer personal identifiable information (PII).[18] Another category of data breached was employee PII, which was compromised 26 percent of the time.[19] Malicious entities obtain personally identifiable information through various attacks.[20] PII is defined as data that includes identifiable information about individuals. This includes names, addresses, phone numbers, and a number of indirect identifiers such as birthday or gender.[21] Because many different organizations handle PII, it can be more vulnerable to cyber-attacks. When sensitive PII is leaked, this can lead to individual harm to those whose information is exposed. While some regulations surround PII, especially in places like the European Union, there are many ways individuals can get around these regulations. Events such as data breaches, data interceptions, direct hacking, and phishing can leak sensitive information.[22]

A common tactic that scammers use to steal an identity is phishing. Phishing is a technique where the hackers send the victim a fraudulent email that looks authentic, such as an email from a boss asking to provide sensitive information or perform some task. PII is often obtained from these kinds of scams, as many people fall for them. It is effective because it often looks legitimate and pressures individuals to act fast so they do not have enough time to verify the information. One of the most common initial cyber-attacks was phishing attempts, which cost companies an average of USD 4.3 million.[23] However, hackers have also engaged in wireless hacking to gain PII. They connect to public WiFi networks or unsecured home networks to steal the victims' personal information. Sometimes, they even install or hack third-party software that can track the victims' websites and the passwords they use.[24]

Once hackers collect PII, that information can be extremely damaging for the victim. Damaged credit, tax issues, money loss, and legal troubles are some consequences a victim of identity theft might suffer. Using someone's social security number, a personal identification number issued to citizens of countries such as the United States and Canada, hackers can open new accounts, make expenditures, and generate debt. That debt, if not paid, will affect the individual's ability to get financing or insurance. Moreover, scammers can use identity theft to file fraudulent tax reports in the victim's name to get cash tax incentives. Hackers could also access the victims' bank accounts, empty their accounts, or make illegal purchases with their names. This can place the victims in legal trouble, as crimes were committed under their names. Ultimately, these are all ramifications of the victims' information being mishandled and threatened.[25]

The United Nations Office on Drugs and Crime (UNODC) has recently responded to these cybercrimes by providing technical services. These include capacity building, prevention and awareness raising, international cooperation, data collection, and research and analysis on cybercrime.[26] The Office launched a consultative platform on identity theft crime, bringing together public sector representatives, businessmen, international organizations, and other stakeholders. Moreover,

16 "Handbook on Identity-related Crime," UN Office on Drugs and Crime, accessed August 26, 2022, https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.
17 *Cost of a Data Breach Report 2021,* (New York: IBM, 2021), https://www.ibm.com/downloads/cas/OJDVQGRY.
18 *Cost of a Data Breach Report 2021.*
19 *Cost of a Data Breach Report 2021.*
20 *Cost of a Data Breach Report 2021.*
21 Aliza Vigderman and Gabe Turner, "What is Personally Identifiable Information (PII)?" Security.org, last modified June 2, 2022, https://www.security.org/identity-theft/what-is-pii/.
22 Vigderman and Turner, "What is Personally Identifiable Information (PII)?"
23 *Cost of a Data Breach Report 2021.*
24 "Common Tactics Thieves Use To Steal Your Identity," Washington State Department of Financial Institutions, accessed August 26, 2022, https://dfi.wa.gov/financial-education/information/common-tactics-thieves-use-steal-your-identity.
25 David Lukic, "Identity Theft Consequences, Why Should you Take it Seriously," IDStrong, last modified June 14, 2021, https://www.idstrong.com/sentinel/identity-theft-consequences-why-should-you-take-it-seriously/.
26 "Index," UN Office on Drugs and Crime, accessed July 15, 2022, https://www.unodc.org/unodc/en/cybercrime/index.html.

in 2011, the UNODC published the Handbook on Identity-related Crime. The Handbook sets out possible solutions or routes to be taken in cases of domestic identity-related crimes. It also discusses challenges in international and regional cooperation and possible partnerships between the public and the private sector.[27]

Impactful action has not only come from the UN. At the start of 2021, The European Union (EU) decided they wanted to create a greener, more resilient, digital Europe for all. The EU created the Agency for Cybersecurity to achieve these goals and passed the EU Cybersecurity Act. The EU Agency for Cybersecurity was built on the structure of the EU Agency for Network and Information Security but with a stronger role and a permanent mandate. Moreover, the Cybersecurity Act includes an EU certification scheme developed to ensure optimal cybersecurity standards for information and communications technology (ICT) products and services. It does so by providing a set of rules, requirements, standards, and procedures that must be strictly adhered to. This certification is EU-wide, and its ultimate goal is to build trust, increase the cybersecurity market's growth, and improve trade amongst EU countries. The Act also incorporates a new mandate for the EU Agency for Cybersecurity, so it does not feel like one country carries the burden.[28] However, there is still much to be done internationally, and countries must unite to combat this international crime.

Impact on the Banking Industry

Another industry heavily impacted by cybersecurity is the financial and banking sector, which has rapidly increased its technology integration in recent years. Banks and technology work hand in hand when it comes to being reliable and efficient for their customers. Banks rely heavily on technology—from phone applications to depositing a check from home. A study in Latin America and the Caribbean showed that 53 percent of respondents review transactions and balances using smartphones.[29] With such a high percentage of users having access to their banking information at their fingertips, it is essential to provide strong digital security. The leading digital security risks globally are: "theft of a critical database… compromise of privileged user credentials and…data loss."[30] This is alarming, considering that in Latin America and the

27 "UNODC Response to Identity-related Crime," UN Office on Drugs and Crime, accessed August 26, 2022, https://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html.
28 "Cybersecurity: How the EU Tackles Cyber Threats," Consilium, last modified May 18, 2022, https://www.consilium.europa.eu/en/policies/cybersecurity/.
29 *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean,* (Canada: OAS, 2018), https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf.
30 *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean.*

Juhan Lepassaar, Executive Director of the European Union Agency for Cybersecurity.

Credit: ENISA

Caribbean alone, 92 percent of banking entities reported some digital security attack against them.[31] Of those same banking entities in the region, 61 percent allocated less than 1 percent of their earnings toward digital security.[32]

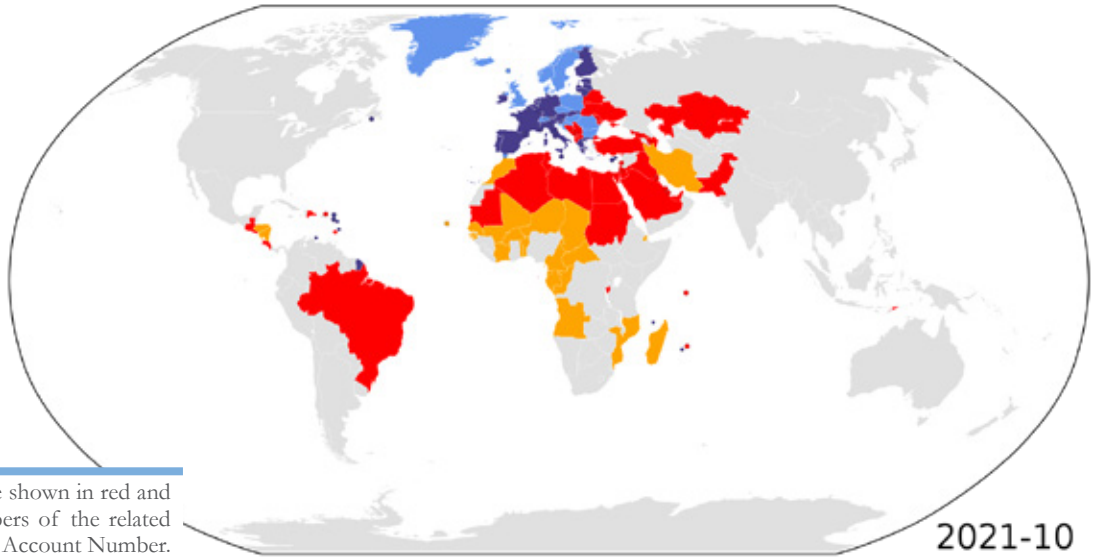
Cybercrime toward financial institutions is not limited to Latin America. In February 2016, Bangladesh's central bank, Bangladesh Bank (BB), was involved in a major cyber attack resulting in nearly USD 100 million in losses. BB became the victim of the most severe cyber theft using the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system.[33] The SWIFT system is a network between many banks and financial institutions that securely transfers information and finances between users. The cyber criminals attempted to transfer nearly USD 1 billion from BB's foreign reserve by sending 35 payment orders to the federal reserve bank using SWIFT.[34] Four of the payment orders were successfully executed, resulting in a significant loss of nearly USD 100 million.[35] However, 30 of these orders were stopped because the bank branch's name was similar to the name of a blacklisted company.[36] The SWIFT system can automatically block payments to and from countries or entities that have been sanctioned or blacklisted. However, this system is not always perfect, and shortly after the BB attack, the same hackers hacked a Russian central bank and stole over USD 31 million.[37]

Spillover effects cause banking cyberattacks to affect many beyond the targeted institution. Not only does hacking banks cause a huge disruption to the banks and the consumers involved, but it becomes a network issue as well. One example is when a hacker group called NotPetya attacked Ukraine. This attack used a computer virus to delete data from the computers of banks and government agencies.[38] However, this attack also affected computer systems around the world, which caused substantial financial losses.[39] Systems in Denmark, India, and the United States were all affected as well by this attack. The connections between the banks and the stock market are highly important, and if a cyberattack were to occur in a country such as the United States, it could affect 38 percent of the market.[40] An attack this large would have the capacity to fuel the next financial crisis.

Whether these hackers are government officials or black-hat hackers trying to make a name for themselves and gain money, the time for action against cybercrime has never been more critical. Today, the United States has a list of over 100 black-hat hackers involved in hacking major banks throughout the United States, many of whom have international backgrounds.[41] It is an issue that impacts the entire world. INTERPOL has recently launched new investigations into these hackers, specifically the ones targeting banks, such as hacking group Carbanak, which has already stolen over USD 1 billion from banks worldwide.[42] Since 2013, Carbanak has attempted to hack banks, financial institutions, e-transaction software, and more. The two-year investigation by INTERPOL revealed that the aforementioned stolen USD 1 billion was just a tiny part of a more significant problem.

Recently, banks have engaged in a technique called "de-risking" to limit financial losses due to cybercrime.[43] The banks will first evaluate their relationships with international financial

31 *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean.*
32 *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean.*
33 "The Bangladesh Bank Heist: Lessons In Cyber Vulnerability," The One Brief, accessed October 11, 2022, https://theonebrief.com/the-bangladesh-bank-heist-lessons-in-cyber-vulnerability/.
34 The One Brief, "The Bangladesh Bank Heist."
35 The One Brief, "The Bangladesh Bank Heist."
36 The One Brief, "The Bangladesh Bank Heist."
37 "Russian Central Bank, Private Banks Lose $31 Mln in Cyber Attacks," *Reuters*, December 2, 2016, https://www.reuters.com/article/us-russia-cenbank-cyberattack/russian-central-bank-private-banks-lose-31-mln-in-cyber-attacks-idUSKBN13R1TO\.
38 Ellen Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes," *The Washington Post,* January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.
39 "Russia/Ukraine War Increases Spillover Risks of Global Cyberattacks," Fitch Ratings, last modified March 4, 2022, https://www.fitchratings.com/research/structured-finance/russia-ukraine-war-increases-spillover-risks-of-global-cyberattacks-04-03-2022.
40 Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," *Journal of Financial Economics* 145, no. 3 (2021): 802-826, https://doi.org/10.1016/j.jfineco.2021.10.007.
41 "How Hackers Stole Millions from Banks All over the World," Network Visibility, last modified March 26, 2015, https://www.garlandtechnology.com/blog/how-hackers-stole-millions-from-banks.
42 "Carbanak Hacking Group Steal $1 Billion from Banks Worldwide," ZDNet, last modified February 16, 2015, https://www.zdnet.com/article/carbanak-hacking-group-steal-1-billion-from-banks-worldwide/.
43 Alois Maluvu, "Corruption, cybercrime and compliance – managing the risks," The Banker, accessed September 30, 2022, https://www.thebanker.com/Corruption-cybercrime-and-compliance-managing-the-risks.



Countries participating in SWIFT are shown in red and blue. Countries in orange are members of the related International Bank Account Number.

Credit: Gfis, Martinvl

institutions. If these institutions are deemed at a higher risk for cybercrime, they will limit contact or break contact altogether. This is due to the high costs associated with anti-money laundering, counter-terrorist financing, corruption, and fraud. However, this has economic consequences for the countries in which there is a higher risk of cybercrime. According to a UN report, African countries lose USD 100 billion annually to illicit financial flows. In fact, almost all African regions have experienced a decrease in banking relationships with foreign banks since 2013.[44] In order to mitigate this, there are better solutions in place within systems like SWIFT. One of the most important strategies is up-to-date bank registries, preventing hackers from slipping into the system under a false bank name. However, this also requires compliance with SWIFT's regulations from banks within every country. In order to prevent economic losses to entire continents, better bank registries and more efficient regulations are necessary.

The banking industry is at risk of several cyber-attacks and groups trying to take advantage of inadequate security measures. There is a need for countries to work together on bank-related cybercrime to take a more aggressive approach toward hackers. This can involve working with black hat hackers and turning them into white hat hackers to prevent and fight cyber-attacks or more cooperation within government agencies to better identify these hackers in the first place.

Hacking strategies have increased by 160 percent over the past 12 months, and many banks note that hackers still fight back against attempts to remove them from their systems. Typically, when hackers notice an intrusion or a chance of being caught, they immediately remove themselves from the situation to prevent this outcome.[45] Hackers, especially those hacking the banking industry, have become bolder, stronger, and more strategic. With such high stakes in the financial and banking industry, the need for international cooperation is crucial.

Cyberterrorism and National Security Concerns

There is a lack of security, punishment, and involvement from world governments when it comes to cybercrime. This makes citizens especially susceptible to hackers but can also compromise entire countries through cyber-attacks or national security vulnerabilities. The link between cyberterrorism, corruption, and national security has become prevalent. Countries like New Zealand have already acknowledged this, taking significant steps to combat these cyber-attacks. Their cyber security system, NCSC-NZ, includes numerous ways

44 Maluvu, "Corruption, cybercrime and compliance."
45 "Banks Are under Siege by Sophisticated Hackers," Futurism, last modified March 26, 2019, https://futurism.com/banks-sophisticated-hackers.

of reporting cyber-attacks as they are happening, especially with larger organizations, and creating specific laws that can prosecute hackers.[46]

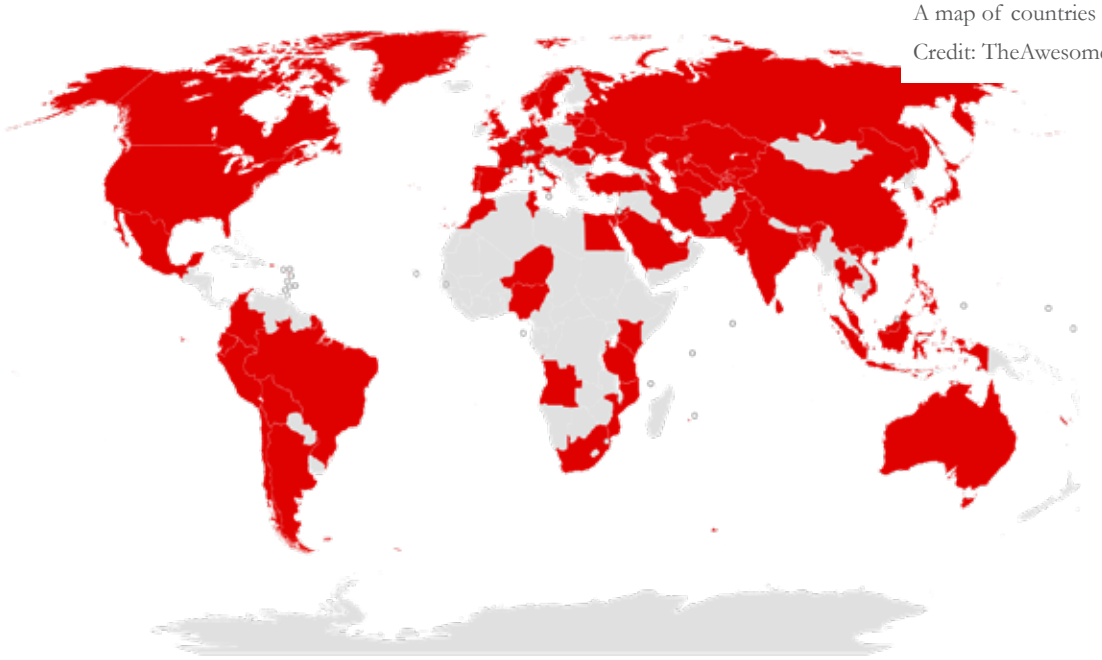
Cyberterrorism is any premeditated, politically motivated attack against information systems, programs, and data that threatens or results in violence.[47] Global cyberterrorism incidents have been rising over the past twenty years as criminal organizations from around the world identify themselves as terrorist organizations and attempt to steal data, money, and information from government officials. Many refer to them as "modern-day pirates."[48]

In December 2017, over 150 countries were attacked by two hacked clients, "WannaCry" and "NotPetya." These hacked clients caused major business disruptions and other losses, including the loss of over USD 300 million in funding. With this loss of funding, customer data, and business, countries like the United States intervened to find the culprit of these attacks.[49] Cyberterrorism, cyberwar, and cyber security are all interlinked. Many countries have shown public support against cyberterrorism. However, with the growing number of attacks and increasingly complex hacking methods, it has become difficult to stop cybercriminals.

The UN has begun a Counter-terrorism Cybersecurity Program under their office of Counter Terrorism unit to give initiatives, plans, and information to teach countries how to prevent cyberattacks and how to secure security systems more. They also provide information to countries on what to do during a cyber-attack and what challenges are faced ahead. They have a yearly meeting in Vienna, Italy, in early December to discuss methods for addressing cybersecurity.[50] Cyberterrorism has already affected hundreds of countries today and caused significant business and development losses. With the number of cybercrimes and corruption rates increasing, companies, organizations, and governments are hiring hackers to counteract and prevent these crimes.

The United States is no stranger to cyber-attacks, from

46 "Cyber Crime and National Security: A New Zealand Perspective," SGOC, accessed July 21, 2022, https://standinggroups.ecpr.eu/sgoc/cyber-crime-and-national-security-a-new-zealand-perspective/.
47 "What Is Cyberterrorism?" TechTarget, last modified January 19, 2022, https://www.techtarget.com/searchsecurity/definition/cyberterrorism.
48 Peter Phillips and Gabriela Pohl, "Hackers, Pirates, and privateers," *SSRN Electronic Journal,* (2022), https://www.researchgate.net/publication/360482158_Hackers_Pirates_and_Privateers.
49 "Global Cyber Terrorism Incidents on the Rise," Marsh McLennan, accessed July 21, 2022, https://www.marshmclennan.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.
50 "Cybersecurity | Office of Counter-Terrorism," United Nations, accessed July 22, 2022, https://www.un.org/counterterrorism/cybersecurity.



A map of countries affected by the WannaCry attack. Credit: TheAwesomeHwyh

domestic incursions such as breaches of information to strategically targeted international attacks. They clearly illustrate how important it is to combat cyber-attacks in the early stages before they grow into larger and larger national security issues. One example is Wikileaks, which leaked data about the US government and military plans in the Middle East. They also revealed information about the Democratic National Committee (DNC) emails that significantly impacted the Democratic party during the 2016 election with Hillary Clinton and President Donald Trump.[51] The US government has claimed that what Julian Assange, the founder of WikiLeaks, did was a threat to national security.

In 2017, Julian Assange released Vault 7, which revealed the CIA hacking tools to the public, expressing in the press release that it could target American citizens and their personal information.[52] While the ethics behind breaches such as these are still debated, these hacks are a national security issue due to hackers' malicious intent when releasing or accessing compromising data. Security breaches can tear governments apart, raise digital anxieties and fears for citizens, and translate to government mistrust. Delegates should come together and create plans, measures, and communication mechanisms to reduce the occurrence of cyber-attacks and corruption.

Types of Hackers

Hackers range on a broad spectrum. The term hacker can usually carry a negative connotation, but not all hackers have ill intentions. Hackers fall under the spectrum of either a white hat hacker, a black hat hacker, or a gray hat hacker. They all have very different intentions, so it is vital to know the difference. Black hat hackers are the ones who commonly carry out cybercrime.

White hat hackers, also known as ethical hackers, are individuals who use hacking skills to identify security vulnerabilities in hardware, software, or networks.[53] White hat hackers typically work for organizations, governments, or businesses that want to know their vulnerabilities and how to fix them. Most financial institutions use a combination of internal and external ethical hackers. PwC, CGI, and HackerOne are among many companies which offer penetration testing services.[54] However, the market for these hackers is minimal. Alternatively, companies such as Apple have made test trials available to the public for anyone to try hacking into their systems. If someone can successfully hack in, they are given compensation. These white hat hackers are not doing anything illegal because they are working for a company to test their system. This business model provides a unique and effective way of testing a company's security. As the problem of cybersecurity and cybercrime becomes more prevalent, the only way for organizations such as banks, governments, and even medical institutions to fight back is to work with hackers who have the experience necessary to find flaws in many of their systems.

It is crucial to highlight black hat hackers and their role in cybercrime. Many banks, governments, and institutions are most worried about this group of individuals. They commit crimes that include information theft, corruption, fraud, disrupting systems, and exploitation. Many of these malicious hackers work for criminal organizations, sometimes specifically terrorist organizations, to steal information and money. There is an FBI Database that carries a list of over 100 of the most wanted black hat hackers throughout the world, with many who hide in different international locations for crimes they have committed on US accounts.[55]

There is also some notoriety regarding individuals in black hat hacker groups. Kevin Mitnick is one example. He was once the most wanted cybercriminal in the world. He began a two-and-a-half-year hacking spree by hacking into 40 major companies, including IBM, Motorola, and even the National Defense warning system "just for the challenge." This landed him on the top of the FBI's most wanted list.[56] After two and

51 "What WikiLeaks Revealed," The Week, last modified February 25, 2020, https://www.theweek.co.uk/101143/what-wikileaks-revealed.
52 "Vault7," Wikileaks, accessed July 21, 2022, https://wikileaks.org/ciav7p1/.
53 Andrew Froehlich, "White hat hacker," TechTarget, accessed September 30, 2022, https://www.techtarget.com/searchsecurity/definition/white-hat.
54 "Why Banks Are Engaging 'White Hat' Hackers," The Banker, last modified February 9, 2019, https://www.thebanker.com/Transactions-Technology/Why-banks-are-engaging-white-hat-hackers?ct=true.
55 "Cyber's Most Wanted," FBI, accessed September 30, 2022, https://www.fbi.gov/wanted/cyber.
56 Steve Morgan, "Cybersecurity's Greatest Showman on Earth: Kevin Mitnick," *Cybercrime Magazine*, May 8, 2020, https://cybersecurityventures.com/cybersecuritys-greatest-show-on-earth-kevin-mitnick/.

half years of black hat Hacking and five years in prison, Mitnik is now a trusted security consultant to a Fortune 500 company and governments worldwide.[57] Mitnik is a prime example of a black hat hacker turning into a white hat hacker after time in jail and compensation. The United States government utilized Mitnik for its gain because he proved that his hacking skills were way ahead of what many security defenses can handle. As cybercrimes and cyber corruption rise, companies worry that some converted hackers will become gray hat hackers.

Gray hat hackers are individuals who are in the gray area. Gray hat hackers abuse moral norms and standards but do not carry the same malicious intent as a black hat hacker. Instead, they expose vulnerable systems, most of the time of their own free will; they are not hired by businesses or governments.[58] These hackers are called gray hat hackers because the morality of their actions is somewhat "gray." While they still commit a crime, their intentions are not harmful and often result in good. An example of a gray hat hacker coming into play is when Apple and the FBI were involved in a dispute. During the San Bernardino shooting in December of 2015, the FBI tried to find a motive for the shooting and immediately looked towards the shooter's phones for evidence. When the iPhones were password protected, the FBI requested that Apple unlock and give access to the phones to the FBI. However, Apple did not follow through on the request because unlocking the phone would have gone against its terms of use. This dispute carried on for months before gray hat hackers stepped in to unlock the phone.[59] After gray hat hackers hacked into the iPhone, the FBI director at the time, James Comey, announced that the hack was only done specifically targeting the terrorist phone and that it was only done against Apple's iOS 9 system. Apple then said they would not take any legal action against the hackers or the FBI.

This is one of many clear cases of gray hat hackers working to benefit and expose security flaws without malicious intent. When it comes to cyberterrorism, employing certain hackers is a strategy that some governments can consider. However, this does not come without risks. Delegates must consider these, as hackers are key players in cybercrime and corruption.

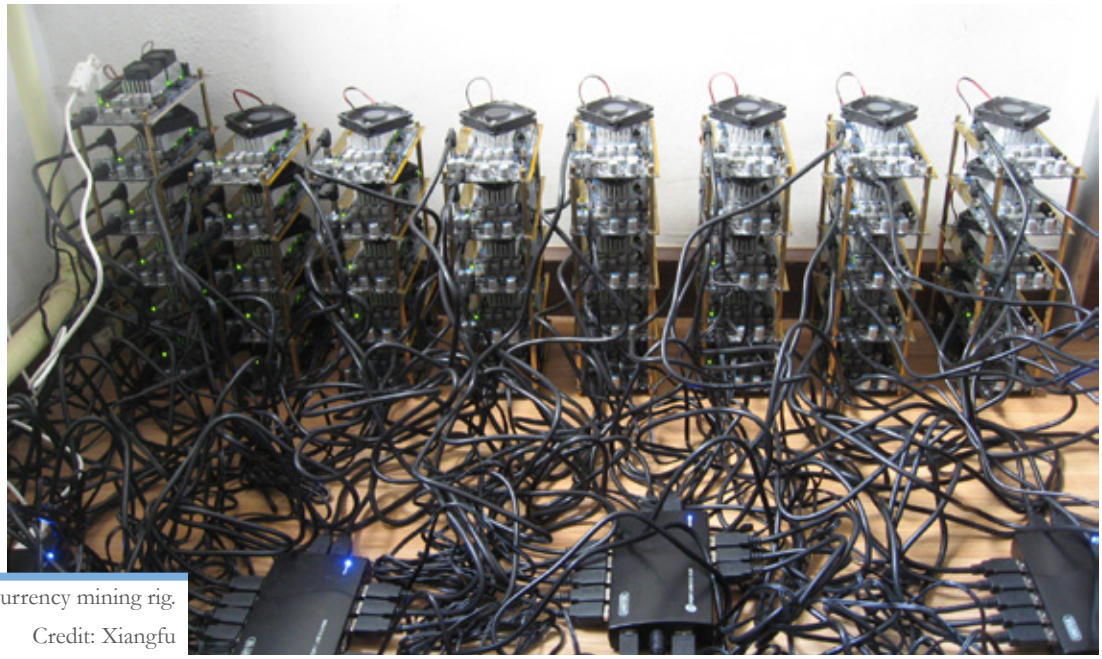
Current Status

Cryptocurrency

The new world of cryptocurrency is a thriving electronic market. Over the past few years, it has made people rich, given countries new economic opportunities, and changed how people view the economy as a whole. Cryptocurrency is a digital currency that is relied on and used under a computer network with no central authority. The New York Stock Exchange may appear as a free market, but businesses and the Federal Trade Commission keep the markets stable. Inflation measures, the regulation of trade, and consumer protection laws are put in place to protect consumers who invest in the stock market. For cryptocurrency, it is the opposite. While there are no solidified rules and regulations, some countries like China, Russia, and the United States have placed restrictions and regulations on specific cryptocurrencies. The market rapidly changes without any people controlling the market, making it highly volatile. Regardless of the cryptocurrency market's imperfections, the leading cause for concern regarding crypto is the lack of security measures and protections the market has today, making it highly vulnerable to corruption.[60]

Cryptocurrency has been exposed to hacks, security breaches, and mishandling since the beginning of its time. Ponzi schemes and specific websites providing Bitcoin, like Bitcoinica, Bitfloor, and more, were hacked and mishandled, which led to millions of dollars being stolen.[61] Typically websites that provide crypto are under attack by cyber hackers, with hackers trying to obtain the cryptocurrency for themselves. Just recently, back in March of 2022, the largest crypto hack took place, leading to over USD 600 million being taken from

57 "Kevin Mitnick," KnowBe4, accessed August 8, 2022, https://www.knowbe4.com/products/who-is-kevin-mitnick/.
58 "What Is a Grey Hat Hacker? Hacking without Malice," RSS, accessed August 8, 2022, https://www.wallarm.com/what/gray-hat-hacker.
59 Eduard Kovacs, "Grey Hat Hackers Helped FBI Hack Iphone: Report," *SecurityWeek*, April 13, 2016, https://www.securityweek.com/grey-hat-hackers-helped-fbi-hack-iphone-report.
60 "Cryptocurrency Regulations Around The World," Comply Advantage, last modified August 25, 2022, https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/.
61 Alex Hern, "A History of Bitcoin Hacks," *The Guardian*, March 18, 2014, https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency.



A cryptocurrency mining rig.
Credit: Xiangfu

user accounts. Ronin Networks, a key platform powering the mobile game Axie Infinity, had over USD 615 million stolen from them and user accounts. Axie Infinity was known to be a blockchain game, and the game used Ethereum to power its in-game economy. The game itself, being crypto-powered, was a way for users to use their crypto to collect exclusive non-fungible tokens (NFTs) in-game and gain status through their leaderboards. Some users took playing the game as their full-time job, as the game used the crypto market to its advantage and to differentiate itself. However, things began to crash once the game was hacked in March.[62] Over USD 615 million was lost, and users did not notice until six days after the attack. Ronin Network then took notice and contacted the authorities on the issue. This case is just one of many concerning the cryptocurrency market, and it shows how impactful hacking into these companies is for people's livelihoods.

Another case of the crypto market was when the blockchain website, Harmony, was hacked for USD 100 million, exposing a major critical vulnerability in their digital ecosystem. The problem with hacking cryptocurrencies and why these blockchain websites are so vulnerable is that crypto is untraceable. The unique ID that many wallets and crypto markets use becomes useless in the long run because the crypto itself becomes untraceable when moved around. To overcome this, Horizon and many other blockchain companies created a digital bridge within their app that people would need to cross through when depositing money from their accounts. Four wallets specifically hold the Horizon bridge. Each wallet is like a security checkpoint that users must go through before they cross the bridge, with each wallet requiring users to sign in, verify their identity, and authenticate each transaction that they make. Because crypto has no trace, apps like Horizon are required to make their trace.

Unfortunately, for the hack against Harmony, the hacker was able to achieve a "private key compromise," which meant he could steal a private key from the website and decrypt encrypted data from each wallet, allowing him to cross through the Horizon bridge. Once individuals have a private key, they can shield themselves from any security measures. Once hidden, the hacking commences, and the money is taken. This strategy is not new for blockchain websites. With the Ronin hack, the hackers were able to employ this tactic to mask themselves from the security that Ronin Networks had and cross through the Ronin bridge. Harmony responded to all of this, ensuring that they contacted authorities and explained the next steps once the funds had been received. However, it can take authorities years to find the culprit, and even then, there are no guarantees that the funds will be returned to their

62 Joe Tidy, "Ronin Network: What a $600m Hack Says about the State of Crypto," *BBC News*, March 30, 2022, https://www.bbc.com/news/technology-60933174.

users.[63]

The Harmony hack was the most recent hack that attacked block-chaining websites this year. Sophisticated hackers are seemingly able to get away with their actions as they hack these blockchain websites and steal millions of dollars each time they gain access. While the blockchain websites are individually impacted, the entire market is also affected. The Ethereum blockchain went down by 60 percent in July, which can be traced back to many of the hacks and slumps that blockchain websites were experiencing.[64] These examples demonstrate the potential vulnerability of the whole system. The economy itself is volatile, and the market can lead to hacking and security breaches from accompanying websites. However, companies still take advantage of the market and ponder new ideas on how to make the market more accessible and profitable.

For example, DeFi is a financial service company that connects with cryptocurrencies. DeFi, whose name derives from "decentralized finance," is the financial advisor for everything crypto-related. They provide consumers with services that include financial advice, decentralized exchanges, lending platforms, prediction market analysis, and more. It removes the middleman aspect and creates smart contracts, creating trustless protocols.[65] Acala Network, a DeFi network, was recently a target of a USD 1.2 billion hack. Their coin, AUSD, dropped down over 99 percent. The hacker noticed the exploit through the Acala Network, where a bug was present in the system. This led the hacker to break into the network, steal as much of the token as he could, and place it in his account. Then, he deposited it using his Ethereum account and connected it with a Binance account. To put the hack more simply, Acala Network has its own coin that they provide to users as an alternative to standard coins like Bitcoin and Ethereum. However, a hacker was able to exploit a bug in the system and bypass the security system in Acala Network, then stole over USD 1.2 billion worth of Alcala's coins. Once taken, the hacker switched the coin over to a blockchain website, Binance, and transferred everything into Ethereum, where he could easily deposit everything without a trace.[66] The anonymity of these events is a major problem; their securities are extremely flawed, and billions of dollars can be lost in the process.

Overall, the whole crypto market is highly vulnerable to hacking and security breaches happening to either the crypto market itself or partnering blockchain companies that provide crypto. The need for more security and cooperation within countries becomes crucial as hacks on these companies are still constantly taking place. Companies are still compromised due to their lack of security. Even communicating with local authorities after the hacks can lead to investigations that take months or years to achieve anything.

Ongoing International Measures

With the surge of cybercrimes and cyber security breaches increasing throughout the past decade, international organizations have now conducted investigations on criminals. In 2021, as part of an investigation done by INTERPOL, a 30-month transcontinental investigation concluded in arrests and Red Notices to be filed in over 194 countries. A Red Notice is also known as an international wanted person alert. In one instance, Red Notices were requested and sent to South Korea, Ukraine, and the United States law enforcement authorities. During the operation, known as Operation Cyclone, INTERPOL agents arrested malware operators in Ukraine who targeted businesses in Korea and the United States. These hackers caused a breach of computer files and networks and demanded ransom to restore access.[67] While this is just one investigation out of many, INTERPOL has acted as the bridge between individual governments and international institutions to catch people committing cybercrime and

63 Olga Kharif, Sidhartha Shukla, and Emily Nicolle, "Hackers Steal $100 Million by Exploiting Crypto's Weak Link," *Time*, June 24, 2022, https://time.com/6190924/hackers-exploit-crypto-weak-link/.
64 Yashu Gola, "Ethereum Risks Another 60% Drop after Breaking below $1K to 18-Month Lows," *Cointelegraph,* June 18, 2022, https://cointelegraph.com/news/ethereum-risks-another-60-drop-after-breaking-below-1k-to-18-month-lows.
65 Jimmy Aki, "How Decentralized Finance Works and Use Cases: Updated March 2020," *BeInCrypto*, June 30, 2021, https://beincrypto.com/learn/decentralized-finance-and-use-cases/.
66 Oluwapelumi Adejumo, "Acala Network Ausd Depegs by 99% as Hacker Issues over 1 Billion Tokens," *BeInCrypto*, August 14, 2022, https://beincrypto.com/acala-network-ausd-depegs-by-99-as-hacker-issues-over-1-billion-tokens/.
67 "LED Operation Takes down Prolific Cybercrime Ring," INTERPOL, last modified November 5, 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring.

corruption throughout the world.

With the increase in breaches, many government organizations have conducted investigations into these cyber hackers. In July 1994, several corporate bank companies realized that a total of USD 400,000 was missing from their accounts. Once discovered, the FBI was immediately contacted, and an investigation was filed to determine how hackers could target banks and steal money from their computer systems. Citibank began working with the FBI during the investigation to monitor where the money was heading. The FBI found that many illegal transactions were being sent to overseas bank accounts, adding up to USD 10 million. The FBI collaborated with the Russian banks that the money was being sent to and pinpointed the exact person who was committing these crimes in the first place.

Vladimir Levin, who once lived in the United States and then in Russia at the time the crimes were happening, was a 30-year-old Russian hacker who stole over USD 10 million from Citibank. His wife attempted to return to the United States with their son to withdraw the money from the accounts, but the Russian accounts were frozen. The FBI quickly found out about this and arrested both individuals. In March of 1995, Levin was lured to London and arrested to be extradited to the United States. He pled guilty in January of 1998.[68] This was the first investigation and the first time the United States worked with the Russian government based on cybercrime, but it would not be the last. Often, with many of these crimes that take place, an international investigation typically happens because many of the hackers do not live in the country they are hacking into.

Digital awareness and education are crucial ways to combat cybercrime and corruption. INTERPOL and other organizations within each country have created campaigns highlighting the importance of being safe on the internet and what digital extortion is today. While this awareness campaign has connected more with countries such as the UK, the USA, and more, it is a start in providing the necessary education needed to combat cybercrimes today.[69] Education has become an essential part of preventing cybercrimes over the past years. As more people are educated on specific hacks, scams, frauds, and more, it becomes easier for individuals to recognize potential cybercrimes and protect themselves. As previously mentioned, the UNODC has started to create strategies and procedures to combat cybercrimes and educate people to identify cybercrimes. However, due to UNODC's lack of reach and lack of specificity toward drugs and crime, many countries view these measures as major oversights rather than resources.

In Slovenia, the European Commission implemented the project Education as a Strategic Method against the Illegal Use of the Internet. It is a framework dedicated to increasing awareness of cybercrime and corruption on the internet. The project involves all areas: educational, technological, psychological, sociological, and legal. It is specifically targeted at children and teenagers, as they are the most naive segment of the population and also the most avid users of digital platforms. Target groups are selected from 10 percent of Slovenian primary schools and include pupils, parents, and teachers. It aims to increase the level of uncovered illegal content, implement faster law enforcement agencies due to greater public awareness, increase incident reports, and ultimately decrease the number of cybercrime and corruption cases. It analyzes critical cybercrime areas, researches possible stakeholders, develops e-learning materials to include in educational modules, and creates e-learning and face-to-face learning methods.[70]

Cybercrime investigations can take months or years to conclude, which is a significant obstacle to combatting this issue due to the frequent nature of this type of crime. The speed and efficiency of these investigations depend on the amount of communication and collaboration between countries involved with cybercrime. Time becomes crucial to many of these investigations because as more time passes, it

68 "A Byte out of History $10 Million Hack, 1994-Style," Rough Diplomacy, last modified June 2, 2019, https://roughdiplomacy.com/a-byte-out-of-history-10-million-hack-1994-style/.
69 "New Campaign Highlights Digital Extortion Threats and How to Keep Safe," INTERPOL, last modified June 1, 2022, https://www.interpol.int/en/News-and-Events/News/2022/New-campaign-highlights-digital-extortion-threats-and-how-to-keep-safe.
70 Julija Lapuh Bele, et al., RAISING AWARENESS OF CYBERCRIME - THE USE OF EDUCATION AS A MEANS OF PREVENTION AND PROTECTION, (10th International Conference Mobile Learning, 2014), https://files.eric.ed.gov/fulltext/ED557216.pdf.

is more likely that a criminal will be caught and more damages will occur. INTERPOL and many others, including the International Telecommunications Union and the UNODC, have collaborated with local governments to investigate these cybercrimes. Nevertheless, the demand for more action to be done and education to increase has been the highest it has ever been.

Sustainable Development Goals

The 2030 Agenda for Sustainable Development was adopted by UN member states to reduce poverty and inequality, improve health and education, stimulate economic growth, and tackle climate change and deforestation. Combating corruption and cybercrime are two essential facets of the United Nations' Sustainable Development Goals. The United Nations Drugs and Crime Division has already created guidelines regarding cyber-attacks and how they relate to drugs and crime. Countries in the UN have collaborated, and comprehensive studies have been published to educate and teach other countries about cybercrimes happening throughout the world.[71]

Latin American countries like Argentina, Cuba, Mexico, Peru, and Venezuela may not have the same cyber footprint comparable to the United States. However, Latin America has recently developed an emerging market in cryptocurrencies. Some even rely on them as a currency, making them prone to cybercrimes and a breach in cybersecurity. Hackers take advantage of weak systems; without the same systems that other stronger countries carry, like the United States, China, South Korea, Japan, and more, other countries become more vulnerable.[72] Considering the vulnerability that some countries face when it comes to cybercrime attacks, ensuring better infrastructure and upgraded technology is directly related to SDG 7. SDG 7: Affordable and Clean Energy aims to strengthen modern and sustainable energy services for all, mainly the least developed countries.[73] Not many countries have the same internet access. Therefore, providing internet access and affordable electricity can be a leading factor in combating cybercrime and corruption.

By addressing the correlation between cybercrime and corruption, countries will take active steps to achieve SDG 16: Peace, Justice, and Strong Institutions. Specifically, Target 16.3 aims to promote the rule of law at the national and international levels and ensure equal access to justice for all. Target 16.5 focuses on reducing corruption and bribery in all forms. Several forms of cybercrimes play significant roles in corruption at different levels. By upholding legal standards and demonstrating a commitment to collaborate in the investigation of cybercrimes, countries are taking steps to reach SDG 16.[74]

Lastly, SDG 17: Partnerships for the Goals is central to combating corruption and cybercrime. Another aspect of sustainable development is utilizing international cooperation to achieve maximum security and a smoother process for specific investigations. Since cybercrimes occur worldwide, countries establishing partnerships can lead to many crime investigations being processed and done more quickly. This goal targets and focuses on the importance of how countries within the UN can prevent many of these crimes from occurring in the first place.[75]

Bloc Analysis

Cybercrime and corruption threaten countries' security at all levels. States have taken measures to ensure strong structures to deal with cyber risks. The Global Cybersecurity Index (GCI), launched in 2015 by the International Telecommunication Union (ITU), measures the member states' commitment to cybersecurity. When a country has stronger cyber security structures, it will be less vulnerable to attacks and consequently to corruption. The GCI aims to identify gaps, encourage the incorporation of good practices, and provide practical standards to enhance cybersecurity structures. The GCI explicitly measures the country's legal, technical,

71 UN Office on Drugs and Crime, "Index."
72 "Latin America Emerging Market & Target of Cybersecurity Risk," ERM Protect, accessed September 30, 2022, https://ermprotect.com/blog/latin-america-cybersecurity-risks/.
73 "SDG 7," United Nations, accessed October 13, 2022, https://sdgs.un.org/goals/goal7.
74 "SDG 16," United Nations, accessed October 13, 2022, https://sdgs.un.org/goals/goal16.
75 "SDG 17," United Nations, accessed October 13, 2022, https://sdgs.un.org/goals/goal17.

organizational, capacity development, and cooperation measures.[76]

Countries Scored 70–100

These countries are not only paving the way for what could come in the future for cyber security, but they are also available to collaborate with other countries, not just themselves, to create a comprehensive plan available for everyone. As cybersecurity measures are different for each country, the countries which take charge of providing measures of security and protection are the ones who can lead each other to protect themselves against cybercrimes and corruption. Countries include Estonia, Saudi Arabia, Singapore, Spain, the United Kingdom, and the United States, among others.[77] These countries also share the similarity of having developed internet infrastructure and wide internet availability.

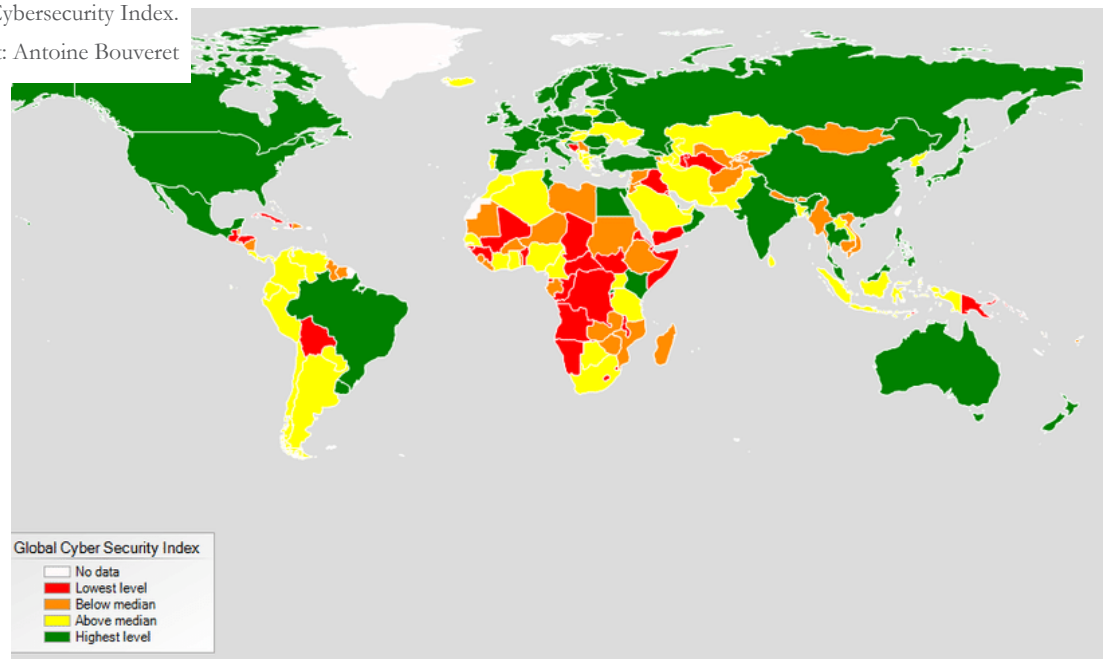
These countries have provided a sense of countermeasures against cybercrimes and threats previously. Moreover, these states monitor and update national cybersecurity strategies, regularly participate in international activities to share good practices, and engage relevant stakeholders in cybersecurity, including the private sector, academia, and civil society.[78] Additionally, since the wider public in these countries already has access to internet technologies, this bloc might consider how to protect their populations and mobilize individuals to identify and report on cybercrime. This bloc deals with sophisticated hackers and cybercriminals who might target the government, private companies, or other individuals. Additionally, since these countries also host big technology companies that might be targets of cybercrime or otherwise connect to the hacker communities, this bloc would be concerned with regulation, definition, and laws around the unchartered aspects of cybercrime. They also would explore partnerships between agencies, firms, and countries, such as cybersecurity Public-Private Partnerships, in order to build communication around cybercrimes.

Countries Scored 30–70

Within this bloc, countries have built some type of security and accreditation schemes. Nevertheless, they lack national bodies that deal with cyber security issues, have weak regulations, lack enforcement mechanisms, or have minimal protection and privacy laws. Considering these states do not

76 *Global Cybersecurity Index,* (Geneva: International Telecommunication Union, 2020), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
77 *Global Cybersecurity Index.*
78 "TOP 6 COUNTRIES WITH THE BEST CYBER SECURITY MEASURES," Analytics Insight, last modified February 18, 2019, https://www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/.

Map showing countries' scores on the Global Cybersecurity Index.
Credit: Antoine Bouveret



have a solid infrastructure to identify and combat cybercrimes, this consequently compromises transparency and may lead to corruption within a government. These countries may be advanced in some aspects of the GCI or lag in others, but their overall average is moderately ranked in terms of legal measures, technical measures, organizational measures, capacity development, and cooperation. These countries have the potential to grow and develop their methods but have not yet reached their full potential.

In some cases, these countries may also be perpetrators of cybercrime. In such cases, the economic, political, social, and other surrounding contexts of a country should be evaluated to find the motivations for such activities. Cybercrimes can sometimes indicate wider societal issues within a country. Countries within this bloc include Peru, Paraguay, Sri Lanka, Cuba, Pakistan, Belarus, and Argentina.[79] Member states from this bloc may want to emphasize the importance of international partnerships and cooperation to combat cybercrime in hopes of more transparent and fair governments. As always, the political alliances and economic ties to certain other countries must be considered when planning and developing the partnerships.

Countries Scored 0–30

Comprehensive cybersecurity measures are needed to prevent acts of cybercrimes. This bloc includes countries without the resources necessary to conduct their cyber security measures. As some countries may not have the same digital footprint as others, the need to address the technological crisis becomes crucial as countries talk about cybersecurity. These countries might push for wider connectivity and resources in their country, as well as education for citizens who are exploring cyberspace.

Countries in this bloc have a limited legal framework regarding cybersecurity measures and do not have the technical capabilities to have solid cybersecurity structures. These countries might look toward proactive solutions for strengthening their security and protection measures and counteracting corruption by developing safety features within networks or other cautionary measures. This bloc includes Yemen, Equatorial Guinea, Burundi, Honduras, Dominica, Afghanistan, and more.[80] As these countries mostly do not host large multinational corporations, this bloc instead would focus more on the impact of cybersecurity on individuals or the government. These countries also have many opportunities for organizational growth around combatting cybersecurity and could eventually look to form agencies around specific cybercrime issues. These countries have the most growth and development opportunities around cyber infrastructure and, as such, should consider ways to strengthen international technological advancements.

Committee Mission

The cyber security and corruption world has been highly complex and constantly changing. Countries are faced with massive challenges along the way as hackers become more complex and harder to catch as more hacks come in. Cyber security in a country highly depends on the functioning of public authorities that are expected to perform their duties honestly and truthfully. Corruption is a threat to cyber security. It can block access to financial and civilian institutions. A transparent public administration and a strong cyber security system can help countries remove corruption from reality. With the ongoing problems that cybercrimes are causing worldwide, it is necessary to act on and attack the problem at hand now before it is too late.

As countries have their own rules and regulations for combating cybercrimes, the need for collaboration is crucial. The UN Convention Against Corruption is the only legally binding universal agency against corruption, so it has the capacity to establish common ethical standards and practices through legal frameworks.[81] While collaboration will be essential, another aspect needed is progress with definitions and regulations. Creating new or improving cyber security measures that countries can follow will bring significant progress in the fight against cyber-attacks. If a country has a successful system already, other countries should learn from them and use its features to create meaningful solutions against

79 *Global Cybersecurity Index.*
80 *Global Cybersecurity Index.*
81 UN Office on Drugs and Crime, "The United Nations Convention against Corruption."

cyber threats and effective ways to define and determine the nature of cyberattacks.

Another vital aspect to consider is countries that may lack the technological advancements other countries have, creating obstacles for countries seeking to strengthen their cybersecurity. Learning from other countries and collaborating while recognizing that not every country has the same technology as each other's is crucial. While the focus is on cyber security, there should be an emphasis and understanding of each country's technological progress and how countries can benefit from each other in combating cybercrimes. Delegates should understand the unique circumstances of their own country and the others in committee, and then collaborate to reduce opportunities for corruption in cyberspace as well as in the real world.

Research and Preparation Questions

Your dais has prepared the following research and preparation questions as a means of providing guidance for your research process. These questions should be carefully considered, as they embody some of the main critical thought and learning objectives surrounding your topic.

Topic A

1. Is press freedom guaranteed in your country? How is it protected? What mechanisms has your country taken to ensure strong anti-corruption policies through the media?
2. Apart from the government, what actors other than the government contribute to the censorship of the press?
3. Are there laws in your country restricting the power of journalists or news outlets? How has the limitation of freedom of expression impacted the development of your country?
4. How does your country's score on the Corruption Perceptions Index compare to its score on the Press Freedom Index? What might that suggest about your country? What are some areas your country can focus on to get a better score?
5. What is your country´s usual response to those optional and strongly encouraged clauses included in the UNCAC?
6. What was your country's stance on national and international journalists when reporting on your country's matters?

Topic B

1. In your country, what policies or governmental bodies deal with identity theft and invasion of privacy?
2. What are the most common forms of identity theft in your country?
3. What legal frameworks already exist in your country to deal with internet fraud? What are the punishments laid out by those frameworks for such a crime?
4. Does the technology exist to prevent or detect illegal domestic or transnational online money transfers? If not, what might they look like? How can the United Nations aid countries in implementing cybersecurity solutions?
5. Are there examples of white, gray, or black hat hacker groups targeting politics in your country? What about international examples?
6. Does the possibility of White Hat hackers being hired for malicious purposes pose a threat to cybersecurity? How, if possible, can UNCAC ensure that these groups operate in good faith only?
7. What other UN documents deal with cybersecurity? How can their approaches be used to counter corruption?

Important Documents

Topic A

Daniels, Dustin R. *Freedom of the Media as Freedom from Corruption*. Florida: Florida State University Libraries, 2011. https://diginole.lib.fsu.edu/islandora/object/fsu:204413/datastream/PDF/view.

Di Tella, Rafael and Ignacio Franceschelli. *Government Advertising and Media Coverage of Corruption Scandals*. Boston: American Economic Journal, 2011. https://www.hbs.edu/ris/Publication%20Files/AEJ_Govt%20advertising%20and%20media%20coverage%20of%20corruption%20scandals_cbb969cd-4266-4818-8656-8d751e9b5b28.pdf.

Reporters Without Borders. "Methodology used for compiling the World Press Freedom Index." Accessed September 27, 2022. https://rsf.org/en/index-methodologie-2022.

Reporting on Corruption A ResourceTool for Governments and Journalists. Vienna: UN Office on Drugs and Crime, 2013. https://www.unodc.org/documents/corruption/Publications/2013/Resource_Tool_for_Governments_and_Journalists_COSP5_ebook.pdf.

Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation. Seoul: G20, 2010. https://www.oecd.org/g20/topics/anti-corruption/48972967.pdf.

Transparency International. "The ABCs of the CPI: How The Corruption Perceptions Index Is Calculated." Accessed July 14, 2022. https://www.transparency.org/en/news/how-cpi-scores-are-calculated.

UN Educational, Scientific, and Cultural Organization. "UN Plan of Action on the Safety of Journalists and the Issue of Impunity." Accessed September 30, 2022. https://en.unesco.org/un-plan-action-safety-journalists.

Topic B

Futurism. "Banks Are under Siege by Sophisticated Hackers." Last modified March 26, 2019. https://futurism.com/banks-sophisticated-hackers.

INTERPOL. "New Campaign Highlights Digital Extortion Threats and How to Keep Safe." Last modified June 1, 2022. https://www.interpol.int/en/News-and-Events/News/2022/New-campaign-highlights-digital-extortion-threats-and-how-to-keep-safe.

Kuepper, Justin. "Cyberattacks and the Risk of Bank Failures." Investopedia. Last modified March 4, 2022. https://www.investopedia.com/articles/personal-finance/012117/cyber-attacks-and-bank-failures-risks-you-should-know.asp.

The Banker. "Why Banks Are Engaging 'White Hat' Hackers." Last modified February 9, 2019. https://www.thebanker.com/Transactions-Technology/Why-banks-are-engaging-white-hat-hackers?ct=true.

UN Office on Drugs and Crime. "Handbook on Identity-related Crime." Accessed August 26, 2022. https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

Works Cited

Committee History

Hunter, Mathias and Scaturro, Ruggero. "UNCAC in a nutshell 2021." U4 Guide, no. 1 (November 2021) 12. https://uncaccoalition.org/wp-content/uploads/UNCAC-in-a-Nutshell-2021.pdf

UN General Assembly, Resolution 58/4, United Nations Convention Against Corruption, A/RES/58/4, (September 18, 2022) https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

United Nations Office on Drugs and Crimes, "United Nations Convention against Corruption," accessed September 18, 2022, https://www.unodc.org/unodc/en/corruption/uncac.html

Topic A

UN Sources

Ben-Hassine, Wafa. "Government Policy for the Internet Must Be Rights-Based and User-Centered." *UN Chronicle*. Accessed September 27, 2022. https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred.

Office of the United Nations High Commissioner for Human Rights. "Women journalists face violence and sexualized attacks - UN expert- #JournalistsToo – Women Journalists Speak Out." Accessed October 21, 2022. https://www.ohchr.org/en/press-releases/2021/11/women-journalists-face-violence-and-sexualized-attacks-un-expert.

UN Chronicle. "Government Policy for the Internet Must Be Rights-Based and User-Centered." Accessed July 15, 2022. https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred.

UNCAC Coalition. "Whistleblowing." Accessed August 3, 2022. https://uncaccoalition.org/learn-more/whistleblowing/.

UN Department of Economic and Social Affairs. "Do you know all 17 SDGs?" Accessed September 27, 2022. https://sdgs.un.org/goals.

UN Department of Economic and Social Affairs. "Goal 16." Accessed September 27, 2022. https://sdgs.un.org/goals/goal16.

UN Department of Economic and Social Affairs. "Goal 17." Accessed September 27, 2022. https://sdgs.un.org/goals/goal17.

UN Economic and Social Council. "ECOSOC Partnerships Forum." Accessed September 27, 2022. https://www.un.org/ecosoc/en/ecosoc-partnerships-forum.

UN Educational, Scientific, and Cultural Organization. "Journalism: a dangerous profession." Accessed September 29, 2022. https://en.unesco.org/courier/2021-4/journalism-dangerous-profession.

UN Educational, Scientific, and Cultural Organization. "The Chilling: Global trends in online violence against women journalists." Accessed October 21, 2022. https://unesdoc.unesco.org/ark:/48223/pf0000377223/PDF/377223eng.pdf.multi.

United Nations Educational, Scientific, and Cultural Organization. ""Threats that Silence: Trends in the Safety of Journalists." Accessed October 21, 2022. https://unesdoc.unesco.org/ark:/48223/pf0000379589/PDF/379589eng.pdf.multi

UN Educational, Scientific, and Cultural Organization. "UN Plan of Action on the Safety of Journalists and the Issue of Impunity." Accessed September 30, 2022. https://en.unesco.org/un-plan-action-safety-journalists.

UN General Assembly. Resolution 58/4. United Nations Convention Against Corruption. A/RES/58/4. September 18, 2022. https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

UN Human Rights. "International Covenant on Civil and Political Rights." Accessed August 14, 2022. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

UN in Western Europe. "Focus on the digital challenge to journalism." Accessed September 29, 2022. https://unric.org/en/focus-on-the-digital-challenge-to-journalism/.

United Nations. "Community radio fights misinformation for Venezuelan refugees and migrants in Brazil." Accessed September 27, 2022. https://www.un.org/en/coronavirus/community-radio-fights-misinformation-venezuelan-refugees-and-migrants.

United Nations. "Human Rights." Accessed September 27, 2022. https://www.un.org/en/global-issues/human-rights.

United Nations. "Press Freedom Day." Accessed October 3, 2022. https://www.un.org/en/observances/press-freedom-day/background.

United Nations Sustainable Development Goals. "Goal 17: Revitalize the global partnership for sustainable development." Accessed September 27, 2022. https://www.un.org/sustainabledevelopment/globalpartnerships/.

UN Plan of Action on the Safety of Journalists and The Issue of Impunity. Paris: United Nations Educational, Scientific, and Cultural Organization, 2011. https://www.ohchr.org/sites/default/files/Documents/Issues/Journalists/UN_plan_on_Safety_Journalists_EN.pdf.

UN Office on Drugs and Crime. "Corruption and Economic Crime 2021 Annual Report." Accessed July 14, 2022. https://www.unodc.org/unodc/en/corruption/2021-annual-report.html.

UN Office on Drugs and Crime. "FOCUS AREAS - WHISTLEBLOWER PROTECTION." Accessed September 29, 2022. https://www.unodc.org/unodc/en/ft-uncac/focus-areas/whistleblower.html.

UN Office on Drugs and Crime. "Resolutions and decisions adopted by the Conference of the States Parties to the United Nations Convention against Corruption." Accessed September 29, 2022. https://www.unodc.org/unodc/en/corruption/COSP/session9-resolutions.html.

UN Office on Drugs and Crime. "The role of the media in fighting corruption." Accessed September 15, 2022. https://www.unodc.org/e4j/en/anti-corruption/module-10/key-issues/the-role-of-the-media-in-fighting-corruption.html.

UN Office on Drugs and Crime. "The United Nations Convention against Corruption." Accessed September 29, 2022. https://www.unodc.org/ropan/en/AntiCorruptionARAC/united-nations-convention-against-corruption.html.

UN Office on Drugs and Crime. "UNODC's Action against Corruption and Economic Crime." Accessed July 13, 2022. https://www.unodc.org/unodc/en/corruption/index.html.

UN Office on Drugs and Crimes. "United Nations Convention against Corruption." Accessed September 18, 2022. https://www.unodc.org/unodc/en/corruption/uncac.html.

Non-UN Sources

Aljazeera. "Abbas demands US seek justice over Shireen Abu Akleh's killing." September 23, 2022. https://www.aljazeera.com/news/2022/9/23/abbas-slams-israels-impunity-over-shireen-abu-aklehs-killing.

Amnesty International. "Myanmar: Cease persecution of journalists." Accessed July 16, 2022. https://www.amnesty.org/en/latest/press-release/2021/05/myanmar-cease-persecution-journalists/.

Arnold, Anne-Katrin and Sumir Lal. *Using Media to Fight Corruption*. Washington: Partnership for Transparency Fund, 2012. https://www.ptfund.org/wp-content/uploads/2018/07/WP01-Media-to-Fight-Corruption.pdf.

Binhadab, Nouf, Breen, Michael, and Gillanders, Robert. "Press freedom and corruption in business-state interactions." *Economic Systems*. 45(4) (2021). https://www.sciencedirect.com/science/article/pii/S0939362521000704.

Becker, Lee B., Teresa K. Naab, Cynthia English, and Tudor Vlad. "Measurement Issues and the Relationship Between Media Freedom and Corruption." *Grady College of Journalism & Mass Communication, University of Georgia,* (June 2013): 6-14. http://grady.uga.edu/coxcenter/Conference_Papers/Public_TCs/Becker_Naab%20_English_Vlad_IAMCR_5_22_2013.pdf.

Carrie Wong, Julia. "Social media may have been blocked during Turkey coup attempt." *The Guardian*. July 15, 2015. https://www.theguardian.com/world/2016/jul/15/turkey-blocking-social-facebook-twitter-youtube.

CIVICUS. "Repression of activists and journalists persist in Myanmar despite Asean rebuke." Accessed July 16, 2022. https://monitor.civicus.org/updates/2021/11/09/repression-activists-and-journalists-persists-myanmar-despite-asean-rebuke/.

Committee to Protect Journalists. "10 Most Censored Countries." Accessed July 14, 2022. https://cpj.org/2015/04/10-most-censored-countries/.

Committee to Protect Journalists. "Colombian legislature passes anti-corruption bill that threatens press freedom." Accessed July 14, 2022. https://cpj.org/2021/12/colombian-legislature-passes-anti-corruption-bill-that-threatens-press-freedom/.

Committee to Protect Journalists. "What We Do." Committee to Protect Journalists. Accessed July 14, 2022. https://cpj.org/about/.

Council on Foreign Relations. "Argentina's Latest Anti-Speech Scandal: Free Press on the Rocks?" Accessed August 3, 2022. https://www.cfr.org/blog/argentinas-latest-anti-speech-scandal-free-press-rocks.

DATAREPORTAL. "Digital Around the World." Accessed September 14, 2022. https://datareportal.com/global-digital-overview.

Diehn, Sonya. "The unprecedented rise in journalist slayings — and what can be done to stop them." *DW*. May 11, 2022. https://www.dw.com/en/the-unprecedented-rise-in-journalist-slayings-and-what-can-be-done-to-stop-them/a-6176342.

Di Tella, Rafael and Ignacio Franceschelli. *Government Advertising and Media Coverage of Corruption Scandals*. Boston: American Economic Journal, 2011. https://www.hbs.edu/ris/Publication%20Files/AEJ_Govt%20advertising%20and%20media%20coverage%20of%20corruption%20scandals_cbb969cd-4266-4818-8656-8d751e9b5b28.pdf.

Elka Pangestu, Mari. "Working in partnership is key to fighting corruption." World Bank Blogs. Last modified September 23, 2020. https://blogs.worldbank.org/voices/working-partnership-key-fighting-corruption.

Estrada, Johannes. "Acromax Media — Albanian Government's Tool for Online Political Censorship." *Exit News*. August 19, 2019. https://exit.al/en/2019/08/19/acromax-media-albanian-governments-tool-for-online-political-censorship/.

European Economic and Social Committee. "Definitions, concepts, and examples." Accessed September 29, 2022. https://www.eesc.europa.eu/en/definitions-concepts-and-examples.

Enikolopov, Ruben, Maria Petrova, and Konstantin Sonin. "Social Media and Corruption." *American Economic Journal* 10, no. 1, (Jan. 2019), 150-174. https://pubs.aeaweb.org/doi/pdfplus/10.1257/app.20160089.

Getz, Arlene. "Number of journalists behind bar reaches global high." Committee to Protect Journalists. Last modified December 9, 2021. https://cpj.org/reports/2021/12/number-of-journalists-behind-bars-reaches-global-high/.

Gibbs, Margot and Agustin Armendariz. "The Landlords." *International Consortium of Investigative Journalists*. November 3, 2021. https://www.icij.org/investigations/pandora-papers/the-land-lords/.

Glickman, Paul. *OFF LIMITS OFF LIMITS OFF LIMITS CENSORSHIP AND CORRUPTION CENSORSHIP AND CORRUPTION*. New York: Human Rights Watch, 1991. https://www.hrw.org/report/1991/07/01/limits/censorship-and-corruption.

Goldman, Russell. "Myanmar's Coup, Explained." *The New York Times*. April 27, 2022. https://www.nytimes.com/article/myanmar-news-protests-coup.html.

Gunter, Joel. "Murder in Accra: The life and death of Ahmed Hussein-Suale." *BBC Africa Eye*. January 30, 2019. https://www.bbc.com/news/world-africa-47002878.

Hunter, Mathias and Ruggero Scaturro. *UNCAC in a nutshell 2021*. Norway: U4 Guide, 2021. https://uncaccoalition.org/wp-content/uploads/UNCAC-in-a-Nutshell-2021.pdf.

Ilyushina, Mary. "Navalny releases investigation into decadent billion-dollar 'Putin palace'." *CNN*. Last updated January 20, 2021. https://www.cnn.com/2021/01/20/europe/putin-palace-navalny-russia-intl/index.html.

Infobae. "Asociaciones que defienden la libertad de prensa en el continente pidieron parar el asedio a periodistas en medio

de la campaña presidencial." Accessed July 14, 2022. https://www.infobae.com/america/colombia/2022/06/15/asociaciones-que-defienden-la-libertad-de-prensa-en-el-continente-pidieron-parar-el-asedio-a-periodistas-en-medio-de-la-campana-presidencial/.

Jenkins, Matthew. "TRACKING CORRUPTION ACROSS THE SUSTAINABLE DEVELOPMENT GOALS." Transparency International. Last modified March 25, 2021. https://www.transparency.org/en/blog/tracking-corruption-across-the-sustainable-development-goals.

Maizland, Lindsay. "Myanmar's Troubled History: Coups, Military Rule, and Ethnic Conflict." Council on Foregin Relations. Last modified January 31, 2022. https://www.cfr.org/backgrounder/myanmar-history-coup-military-rule-ethnic-conflict-rohingya.

Mao, Frances. "Aung San Suu Kyi: Myanmar sentences ex-leader to jail for corruption." *BBC News*. April 27, 2022. https://www.bbc.com/news/world-asia-61239881.

Mendes, Mara. *Overview of corruption in the media in developing countries.* Germany: Transparency International, 2013. https://assets.publishing.service.gov.uk/media/57a089fbe5274a27b2000367/expertanswer-368.pdf.

Normile, Dennis. "Science suffers as China's internet censors plug holes in Great Firewall." Science.org. Last modified August 30, 2017. https://www.science.org/content/article/science-suffers-china-s-internet-censors-plug-holes-great-firewall?cookieSet=1.

Norway in Saudi Arabia. "New strategy for promoting freedom of expression in foreign and development policy." Accessed September 29, 2022. https://www.norway.no/en/saudi-arabia/norway-sa/news-events/new-strategy-for-promoting-freedom-of-expression-in-foreign-and-development-policy/.

Pandora Papers reporting team. "Pandora Papers: A simple guide to the Pandora Papers leak." *BBC News*. Last updated 5 October 2021. https://www.bbc.com/news/world-58780561.

Posetti, Julie, Harrison, Jackie, and Waisbord, Silvio. *Online Attacks on Women Journalists Leading to 'Real World' Violence, New Research Shows*. Washington: International Center for Journalists, 2022. https://docs.google.com/document/d/1k4sn6jl4gVc8GS4CAeRE53dntsjk9WUQy0SKURkVITs/edit.

Radio Television Marti. "Maduro con el control casi absoluto de la prensa; sólo sobrevive." Last modified July 26, 2018. https://www.radiotelevisionmarti.com/a/cierre-de-medios-en-venezuela-deja-la-cobertura-en-manos-del-estado/190947.html.

Reporters Without Borders. "Denmark." Accessed September 27, 2022. https://rsf.org/en/country/denmark.

Reporters Without Borders. "Detailed Methodology." Accessed September 27, 2022. https://rsf.org/en/index-methodologie-2011-12.

Reporters Without Borders. "Methodology used for compiling the World Press Freedom Index." Accessed September 27, 2022. https://rsf.org/en/index-methodologie-2022.

Reporters Without Borders. "North Korea." Accessed September 27, 2022. https://rsf.org/en/country/north-korea.

Reporters Without Borders. "Venezuela." Accessed August 28, 2022. https://rsf.org/en/country/venezuela.

Schauseil, Wasil and David Jackson. *Media and anti-corruption.* Norway: U4 Anti-Corruption, 2013. https://www.u4.no/publications/media-and-corruption.pdf.

Starke, Christopher, Teresa K. Naab, and Helmut Scherer. "Free to Expose Corruption: The Impact of Media Freedom, Internet Access, and Governmental Online Service Delivery on Corruption." *International Journal of Communication*, 10, (2016), 4702-4722. https://ijoc.org/index.php/ijoc/article/view/5712/1793.

Solis, Jonathan A. and Leonardo Antenangli. *Corruption is Bad News for Free Press: Reassessing the Relationship Between Media Freedom and Corruption*. Wiley Online Library, August 2017. https://onlinelibrary.wiley.com/doi/pdf/10.1111/ssqu.12438.

Sorak, Nicholas. *Internet, Censorship, and Corruption.* University of Gothenburg, 2016. https://www.gu.se/sites/default/files/2020-05/QoGWP_2016_17_Sorak.pdf.

Sosa Cordero, Mariana. "Three ways to fight corruption in the media." Transparency International. Last modified November 18, 2016. https://www.transparency.org/en/news/three-ways-to-fight-corruption-in-the-media.

Stolen Asset Recovery Initiative. "UNCAC." Accessed September 27, 2022. https://star.worldbank.org/focus-area/uncac.

Strategy for promoting freedom of expression in Norwegian foreign and development policy. Norway: Ministry of Foreign Affairs. https://www.regjeringen.no/globalassets/departementene/ud/vedlegg/mr/strategy_expression.pdf.

Strengthening the Implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity. Geneva: UNESCO and the UN Office of the High Commission on Human Rights, 2017. https://www.ohchr.org/sites/default/files/Documents/Issues/Journalists/OutcomeDocument.pdf.

Study in Denmark. "Nordic countries top 2021 World Press Freedom Index." Accessed September 29, 2022. https://studyindenmark.dk/news/nordic-countries-top-2021-world-press-freedom-index.

Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation. Seoul: G20, 2010. https://www.oecd.org/g20/topics/anti-corruption/48972967.pdf.

The Guardian. "How to expose corruption, vice, and incompetence - by those who have." Last modified October 14, 2021. https://www.theguardian.com/membership/2021/oct/14/laws-changed-around-the-world-why-investigative-journalism-matters.

The Role of the Media and Investigative Journalism in Combating Corruption. OECD, 2018. https://www.oecd.org/daf/anti-bribery/The-role-of-media-and-investigative-journalism-in-combating-corruption.pdf.

Transparency International. "Corruption Perception Index." Accessed September 30, 2022. https://www.transparency.org/en/cpi/2020.

Transparency International. "Country Data." Accessed September 14, 2022. https://www.transparency.org/en/countries/china.

Transparency International. "CPI 2021 FOR EASTERN EUROPE & CENTRAL ASIA: DEMOCRATIC HOPES IN THE SHADOW OF GROWING AUTHORITARIANISM." Last modified January 25, 2022. https://www.transparency.org/en/news/cpi-2021-eastern-europe-central-asia-democratic-hopes-growing-authoritarianism.

Transparency International. "CPI 2021 FOR SUB-SAHARAN AFRICA: AMID DEMOCRATIC TURBULENCE, DEEP-SEATED CORRUPTION EXACERBATES THREATS TO FREEDOMS." Last modified January 25, 2022. https://www.transparency.org/en/news/cpi-2021-sub-saharan-africa-amid-democratic-turbulence-deep-seated-corruption.

Transparency International. "The ABCs of the CPI: How The Corruption Perceptions Index Is Calculated." Accessed July 14, 2022. https://www.transparency.org/en/news/how-cpi-scores-are-calculated.

Transparency International. "What is Corruption?" Accessed September 29, 2022. https://www.transparency.org/en/what-is-corruption.

University of Toronto. "International Country Risk Guide (ICRG) Researchers Dataset." Accessed September 29, 2022. https://mdl.library.utoronto.ca/collections/numeric-data/statistics/international-country-risk-guide-icrg-researchers-dataset.

Untold Stories: How Corruption and Conflicts of Interest Stalk the Newsroom. London: Ethical Journalism Network, 2015. https://dev.ethicaljournalismnetwork.org/wp-content/uploads/2016/08/untold-stories-full.pdf.

Vanderwicken, Peter. "Why the News Is Not the Truth." Harvard Business Review. Last modified June 1995. https://hbr.org/1995/05/why-the-news-is-not-the-truth.

Vurmo, Gjergji. "Nations in Transit 2021: Albania." Freedom House. Accessed September 27, 2022. https://freedomhouse.org/country/albania/nations-transit/2021.

Windelspecht, Devin and Ume A Sarfaraz. "In Sierra Leone, a rare opening for press freedom." *International Journalists' Network*. July 8, 2022. https://ijnet.org/en/story/sierra-leone-rare-opening-press-freedom.

Yaw Asomah, Joseph. "Why some of Ghana's private media fight corruption: reasons, rules, and resources." The Conversation. Last modified October 21, 2021. https://theconversation.com/why-some-of-ghanas-private-media-fight-corruption-

reasons-rules-and-resources-169254.

Topic B

UN Sources

United Nations. "Cybersecurity | Office of Counter-Terrorism." Accessed July 22, 2022. https://www.un.org/counterterrorism/cybersecurity.

United Nations. "SDG 7." Accessed October 13, 2022. https://sdgs.un.org/goals/goal7.

United Nations. "SDG 16." Accessed October 13, 2022. https://sdgs.un.org/goals/goal16.

United Nations. "SDG 17." Accessed October 13, 2022. https://sdgs.un.org/goals/goal17.

UN Office on Drugs and Crime. "Handbook on Identity-related Crime." Accessed August 26, 2022. https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

UN Office on Drugs and Crime. "Index." Accessed July 15, 2022. https://www.unodc.org/unodc/en/cybercrime/index.html.

UN Office on Drugs and Crime. "UNODC Response to Identity-related Crime." Accessed August 26, 2022. https://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html.

Non-UN Sources

Aaron Dennis, Michael. "Cybercrime." Accessed September 30, 2022. https://www.britannica.com/topic/cybercrime.

Abdul Manap, Nazura, Anita Abdul Rahim, and Hossein Taji. "Cyberspace Identity Theft: An Overview." *Mediterranean Journal of Social Sciences* 6, no. 4 (2015): 290. https://www.richtmann.org/journal/index.php/mjss/article/view/7290.

Adejumo, Oluwapelumi. "Acala Network Ausd Depegs by 99% as Hacker Issues over 1 Billion Tokens." *BeInCrypto*. August 14, 2022. https://beincrypto.com/acala-network-ausd-depegs-by-99-as-hacker-issues-over-1-billion-tokens/.

Aki, Jimmy. "How Decentralized Finance Works and Use Cases: Updated March 2020." *BeInCrypto*. June 30, 2021. https://beincrypto.com/learn/decentralized-finance-and-use-cases/.

A., Julija. "20 Worrying Identity Theft Statistics for 2022." Fortunly. Last modified February 17, 2022. https://fortunly.com/statistics/identity-theft-statistics/#gref.

Analytics Insight. "TOP 6 COUNTRIES WITH THE BEST CYBER SECURITY MEASURES." Last modified February 18, 2019. https://www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/.

BBC News. "Internet fraud: Nigerian scammer 'pulls off $1m heist' from prison." November 19, 2019. https://www.bbc.com/news/world-africa-50480495.

Bitaab, Marzieh. *Scam Pandemic: How Attackers Exploit Public Fear through Phishing*. Arizona: Arizona State University. https://www.ftc.gov/system/files/documents/public_events/1582978/scam_pandemic_how_attackers_exploit_public_fear_through_phishing.pdf.

Comply Advantage. "Cryptocurrency Regulations Around The World." Last modified August 25, 2022. https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/.

Consilium. "Cybersecurity: How the EU Tackles Cyber Threats." Last modified May 18, 2022. https://www.consilium.europa.eu/en/policies/cybersecurity/.

Cost of a Data Breach Report 2021. New York: IBM, 2021. https://www.ibm.com/downloads/cas/OJDVQGRY.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee. "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis." *Journal of Financial Economics* 145, no. 3 (2021): 802-826. https://doi.org/10.1016/j.jfineco.2021.10.007.

ERM Protect. "Latin America Emerging Market & Target of Cybersecurity Risk." Accessed September 30, 2022. https://ermprotect.com/blog/latin-america-cybersecurity-risks/.

FBI. "Cyber's Most Wanted." Accessed September 30, 2022. https://www.fbi.gov/wanted/cyber.

Ferdman, Roberto A. "4.4 Billion People around the World Still Don't Have Internet. Here's Where They Live." *The Washington Post*. November 25, 2021. https://www.washingtonpost.com/news/wonk/wp/2014/10/02/4-4-billion-people-around-the-world-still-dont-have-internet-heres-where-they-live/.

Fitch Ratings. "Russia/Ukraine War Increases Spillover Risks of Global Cyberattacks." Last modified March 4, 2022. https://www.fitchratings.com/research/structured-finance/russia-ukraine-war-increases-spillover-risks-of-global-cyberattacks-04-03-2022.

Fortinet. "What is internet fraud?" Accessed August 26, 2022. https://www.fortinet.com/resources/cyberglossary/internet-fraud.

Froehlich, Andrew. "White hat hacker." TechTarget. Accessed September 30, 2022. https://www.techtarget.com/searchsecurity/definition/white-hat.

Futurism. "Banks Are under Siege by Sophisticated Hackers." Last modified March 26, 2019. https://futurism.com/banks-sophisticated-hackers.

Global Cybersecurity Index. Geneva: International Telecommunication Union, 2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Gola, Yashu. "Ethereum Risks Another 60% Drop after Breaking below $1K to 18-Month Lows." *Cointelegraph*. June 18, 2022. https://cointelegraph.com/news/ethereum-risks-another-60-drop-after-breaking-below-1k-to-18-month-lows.

Hern, Alex. "A History of Bitcoin Hacks." *The Guardian*. March 18, 2014. https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency.

INTERPOL. "LED Operation Takes down Prolific Cybercrime Ring." Last modified November 5, 2021. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring.

INTERPOL. "More than 20,000 Arrests in Year-Long Global Crackdown on Phone and Internet Scams." December 9, 2020. https://www.interpol.int/en/News-and-Events/News/2020/More-than-20-000-arrests-in-year-long-global-crackdown-on-phone-and-Internet-scams.

INTERPOL. "New Campaign Highlights Digital Extortion Threats and How to Keep Safe." Last modified June 1, 2022. https://www.interpol.int/en/News-and-Events/News/2022/New-campaign-highlights-digital-extortion-threats-and-how-to-keep-safe.

Kharif, Olga, Sidhartha Shukla, and Emily Nicolle. "Hackers Steal $100 Million by Exploiting Crypto's Weak Link." *Time*. June 24, 2022. https://time.com/6190924/hackers-exploit-crypto-weak-link/.

KnowBe4. "Kevin Mitnick." Accessed August 8, 2022. https://www.knowbe4.com/products/who-is-kevin-mitnick/.

Kovacs, Eduard. "Grey Hat Hackers Helped FBI Hack Iphone: Report." *SecurityWeek*. April 13, 2016. https://www.securityweek.com/grey-hat-hackers-helped-fbi-hack-iphone-report.

Lapuh Bele, Julija, Maja Dimc, David Rozman, and Andreja Sladoje Jemec. RAISING AWARENESS OF CYBERCRIME - THE USE OF EDUCATION AS A MEANS OF PREVENTION AND PROTECTION. 10th International Conference Mobile Learning, 2014. https://files.eric.ed.gov/fulltext/ED557216.pdf.

Legal Information Institute. "Wobbler." Accessed July 15, 2022. https://www.law.cornell.edu/wex/wobbler.

Lukic, David. "Identity Theft Consequences, Why Should you Take it Seriously." IDStrong. Last modified June 14, 2021. https://www.idstrong.com/sentinel/identity-theft-consequences-why-should-you-take-it-seriously/.

Maluvu, Alois. "Corruption, cybercrime and compliance – managing the risks." The Banker. Accessed September 30, 2022. https://www.thebanker.com/Corruption-cybercrime-and-compliance-managing-the-risks.

Marsh McLennan. "Global Cyber Terrorism Incidents on the Rise." Accessed July 21, 2022. https://www.marshmclennan.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.

Morgan, Steve. "Cybersecurity's Greatest Showman on Earth: Kevin Mitnick." *Cybercrime Magazine*. May 8, 2020. https://

cybersecurityventures.com/cybersecuritys-greatest-show-on-earth-kevin-mitnick/.

Nakashima, Ellen. "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes." *The Washington Post.* January 12, 2018. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Network Visibility. "How Hackers Stole Millions from Banks All over the World." Last modified March 26, 2015. https://www.garlandtechnology.com/blog/how-hackers-stole-millions-from-banks.

Phillips, Peter and Gabriela Pohl. "Hackers, Pirates, and privateers." *SSRN Electronic Journal,* (2022). https://www.researchgate.net/publication/360482158_Hackers_Pirates_and_Privateers.

Plis, Michael. "Top 10 Countries Where Security Hackers Come from & their Types." Cyberkite. Last modified July 22, 2021. https://www.cyberkite.com.au/post/hackers-top-10-countries-where-they-come-from-hacker-types.

Reuters. "Russian Central Bank, Private Banks Lose $31 Mln in Cyber Attacks." December 2, 2016. https://www.reuters.com/article/us-russia-cenbank-cyberattack/russian-central-bank-private-banks-lose-31-mln-in-cyber-attacks-idUSKBN13R1TO\.

Rodriguez, Katitza and Meri Baghdasaryan. "UN Committee To Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope." *Electronic Frontier Foundation.* February 15, 2022. https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among.

Rough Diplomacy. "A Byte out of History $10 Million Hack, 1994-Style." Last modified June 2, 2019. https://roughdiplomacy.com/a-byte-out-of-history-10-million-hack-1994-style/.

RSS. "What Is a Grey Hat Hacker? Hacking without Malice." Accessed August 8, 2022. https://www.wallarm.com/what/gray-hat-hacker.

SGOC. "Cyber Crime and National Security: A New Zealand Perspective." Accessed July 21, 2022. https://standinggroups.ecpr.eu/sgoc/cyber-crime-and-national-security-a-new-zealand-perspective/.

State of Cybersecurity in the Banking Sector in Latin America and the Caribbean. Canada: OAS, 2018. https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf.

TechTarget. "What Is Cyberterrorism?" Last modified January 19, 2022. https://www.techtarget.com/searchsecurity/definition/cyberterrorism.

Tidy, Joe. "Ronin Network: What a $600m Hack Says about the State of Crypto." *BBC News.* March 30, 2022. https://www.bbc.com/news/technology-60933174.

The Banker. "Why Banks Are Engaging 'White Hat' Hackers." Last modified February 9, 2019. https://www.thebanker.com/Transactions-Technology/Why-banks-are-engaging-white-hat-hackers?ct=true.

The One Brief. "The Bangladesh Bank Heist: Lessons In Cyber Vulnerability." Accessed October 11, 2022. https://theonebrief.com/the-bangladesh-bank-heist-lessons-in-cyber-vulnerability/.

The United States Department of Justice. "Identity Theft." Last modified November 16, 2020. https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

The Week. "What WikiLeaks Revealed." Last modified February 25, 2020. https://www.theweek.co.uk/101143/what-wikileaks-revealed.

Vigderman, Aliza and Gabe Turner. "What is Personally Identifiable Information (PII)?" Security.org. Last modified June 2, 2022. https://www.security.org/identity-theft/what-is-pii/.

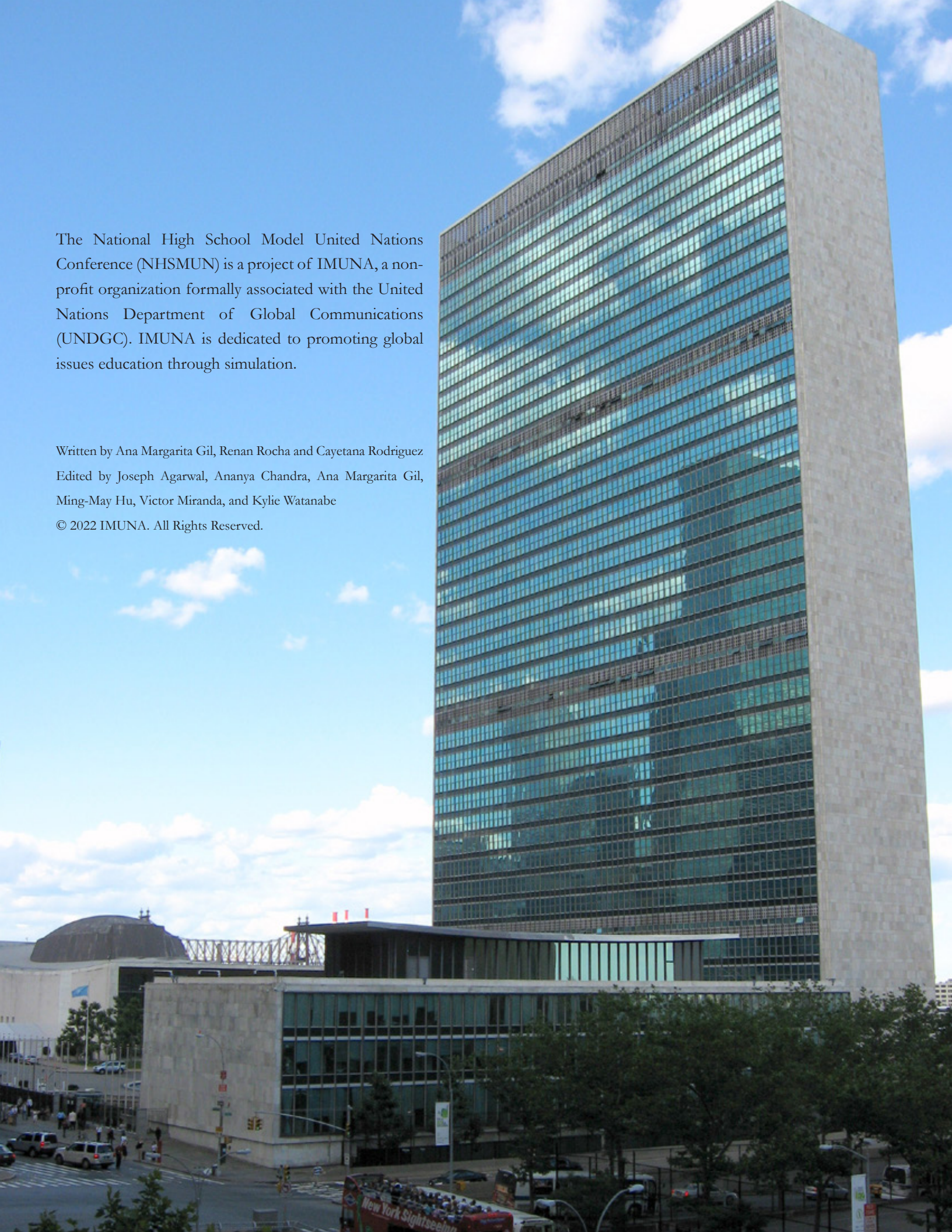
Vojinovic, Ivana."Exploring Identity Theft Statistics in the Age of Data Breaches." *DataProt.* March 15, 2022. https://dataprot.net/statistics/identity-theft-statistics/.

Washington State Department of Financial Institutions. "Common Tactics Thieves Use To Steal Your Identity." Accessed August 26, 2022. https://dfi.wa.gov/financial-education/information/common-tactics-thieves-use-steal-your-identity.

Wikileaks. "Vault7." Accessed July 21, 2022. https://wikileaks.org/ciav7p1/.

World Population Review. "Internet users by country 2022." Accessed August 10, 2022. https://worldpopulationreview.com/country-rankings/internet-users-by-country.

ZDNet. "Carbanak Hacking Group Steal $1 Billion from Banks Worldwide." Last modified February 16, 2015. https://www.zdnet.com/article/carbanak-hacking-group-steal-1-billion-from-banks-worldwide/.



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 Ana Margarita Gil, Renan Rocha and Cayetana Rodriguez
Edited by Joseph Agarwal, Ananya Chandra, Ana Margarita Gil, Ming-May Hu, Victor Miranda, and Kylie Watanabe