NHSMUN

CCPCJ

BACKGROUND GUIDE

Secretary-General
Grace Stanton

Director-General
Zoie Petrakis

Conference Directors
Jena Liebscher
Dimitri Henry

Chiefs of Staff
Justin May
Kevin O'Dell

Directors of Security
Zachary Boros
Joe Cohen

Under-Secretaries-General
Alex Burr
Antonio García
Luis González
Merve Karakas
Ashish Kaushik
Anthony López
Emily Michels
Vijittra Puckdee
Mateen Saki
Ana Treviño
Althea Turley
Andrew Zhao

Dear Delegates,

It is my absolute pleasure to present to you the Background Guide for the Commission on Crime Prevention and Criminal Justice (CCPCJ) at NHSMUN 2019! My name is Lina Saleh, and I am so incredibly thrilled to serve as your Session I Director for CCPCJ this March. My Co-Director Arjun and I are so ecstatic to meet you all at NHSMUN and watch you apply your knowledge in action.

NHSMUN 2019 will be my fifth year attending this conference and my second year on staff. This conference is one that is near and dear to my heart due to my positive experiences both as a delegate back in high school and as the Assistant Director for the World Trade Organization last year. NHSMUN provided me with an unimaginable opportunity to learn and grow as an individual throughout high school, and I am so glad to have the chance to contribute back to this wonderful program.

I am currently a second-year public health and English double major in the Honors College at the University of South Carolina, and I hope to work towards advocating for health issues in public policy. Currently, I am working as a research assistant on a nutrition study focused on African American populations, and I'm also doing individual research looking at health disparities. Outside of classes, I work as the Sponsorship Chair on the Executive Board for St. Jude Up 'Til Dawn, an organization that seeks to raise money for childhood cancer research and treatment, as well as the Community Chair for GlobeMed. In my free time, I love writing, reading, creating artwork, and collecting adorably strange knick-knacks.

Arjun and I have invested a great deal of time in choosing these topics for committee. We hope these subjects will allow you to understand pertinent global crime issues and develop solutions that address the topics from multiple perspectives. As a public health major, the topic of fraudulent medicine is incredibly interesting because the issue concerns the health and quality of life of individuals all across the globe. The second topic, understanding how exactly to formulate the legal system around the ever-growing and seemingly limitless realm of the internet, is one that is incredibly pertinent in our rapidly-changing time. Cybercrime is a crucial concern in the modern information age, and this fact, paired with concerns over election legitimacy, makes this subject one that requires the utmost attention. While these topics cover two very different areas, the overall goal between them is the same. We hope that you can all focus on long-term planning and create solutions that look critically at what has been done.

As you all explore the background guide and other sources for information, Arjun and I urge you to use us as a resource to further your understanding of the material. Also, feel free to say hello and give us a little introduction about yourself! We're all going to be working together in March, and we would love to get a sense of who you are.

Kindest Regards,

Lina Saleh
Commission on Crime Prevention and Criminal Justice, Session I
lina.saleh@imuna.org

NHSMUN
National High School Model United Nations

Secretary-General
Grace Stanton

Director-General
Zoie Petrakis

Conference Directors
Jena Liebscher
Dimitri Henry

Chiefs of Staff
Justin May
Kevin O'Dell

Directors of Security
Zachary Boros
Joe Cohen

Under-Secretaries-General
Alex Burr
Antonio García
Luis González
Merve Karakas
Ashish Kaushik
Anthony López
Emily Michels
Vijittra Puckdee
Mateen Saki
Ana Treviño
Althea Turley
Andrew Zhao

Delegates,

I am excited to present the Commission on Crime Prevention and Criminal Justice at NHSMUN 2019! My name is Arjun Ahuja and I am so thankful to say that I will be your Session II Director for CCPCJ. Along with my Co-Director, Lina, we hope that you will use this guide as a tool to not only help better understand the nuance of the topics that we are so excited to present, but also as a tool to further your research abilities when posed with tasks like this in the future. Before we get into the topics in detail, I would like to introduce myself.

NHSMUN 2019 will be my second year involved with this wonderful conference and conglomeration of people. Last year I served on the dais as an Assistant Director of SOCHUM. This year, I am excited to take on the role of Director and allow delegates to flourish as I know they are so capable of doing. My time with NHSMUN has seen me focused largely on the legality of the issues that are being discussed, so CCPCJ was a match that I thoroughly enjoyed.

I am currently a sophomore at the University of Connecticut where I hope to pursue a double major in Political Science and Philosophy with a hope to attend Law School upon graduating. My coursework at school wonderfully compliments my concentration at NHSMUN as I regularly study public policy, international law, and the philosophies behind legal frameworks. At school, I contribute to scholarly publications such as the Political Review and Law Review. This upcoming year I hope to work more intently with the law school and begin more research on topics that I enjoy outside of the international scope and more domestically focused.

As Lina and I have worked to formulate the best topics for simulation, we tried to combine the innovative nature of legal news along with important, broad ranging issues that will last far beyond our time. This first topic on falsified medicines encompasses the ambiguous nature of criminal justice reform with issues that are very under the radar, and deals with topics that directly affect people's physical manifestation along with the pockets of those who seek to profit from it. The second topic asks delegates to create a legal framework to stop cyber crimes in elections. Delegates are tasked with finding solutions that keep all involved parties satisfied without breaching sovereignty.

As delegates begin to dive headfirst into research, Lina and I urge you to contact us with any questions or concerns, as well as advice on further research. We hope that you find the Background Guide to helpful in guiding you through your research. Feel free to email us with any questions or simply to say hello!

Arjun Ahuja
Commission on Crime Prevention and Criminal Justice, Session II
arjun.ahuja@imuna.org

Table of Contents

A Note on the NHSMUN Difference

Esteemed Faculty and Delegates,

Welcome to NHSMUN 2019! My name is Zoie Petrakis and I am this year's Director-General. I hope you are as thrilled as I am to prepare for and attend the world's largest Model United Nations conference for secondary school students this March!

A space for collaboration, consensus, and compromise, NHSMUN strives to help 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.

Debate founded on strong knowledge: With knowledgeable staff members and delegates, NHSMUN can facilitate an enriching experience reliant on substantively rigorous debate. To ensure this high quality of debate, our staff members produce extremely detailed and wide-reaching topic overviews (like the one below) to prepare delegates for the complexities and nuances inherent in global issues. This process takes six months, during which the Directors who lead our committees develop their topics with the valuable input of expert contributors. Because these topics are impossible to fully address in a short Background Guide, NHSMUN also produces Update Papers that are intended to bridge the gap 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.

Extremely prepared and engaged staff: The detailed knowledge that our Directors provide in this Background Guide through diligent research is aimed at spurring critical thought within delegates at NHSMUN. Prior to the conference, our Directors and Assistant Directors are trained rigorously through copious hours of both virtual and in-person exercises and workshops in an effort to provide the best conference experience possible. Beyond this, our Directors and Assistant Directors read every position paper submitted to NHSMUN and provide thoughtful insight 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.

Emphasis on Participation: The UN relies on the voices of all of its Member States to create resolutions most likely to make a dramatic impact on the world. That is our philosophy at NHSMUN, too. We believe that in order 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 are focused on making every voice in the committee heard, regardless of delegates' country assignments or skill level. However, 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 also connect students with other action-oriented organizations at the conference to encourage further work on the topics.

Focused committee time: NHSMUN prohibits the use of any electronic devices during committee sessions. 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 a no-technology policy is also a way to guarantee that every delegate has an equal opportunity to succeed in committee. We staff a very dedicated team in our office who type up and format draft resolutions and working papers so that committee time can be focused on communication and collaboration. Please note that the dais is permitted a laptop for communicating with respective Under-Secretaries-General and other members of Senior Staff, as well as for administrative needs.

Educational emphasis, even for awards: At the heart of NHSMUN lies education and compromise. As such, when NHSMUN does distribute awards, we de-emphasize their importance in comparison to the educational value of Model UN as an activity. NHSMUN seeks to reward schools whose students 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. We always prioritize a dedication to teamwork and encourage our delegates to engage with others in a diplomatic and inclusive manner. In particular, our daises look for and promote constructive leadership that strives towards consensus, as delegates do in the United Nations.

As always, I welcome any questions or concerns about the substantive program at NHSMUN 2019 and would be happy to discuss NHSMUN pedagogy with faculty or delegates.

Delegates, it is my sincerest hope that your time at NHSMUN will be thought-provoking and stimulating. I look forward to seeing you grow as both students and global citizens at the conference.

Best,

Zoie Petrakis
Director-General

A Note on Research and Preparation

Delegate research and preparation is a critical element of attending NHSMUN and enjoying the conference's intellectual and cosmopolitan perspective. We have provided this Background Guide to introduce the topics that will be discussed in your committee. This document is designed to give you a description of the committee's mandate and the topics on its agenda. We do not intend to represent exhaustive research on every facet of the topics. 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. Delegates must be prepared to intelligently utilize your knowledge and apply it to your country's unique policy.

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.

An essential part of representing a state in an international body is the ability to articulate a given state's views in writing. Accordingly, NHSMUN requires each delegation (the one or two delegates representing a country in a committee) to write a position paper for both topics on the committee's agenda. In delegations with two students, we strongly encourage each student to participate in the research for both topics, to ensure that both students are prepared to debate no matter what topic is selected first. Position papers should be structured into three sections, described below.

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 background, 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 per topic double-spaced with standard margins and font size. **We recommend 2-4 pages per topic as a suitable length**. The paper must be written from the perspective of the country you are representing at NHSMUN 2019 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 our online upload process on or before **13 February 2019**. If a delegate wishes to receive detailed feedback from the committee's dais, a position must be submitted on or before **23 January 2019**. 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 the email submitted at registration. If delegations are unable to submit their position papers on time, they should contact us at info@imuna.org as soon as possible.

Delegations that do not submit position papers to directors will be <u>ineligible</u> for awards.

Committee History

The Commission on Crime Prevention and Criminal Justice (CCPCJ) is a functional committee of the Economic and Social Council (ECOSOC) and is the principal body of the United Nations concerning transnational crime and criminal justice. In the early 1990s, the UN developed a greater interest in criminal justice policy, leading to a recommendation for the creation of the CCPCJ by the UN General Assembly.[1] Its predecessor, the Committee on Crime Prevention and Control, was dissolved with the intent of intensifying "international cooperation in crime prevention and criminal justice" and increasing coordination between existing UN agencies.[2]

In 1992, the ECOSOC established the CCPCJ as a commission of the UN Office on Drugs and Crime (UNODC) with the passage of Resolution 1992/1. The Commission is composed of 40 member states, with terms of three years and quotas for each region of the world to ensure broad discussion and cooperation. Resolution 1992/22 further defined the priorities of the CCPCJ, including: "To plan, implement and evaluate crime prevention and criminal justice assistance projects and to serve as a facilitating agent…with which to assist countries in preventing crime, promoting security, sustaining national development and enhancing justice and respect for human rights."[3] With such a guideline, the CCPCJ has adopted thematic discussions ranging from money laundering to crime prevention in urban areas.

The Commission is also responsible for directing the United Nations Congress on Crime Prevention and Criminal Justice, which meets every five years. The Congress brings together leading policy makers, governmental agencies, non-governmental organizations, and several other parties for greater discussion and collaboration on work pertaining to the CCPCJ. The most recent Congress met in Doha, Qatar in April 2015 and addressed the integration of crime prevention and criminal justice with the wider UN agenda to promote social and economic development and the promotion of the rule of law at national and international levels.[4] Accordingly, recommendations were adopted by CCPCJ concerning the changing trends of crime prevention and criminal justice in tandem with considerations about economic development, transnational crime and the rule of law.

The most recent -and 24th - session of the CCPCJ was held in May 2015. This session discussed the thematic follow-up of the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice.[5] This led to a draft resolution concerning the contribution of the UN crime prevention effort on the post-2015 development agenda. Accordingly, during this session the CCPCJ reaffirmed "that the rule of law is both an outcome and an enabler for development and recognized the crucial need to include rule of law and strengthening criminal justice systems in the post-2015 development agenda."[6]

This Commission also serves other administrative matters. The CCPCJ governs the UNODC through its responsibility to approve the budget of the United Nations Crime Prevention and Criminal Fund, providing resources and technical assistance for worldwide crime prevention and criminal justice.[7] Following its mandate of collaboration, the CCPCJ works with the UN Crime Prevention and Criminal Justice Programme Network. This Network links several institutes that gather data, exchange information, research, train, and educate others in matters concerning illicit activity.

Unlike other UN agencies, the CCPCJ focuses solely on crime prevention and criminal justice. Yet this does not mean that collaboration does not occur. Instead, the CCPCJ, as emphasized in several clauses of A/RES/46/152, works cooperatively with

1   A/RES/46/152, "Creation of an Effective United Nations Crime Prevention and Criminal Justice Programme," 18 December 1991.
2   Ibid.
3   E/1992/22, "Implementation of General Assembly Resolution 46/152," 30 July 1992.
4   A/CONF.222/INF/1, "Thirteenth United Nations Congress on Crime Prevention and Criminal Justice […] Information for Participants," 12 January 2015.
5   E/CN.15/2015/CRP.2, "Report on the Twenty-fourth Session," 7 May 2015.
6   Ibid. 2.
7   "UNODC: Commissions," *United Nations Office on Drugs and Crime*, 30 June 2010, accessed 11 May 2018, http://www .unodc.org/unodc/en/commissions/index.html?ref=menuside.

other UN agencies, including the Security Council, the UNODC, the Commission on Narcotic Drugs, and the Conference of the States Parties to the United Nations Convention against Corruption.[8] The CCPCJ also acts as a coordinator, providing support to member states and managing the activities of regionalized institutes on crime prevention and criminal justice.[9] The CCPCJ encourages the sharing of information and constantly invites states and governments to participate in international dialogues to strengthen cooperation.

Moving forward, the CCPCJ plans to address issues of crime prevention and criminal justice. Through the work of the CCPCJ, the UN can better prevent illicit activities and continue to foster greater international cooperation for the benefit of all states.

---

8 Ibid.
9 DPI/1642/CRM, "The United Nations Crime Prevention and Criminal Justice Programme," April 1995, accessed 15 May 2018, http://www.unodc.org/documents/congress//Previous_Congresses/9th_Congress_1995/031_Backgrounder_United_Nations_Crime_Prevention_and_Criminal_Justice_Programme.pdf.

Simulation

Delegates to the Commission on Crime Prevention and Criminal Justice for NHSMUN 2016 are charged with a difficult task: serving as legal advisors to the UN General Assembly in order to prevent transnational crimes. With multifaceted intricacies, these elaborate issues require complex and detailed resolutions. To pass resolutions, debate should be kept active and orderly, addressing each facet without distractions and tangents.

Such debate necessitates diplomacy and compromise. Delegates should work together with one another when developing cohesive solutions and remain open to new ideas and input. While collaboration and compromise will certainly occur, delegates should remain on policy, in accordance with their respective countries' stance on the topic at hand. Especially in the CCPCJ's smaller setting, every delegate will be given the chance to express their country's position and contribute to forming resolutions. Country blocs containing those countries with similar stances will help build consensus and gain support for a particular stance. These blocs will play an important role in generating ideas and helping delegates remain on policy, but delegates are encouraged to work with other blocs and combine ideas into a wide-reaching resolution. Nevertheless, a delegate can never abandon his country´s policy in the quest for consensus. Precisely, the challenge lies in achieving compromise between differing points of view.

Mutual respect and absolute professionalism are integral components of diplomacy. Decorum, the expected behavior in committee, will be enforced throughout the entire conference. To ensure that debate is lively, delegates should be as prepared as possible, not only researching to form a country position but also keeping up to date with the committee's most current topics. Recent developments may have profound changes on country positions and new paths of action, requiring constant research until the start of the conference.

For the committee, the dais is composed of a Director and an Assistant Director, who are responsible for the preparations and development of this year's session. Delegates are highly encouraged to use both the Director and Assistant Director as valuable resources for substantive and procedural concerns. The dais will also manage the proceedings of the committee, moderating debate and fielding any motions.

The ultimate goal of committee is to produce one or more comprehensive resolutions to the debated topic. This process starts with producing a "set of ideas" or a working paper. Because the CCPCJ is a smaller committee, working papers have greater importance. These papers are expected to be as specific as possible, with clear, outlined policies and solutions. This way, a working paper can test the support of its propositions in the committee before becoming formalized into a formal, draft resolution. By testing the sentiment of the committee, working papers also allow for cooperation and compromise between two or more separate working papers.

Once a working paper has been debated and re-written into resolution format, it becomes a draft resolution to be presented in front of the committee. Any changes to draft resolutions must occur through unfriendly amendments (all amendments at NHSMUN are considered unfriendly). This means that the entire committee must hold a simple majority vote on the amendment, regardless of sponsor support for the amendment. Since this process lengthens voting procedures and eliminates debate, changes to working papers before submitting draft resolutions are highly encouraged. If this is not possible or debate is necessary, then the dais will certainly accept any and all amendments.

Substantive debate can be conducted either formally or informally. Formal debate is guided by the speakers list, which records those countries wishing to speak. Delegates should use this time to address their general stance and their country's policy on the topic. Delegates can then identify like-minded parties who can work together to draft a working paper. Informal debate occurs

during either moderated or unmoderated caucusing. With many speakers and a shorter speaking time, moderated caucuses move at a faster pace than formal debate. These sessions are used to debate specific details and one dimension of the topic. Unmoderated caucusing suspends the rules for a set period of time, allowing delegates to convene and converse more freely, discuss possible solutions, and work together to form resolutions.

While the process may appear long and arduous, active participation, negotiation, and debate will lead to innovative solutions to the committee's topics and aid in combating international crimes across the world.

TOPIC A:

PREVENTING THE DISTRIBUTION OF COUNTERFEIT AND FALSIFIED MEDICINE

Introduction

In today's world, illegal drug trade creates an image of criminal groups profiting from the sale of substances, such as heroin, cocaine, and methamphetamines. However, the most profitable drugs of the trade are far more inconspicuous, appearing entirely legal on the surface until the effects take hold on users. This type is referred to as fake medicine. Counterfeit and substandard medication accounts for a major criminal industry which carries an increased criminal threat from the black market of dangerous goods, but also the concerns of an ever-growing public health crisis.[1] Counterfeit or falsified medication refers to medical products which have a deliberately misrepresented identity, composition, or source.[2] Such substandard medicine refers to authorized and legitimate products containing expired, inactive, or other ingredients that reduce the quality of the medication or increase its chances of inflicting harm on the user.[3]

According to a World Health Organization (WHO) report, approximately 10% of medical products in low and mid-level income countries is substandard or falsified (SF), with 1,500 reported cases since 2013 and 41% of those cases coming from the African continent.[4] The actual number of cases is potentially much higher since many cases go unreported, but now with 550 WHO trained regulators in 141 countries there is hope to increase data on the effects and harm caused by SF medicine.[5] In July 2013, WHO established the Global Surveillance and Monitoring System, which works with member states and their national medicine regulatory authorities to collect information that allows for improved prevention, detection, and response to harmful products in order to better protect public health.[6]

While the topic of SF medicine is largely centered around health and safety issues, the sale and spread of unsafe medicine is encroaches on criminal territory for theft, fraud, smuggling, money laundering, and other infractions associated with organized crime.[7] SF medical products tend to circulate due to lack of access to healthcare and affordable medicine as well as from cultural embarrassment or shame about seeking medical products for certain conditions.[8] Certain medical issues, such as erectile dysfunction, hair loss, and weight allow the SF medicine market to take advantage of self-conscious consumers who are uncomfortable approaching a doctor for embarrassing or taboo medical needs; SF products then flow into the medicinal marketplace through online pharmacies and border smuggling, ultimately evading regulation.[9] With the grave implications of organized pharmaceutical crimes, preventing the introduction and distribution of counterfeit and falsified medicines is crucial to preserving the integrity of medicinal practices around the world.

History and Description of the Issue

Vulnerable Consumers

Users of SF medicine are at the greatest risk of exploitation and physical harm from these products. Effects can range from psychological to physical harm or even death.[10] These

1 "Substandard and Falsified Medical Products," *World Health Organization (WHO)*, accessed 26 June 2018, www.who.int/news-room/factsheets/detail/substandard-and-falsified-medical-products.

2 Ibid.

3 Ibid.

4 "1 in 10 Medical Products in Developing Countries is Substandard or Falsified," *WHO*, last modified 28 November 2017, www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.

5 Ibid.

6 "WHO Global Surveillance and Monitoring System," *WHO*, accessed 28 June 2018, www.who.int/medicines/regulation/ssffc/surveillance/en/.

7 "Pharmaceutical Crime," *INTERPOL*, accessed 20 May 2018, www.interpol.int/Crime-areas/Pharmaceutical-crime/Pharmaceutical-crime.

8 "Counterfeit Medicines and Organised Crime," *United Nations (UN) Interregional Crime and Justice Research Institute*, accessed 20 May 2018, www.unicri.it/topics/counterfeiting/medicines/report/Ctf_medicines_and_oc_advance_unedited2013.pdf.

9 "Growing Threat from Counterfeit Medicines," *WHO,* last modified April 2010, www.who.int/bulletin/volumes/88/4/10-020410/en/.

10 Andreas Seiter, "Health and Economic Consequences of Counterfeit Drugs," *Clinical Pharmacology and Therapeutics,* 85 (2009): 576-578,

risks are the direct results of harmful additives or lack of proper active ingredients in these medicines that are crucial to properly treat the medical conditions for which the medicine was created.[11] Alongside fake or harmful ingredients, consumers are also vulnerable to expired and substandard medications on the pharmaceutical black market.[12]

While all consumers of medication are vulnerable, those from countries with less monitored and accessible healthcare systems and lower economic status are affected more severely.[13] Those from lower-income countries with less access to healthcare or without a national medicine regulatory agency typically are inclined to purchase counterfeit and fraudulent life-saving medications for diseases such as malaria when the option of affording it legally is especially challenging.[14] Because these consumers are not protected by a proper pharmaceutical regulatory agency, the SF medications purchased can pose an unknown or fatal risk to them.[15] Meanwhile, in

A pharmacist hands a patient a prescription that she has filled.

higher-income countries where a national regulatory agency may have a stronger presence, counterfeit medications are likely to simply be copies of well-known brands that contain the appropriate active or alternative ingredients.[16]

In an attempt to combat the willingness of consumers to purchase medication from dishonest sources, awareness campaigns have taken place as a part of partnerships between the pharmaceutical industry, medical safety organizations, and law enforcement.[17] However, for those who seek out life-saving medicines for conditions they cannot afford to pay for legally, awareness does not attempt to reach the core of the issue.

Pharmacy Supply Chains

As pharmacy supply chains continue to grow in the global medicine market, criminals are provided with additional opportunities to breach the system and introduce fake medications to the public.[18] When pharmaceutical companies ship their products overseas, proper security measures are often poorly maintained, allowing counterfeiters to obtain the necessary information pertaining to the packaging, barcodes, and serial numbers required to create a convincing fake product.[19] This lack of proper security and mindfulness also applies to intermediary, parallel, and wholesale distributors, who are able to operate without a license.[20] An intermediary seller refers to those that serve in between the manufacturer's distribution of the product and when hospitals and doctors receive the product, with roles such as wholesaler and repackager being the types of intermediaries that can occur in the distribution chain.[21] When discussing wholesalers, it is important to

www.researchgate.net/publication/24436694_Health_and_Economic_Consequences_of_Counterfeit_Drugs.
11 Ibid.
12 Ibid.
13 Abubakr A. Alfadl et al, "The Impact of Demographic Characteristics on Vulnerability of Consumers to Counterfeit Drugs in a Developing Country," *Journal of Socialomics*, Vol. 2, no. 102 (June 2013), accessed 23 June 2018, www.omicsonline.org/open-access/the-impact-of-demographic-characteristics-on-vulnerability-of-consumers-to-counterfeit-drugs-in-a-developing-country-2167-0358.1000102.php?aid=21180.
14 Ibid.
15 Sankalp Yadav & Gautam Rawal, "Counterfeit Drugs: Problem of Developing and Developed Countries," *International Journal of Pharmaceutical Chemistry and Analysis* 2, (2015): 46-50, accessed 20 May 2018, www.researchgate.net/publication/277301823_Counterfeit_drugs_problem_of_developing_and_developed_countries.
16 Ibid.
17 "Operation Pangea," *United States Immigration and Customs Enforcement (ICE)*, last modified 3 June 2014, www.ice.gov/factsheets/ipr-pangea#wcm-survey-target-id.
18 Rüdiger Lomb, "Securing the Global Pharmaceutical Supply Chain Against the Threat of Counterfeit Drugs."
19 Ibid.
20 "Counterfeit Medicines and Organised Crime."
21 Committee on Understanding the Global Public Health Implications of Substandard, Falsified, and Counterfeit Medical Products, *Countering the Problem of Falsified and Substandard Drugs,* Washington, DC: National Academies Press, 2013, accessed 20 May 2013, www.ncbi.nlm.

Pharmaceutical packaging line which produces authentic drug packaging for distribution.

note that there are two distinct types of wholesalers in the pharmaceutical distribution chain.[22] Primary wholesalers are those who have written distribution contracts with the manufacturer and by their product directly from them. Secondary wholesalers are distributors that buy their product from other intermediaries rather than directly from the manufacturer, which carries a lesser degree of accountability depending on the wholesaler agency in question.[23] Parallel distribution is the reselling of goods between countries that takes place without the consent of the manufacturer, occurring at the same level of intermediary and wholesale distribution.[24] In Europe, the European Union (EU) policies on pharmaceuticals consider parallel distribution as a way of increasing price competition compared to other markets, obtaining profit through buying goods at relatively low prices and reselling them at more competitive prices in places where the prices are higher.[25] Because intermediary and parallel distributors conduct themselves on a secondary level of the market and do not have formal

agreements with manufacturers, their supply sources are often unknown.[26] While these distributors act within the accepted system of the legal pharmaceutical market, their general lack of security means their supply can become contaminated with illegal counterfeits more easily.[27] In addition, these intermediaries are able to act with significant negligence, as they do not have the same reputational risks as national distributors.[28]

The pharmaceutical intermediary system is largely responsible for the difficulties in controlling and regulating how fraudulent medicine can enter the supply chain.[29] In developed, high-income countries, the distribution system is structured so that products go from manufacturer, to a primary wholesale distributor, to hospitals and pharmacies, and finally to patients, with intermediaries falling in between the second and third steps of this process.[30] In this system, the infiltration of the supply chain with fake pharmaceuticals occurs in the intermediaries, with unaccountable secondary wholesale distributors and repackagers leaving an open door for fraudulent medication.[31] However, in between these steps, secondary distributors and repackagers also act as intermediaries, complicating the process and allowing for the introduction of fraudulent and counterfeit medicines into the supply chain.[32] The process of the supply chain is further complicated in low and middle-income countries, which regional distribution systems that overlap and non-governmental clinics, aid workers, and community health workers only adding to the complexity and providing more outlets for counterfeiters.[33] In both cases, fake medicine distributors take advantage of the many avenues of infiltration in the industry and provide their fraudulent supplies; however, in certain instances these illegal fake medicine distributors are invited into the supply chain.[34] If a shortfall

nih.gov/books/NBK202523/.
22   Ibid.
23   Ibid.
24   "What is Parallel Distribution?," *European Association of Euro-Pharmaceutical Companies,* www.eaepc.org/about-parallel-distribution/what-is-parallel-distribution.
25   Karima Pat Treacy & Noel Watson-Doig, "What is Parallel Trade and How Does it Affect Pharma?"
26   "Counterfeit Medicines and Organised Crime."
27   Ibid.
28   Committee on Understanding the Global Public Health Implications of Substandard, Falsified, and Counterfeit Medical Products, *Countering the Problem of Falsified and Substandard Drugs,* Washington, DC: National Academies Press, 2013, accessed 20 May 2013, www.ncbi.nlm.nih.gov/books/NBK202523/.
29   Ibid.
30   Ibid.
31   Ibid.
32   Ibid.
33   Ibid.
34   Alexandra Ossola, "The Fake Drug Industry is Exploding, and We Can't Do Anything About It," *Newsweek,* 17 September 2015, ac-

of necessary medications occurs at any point on the supply chain, whether in doctor's offices, pharmacies, or in the hands of primary distributors, the point in question might turn to outside sources to fulfill the amount requirement.[35] This allows for fake medicine suppliers to enter the scene and provide their fake product to a legal distribution avenue, infecting consumers with fraudulent medicine without their knowledge or consent.[36]

Intricacies of Packaging

Whether it is medicine or profitable luxury items, packaging is often the most crucial element of ensuring an object's surface-level legitimacy in the illicit business of counterfeit goods.[37] In recent years, pharmaceutical packaging technology has gone through an extensive evolution in order to allow for better protection of the validity of the products through the supply chain on its way into the hands of consumers.[38] In the past decade, companies have taken steps to develop safeguards and precautions on packaging as well as increase methods for authentication by adding both visible and concealed security features, such as hologram labels and brand protection features.[39] Although these attempts have heavily deterred and prevented counterfeiters, some of these safeguarding measures have eventually been duplicated and thus fail to thwart counterfeiting efforts. However, some of the features have shown promise in reducing the ability of counterfeiters, making successful gains in the field of reducing fake medicine.[40]

For the work of counterfeiters, it is crucial to obtain inside information about the exact descriptions and mechanisms of medicine packaging in order to have enough knowledge to replicate the material.[41] When pharmaceutical products cross borders and travel through various countries and the hands of numerous importers, retailers, and distributors, repackaging often takes place during the distribution and shipment.[42] This allows counterfeiters additional opportunities to copy packaging information and introduce the counterfeit products into supply channels.[43] In addition, although original packaging should be destroyed once it is replaced by repackaging intermediaries, counterfeiters often get a hold of the old material in order to reuse it or copy it for the future sale of fraudulent medicine.[44] Counterfeiters may also attempt to retrieve this knowledge of packaging is through the utilization of rejected hospital material.[45] By gaining access to a hospital's disposal system, counterfeiters are able to collect knowledge on the appearance and features of the packaging in order to recreate it.[46]

The specific anti-counterfeit packaging technologies criminals must replicate to insure authenticity are serial numbers, barcodes, holograms, and radio frequency identification devices (RFID).[47] In recent years, serialization regulations have aggressively attempted to keep up with counterfeiting attempts, with the United States implementing the Drug Supply Chain Security ACT (DSCA) in 2015 and the EU similarly implementing the Fraudulent Medicine Directive (FMD), both programs aimed at increasing traceability in the supply chain, verifying medicine legitimacy, and streamlining the medicine recall process.[48] Barcodes are another visible feature that assists in confirming the authenticity of packaging, with laser technology producing high-quality small images and two-

cessed 29 July 2018, www.newsweek.com/2015/09/25/fake-drug-industry-exploding-and-we-cant-do-anything-about-it-373088.html.
35   Ibid.
36   Ibid.
37   Shirley Redpath, "Trade in Illegal Medicine Hits Pharmaceutical Sector," *World Finance*, last modified 20 April 2012, accessed 20 May 2018, www.worldfinance.com/special-reports/trade-in-illegal-medicine-hits-pharmaceutical-sector.
38   Rüdiger Lomb, "Securing the Global Pharmaceutical Supply Chain Against the Threat of Counterfeit Drugs," World Courier, accessed 20 May 2018, www.samedanltd.com/uploads/pdf/white_paper/77c80fbbe302eb215115d72b1c3e2812.pdf.
39   Lomb, "Securing the Global Pharmaceutical Supply Chain Against the Threat of Counterfeit Drugs."
40   Ibid.
41   Ibid.
42   "Counterfeit Medicines and Organised Crime."
43   Ibid.
44   Ibid.
45   Ibid.
46   Ibid.
47   Ruchir Y. Shah, Prajesh N. Prajapati, and Y. K. Agrawal, "Anticounterfeit Packaging Technologies," *Journal of Advanced Pharmaceutical Technology & Research* Vol. 1, no. 4 (October 2010): 368-373, accessed 23 June 2018, www.ncbi.nlm.nih.gov/pmc/articles/PMC3255398/.
48   Kelly Waters, "Decoding Serialization Regulations," Pharmaceutical Technology Vol. 41, no. 6 (June 2017): 64-65, accessed 23 June 2018, www.pharmtech.com/decoding-serialization-regulations-0.

Two nearly identical drug packages; one (left) is genuine and one (right) is counterfeit.

dimensional barcodes that are scanned and sent to a central database.[49] In the past, standard inkjet printing was most commonly used for printing directly onto the packaging; however, this process is significantly more untidy and does not always provide the necessary quality for creating small enough codes that require staying clear and legible enough for weeks or sometimes months to come, thus leading to the development of the modern barcode.[50] Holograms have also been implemented, producing three-dimensional images formed from the interference of patterns created through the contact of laser beams that are later reformed under white light.[51] Holograms are widely available in numerous formats and can have complexities that vary between three-dimensional images to two-dimensional computer generated diffraction patterns.[52] However, despite how difficult holograms are to reproduce,

criminal groups still have found ways to replicate the constantly developing technology.[53] Even so, the intrinsic security features of holograms insure that they are not able to be replicated with complete accuracy, guaranteeing additional layers of safety even in the midst of the counterfeiting industry.[54]

Next to these three visible features, pharmaceutical companies have also implemented discrete, hidden security measures only recognizable and detectable by the manufacturers, including microscopic particles of specified colors as well as labels printed with chosen color combinations.[55] Another anti-fraud technology is RFID (Radio Frequency Identification Device), which is a tag that has an antenna with a microchip at its center.[56] Unlike barcodes, however, RFID includes information that can be interpreted at a distance without requiring the line of sight.[57]

49   Shah, Prajapati, and Agrawal, "Anticounterfeit Packaging Technologies," 368-373.
50   Ibid.
51   Ibid.
52   Ibid.
53   Ian Lancaster, "Sophisticated Replication Techniques Have Made Counterfeiting and Fraud a Serious Threat to the Pharmaceutical Industry," *Pharmaceutical Technology* 32, no. 4 (April 2008), www.pharmtech.com/trends-holograms-and-anticounterfeiting.
54   Ibid.
55   Shah, Prajapati, and Agrawal, "Anticounterfeit Packaging Technologies," 368-373.
56   Ibid.
57   Ibid.

Despite the aforementioned shortfalls, new and unique methods for securing medicine packaging have been developing around the world. In Mali, a new technology that uses thin wire probes connected to electrodes is being introduced in packaging that rapidly analyzes medicine for substandard ingredients.[58] While this technology had been previously available in Europe, the first affordable version was recently introduced to Mali, where the problem of substandard drugs is significant.[59] In Ghana, another security measure being implemented instead relies on individuals outside of the physical packaging itself.[60] Regardless of where their medicines are purchased, the system being implemented in Ghana would allow consumers across the country to send the label code by text message from a mobile to a verification service, and the response would confirm whether the medicine is from a legitimate source within seconds.[61] These two examples represent the search for a method of anti-counterfeiting technology that can engage the consumers being affected and protect pharmaceutical products in a way that criminals cannot replicate.

Online Pharmacies

The rapid growth of technology in recent decades has allowed for organized crime and criminal groups to evolve significantly, making use of the internet as an avenue for evading detection by police and improving communication with potential consumers.[62] This integration of the internet into organized crime has made online pharmacies an ideal method for the sale and distribution of fake medicine.[63] Online pharmacies are a relatively new innovation, developed in the 1990s to create convenience and advancement in the prescription medication healthcare system.[64] In 1999, the websites *Drugstore.com*

and *PlanetRx* were launched.[65] While they were not the first online pharmacies, they were the first to provide a safe and secure way to purchase prescription medications online.[66] As the digital marketplace began to progress and the prices of prescription drugs remained high, online pharmacies began taking advantage of the looser rules of online commerce to avoid supply restrictions and, therefore, reduce the cost to consumers, increasing company profits.[67] With the international proliferation of these sites came the introduction of fraudulent ones seeking to take advantage of the innovative arrangement of purchasing prescription medication, helping to create the pressing topic of criminal sale of counterfeit pharmaceuticals that has only grown in recent years.[68]

As illegal or falsified online pharmacies continue to expand, and as intermediaries and supply chain networks extend throughout the globe, the issue has outgrown the capabilities of individual countries' law enforcement agencies to resolve.[69] To integrate these standalone efforts and combat the issue properly, the International Criminal Police Organization (INTERPOL) alongside the Permanent Forum on International Pharmaceutical Crime (PFIPC) founded the project Operation Pangea, which was the first international program focused on targeting the fake medicine sold on the internet.[70] By coordinating law enforcement, customs, and drug regulators throughout the world and raising public awareness on safe purchasing, Operation Pangea identifies and develops the most comprehensive approach to combat the issue or falsified medicine.[71] Since 2008, the operation has had individual countries in participation, along with international organizations such as the World Customs Organization (WCO) and

---

58 Redpath, "Trade in Illegal Medicine Hits Pharmaceutical Sector."
59 Ibid.
60 Ibid.
61 Ibid.
62 "A Glimpse into the Dark World of Organized Cybercrime," *IBM Journal*, accessed 7 July 2018, www.ibmjournal.com/security/dark-world-organized-cybercrime.
63 Kah Seng Lee, et al., "Combating Sale of Counterfeit and Falsified Medicines Online: A Losing Battle." Frontiers in Pharmacology no. 8 (2017), 268, accessed 20 June 2018, www.ncbi.nlm.nih.gov/pmc/articles/PMC5432535/.
64 "Online Pharmacies - A Brief History," *CareFirst Specialty Pharmacy,* accessed 4 July 2018, www.cfspharmacy.pharmacy/blog/post/online-pharmacies-a-brief-history.
65 Ibid.
66 Ibid.
67 Ibid.
68 Ibid.
69 Kah Seng Lee, et al., "Combating Sale of Counterfeit and Falsified Medicines Online: A Losing Battle."
70 "Operation Pangea."
71 Ibid.

the Universal Postal Union (UPU).[72]

While the health risks of receiving medications from online pharmacies remains high, consumers continue to purchase unlicensed, substandard, and falsified medicines for a variety of reasons.[73] The lower cost of such medications, whether due to outside supply chain agreements that allow the products to be breached or due to organized crime operations that use non-effective ingredients in fake medications, serves as an effective argument for convincing consumers to invest in these fake medical products.[74] In some cases, these medicines are intended to treat embarrassing conditions, such as erectile dysfunction, hair growth, and weight loss, that make consumers too embarrassed to seek legal prescriptions from healthcare professionals.[75] While these conditions apply to lifestyle medications purchased by consumers in the developed world, those in the developing world also seek to avoid the shame of sharing personal information with a professional in order to obtain medication for embarrassing conditions.[76]

Pharmaceutical Companies

Although unwitting consumers are typically the initial victims of the harm caused by fake medicine, the pharmaceutical companies producing the original product also suffer at the hand of criminal groups engaging in the fraudulent medicine market.

While counterfeits are incredibly profitable for criminal groups, they have proven to be an expensive loss for pharmaceutical companies.[77] This issue costs them an estimated $46 billion annually in profit, largely due to the fact that research and development of these medications costs an incredibly high amount over several years.[78] Typically, the average selling price of medicine that has already been patented is many times over the cost of the basic ingredients, and the "sunk" costs associated with research and development of pharmaceuticals must be recouped within a very specific time period.[79] Therefore, the interference of counterfeit producers makes the issue significantly financially taxing for pharmaceutical companies.[80]

There are three types of intellectual property rights most commonly violated in counterfeit pharmaceutical products: patents, trademarks, and industrial design.[81] The infringement of patent rights occurs when there is unauthorized production, use, sale, importation of a patented active ingredient or excipient, or use of a process or method. Infringement on trademarks occurs when there is unauthorized use of a trademark on the packaging.[82] Finally, infringement on the industrial design refers to the physical contents and method of creation for the product, whether that be the formula for medicine, or the design instructions for building a medical device.[83] As the issue progresses, it becomes increasingly difficult for authorities to tell counterfeit ingredients from the original ones produced by the industry, especially in reference to Active Pharmaceutical Ingredients (APIs), the most important components of a medical product.[84] Some of the difficulty in distinguishing the sources of these ingredients stems from the fact that authorities often lack the necessary capacity and technology to do so, as these ingredients are often manufactured in bulk and typically imported from foreign jurisdictions, meaning there is considerable difficulty for authorities to control and detect counterfeit APIs entering the border.[85] Genuine APIs are protected by trademarks, and counterfeiting activities that infringe upon these rights are incredibly vol-

72 Ibid.
73 "Online Pharmacies - A Brief History."
74 Ibid.
75 Kah Seng Lee, et al., "Combating Sale of Counterfeit and Falsified Medicines Online: A Losing Battle."
76 Ibid.
77 David Wyld, "Genuine Medicine? Why Safeguarding the Pharmaceutical Supply Chain from Counterfeit Drugs with RFID is Vital for Protecting Public Health and the Health of the Pharmaceutical Industry," Competitive Review: An International Business Journal 18, no. 3 (2008), www.emeraldgrouppublishing.com/learning/management_thinking/articles/pdf/medicine.pdf.
78 Ibid.
79 Ibid.
80 Ibid.
81 "The Economic Impact of Counterfeiting and Piracy."
82 Ibid.
83 Ibid.
84 Ibid.
85 Ibid.

atile, with increased concerns if they are created in conditions inconsistent with health and safety regulations that are prime for contamination or incorrect potency dosages.[86]

In addition to being the expensive loss for pharmaceutical companies, infringement upon intellectual property rights also causes the total industry serious, long-term harm.[87] Oftentimes, the trademark for a pharmaceutical company can be its most valuable asset, providing an additional incentive for counterfeiters who are able to take advantage of the reputation and product integrity associated with it.[88] When these counterfeit products make use of the trademarks and cause harm to unknowing consumers, people then develop negative opinions of legitimate pharmaceutical companies.[89]

In an attempt to combat these issues, the pharmaceutical industry has been attempting to introduce better methods of counterfeit detection in packaging and authentication technology.[90] Among these steps in the industry response is the partnership between companies, law enforcement, and international organizations, such as INTERPOL's Operation Pangea program, which in 2014, led to 9.6 million counterfeit medications being seized that totaled more than USD 32 million, 434 arrests, and over 11,800 websites shut down, sending a powerfully aggressive message through industry and legal partnerships to would-be counterfeiters.[91]

Financing Criminal Activity

Fraudulent products have been a known source for criminal groups and organizations to obtain funding for illicit activities, and among the goods worth engaging in, counterfeit and falsified medicine are some of the most profitable.[92] This status

Pharmaceutical development plant in China.

as a wealth-bringer to criminal groups has made fraudulent medicine a staple among organized crime groups, particularly for large-scale national and international terrorist groups.[93] Many organizations have been discovered to have involvement in this fake medicine industry, from the Russian mafia and Colombian drug cartels to Chinese triads and Mexican drug gangs, numerous unscrupulous and dangerous groups have used the trade for profit.[94] However, the most concerning among these powerful players in the unscrupulous black market industry are terrorist groups, such as Hezbollah and al Qaeda, which have been connected directly to the trade.[95] In Syria's capital Damascus, a major and longstanding counterfeit drug operation was discovered, and as its members fled in hopes of revitalizing the business, the opportunities for funding illicit affairs and dangerous activity could easily see resurgence.[96] The implications of terrorist organization involvement are dire, as they present the threat of implementing terrorist connections in the industry as a means of bioterrorism.[97] Substandard and falsified medications are dangerous to global consumers, and to cause terror through biological and medical implications would be a simple task to undertake

86   Alexandra Ossola, "The Fake Drug Industry is Exploding, and We Can't Do Anything About It."
87   Ibid.
88   Ibid.
89   Ibid.
90   David Campbell, "Fake Medications, Real Solutions," *Pharmaceutical Executive* Vol. 35, no. 5 (May 2015), accessed 23 June 2018, www.pharmexec.com/fake-medications-real-solutions.
91   Ibid.
92   Brian D. Finlay, "Counterfeit Drugs and National Security," *The Stimson Center*, www.stimson.org/sites/default/files/file-attachments/Full_-_Counterfeit_Drugs_and_National_Security_1.pdf
93   Ibid.
94   Ibid.
95   Boaz Ganor, "The Infiltration of Terrorist Organizations into the Pharmaceutical Industry: Hezbollah as a Case Study," *Studies in Conflict and Terrorism* Vol. 36, no. 9 (August 2013): 699-712, accessed 23 June 2018.
96   Roger Bate, "The Deadly World of Fake Medicine," *CNN*, 17 July 2012, accessed 20 June 2018, www.cnn.com/2012/07/17/health/living-well/falsified-medicine-bate/index.html.
97   Miri Halperin Wernli and Boaz Ganor, "Pharmaceuticals: Target for Terrorism," *Actelion Pharmaceuticals Ltd,* accessed 20 May 2018, www.ict.org.il/UserFiles/Pharmaceuticals%20Target%20For%20terrorism.pdf.

for groups already embedded in the topic.[98]

Regardless of whether terrorist groups see this as an avenue for bioterrorism, the fake medicine industry remains an incredibly profitable source of funding for already existing illegal activity, giving this issue unique concerns that require a resolution to ensure proper national and international security, both in medicine and outside of it. However, it is crucial for delegates to note here that while the organized crime activities and terrorist acts of these groups do fall within the mandate of CCPCJ to address, they should not be the sole focus of this topic. Instead, delegates should look to understand and create solutions based on the systems in place that allow organized crime groups to take advantage of the fake medicine trade, and the tools such as money laundering and smuggling that guarantee their profits from this trade. While the acts they commit using the money gained through fake medicine sales warrant the Commission's attention, the topic at hand requires that delegates not delve into counter terrorism prevention and instead, continue to focus on the issues that allow for these groups to profit from fake medicine and the dangerous, resulting implications.

Current Status

Recent Public Health Crises

The pharmaceutical industry is constantly innovating, with new technologies, practices, and procedures developing at an ever-increasing rate. Just as the medical industry is changing, so is the landscape of the public health crisis. As global health continues to change and evolve, the fake medicine industry follows suit, hoping to take advantage of new and innovating medical products as well as public health crises that require

medical products and open new avenues for infiltration by fake medicine suppliers.

In 2015, WHO adopted the Global Technical Strategy for Malaria (GTS) for 2030.[99] The GTS is a plan focused on the goal of eliminating Malaria in 35 countries, reducing Malaria incidence and deaths by 90%, and preventing resurgence in all Malaria free countries.[100] However, while the goal of reducing Malaria rates has seen significant progress over the years, with incidence rates falling by 37% and mortality rates by 50%, the highly infectious disease has seen a resurgence due to falling investment and treatment spending.[101] Another major reason for continued and rising death rates due to Malaria are fake and ineffective medicines.[102] Research has shown globally that at least 200,000 preventable deaths occur each year due to anti-Malarial drugs that do not work, whether due to counterfeit status, substandard condition, or other fraudulent reasons.[103] This issue is all the more dire in sub-Saharan Africa, where fake antimalarials may be responsible for up to 116,000 Malaria deaths alone.[104] Malaria on its independently is incredibly infectious and deadly, but with the added negative and harmful contributions of counterfeit, fraudulent medicine, the problem can only grow more complicated.

In contrast to the recent resurgence of Malaria, the opioid crisis in the United States has seen a slow and steady increase, and has culminated into a national health crisis.[105] With the increased availability of fentanyl, a synthetic opioid significantly cheaper and strikingly more powerful than heroin, drug counterfeiters have made use of the growing black market of people seeking prescription painkillers.[106] In the growing storm of a worsening national health crisis surrounding opioids, physicians are prescribing fewer opioids, in part out of fear due to the legal steps put in place to limit opioid prescrip-

---

98   Ibid.
99   Tanvi Nagpal, "Back on the Rise, Malaria Rates Call for Global Spending Surge," *Axios*, 7 April 2018, accessed 10 July 2018, www.axios.com/back-on-the-rise-malaria-rates-call-for-global-spending-surge-73fc1577-19ba-4630-9ca0-8ba5dea96002.html.
100 Ibid.
101 Ibid.
102 Jackson Thomas et al., "Are Fake Drugs the Reason Malaria Sickens Millions a Year," *Smithsonian Magazine*, last modified 24 April 2018, www.smithsonianmag.com/science-nature/fake-drugs-are-one-reason-malaria-still-kills-so-many-180968882/.
103 Ibid.
104 Ibid.
105 Corky Siemaszka, "Fentanyl Figures in Most Fatal Drug Overdoses in U.S., Researchers Say," *NBC News*, 1 May 2018, accessed 10 July 2018, www.nbcnews.com/storyline/americas-heroin-epidemic/fentanyl-figures-most-fatal-drug-overdoses-u-s-researchers-say-n870481.
106 Katie Zezima, "Counterfeit Opioid Pills are Tricking Users — Sometimes with Lethal Results," *The Washington Post,* 19 November 2017, accessed 10 July 2018, www.washingtonpost.com/national/counterfeit-opioid-pills-are-tricking-users--sometimes-with-lethal-results/2017/11/19/d34edb14-be4b-11e7-8444-a0d4f04b89eb_story.html?noredirect=on&utm_term=.83b35c799e21.

tions intended towards preventing addiction and overdose deaths.[107] However, this has left some in need of opioids without and forced to seek them elsewhere, specifically counterfeit prescription opioids from cartels and drug dealers.[108] These counterfeit prescription opioids are made largely from fentanyl, but also act as a potent cocktail of other unknown substances, which pose greater risk to the consumer.[109] According to the United States Drug Enforcement Agency (DEA), one kilogram of fentanyl can produce one million counterfeit pills, bringing in USD 10 to 20 million in revenue.[110] Without having to illegally obtain real prescription opioid medications and instead just recreating the product with the much cheaper synthetics, the trade is incredibly lucrative.[111]

In each of these major public health crises, fake medicine has come to play a deadly role. With the advent of medications to alleviate certain conditions and illnesses, the threat of fake medicine looms over to damage overall health and further effect already existing medical crises.

Fakeshare Project

Fakeshare, and its subsequent program Fakeshare II, is a EU project coordinated by the Italian Medicines Agency (AIFA) and co-funded by the Prevention of and Fight against Crime program of the European condition.[112] Aimed at developing initiatives through investigation, campaigning, and training, these programs target the prevention of the illegal distribution of medicines by making use of resources on the national and international level.[113] Launched in 2013, the project's main goal is to encourage both intersectional and international cooperation between health, law enforcement, and customs au-

thorities against pharmaceutical crime in the EU.[114]

During the initial run of the first Fakeshare program, the project offered a web platform and tools specifically for strategic prevention against the role of the internet in contributing to fraudulent pharmaceutical crime.[115] This web tool known as LegitScript is a leading source of information on internet pharmacies, and conducts threat assessments and risk analysis for rogue online pharmacies.[116] LegitScript targets the advertising of fraudulent general medication, with specific attention devoted to high-risk healthcare products.[117] The program monitors internet advertisements by cooperating with search engine companies like Google and Yahoo-Bing to disable promotional links that direct users to websites violating online pharmacy standards, as well as shutting down those websites entirely.[118] Supplementing this web-based approach, the Fakeshare program also worked with enforcement and regulatory agencies across the EU, which acted as associate partners of the project, to gather data and promote information exchange between the groups.[119] In addition, public health awareness campaigns were conducted with the assistance of member state governments and non-profit organizations, with the extent of the campaigns dependent on the amount of internet pharmaceutical traffic found in the collected data.[120]

Following the conclusion of the initial Fakeshare project run in 2015, the program has been relaunched as Fakeshare II to allow the natural progression of the project to continue.[121] Non-EU member states were invited to share the Fakeshare web platform and information, as well as countries such as Mexico and Chile, which fall far outside the bounds of the

---

107   Ibid.
108   Ibid.
109   Ibid.
110   Ibid.
111   Ibid.
112   "Against Falsified Medicine, the Best Medicine," *Prevention of and Fight against Crime Programme of the European Union,* accessed 30 May 2018, www.fakeshare.eu/sites/default/files/downloads/Vademecum.pdf.
113   "Fakeshare and Fakeshare II: The Projects," *Prevention of and Fight against Crime Programme of the European Union,* www.fakeshare.eu/en/project.
114   "Against Falsified Medicine, the Best Medicine."
115   "Fakeshare and Fakeshare II: The Projects."
116   "LegitScript," *Prevention of and Fight against Crime Programme of the European Union,* accessed 27 May 2018, www.fakeshare.eu/en/partners/legitscript.
117   Ibid.
118   Ibid.
119   "Fakeshare and Fakeshare II: The Projects."
120   Ibid.
121   Ibid.

European continent.[122]

Alongside these two projects, the European Commission has also taken on several public health directives in order to combat the problem of fake medicine, such as the effort to introduce the common logo.[123] Adopted through Implementation Regulation 699/2014, the common logo exists to help identify websites operating legally and guarantees the safety of that site's medical products.[124] This logo only appears on the websites of online medicine retailers registered with their national regulatory authority and must display the country's flag, as any image that displays the EU as its flag is incorrect.[125] These logos link to each country's national regulatory agency, specifically to a page that lists of registered online medicine retailers upon which a consumer should be able to find the online pharmacy in question and are advised to not continue with their purchase if the name cannot be found.[126]

The issue of fake medicine is a difficult problem to contend with, as it requires a solution driven approach on numerous fronts, including customs officials, individual countries' national medicine regulatory agencies, consumer awareness, and internet regulation of online pharmacies. However, Fakeshare, as well as other directives put out by the European Commission to increase public health, is an interesting solution that looks to take on these different needs of the fake medicine issue.

Sustainable Development Agenda

Three years before the predetermined end of the Millennium Development Goals (MDG), the global community created a follow-up successor to continue the progress made.[127] This successor was born during the 2012 United Nations Conference on Sustainable Development in Rio de Janeiro, originating with the objective of producing a universal set of goals to meet the urgent challenges facing our world.[128] In 2015, the United Nations adopted its new Sustainable Development Goals (SDGs), with an outlined seventeen goals and 169 associated targets directed at the environmental, health and safety, and economic issues receiving major concern on the international stage.[129] While the former MDGs focused on making strides on subjects such as education, reducing poverty, and action against climate change, the new SDGs take aim at continuing such progress and making further improvements on the base of change that occurred during the timeframe of the previous MDGs.[130] While nearly all of the goals in question relate in some way, shape, or form to CCPCJ's mandate, one goal in particular is connected at its core to the topic of fraudulent medicine, and is important to highlight in the crime centered focus of this committee's mission.[131]

"Ensure healthy lives and promote well-being for all at all ages" is the third SDG, and while appearing on the surface to be associated only with matters of the spread of disease, maternal and childhood health, safe water, sanitation, and hygiene services, the topic of the fake medicine industry is crucial in terms of discussing the long-term health and well-being of individuals throughout the world.[132] Since the topic of fraudulent medicine is one that affects all countries regardless of wealth or status, it is important to analyze this issue through the lens of the SDGs, which seek to create progress for all areas of the globe.[133]

Equally important to the core health-centered goal of this topic is the subject of cooperation, outlined in the seventeenth SDG, "strengthen the means of implementation and revitalize

122 Ibid.
123 "Against Falsified Medicine, the Best Medicine."
124 Ibid.
125 Ibid.
126 Ibid.
127 "Background on the Goals," *United Nations Development Programme,* accessed 6 June 2018, www.undp.org/content/undp/en/home/sustainable-development-goals/background.html.
128 Ibid.
129 "Division for Sustainable Development Goals," *United Nations Department of Economic and Social Affairs,* accessed 12 June 2018, www.sustainabledevelopment.un.org/about.
130 Ibid.
131 "Sustainable Development Goal Three," *United Nations Department of Economic and Social Affairs,* accessed 12 June 2018, www.sustainabledevelopment.un.org/sdg3.
132 Ibid.
133 "1 in 10 Medical Products in Developing Countries is Substandard or Falsified."

the global partnership for sustainable development."[134] Reiterating that the issue at hand is one that affects all countries, it is crucial these individual states to cooperate with one another, with NGOs, and with the pharmaceutical industry to combat the fake medicine industry.[135] Coordinating law enforcement efforts, creating cross-regional awareness campaigns, and presenting a unified front to this public health concern is the best way to properly reduce the negative effects brought on by this criminal onslaught.[136]

The Sustainable Development Goals, while not explicitly focused on crime, connect strongly to the CCPCJ mandate, especially when considering the implications and effects of the subject of fake medicine. By implementing the ideals held in SDGs about looking towards long-term progress and positive developments, a future with the fake medicine industry reduced can be envisioned.

Bloc Analysis

While certain countries, particularly developing states that fall between being low and middle income, certainly face the negative results of fraudulent medicine more heavily, all wealth and development classifications of countries have been forced in recent years to confront the issue, albeit in different ways.[137] What truly divides countries in what they face from this issue is not exclusively wealthy; instead the primary point of division is the level of access to healthcare.[138] Healthcare, and whether a country's citizens have an adequate level of access, can make determinations as to the overall quality of health of the state, as well as what medications they might look to seeking illegally.[139] These medications can range from products intended to

treat deadly diseases caused by genetics and the surrounding environment, to medicines intended to relieve chronic conditions, and even lifestyle medications.[140] There has also been the idea of introducing an international medicine regulatory authority, which has the purpose of regulating the production and manufacturing of medicine by pharmaceutical companies, and the quality of the products the pharmaceutical supply chain brings into the country.[141] The lack of this sort of agency, or an inadequate agency that fails to properly regulate the quality of pharmaceutical products encourages more rampant and careless action by the fake medicine industry, allows them more leeway for tricking vulnerable consumers.[142]

Countries with Strong Access to Health Care and National Medicine Regulatory Authorities

Countries with sufficient overall access to healthcare and national medicine regulatory authorities are likely to have well-established guidelines for regulating the production and distribution of pharmaceuticals, and have strong enforcement behind these regulations.[143] Those that fall within this category include countries such as Germany, Switzerland, and Sweden.[144] Each of these states have healthcare systems that are generally lauded by the international community for their unique innovations in treating their population, and generally are able to sufficiently tackle the issue of fake medicine.[145] Well-organized pharmacy supply chains in these countries ensure the likelihood of substandard medications being introduced to the market, whether through improper storage, negligence in transportation, or deterioration.[146] In 2011, it was discovered that Sweden had been acting as Europe's primary distribution hub for counterfeit medicines in the region

134 "Sustainable Development Goal Seventeen," *United Nations Department of Economic and Social Affairs,* accessed 12 June 2018, www.sustainabledevelopment.un.org/sdg17.
135 Ibid.
136 Ibid.
137 Ibid.
138 Sankalp Yadav & Gautam Rawal, "Counterfeit Drugs: Problem of Developing and Developed Countries."
139 Ibid.
140 Kah Seng Lee, et al., "Combating Sale of Counterfeit and Falsified Medicines Online: A Losing Battle."
141 "Counterfeit Medicines and Organised Crime."
142 Ibid.
143 Yadav and Rawal, "Counterfeit Drugs: Problem of Developing and Developed Countries."
144 "Ranking the Top Healthcare Systems by Country," *International Travel Insurance Group, a*ccessed 29 May 2018, www.internationalinsurance.com/news/ranking-top-eleven-healthcare-systems-country.php.
145 Rae Ellen Bichell, "Fake Drugs Are A Major Global Problem, WHO Reports," *National Public Radio,* 2017 November 29, accessed 29 May 2018, www.npr.org/sections/goatsandsoda/2017/11/29/567229552/bad-drugs-are-a-major-global-problem-who-reports.
146 Ibid.

and beyond.[147] In 2015, Germany authorities confiscated four million counterfeit tablets alone.[148] According to Switzerland's interior ministry, an estimated 20,000 shipments of fake pharmaceuticals arrive each year into the country.[149]

These countries' overall levels of healthcare access and status of economic development also affect the types of medical products that are sold in black market pharmacies. Medicines to treat health conditions considered "taboo" by society, or ones that might cause the consumer shame or embarrassment when obtaining the drugs legally, including lifestyle medications, are common.[150] This leads to individuals using black market pharmacies in an attempt to self-medicate in a more discreet and anonymous fashion.[151] Additionally, with the rise in chronic ailments in developed countries with access to healthcare, black market pharmaceuticals targeting these conditions are commonly purchased by consumers searching for a cheaper option.[152] Black market drugs to treat cancer are fairly common due to the high cost of these medications when purchased legally.[153] Countries in this bloc are likely to advocate for raising public awareness of the deadly scams of black market pharmacies, working with online servers to prevent illegal sales through the internet, and controlling how these drugs enter the supply chain outside their borders through stringent regulations that make substandard and falsified medicines difficult to create and sell within the countries.

Countries with Moderate Access to Healthcare and National Medicine Regulatory Authorities

Countries with varying access to healthcare and a sufficient national medicine regulatory authority differ from the previous bloc in their unequal access to adequate healthcare, which can affect the demand for counterfeit and fraudulent pharmaceuticals. Those without the ability to afford medicine legally may turn to purchasing fake medicine due to their lower cost for consumers. Countries in this category include the United States, New Zealand, and Thailand, among others. [154] This bloc would also include countries that have regulatory agencies for medicine, but varying access to adequate, affordable healthcare.[155] In the countries like the United States, these healthcare inequalities stem from already existing wealth disparities between individuals in the country, leaving the poor who are unable to afford it with significantly reduced healthcare outcomes.[156]

Countries in this bloc have the ability to support regulations in the pharmaceutical supply chain for the betterment of public health and are more likely to look towards solutions focused on filling in regulatory gaps for pharmaceutical supply chain management, while also promoting awareness to consumers about this issue.[157] In one such example of this, New Zealand law enforcement showed cooperation with INTERPOL's Operation Pangea and held back 173 packages from 31 different countries to undergo further investigation.[158] Medsafe, New Zealand's Medicines and Medical Devices Safety Authority, has been raising awareness on the topic since early 2005,

---

147   "Large Quantities of Counterfeit Medicines Distributed from Sweden," *European Communities Trade Mark Association,* last modified 30 May 2011, www.ecta.org/uploads/press-doc/ecta_press_release_30_may_2011.pdf.

148   Peter Behner, Dr. Marie-Lyn Hecht & Dr. Fabian Wahl, "Fighting Counterfeit Pharmaceutical: New Defenses for an Underestimated–and Growing–Menace," *Strategy&,* last modified 29 June 2017, www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals.

149   "Cabinet Seeks to Crack Down on Fake Drugs," *Swiss Broadcasting Corporation*, last modified 22 February 2017, www.swissinfo.ch/eng/health-hazard_cabinet-seeks-to-crack-down-on-fake-drugs/42979536.

150   Kah Seng Lee, et al., "Combating Sale of Counterfeit and Falsified Medicines Online: A Losing Battle."

151   Ibid.

152   "Bad Medicine," *The Economist*, 13 October 2012, accessed 23 June 2018, www.economist.com/international/2012/10/13/bad-medicine.

153   Ibid.

154   Ibid.

155   "Ranking the Top Healthcare Systems by Country," *International Travel Insurance Group,* accessed 29 May 2018, www.internationalinsurance.com/news/ranking-top-eleven-healthcare-systems-country.php.

156   Carolyn Y. Johnson, "America is a World Leader in Healthcare Inequality," *Washington Post,* 5 June 2017, accessed 12 August 2018, www.washingtonpost.com/news/wonk/wp/2017/06/05/america-is-a-world-leader-in-health-inequality/?utm_term=.08e4ce715856.

157   "Counterfeit Medicines and Organised Crime."

158   "Medsafe Highlights Dangers of Online Medicines," *New Zealand Ministry of Health,* last modified 16 June 2016, accessed 10 August 2018, www.health.govt.nz/news-media/media-releases/medsafe-highlights-dangers-online-medicines.

through public awareness campaigns.[159]

Countries with Poor Access to Healthcare and National Medicine Regulatory Authorities

Countries with limited access to healthcare and limited national medicine regulatory authority are likely to have individuals seeking cheaper black market pharmaceutical options for fatal illnesses and serious conditions, as is the case in developing countries facing diseases such as Malaria that are treatable with proper medication and treatment.[160] Countries in this category include Chad, Guinea, and Liberia, among others[161] These countries are likely to face the brunt of fake medicines' harmful effects, with the majority of counterfeit and fraudulent medicine being used in the developing world.

In response to the detrimental effects faced in the developing world from fraudulent medicine, states within this bloc should attempt to not only support awareness of the problem of fake medicine, but also find alternative methods to assist the vulnerable consumers, to counter the incentive to purchase medicine illegally. Many countries in this bloc have taken steps to inform their citizens of the negative implications of fake medicine, through promoting awareness and educational campaigns on the dangers of counterfeit medicines, and dispatching of monitoring and inspecting teams to combat the issue in production.[162] Promotion of cooperation with non-profit and non-governmental organizations is another key element of policies within this bloc.[163] Finding effective methods for individuals to purchase legitimate products would ensure a healthier population in these countries, and is at the forefront of international healthcare agendas.

Committee Mission

As the governing body of the United Nations Office on Drugs and Crime (UNODC), the topic of fraudulent medicine is one that falls squarely within the jurisdiction of CCPCJ.[164] This committee's mandate heavily focuses on addressing organized and economic crime, making the issue of fake medicine and pharmaceutical crime a major concern.[165] During the twentieth session of the CCPCJ, the committee adopted Resolution 20/6 to address fraudulent medicine, highlighting the United Nations International Convention against Transnational Organized Crime (UNTOC) for its possible role in reinforcing international cooperation against the issue.[166] Working alongside civil society organizations, government agencies, pharmaceutical companies, and the General Assembly, CCPCJ must devote its attention to combating the issue through law enforcement and data collection, while also encouraging individual governments to examine and address the issue on a national scale.[167] It is crucial for delegates in this committee to understand the overall role CCPCJ must serve in not only mitigating these negative effects, such as the harmful health consequences consumers of fake medication face and the resulting public health crises, but also look to cooperating with other bodies and organizations to find effective ways of reducing the causes that have allowed the problem to progress forward. Delegates should also seek to understand the root issue of economic and developmental inequalities, and how these factors impact an individual's access to safe and affordable medication. The role of the CCPCJ grows only more imperative for developing solutions that pay regard to gaps in regulatory frameworks, weaknesses in capacity, and lack of resources of law enforcement, to protect the health and well-being of those affected by this criminal industry.[168]

159 Medsafe Pharmacovigilance Team, "Counterfeit Medicines - Don't Fake Concern, *New Zealand Ministry of Health,* last modified June 2005, accessed 10 August 2018, www.medsafe.govt.nz/profs/PUarticles/counterfeit.htm.
160 Ibid.
161 "25 Countries with Limited Access to Health Care," accessed 29 May 2018, accessed 8 August 2018, www.worldatlas.com/articles/the-countries-with-the-fewest-doctors-in-the-world.html.
162 "Counterfeit Drug War in Liberia," *IRIN News,* last modified 29 January 2017, accessed 12 August 2018, www.irinnews.org/report/99551/counterfeit-drug-war-liberia.
163 Ibid.
164 "Mandate and Functions," *United Nations Office on Drugs and Crime,* accessed 6 June 2018, www.unodc.org/unodc/en/commissions/CCPCJ/CCPCJ_Mandate-Functions.html.
165 Ibid.
166 "Trafficking in Fraudulent Medicine," *United Nations Office on Drugs and Crime,* accessed 6 June 2018, www.unodc.org/unodc/en/fraudulentmedicines/introduction.html.
167 Ibid.
168 Ibid.

TOPIC B:

ADDRESSING CYBER CRIME TO PROTECT ELECTION LEGITIMACY

Introduction

The advancement and development of technology since the dawn of the 21st century has undoubtedly changed the process and influence of elections at every level. The methods by which communities consume information directly correlates with how states conduct elections.[1] CCPCJ is committed to upholding the ideals espoused in Article 21 of the United Nations Declaration of Human Rights (UDHR), which reads, *"(1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives,(2) Everyone has the right of equal access to public service in his country, (3) The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures."[2]*

In accordance with this, this council has the authority to regulate the vastly unexplored domain of the Internet.[3] States around the world deal with nuances around the same problem of how to tackle threats to election integrity from both intrinsic and extrinsic actors. States must also consider the various progress made on technological fronts by their own country and how that correlates to the security of their election. The veracity in which states handle cybercrime can be attributed to the type of crime they are dealing with. With this, delegates are tasked with finding solutions to the nuanced issue of cybercrime as it relates to the legitimacy of elections.

Delegates should consider past precedence of international law and the provisions of the International Covenant of Civil and Political Rights (ICCPR) to understand election interference. The ICCPR guarantees an individual's right to privacy, guaranteeing that individuals are not "subjected to arbitrary or unlawful interference with [their] privacy."[4] Hackers who obtain information from an election system, including voting rolls and results, have intentionally violated this international act of privacy.[5] Citizens of the 169 states who are signatories of the ICCPR also have guaranteed rights to genuine elections, a right that could be restricted if states do not adequately protect their voting infrastructure from unlawful interference. The ICCPR obligates states to hold "genuine, periodic elections" without "unreasonable restrictions."[6] In summary, election related cybercrime threatens "the right of every sovereign State to conduct its affairs without outside interference."[7]

History and Description of the Issue

As long as democratic institutions have existed, so has voter fraud: dead people voting, vote-buying, theft or burning of ballots, threats of violence, rigged counting.[8] In tandem with the cybersecurity industry boom of the last three decades, voting has become increasingly reliant on secure, accurate, and speedy voting technology. The prevalence of cybersecurity in voting has been critical for the integrity of Democracies around the world, as elections can be won or lost on a single district or set of machines. For example, in 1988, Mexican opposition candidate Cuauhtemoc Cardenas was winning the election to the majority party candidate Carlos Salinas until the voter tabulation system failed due to "failed phone lines," costing him the election.

In this burgeoning era of globalization, it is important to define the integral factors of voting infrastructure. Voting infrastructure problems and its exemplifying factors must be defined in order to understand the issues of critical internal voting. In doing so, it is vital to differentiate pure election security issues from broader information operations or covert influence campaigns, as well as even broader cybercrime is-

1   David P. Fidler, "The U.S. Election Hacks, Cybersecurity, and International Law." AJIL Unbound 110 (2016): 337-42. doi:10.1017/aju.2017.5. www.cfrd8-files.cfr.org/sites/default/files/report_pdf/CyberBrief_Fidler_Elections_OR_2.pdf.
2   Ibid.
3   Ibid.
4   Ibid.
5   Ibid.
6   Ibid.
7   Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).
8   Andrea Rodriguez, "Ahead of Mexico's presidential election, fears and warnings over possible fraud," *Chicago Tribune,* 29 June 2018, accessed 6 October 2018, www.chicagotribune.com/news/nationworld/ct-mexico-election-fraud-warning-20180629-story.html.

sues.[9]

Due to its large breadth and application, the voting process has lagged behind in technical advancements. This lag in reform and innovation has led to its increased susceptibility to abuse by hackers since voting processes were hastily ushered into the digital age. At least five areas of the electoral process are potentially vulnerable to hacking. These are: (1) the information received by voters in the lead-up to the election; (2) the electoral rolls used to check voters in on Election Day; (3) the machines on which voters cast their ballots; (4) the tabulation mechanisms for determining the winners; and (5) the dissemination systems used to spread news of the results.[10]

Electronic Voting Technologies

In order to understand current online voting technologies, it is necessary to dissect the history of electronic voting technologies. Electronic voting refers either to the use of computers or computer technologies in voting systems.[11] The main disadvantages of a purely electronic voting system is the lack of a paper trail: recounts are impossible and voting data, when administrative access is given to the wrong party, can be manipulated without a physical backup.

Early electronic voting systems were machine counting systems: machine-readable ballots that were filled in by pen, pencil, stylus, or mechanical hole puncher.[12] The main advantage of a machine-readable ballots is speed. Other advantages included a unified voting system, a faster recount speed, and a more universal way of reading ballots that is blind to human bias. But the latter two methods of machine counting, namely the stylus and the machine hole puncher, caused contentious and potentially election-changing issues. Stylus' or machine hole punchers created divots or "chads" in the ballots.

Standard voting booths at a polling station in the United States.

Chad or "hanging chads" became notorious in the 2000 United States presidential election. A "hanging chad" is a chad that has not completely broken off the ballot, which caused some 178,000 misreported ballots in the state of Florida— enough of a swing vote to cost incumbent candidate Al Gore to lose the election to then President George W. Bush.[13] In addition, these older legacy electronic machines break down with time; some older machines from the 1990s have such small memory cards that they overflow and crash the machine, others have internal glue which holds the touch digitizer to the screen and may unstick, gunk up, and therefore misinterpret votes.[14] Most importantly, older machines are susceptible to hackers due to their well published designs, known vulnerabilities, and outdated hardware.[15]

Today, archaic electronic voting machines have evolved to computer voting and online voting. While not all voting centers around the world have moved past electronic voting, the advantages of computer voting and electronic voting are clear: not ballot miss-reporting. Computer voting is defined as Direct-recording electronic (DRE) machines, machines that directly take the voter input and adds them to a running tally.[16] Originally, these computer voting systems were just improved electronic voting rigs, but today have evolved to be much more sophisticated; less moving parts, better software,

---

9   Susan Hennessey, "Cybersecurity of Voting Machines," *Brookings*, 4 December 2017, accessed 25 June 2018, www.brookings.edu/testimonies/cybersecurity-of-voting-machines/.; www.americanprogress.org/issues/democracy/reports/2017/09/11/438684/election-infrastructure-vulnerabilities-solutions/
10   Ibid.
11   "Online Voting," *Parliamentary Office of Science and Technology,* May 2001, accessed 30 September 2018, www.parliament.uk/documents/post/pn155.pdf.
12   Ibid.
13   Ed Plinkington, "Hanging chad redux? US heading for 2000-style election catastrophe, report finds," *The Guardian,* 15 September 2015, accessed 30 September 2018, www.theguardian.com/us-news/2015/sep/15/2016-election-old-voting-machines-hanging-chad.
14   Ibid.
15   Ibid.
16   "Online Voting."

and improved ATM-like security, have made computer voting the number one on-site tallying choice of voting.[17]

The most recent and most technologically advanced type of voting is online voting. Online voting can be broken down into four types: poll site, regional poll site, kiosk, and remote.[18] Regardless of type, the advantages are clear: it is quick, efficient, and paperless. The first instance of online voting occurred in August 1996 by the Reform Party in the United States presidential election with around 2000 online voters.[19] As of May 2017, fourteen nations have implemented online voting, with Estonia being the first and only to implement permanent national online voting.[20] Since its implementation in 2005, the rate of online voting in Estonia has risen from 1.9% to over 30% from 116 countries; one large contributor to the efficacy of Estonia's online voting system has been its exemplary state of the art digital ID cards.[21]

Voting Registration and Voter Information

Another critical vulnerability in election infrastructure is voting registration and voting machines. The issue of voter registration is ubiquitously contentious, raising issues in developed countries and developing countries alike. Article 21 of the UN Declaration of Human Rights declared that everyone has the right to "elections… held by secret vote or by equivalent free voting procedures" and as such, many democracies around the world have pushed to have increased voter registration. However, hackers may attempt to delete registered voter entries from the poll book just prior to the election, making it difficult for voters to check in on Election Day, contributing to delay and undermining systematic trust.[22] This criminal action violates protected rights by denying people their ability to contribute to the democratic process.

Hacks on registered voter information databases also violate privacy rights. In order to cover up nefarious activity, hackers may attempt to change voter information or to steal private information like personal government issued identification numbers.[23] To do so, the computers of election administrators or companies can be hacked in order to gain access to the personal information stored on voter registration software.[24] Individuals who are registered with a party that another group is aiming to undermine may be targeted.[25] Hackers may implant malicious computer code on computers belonging to the targeted party members or supporters. Additionally, personal information such as documents and private emails may be stolen.[26] Stolen names and personal information could be used to sway voting outcomes, influence popular opinion, or change policy wording.

During the conversation around net neutrality in the United States in 2017, millions of Americans filed claims that their identities or the identities of their deceased loved ones were used to write comments supporting internet regulation.[27] The identities used to post comments match those compromised in recent data breaches and were used to appear as if real people were supporting policy changes. The comments were intended to influence the vote of the Federal Communications Commission (FCC) on whether or not to dismantle net neutrality rules for Internet providers.[28] Since the FCC values public comments as a way to solicit feedback from Americans before it votes to make significant policy changes, the hack

17   Ibid.
18   Ibid.
19   Ibid.
20   Gabriella Mulligan, "Has the time now come for internet voting?" The BBC, 30 May 2017, www.bbc.com/news/business-39955468.
21   Ibid.
22   Susan Hennessey, "Cybersecurity of Voting Machines," Brookings, 4 December 2017, accessed 25 June 2018, www.brookings.edu/testimonies/cybersecurity-of-voting-machines/;   www.americanprogress.org/issues/democracy/reports/2017/09/11/438684/election-in-frastructure-vulnerabilities-solutions
23   Massimo Calabresi, "Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say," *Time,* 22 June 2017, accessed 30 September 2018, time.com/4828306/russian-hacking-election-widespread-private-data/
24   Ibid.
25   The United States District Court for the District of Columbia, Case 1:18-cr-00215-ABJ, 13 July 2018, accessed 30 September 2018, www.justice.gov/file/1080281/download.
26   Ibid.
27   Brian Fung, "FCC net neutrality process 'corrupted' by fake comments and vanishing consumer complaints, officials say," *The Washington Post,* 24 November 2017, accessed 30 September 2018, www.washingtonpost.com/news/the-switch/wp/2017/11/24/fcc-net-neutrality-process-corrupted-by-fake-comments-and-vanishing-consumer-complaints-officials-say/?utm_term=.a7bc897ae63a
28   Ibid.

and impersonations were a strategic and calculated move.[29] This example of identity fraud illustrates the capability and method by which some groups may attempt to subvert the integrity of democratic processes.

More advanced criminal ploys could employ creative tactics to disguise skewed vote totals or other altered election results and information. Hackers could theoretically modify voter registration databases by adding in fictitious voters or changing information for certain voters.[30] Another possible method for the cover up is registering dead voters to conceal the skewed vote totals and make them appear as legitimate votes cast by real people. Oftentimes, systems in place to detect and remove deceased voters are out of date and flawed. In the United States, a study by the Pew Center on the States found that more than 1.8 million dead people were still registered to vote in 2012.[31] Proposed simple fixes for voter registration fraud include signature verification, a low-tech tool preventing people from impersonating others.[32]

Benefits of Online Voting

With the growing concern of threats to voting infrastructures, a new solution has emerged that takes advantage of the

Ballot used to cast an electoral vote in France.

growth in the technological field. While online voting has not yet garnered a massive following, it gives voters an opportunity to voice their opinion with added convenience and security. Through online voting, individuals whose employment hours are not compatible with their respective states' voting hours can now cast their ballots independently. First introduced in the United States in 2000, remote internet voting is now available in fourteen countries, including Canada, France, and Switzerland.[33] This new technology shows vast potential in a growing global and technology-based world. Countries that experience large amounts of expatriate voters may seek to utilize online voting as a means to streamline the voting and tallying process.[34]

Despite the positive aspects of online voting, there stand some pitfalls. There stands the general issue of internet security and the vulnerabilities of a system based on a public system of information. Consumers may not have full trust in the security of online voting and may then refrain from partaking in such. Online voting also requires a prerequisite knowledge of computer skills and technical expertise and any gap in understanding of these may discourage a voter from using this method.[35] Internet voting also shares an inherent flaw with postal voting systems, in that the validity of the individual casting the vote cannot be confirmed. Despite this, both methods are currently considered to meet the standards of secrecy by the Venice Commission.[36]

The global technology boom in cryptology has led to the adoption of electronic voting (e-voting) and automated electronic voting machines (EVMs) and within EVMs direct-recording electronic voting machines (DREs) around the world.[37] There are two types of E-voting that are utilized in nations that use the technology: (1) On-site e-Voting - supervised by representatives of governmental with E-voting machines at the polling station); and (2) Remote E-voting - not physically super-

29 Ibid.
30 Laura Hautala, "Voter fraud and dead people: How tech sets things right," *CNET,* 19 October 2016, accessed 1 October 2018, www.cnet.com/news/how-tech-eases-trump-election-rigging-voter-fraud-concerns/.
31 Ibid.
32 Ibid.
33 "Internet Voting," *National Democratic Institute*, 25 November 2013, www.ndi.org/e-voting-guide/internet-voting.
34 Ibid.
35 Ibid.
36 Ibid.
37 Aboubakr Ebrahim Elewa et al., "Challenges of Electronic Voting - A Survey," *Advances in Computer Science: An International Journal,* [S.l.], p. 98-108, ISSN 2322-5157, 2015 November, accessed 1 October 2018, www.acsij.org/acsij/article/view/379.

vised like voting using computer via the internet, using mobile phones via SMS, or at public kiosks.[38] The technology of E-voting helps to speed up the counting of ballots, reduce the cost of paying staff to count votes manually and can provide improved accessibility for disabled voters.[39]

Cyber Threats to Voting Machines

Because electronic voting and online voting are so new, they face unique challenges that are easily exploitable by cyber attacks. Professor Stephen Schneider, professor in security for the department of computer science at the University of Surrey, has stated specifically in reference to online voting that "the main security threat to online voting would be from malware on personal computers, which could potentially change votes cast via the internet."[40] In a similar vein, Professor Schneider has also stated that electronic voting, specifically on older voting machines like those found in the United States are "more easy to subvert."[41]

The data from the elections are held in what is supposed to be secured servers and tabulated to come to a consensus on the issues being voted on. Direct-recording electronic voting machines (DREs) process data by means of a computer program that records voting data and ballot images in memory components. After the election, DREs produce a tabulation of the voting data stored in a removable memory component and as printed copy which aggregates the results of an election.[42] While it is true that not every country uses an online or electronic system to register voters, trends show that more and more countries are registering higher and higher amounts of people to vote as accessibility increases and online capacities increase. These tabulation systems are vulnerable to breaches

in security. At the precinct level, some attacks on voting machines can manipulate tabulation. More centrally, attackers might be able to affect tabulation between precincts.[43] A hack of the Ukrainian voting system in 2014 removed important files from the informational reserve infrastructure just prior to the election, requiring officials to rely on backups, according to the Michigan Law Review.[44]

This adoption of technology may have its benefits, but it also has it potential consequences. Attacks on E-voting systems and voting machines are entirely possible, which makes the stored data possibly compromised and unusable in an election.[45] The widespread lack of standardization throughout the international community leaves voting infrastructure vulnerable.[46] Security audits of these voting machines reveal that the vast majority have weak encryption networks and insecure (or sometimes non-existent) passwords.[47] While these physical machines are "air-gapped," meaning they are not connected to the internet, even more vulnerabilities arise when the aforementioned out of date operating systems are probed; counties and municipalities alike suffer from lack of standardization and electronic prowess.[48]

Proposed Solutions

Public-Private Partnerships occur when the public sector contracts services from a private party and the burden of project ownership and efficient operations fall to the private sector supplier.[49] PPPs act as mechanisms for public entities to use private companies to do jobs that are more suited to the private sector to come to the most efficient solution. This model has been employed extensively by actors within the EU, with the goal of bolstering the cyber sphere as the backbone of the

38 Ibid.
39 Ibid.
40 Gabriella Mulligan, "Has the time now come for internet voting?" *The BBC*, 30 May 2017, www.bbc.com/news/business-39955468.
41 Ibid.
42 Ibid.
43 Ibid.
44 Ibid.
45 Elewa et al., "Challenges of Electronic Voting - A Survey."
46 Susan Hennessey, "Cybersecurity of Voting Machines," *Brookings*, 4 December 2017, accessed 25 June 2018, www.brookings.edu/testimonies/cybersecurity-of-voting-machines/.; www.americanprogress.org/issues/democracy/reports/2017/09/11/438684/election-infrastructure-vulnerabilities-solutions
47 Ibid.
48 Ibid.; www.economist.com/united-states/2018/07/19/voting-machines-in-america-are-reassuringly-hard-to-hack
49 *Willis - Global Risk Advisor, Insurance and Reinsurance Broker*, 19 accessed July 2018, www.willis.com/Client_Solutions/Services/PPP-PFI_(Public_Private_Partnerships_and_Private_Finance_Initiative)/.

European society and economy.[50]

As previously outlined, the effects of cyber attacks on elections lead to distrust among the electorate. In accordance with this, only 22% of Europeans feel confident in search engines, social networking sites, and email services.[51] The benefits of these proposed partnerships being considered for elections include improved infrastructure, security in online systems, and an improved level of trust between voters and election procedures. The operational and project execution risks are transferred from the government to the private participant, an entity which typically has a background in the relevant field.[52] By increasing the efficiency of the government's investment, government funds can be redirected to other important socio-economic areas.[53]

A key issue with PPPs arises with the fragmentation of the EU cybersecurity industry. While cybersecurity threats are borderless by nature, the EU cybersecurity market is highly fragmented due to solutions driven by individual governmental needs and a lack of trust for cross border purchasing.[54] The impact of this is seen in furthered disadvantages for businesses competing on a global level. For consumers, it reduces choice of innovative, competitive, and user-friendly technology that considers European rules & values.[55]

Current Status

Case Study: US 2016 Presidential Election

Since the initial announcement of the 2016 Presidential election result, the topic of possible Russian interference has been a recurring theme in the global discussion on the President's role. A number of individuals and groups have been linked to breaches of American electoral security, including contracted

Donald Trump (Left) and Hillary Clinton (Right), nominees for the 2016 presidential election in the United States.

private entities, lone wolf actors, and the Russian government. It is important to understand how deep this interference runs, in order to understand its corresponding effects. The alleged Russian interference affected 39 states and in one instance attempted to delete and alter voting data.[56] The interference highlighted weaknesses in American election voting infrastructure. Composed of software companies, online voting registration sites, and confidential emails, the internal infrastructure within the American electoral system left voting systems susceptible to potential interference.[57] For example, in Illinois, cyber intruders attempted to alter or delete the voter data of fifteen million registered voters.[58] Hackers in another state attempted to reveal data they acquired from a campaign finance database, which gave them insight into the financial connections between certain voters and candidates.[59] This is problematic due to the nature of the information leaked; that possession of such information led to a targeted misinformation campaign. The publication of this sensitive information would lead to more external discord that would continually add to the growing ever-hostile political climate.

In July 2016, infamous conspiracy news resource WikiLeaks published a series of confidential emails exchanged between

---

50   "Cybersecurity in the European Digital Single Market," *European Commission: High Level Group of Scientific Advisors,* No. 2 (2017), accessed June 25, 2018, ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf.
51   Ibid.
52   Juan Rodriguez, "The Benefits and Disadvantages of P3," *The Balance Small Business*, 28 March 2018, accessed 19 July 2018, www.thebalancesmb.com/public-private-partnership-pros-and-cons-844713.
53   Ibid.
54   Ibid.
55   Ibid.
56   Alex Ward, "Russia Hacked Voting Systems in 39 States before the 2016 Presidential Election," *Vox*, 13 June 2017, accessed 26 June 2018, www.vox.com/world/2017/6/13/15791744/russia-election-39-states-hack-putin-trump-sessions.
57   Ibid.
58   Ibid.
59   Ibid.

several key members of the Democratic National Committee (DNC), supposedly leaked via an anonymous source.[60] These emails included the DNC's off-the-record correspondences with the media, severe derision of the Bernie Sanders campaign by some key members of the Democratic Party, and highly sensitive financial information concerning high-profile donors in the Clinton campaign.[61] The aforementioned correspondence regarding the Sanders campaign exacerbated internal dissidence within the DNC, causing the chaos the hackers intended. Another important caveat to this hacking is that the US, specifically the Obama administration's White House, was aware of the intrusion.[62] While staffers within the administration desired to go public, the White House decided that the revelation was not worth risking the American people's faith in the very institution of elections.[63] However, this hush-hush approach would prove costly. It meant that Russian hackers could breach the committee's network for nearly seven months before top DNC officials were alerted to the attack, at which point cyber experts were hired to protect the DNC systems.[64] In the meantime, the hackers moved on to targets outside the DNC, including Hillary Clinton's campaign chairman, John D. Podesta, whose private email account was hacked months later.[65] The fallout led to the resignation of the DNC chairwoman as well as the party reeling.[66]

From this situation there are many takeaways for all parties involved as well as the international community as a whole. For Russian hackers, it shows why a state would want to interfere in other countries electoral process. Through the exposure of confidential material used to sow seeds of discord within the electorate, the Russians succeeded in creating an environment within the US in which the institution of elections was questioned. They did not change votes, or hack directly into U.S. voting machines. Instead, they threatened the trust of US voters in the electoral system.[67]

The international community and delegates of this committee must understand the ramifications of electoral interference and a weakened level of trust from the public. Countries such as the United States are global powers and a plunge into cyber warfare with another world power such as Russia would not be beneficial to either respective state or the international community at large. With this comes a point of distinction between cyber warfare and other methods of crime addressed by the CCPCJ. The nature of cybercrime is political. As we continue to move forward in an increasingly cyber dominant world, all states must understand that cybersecurity and its implementation are no longer a luxury, but an international necessity.

Sustainable Development Agenda

September 2015 marked the dawn of a new international era of giving in a global sense. The 2030 Agenda for Sustainable Development was adopted by world leaders in order to combat the global issues of inequality, poverty, and climate change.[68] Goal sixteen of the Sustainable Development Goals (SDGs) falls directly within the scope of discussion for this committee, as it intends to "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels."[69] Strengthening election infrastructure relates directly to this mission, and deterring cybercrime may be discussed within the context of the CCPCJ.

In accordance with Article 21 of the UN Declaration of Human Rights, the right to a free and fair election is critical to the success and foundation of a country's future endeavors. To further carry out the goals enshrined in the agenda, a

60   Harold Stark, "How Russia 'Hacked' Us In 2016 [And What We Did Wrong]," *Forbes,* 29 April 2017, accessed 26 June 2018. www.forbes.com/sites/haroldstark/2017/01/24/how-russia-hacked-the-election/#2c5030684a9f.
61   Ibid.
62   Ibid.
63   Eric Lipton, David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, 14 May 2018, accessed 26 June 2018, www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.
64   Ibid.
65   Ibid.
66   Ibid.
67   Ibid.
68   "A New Sustainable Development Agenda," *United Nations Development Programme*, accessed 13 July 2018, www.undp.org/content/gcp/en/home/2030agenda/.
69   Ibid.

state must first ensure the stability of its government through transparent reporting. Opaque, burdensome, and inefficient regulations and procedures nurture opportunities for corrupt officials to extract bribes or unofficial payments. In 2015, over 18% of firms worldwide reported receiving at least one bribery payment request.[70] The share of firms in low and lower-middle-income countries totaled 25%, compared to 4% in high-income countries.[71] To provide a sound basis for development, countries and their leaders must not be privy to outside influences. If a government is susceptible to these vices at all levels, then their transparency and corruption safeguards leave them privy to large scale instructions or instances of cyber activity.

In accordance with the 2030 agenda set forth by the United Nations, CCPCJ must recognize the ongoing struggle of states to implement freedom of information legislation.[72] The freedom of information and its subsequent flow is vital to fostering an environment in which election related information can be displayed without fear of retributions. Legislation that calls for freedom of information has increased steadily, but slow or inefficient implementation of such laws remains a concern. More than 110 countries have adopted freedom of information legislation and policies. However, expert assessments suggest that 47 of those countries fall short of having clear legal provisions for exceptions to that right, while another 47 countries lack sufficient provisions for public education.[73]

Bloc Analysis

Member states of CCPCJ have varying levels of institutional strength. Blocs within this topic are primarily based on individual states' abilities to cultivate fair and free elections. This distinction is made in consideration of the strength and safe-

guards of a state's electoral institutions, the consistency of fair elections, the corruption of the overall government, and the freedom of the press to politically report truthful news. Another major factor to consider between the blocs is the type of cyber-security threats that they would receive. Serving as an empirical indicator of each factor, the World Bank index on the fairness of elections measures a state's capacity to hold fair elections, and ranks it on a scale in comparison to its peers.[74] It is important to note that while the ability to hold free and fair elections is not perfect indicator of a country's position on election cybercrime and its solutions, the correlation between countries that have low election safeguards and the likelihood that cybercrime occurs is notable.[75] Additionally, the Information and Communication Technology (ICT) data is measured with the ICT Development Index (IDI) by the United Nations International Telecommunication Union.[76] This index is useful in investigating the digital divide, which will be divisive when forming blocs. For developed countries where internet usage rates are double usage rates in developing countries, hacking and other cyber attacks are problems already.[77] For countries with lower IDI values, addressing cybercrime is not the most pressing way to improve election legitimacy. In the least developed countries, internet communication networks, social media, and online voting or electronic voting machines are nearly nonexistent."[78]

States with Environments Conducive to Safe and Fair Elections

Member states within this bloc have two primary defining factors; their institutions are strong enough to withstand and counteract cyber attacks and their problems arise from primarily external actors. States with strong cyber infrastructure and security measures in digital communication are less likely

---

70 "Goal 16: Sustainable Development Knowledge Platform," *Sustainable Development Goals*, accessed 18 July 2018, www.sustainabledevelopment.un.org/sdg16.
71 Ibid.
72 Ibid.
73 Ibid.
74 "GovData360: Free and Fair Elections," *GovData360 - Governance Data*, accessed 29 May 2018. www.govdata360.worldbank.org/indicators/h7a147898?country=BRA&indicator=28751&countries=MEX,VEN,ARG&viz=bar_chart&years=2016#table-link.
75 Ibid.
76 "Measuring the Information Society Report 2016: Key Findings," *International Telecommunication Union,* accessed 30 September 2018, www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-KeyFindings.pdf.
77 Ibid.
78 Ibid.

to fall victim to an election hack. These are likely developed and democratic countries who hold election integrity to high standards. Many already have internal mechanisms in place to stop electoral misnomers, which demonstrates a cognizant effort to deter the problem. Further, countries of this bloc are likely countries with high IDI values that have established internet communication networks and populations accustomed to using it. The citizens will be invested in electoral technologies and improving its security. For reference, countries in Europe have the highest average IDI values.[79]

In order to effectively represent countries within this bloc, delegates must understand the critical electoral infrastructure predicament. These countries are acutely aware of the nuanced nature of cybersecurity and election legitimacy. They are countries who historically take liberal ideologies very seriously, including freedom of information flow, an unabridged press, and widespread suffrage. Delegates must derive country policy from the state of cyber infrastructure and security in their country, and how said infrastructure can be utilized to ensure a safe and fair electoral environment. Member states include countries such as Germany, The United Kingdom, and Canada.

States without Environments Conducive to Safe and Fair Elections

States with lower indexes of developed election infrastructure have electoral institutions which are easily susceptible to foreign and domestic meddling. Internal dissidence comes at the expense of weak institutions. This often leads to a lack of transparency and ensuing corruption within a government, and a heightened risk of interference from a host of outside actors. These may include hacking groups looking for political sway, terrorist organizations vying for power in the region, and even political leaders looking after their own financial or party interests. These states may also be perpetrators of cybercrime. Combined with the lack of preventive measures and institutional safeguards, it is understandable how these states could be considered vulnerable to electoral hacking. States

within this bloc are Iran, Syria, Russia, and China.

Chinese president Xi Jinping proudly announced that his country is "blazing a new trail" for developing countries to follow, but the NGO Freedom House and other entities have noted that China's path is of politicized courts, intolerance for dissent, and predetermined elections.[80] If such trends modeled by China, Russia, and other countries of this bloc continue, then global democratic norms will be replaced with authoritarian practices.[81] Elections will not be free. Instead, the current administration's victory will be the undoubted outcome. These countries would not be extremely concerned with tough regulations or punishments on electoral fraud. Countries with elections that do not enable new parties or candidates to enter the political system and overall disrupt smooth transitions of power, or prohibit power transitions completely, are examples of states without environments conducive to safe and fair elections.

States with Limited Exposure to Technology

Countries in this bloc might have some populations using the internet and other communication technologies. However, the technology would not be as widespread and might be relatively new; in 2015, only 34 percent of households in developing country regions had internet access, though this figure is increasing.[82] Therefore, the population might not be as trusting of voting technologies, if they are even available. It is likely that the introduction of online voting or electronic voting machines will not be introduced to the countries of this bloc for a while longer. These countries might look toward proactive solutions for counteracting election interference, such as education campaigns, security and safety features within networks, or other cautionary measures. Within these blocs, there is likely a lack of infrastructure for recognizing and then combatting the cyber crimes which might compromise election integrity.

Other countries within this bloc might have little to no expo-

79 "Measuring the Information Society Report 2016," *International Telecommunication Union.*
80 Elen Aghekyan et al., "Freedom in the World 2018; Democracy in Crisis," *Freedom House,* 2018, accessed 6 October 2018, freedomhouse.org/report/freedom-world/freedom-world-2018.
81 Ibid.
82 "Human Development Report 2015: Work for Human Development," *United Nations Development Programme,* accessed 30 September 2018, hdr.undp.org/sites/default/files/2015_human_development_report.pdf.

Voting in the 2005 nationwide elections in Iraq.

sure to cybercrime since only seven percent of households in the least developed countries even had internet access at the end of 2015.[83] Resultantly, countries in this bloc would be least affected by the issue. Countries of this bloc might advocate for fortifying election systems and holding individuals accountable as opposed to trusting electronic machines. However, corruption itself might be a familiar issue within such countries, so these countries might focus more on the preventing and combating criminal interference with elections. This bloc might also emphasize the importance of international cooperation to combat cybercrime in hopes of bridging the digital divide through partnership on the topic of cybertechnology.

Committee Mission

The Commission on Crime Prevention and Criminal Justice acts as the governing body to the United Nations Office on Drugs and Crime (UNODC), and as a policymaking body on international crime and drug related issues.[84] ECOSOC has outlined the CCPCJ's mandates and priorities in resolution 1992/22, which include improving international action to combat national and transnational crime and the efficiency

and fairness of criminal justice administration systems.[85] Delegates should consider factors including, but not limited to: the topic of discussion at hand, the committee's mandate, a state's respective current position on the topic, precedent of the committee, and the desired solution.

At the forefront of discussion within the CCPCJ is protecting the legitimacy of elections around the world. Member states and the delegates representing them are encouraged to research all facets of their countries position and the issue itself when considering new perspectives and solutions. Diplomacy and cooperation among delegates, and among member states with contrasting ideas, will be vital to the success of this committee. With the United Nations Sustainable Development Goals in close consideration, the CCPCJ must form a solution that will work to alleviate the threat of cybersecurity facing elections across the international community.

83   Ibid.
84   "United Nations Office on Drugs and Crime," *UNODC,* accessed 25 July 2018, www.unodc.org/unodc/en/commissions/CCPCJ/index.html.
85   Ibid.

Research and Preparation Questions

Your dais has prepared the following research and preparation questions as a means of providing guidance for your research process. Delegates are NOT obligated to formally answer these questions either in committee or in position papers. Rather, these questions should be carefully considered, as they embody some of the main critical thought and learning objectives surrounding your topic.

Topic A

1. Describe and evaluate your country's level of access to healthcare for its population and how it affects your country's entanglement in fraudulent pharmaceuticals? Are there populations in your country that are most susceptible to its adverse effects?

2. What has your country done in the past to combat fake medicine and how have their pharmaceutical regulations strengthened or worsened over time?

3. Are there public health crises, both past and ongoing, that have been influenced by the fake medicine industry in your country? In what ways can fake medicine infiltrate future health crises?

4. Describe your country's regulations on pharmaceutical drugs and devices and how that has affected the prevalence of fake medicine? In this same vein, how have pharmaceutical intellectual property laws impacted the issue?

5. What strategies might your country implement to incorporate non-state actors into tackling fake medicine, and what strategies if any has it undertaken in the past? How can your country increase cooperation between government and non-government agencies on this subject?

Topic B

1. What is the historical context in regard to your country's stance on sovereignty, do you think this stance would also be applicable to those having to do with cyber-sovereignty? What are the possible limits of the domain in question (the internet)? How does your state, on historic level, deal with territorial disputes?

2. In the past, how has your country advanced to be up to date with technological infrastructure issues? Is your country equipped to handle cyber attacks and disasters with the infrastructure already in place? How has history affected the answer to the previous question and how will it impact the future?

3. What is the relationship between your country's government and Non-State Actors as it applies to cyber-security affairs? What are the benefits and disadvantages that come along with allowing NSA's to have knowledge and access to governmental information?

4. When it comes to media and reporting, does your country have any safeguards in place to protect against blatant, malicious misinformation? If so, does your state support this type of 'regulation'? Or, does it maintain a neutral stance towards the media, regardless of its consequences?

5. Does your country have any stance or prior experience with online voting? Does it have the proper channels to conduct said activity legitimately? If not, what political and domestic barriers stand in its way?

Important Documents

Topic A

"1 in 10 Medical Products in Developing Countries is Substandard or Falsified." *World Health Organization.* Last modified 28 November 2017. www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.

This source from the World Health Organization details the results of statistical surveys on the current status on the prevalence of counterfeit and falsified medicines globally.

Blackstone, Erwin A., Joseph P. Fuhr Jr., and Steve Pociask. "The Health and Economic Effects of Counterfeit." *American Health and Drug Benefits* Vol. 7, no. 4 (2014): 216-224. Accessed 20 May 2018. www.ncbi.nlm.nih.gov/pmc/articles/PMC4105729/.

While the article's primary focus is toward the United States healthcare system, this paper provides strong explanations and materials on the complicated effects counterfeit drugs have on healthcare and pharmaceutical companies that can be applied generally.

"Counterfeit Medicines and Organised Crime." Accessed 20 May 2018, www.unicri.it/topics/counterfeiting/medicines/report/Ctf_medicines_and_oc_advance_unedited2013.pdf.

This paper details the major differences and similarities between counterfeit medications distributed in developed countries and developing countries and the factors behind the two that aid in this perpetuating this gap.

Khan, Mohiuddin H et al. "Perceptions and Practices of Pharmaceutical Wholesalers Surrounding Counterfeit Medicines in a Developing Country: A Baseline Survey." *BMC Health Services Research* Vol. 11, no. 1 (November 2011). Accessed 23 June 2018. www.ncbi.nlm.nih.gov/pmc/articles/PMC3225320/.

This research paper looks at surveys conducted on wholesalers in the pharmaceutical industry scattered throughout the world and their knowledge on distribution issues related to counterfeit medicines and how to handle such cases.

"Substandard and Falsified Medical Products." *World Health Organization.* Last modified 31 January 2018. www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products.

This webpage from the World Health Organization helps to define some of the terms and key facts in the issue of fraudulent medicine, as well as provide information on ways to identify illegal and unregulated medical products.

Treacy, Karima Pat & Noel Watson-Doig. "What is Parallel Trade and How Does it Affect Pharma?" *KNect365, Informa.* Last modified 1 December 2016. knect365.com/complaw-blog/article/073ed81f-0d17-4c0e-a819-38ff60332dec/what-is-parallel-trade-and-how-does-it-affect-pharma.

This webpage explains the concept of parallel trade in the pharmaceutical system and the overall effect it brings to security of medicines and the supply chain.

Topic B

Anderson, Janna, and Lee Rainie. "The Future of Truth and Misinformation Online." Pew Research Center: Internet, Science & Tech. October 19, 2017. Accessed June 26, 2018. www.pewinternet.org/2017/10/19/the-future-of-truth-and-misin-

formation-online/.
Another statistical breakdown of the future of misinformation in media and how it will manifest itself in the coming elections across the world.

Cook, Steven A. "Turkey's Elections: Partially Free, Fair, and Fake." Council on Foreign Relations. June 25, 2018. Accessed June 26, 2018. www.cfr.org/blog/turkeys-elections-partially-free-fair-and-fake.
Another case study on how Turkey's fake elections leaves them open to cyber issues in the future and the present.

DeNardis, Laura, Gordon Goldstein, and David A. Gross. "The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance." Tech and Policy Initiative at Columbia School of International Affairs, November 2016. sipa.columbia.edu/sites/default/files/The%20Rising%20Geopolitics_2016.pdf
Highlights the importance of geopolitics when determining domain in an internet dispute.

Max Abrahams, William Rose, and Rysia Murphy, "Correspondence: Does Terrorism Ever Work? The 2004 Madrid Train Bombings," Belfer Center for Science and International Affairs, 2007, accessed July 18, 2018, www.belfercenter.org/publication/correspondence-does-terrorism-ever-work-2004-madrid-train-bombings.
Outlines the ideals of terrorisms and its corresponding results.

"More State Election Databases Hacked than Previously Thought." CBS News. September 28, 2016. Accessed June 25, 2018. www.cbsnews.com/news/more-state-election-databases-hacked-than-previously-thought/.
Highlights the importance of protecting voter registration and yet another subtopic within a subtopic to protect internal voting mechanisms.

Silverman, Craig. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook." BuzzFeed. Accessed June 25, 2018. www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.ecb9ZWLG5#.cjr0oblxp.
Outlines how prevalent fake news was in the recent election.

Velde, Jacqueline Van De. "The Law of Cyber Interference in Elections." SSRN Electronic Journal, 2017. doi:10.2139/ssrn.3043828. law.yale.edu/system/files/area/center/global/document/van_de_velde_cyber_interference_in_elections_06.14.2017.pdf
Offers legal insight on how interference with elections coincides with already put in place precedent.

Works Cited

Committee History and Simulation

A/RES/46/152. "Creation of an Effective United Nations Crime Prevention and Criminal Justice Programme." 18 December 1991.

In this resolution, the General Assembly recommended the creation of a comprehensive criminal justice Programme and established a functional commission of the Economic and Social Council to achieve this aim. This resolution also includes a statement of principles elaborated by the international community in this matter.

A/CONF.222/INF/1. "Thirteenth United Nations Congress on Crime Prevention and Criminal Justice […] Information for Participants." 12 January 2015.

This document was presented for the participants of the Thirteenth –and most recent – Congress on Crime Prevention in Doha, Qatar. Thus, it contains the most recent preoccupations the international community that CCPCJ must address.

DPI/1642/CRM. "The United Nations Crime Prevention and Criminal Justice Programme." April 1995. Accessed 15 May 2018, http://www.unodc.org/documents/congress//Previous_Congresses/9th_Congress_1995/031_Backgrounder_United_Nations_Crime_Prevention_and_Criminal_Justice_Programme.pdf.

This document was elaborated for the Ninth Congress on the prevention of crime, and it illustrates the work CCPCJ has done in the past.

E/1992/22. "Implementation of General Assembly Resolution 46/152." 30 July 1992.

With this resolution, the Economic and Social Council states the importance to develop and effective strategy on responsible crime prevention and tasks the CCPCJ to fulfill this goal. It also includes relevant definitions of what "crime prevention" and "responsible crime prevention" means.

E/CN.15/2015/19. "Report on the Twenty-fourth Session." 7 May 2015.

This report illustrates the issues addressed at the most recent meeting of the CCPCJ. At the last session, CCPCJ recommended resolution pertaining to trafficking of persons, the quality of criminal statistics.

"UNODC: Commissions." *United Nations Office on Drugs and Crime.* Last Modified 30 June 2010. http://www.unodc.org/unodc/en/commissions/index.html?ref=menuside.

This website shows CCPCJs role as the governing body of the United Nations Office on Drugs and Crime and importance in administrative affairs.

Topic A

UN Sources

"Mandate and Functions." *United Nations Office on Drugs and Crime.* www.unodc.org/unodc/en/commissions/CCPCJ/CCPCJ_Mandate-Functions.html.

This source elaborates on the role CCPCJ has in tackling bad medicine and explains the history of such action.

"Division for Sustainable Development Goals." *United Nations Department of Economic and Social Affairs.* sustainabledevelopment.un.org/about.

This source explains how the Sustainable Development Goals compliment the work of CCPCJ in fighting against the harmful medicine trade.

"Growing Threat from Counterfeit Medicines." *World Health Organization.* Last modified April 2010. www.who.int/bulletin/
      volumes/88/4/10-020410/en/.
This webpage from the World Health Organization details certain crucial events that led to the recognition of fraudulent medicine as a major international issue, as well as illuminating statistics that aid in the introduction of the topic.

"Sustainable Development Goal Three," *United Nations Department of Economic and Social Affairs,* sustainabledevelopment.un.org/
      sdg3.
This webpage from the United Nations Department of Economic and Social Affairs defines and outlines the purpose behind the third sustainable development goal.

"Sustainable Development Goal Seventeen," *United Nations Department of Economic and Social Affairs*, sustainabledevelopment.
      un.org/sdg17.
This webpage from the United Nations Department of Economic and Social Affairs defines and outlines the purpose behind the seventeen sustainable development goal.

"Trafficking in Fraudulent Medicine." United Nations Office on Drugs and Crime. www.unodc.org/unodc/en/fraudulentmedi-
      cines/introduction.html.
This webpage from UNODC examines CCPCJ's role in tackling the issues around the trafficking of fake medicine.

"WHO Global Surveillance and Monitoring System." World Health Organization. www.who.int/medicines/regulation/ssffc/
      surveillance/en/.
This webpage from the World Health Organization explains the body's regulation and monitoring system concerning the issue of falsified and substandard medicines.

Non-UN Sources

"25 Countries with Limited Access to Health Care." Accessed 29 May 2018. www.worldatlas.com/articles/the-countries-with-
      the-fewest-doctors-in-the-world.html.
This webpage streamlines a list of details and information on countries with limited access to health care.

"A Glimpse into the Dark World of Organized Cybercrime." *IBM Journal.* www.ibmjournal.com/security/dark-world-organized-
      cybercrime.
This source details the intricacies of the internet's role in organized crime.

"Against Falsified Medicine, the Best Medicine," *Prevention of and Fight against Crime Programme of the European Union,* www.fake-
      share.eu/sites/default/files/downloads/Vademecum.pdf.
This resource explains the history and purpose of the European Union's Fakeshare Project and what it has done to combat the issue of fake medicine in the region.

Alfadl, Abubakr A et al. "The Impact of Demographic Characteristics on Vulnerability of Consumers to Counterfeit Drugs in a Developing Country." *Journal of Socialomics* Vol. 2, no. 102 (June 2013). Accessed 23 June 2018. www.omicsonline.org/open-access/the-impact-of-demographic-characteristics-on-vulnerability-of-consumers-to-counterfeit-drugs-in-a-developing-country-2167-0358.1000102.php?aid=21180.

This journal article looks into characteristics that insure consumers from certain demographics are more vulnerable to the negative and harmful impacts of fraudulent medicine.

"Background on the Goals." *United Nations Development Programme.* www.undp.org/content/undp/en/home/sustainable-development-goals/background.html.

Provides a history of how the Sustainable Development Goals were developed

"Bad Medicine." *The Economist*, 13 October 2012. Accessed 23 June 2018. www.economist.com/international/2012/10/13/bad-medicine.

This source from the Economist examines the role of fake pharmaceuticals in the public health of the global community.

Bate, Roger. "The Deadly World of Fake Medicine." *CNN*, 17 July 2012. Accessed 20 June 2018. www.cnn.com/2012/07/17/health/living-well/falsified-medicine-bate/index.html.

This article about the dangers of fraudulent and counterfeit medicine explores some of the history behind terrorist groups and their link to pharmaceutical crimes.

Behner, Peter, Marie-Lyn Hecht & Fabian Wahl. "Fighting Counterfeit Pharmaceuticals: New Defenses for an Underestimated—and Growing—Menace." *Strategy&*. Last modified 29 June 2017. www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals.

This webpage on pharmaceutical supply chain strategies explains new generation anti-counterfeiting and supply chain management techniques for reducing fraudulent medicines and aiding in their recall.

Bichell, Rae Ellen. "Fake Drugs Are A Major Global Problem, WHO Reports." *National Public Radio,* 2017 November 29. Accessed 29 May 2018. www.npr.org/sections/goatsandsoda/2017/11/29/567229552/bad-drugs-are-a-major-global-problem-who-reports.

This piece from NPR highlights many of the crucial points and topics in the every-burgeoning fake medicine industry.

Cabinet Seeks to Crack Down on Fake Drugs," Swiss Broadcasting Corporation, last modified 22 February 2017, www.swissinfo.ch/eng/health-hazard_cabinet-seeks-to-crack-down-on-fake-drugs/42979536.

This source details the Swiss government's attempt to crack down on the growing presence of fake pharmaceuticals in the country.

Campbell, David. "Fake Medications, Real Solutions" *Pharmaceutical Executive* Vol. 35, no. 5 (May 2015). Accessed 23 June 2018. www.pharmexec.com/fake-medications-real-solutions.

This source details possible solutions and methods for pharmaceutical companies to address the growing threat of fraudulent and counterfeit medication.

"Canadian Drug Firm Admits Selling Counterfeit and Misbranded Prescription Drugs Throughout the United States." *United States Food and Drug Administration.* Last modified 13 April 2018. www.fda.gov/ICECI/CriminalInvestigations/

ucm605139.htm.

This press release from the United States Food and Drug Administration examines the history behind the legal case of the Canadian drug firm in question.

Clark, Fiona. "Rise in Online Pharmacies Sees Counterfeit Drugs Go Global." *The Lancet.* Vol. 386, no. 10001 (October 2015): 1327-1328. Accessed 23 June 2018. www.thelancet.com/journals/lancet/article/PIIS0140-6736(15)00394-3/fulltext?code=lancet-site

This report examines the elements behind the increasing threat of online pharmacies within the danger of counterfeit drugs.

Committee on Understanding the Global Public Health Implications of Substandard, Falsified, and Counterfeit Medical Products. *Countering the Problem of Falsified and Substandard Drugs.* Washington, DC: National Academies Press, 2013. Accessed 20 May 2013. www.ncbi.nlm.nih.gov/books/NBK202523/.

This source helps to provide an overview of drug distribution methods and weaknesses in the pharmaceutical supply chain.

"Counterfeit Drug War in Liberia." *IRIN News.* Last modified 29 January 2017. www.irinnews.org/report/99551/counterfeit-drug-war-liberia.

This source examined the topic of fake medicine in Liberia and how it has affected the population there.

Di Giorgio, Domenico and Marta Gramazio. "Pharmaceutical Crime (Fakeshare)." *Italian Medicines Agency*, (2017). Accessed 20 May 2018. www.researchgate.net/publication/317184540_Pharmaceutical_Crime_Fakeshare

A summary of the general features and recent developments of a European Union project looking to combat pharmaceutical crime.

"Fakeshare and Fakeshare II: The Projects." *Prevention of and Fight against Crime Programme of the European Union.* www.fakeshare.eu/en/project.

A description of the Fakeshare partnership in the European Union and its revival.

Finlay, D. Brian. "Counterfeit Drugs and National Security." *The Stimson Center*, www.stimson.org/sites/default/files/file-attachments/Full_-_Counterfeit_Drugs_and_National_Security_1.pdf

This document examines the important relationship between counterfeit medications and national security through the deadly implications of bioterrorism through pharmaceutical falsification.

G. Jackson. "Faking It: The Dangers of Counterfeit Medicine on the Internet." *International Journal of Clinical Practice* Vol. 63, no. 2 (January 2009): 181-183.

This journal article provides useful insight on the dangers of the rise of the internet's involvement in the ever-growing field of illegal counterfeit medicines.

Ganor, Boaz. "The Infiltration of Terrorist Organizations into the Pharmaceutical Industry: Hezbollah as a Case Study." *Studies in Conflict and Terrorism* Vol. 36, no. 9 (August 2013): 699-712.

This research case study looks at the terrorist group Hezbollah and details how such groups became linked to pharmaceutical crimes.

"How to Buy Medicines Safely from an Online Pharmacy." *United States Food and Drug Administration.* Last modified 1 January 2018. www.fda.gov/ForConsumers/ConsumerUpdates/ucm048396.htm.

This webpage from the United States Food and Drug Administration provides useful information and insight on key details that distinguish legitimate online pharmacies from illegal ones.

"International Conference Fakeshare: Conclusion and Results." *Agenzia Italiana del Farmaco (AIFA).* Last modified 24 April 2015. www.aifa.gov.it/en/content/international-conference-fakeshare-conclusions-and-results.
This webpage from the Italian medicines agency reveals the conclusion and results of European Union Fakeshare project.

Isles, Mike. "What's in a Word? Falsified/Counterfeit/Fake Medicines - The Definitions Debate." *Medicine Access @ Point of Care* Vol. 1, no. 1 (April 2017). Accessed 4 April 2017. journals.sagepub.com/doi/10.5301/maapoc.0000008.
This research paper delves into the nomenclature surrounding the topic of fraudulent medicine as well as many elements within the European Union pharmaceutical crime Fakeshare project.

Johnson, Carolyn Y. "America is a World Leader in Healthcare Inequality." *Washington Post,* 5 June 2017. Accessed 12 August 2018. www.washingtonpost.com/news/wonk/wp/2017/06/05/america-is-a-world-leader-in-health-inequality/?utm_term=.08e4ce715856.
This news article details the difficulty in the United States for healthcare equality and lessened wealth disparities in relation to citizens' overall long-term quality of life.

Lancaster, Ian. "Sophisticated Replication Techniques Have Made Counterfeiting and Fraud a Serious Threat to the Pharmaceutical Industry." *Pharmaceutical Technology* 32, no. 4 (April 2008). www.pharmtech.com/trends-holograms-and-anticounterfeiting.
Article that discusses some of the innovative techniques that illicit organizations are using to reproduce the labels of pharmaceuticals

"Large Quantities of Counterfeit Medicines Distributed from Sweden," *European Communities Trade Mark Association,* last modified 30 May 2011, www.ecta.org/uploads/press-doc/ecta_press_release_30_may_2011.pdf.
This source details the discovery of Sweden as Europe's primary hub of distribution for counterfeit medication in the region.

"LegitScript." *Prevention of and Fight against Crime Programme of the European Union.* www.fakeshare.eu/en/partners/legitscript.
This source explains the purpose and workings of the Legitscript program and its attempts to combat the sale of fake medicine online.

Lomb, Rüdiger. "Securing the Global Pharmaceutical Supply Chain Against the Threat of Counterfeit Drugs." World Courier. Accessed 20 May 2018. www.samedanltd.com/uploads/pdf/white_paper/77c80fbbe302eb215115d72b1c3e2812.pdf.
This source details some methods and implemented strategies created in order to combat the sale of counterfeit pharmaceuticals.

Lisaius, Ken. "Major Canadian Online Pharmacy Caught Red Handed Selling Fake Drugs to the U.S." *Biotechnology Innovation Organization.* Last modified 19 December 2017. www.biotech-now.org/health/2017/12/icymi-major-canadian-online-pharmacy-caught-red-handed-selling-fake-drugs-to-the-u-s.
This webpage from a biotechnology organization details the legal onslaught surrounding a counterfeit drug scheme in a legal Canadian online pharmacy.

Mackey, Tim, Bryan Liang, Peter York, Thomas Kubic. "Counterfeit Drug Penetration into Global Legitimate Medicine Supply Chains: A Global Assessment." *American Journal of Tropical Medicine and Hygiene* 92, no. 6 (2015): 59-67. Accessed 20 May

2018. www.ncbi.nlm.nih.gov/pmc/articles/PMC4455087/

This source details information about the illegal distribution of counterfeit medications that indicates particular country characteristics involved in the problem.

Mangan, Dan. "Canada Pharmacy Charged in $78M Drug Export Scheme." *CNBC*, 19 August 2015. Accessed 23 June 2018.
www.cnbc.com/2015/08/19/canada-pharmacy-charged-in-78m-drug-export-scheme.html.

This article examines the details behind the events of the counterfeit drug export scheme taking place through a Canadian online pharmacy.

"Medsafe Highlights Dangers of Online Medicines," *New Zealand Ministry of Health,* last modified 16 June 2016, www.health.
govt.nz/news-media/media-releases/medsafe-highlights-dangers-online-medicines.

This source from the New Zealand Ministry of Health reveals actions the country recently took alongside INTERPOL to combat the threat of fake medicine.

Medsafe Pharmacovigilance Team, "Counterfeit Medicines - Don't Fake Concern, *New Zealand Ministry of Health,* last modified
June 2005, www.medsafe.govt.nz/profs/PUarticles/counterfeit.htm.

This source from the New Zealand Ministry of Health written back in 2005 shows the country's awareness and concern on the issue of fake medicine at a time when even the World Health Organization hadn't collected a large quantity of data on the subject.

Morgan, Oliver. "Parallel Trade in Drugs Puts EU Patients at Risk." *The Guardian*, 28 June 2008. Accessed 28 May 2018. www.
theguardian.com/business/2008/jun/29/pharmaceuticals.

This article looks at the pharmaceutical supply chain concept of parallel trade and how it affects those living in the European Union.

Nagpal, Tanvi. "Back on the Rise, Malaria Rates Call for Global Spending Surge." *Axios*, 7 April 2018. Accessed 10 July
2018. www.axios.com/back-on-the-rise-malaria-rates-call-for-global-spending-surge-73fc1577-19ba-4630-9ca0-8ba-
5dea96002.html.

This source details the recent rise of malaria rates and the resulting need for global spending to resolve the issue.

"Online Pharmacies - A Brief History." *CareFirst Specialty Pharmacy.* www.cfspharmacy.pharmacy/blog/post/online-pharmacies-
a-brief-history.

This source looks through the history behind the rise of online pharmacies.

Ossola, Alexandra. "The Fake Drug Industry is Exploding, and We Can't Do Anything About It." *Newsweek,* 17 September 2015.
Accessed 29 July 2018. www.newsweek.com/2015/09/25/fake-drug-industry-exploding-and-we-cant-do-anything-
about-it-373088.html.

This piece details statistics and resulting tragedies from the world crisis of fake medicine.

"Pharmaceutical Crime." *INTERPOL.* Accessed 20 May 2018. www.interpol.int/Crime-areas/Pharmaceutical-crime/Pharma-
ceutical-crime.

This webpage from Interpol provides a clear, easy to follow outline of what pharmaceutical crime is as well as its connections to organized crime, making it a beneficial source for those just being introduced to the topic.

"Pharmaceutical Industry Initiative to Combat Crime." *INTERPOL*. www.interpol.int/Crime-areas/Pharmaceutical-crime/
    Pharmaceutical-Industry-Initiative-to-Combat-Crime.
*This webpage from Interpol details information on a partnership between itself pharmaceutical companies in order to combat the threat of fraudulent
medicine.*

"Ranking the Top Healthcare Systems by Country." *International Travel Insurance Group*. Accessed 29 May 2018. www.internation-
    alinsurance.com/news/ranking-top-eleven-healthcare-systems-country.php.
This source looks at the which countries in the word contain the best and most efficient health care systems.

Redpath, Shirley. "Trade in Illegal Medicine Hits Pharmaceutical Sector." *World Finance*. Last modified 20 April 2012. Accessed
    20 May 2018. www.worldfinance.com/special-reports/trade-in-illegal-medicine-hits-pharmaceutical-sector.
This article details alarming information about the organized crime taking place in the pharmaceutical sector.

Seiter, Andreas. "Health and Economic Consequences of Counterfeit Drugs." *Clinical Pharmacology and Therapeutics,* 85 (2009): 576-
    578. www.researchgate.net/publication/24436694_Health_and_Economic_Consequences_of_Counterfeit_Drugs.
This source provides strong information on the health and economic consequences for individuals engaged in purchasing counterfeit medicines.

Seng Lee, Kah et al. "Combating Sale of Counterfeit and Falsified Medicines Online: A Losing Battle." *Frontiers in Pharmacology*
    8, no. 268 (2017). www.ncbi.nlm.nih.gov/pmc/articles/PMC5432535/.
*This paper examines the effects of the internet on the growth of pharmaceutical crime and counterfeit medicine along with multiple case studies dem-
onstrating the result.*

Shah, Ruchir Y, Prajesh N. Prajapati & Y. K. Agrawal. "Anticounterfeit Packaging Technologies." *Journal of Advanced Pharmaceuti-
    cal Technology & Research* Vol. 1, no. 4 (October 2010): 368-373. Accessed 23 June 2018. www.ncbi.nlm.nih.gov/pmc/
    articles/PMC3255398/.
*This journal article discloses crucial information on packing, authentication, and tamper-proof technologies aimed at reducing the distribution of
counterfeit medicines.*

Siemaszka, Corky. "Fentanyl Figures in Most Fatal Drug Overdoses in U.S., Researchers Say." *NBC News*, 1 May 2018. Accessed
    10 July 2018. www.nbcnews.com/storyline/americas-heroin-epidemic/fentanyl-figures-most-fatal-drug-overdoses-u-s-
    researchers-say-n870481.
*This news piece details the damaging, harmful effects of fentanyl in the already dangerous public health crisis of the opioid epidemic in the United
States.*

"The Economic Impact of Counterfeiting and Piracy." Paris, France: OECD Publications, 2008. Accessed 20 May 2008. apps.
    who.int/medicinedocs/documents/s19845en/s19845en.pdf
This paper examines the damaging effect of counterfeit medicine and pharmaceutical crimes on the intellectual property rights.

Thomas, Jackson et al. "Are Fake Drugs the Reason Malaria Sickens Millions a Year." *Smithsonian Magazine*. Last modified 24 April
    2018. www.smithsonianmag.com/science-nature/fake-drugs-are-one-reason-malaria-still-kills-so-many-180968882/.
This source looks into the possible connections between fake medicine and the ever-present concern of rising malaria rates.

Toscano, Paul. "The Dangerous World of Counterfeit Prescriptions." *CNBC*, 4 October 2011. Accessed 22 June 2018. www.cnbc.com/id/44759526.

This report details some of the possible negative health outcomes for consumers involved in purchasing of fraudulent medicine.

Waters, Kelly. "Decoding Serialization Regulations." *Pharmaceutical Technology* Vol. 41, no. 6 (June 2017): 64-65. Accessed 23 June 2018. www.pharmtech.com/decoding-serialization-regulations-0.

This article from a pharmaceutical technology journal compares recent changes in serialization regulations on medicine between the United States and the European Union.

Wernli, Miri Halperin and Boaz Ganor. "Pharmaceuticals: Target for Terrorism." *Actelion Pharmaceuticals Ltd,* Accessed 20 May 2018. www.ict.org.il/UserFiles/Pharmaceuticals%20Target%20For%20terrorism.pdf

This document explains the relationship between the sale of counterfeit medications and the connection and financial benefits to terrorist groups, as well as possible methods to remedy the issues present.

Whalen, Jeanne. "Guilty Pleas in Canada Drugs Counterfeit-Medicines Cases." *The Wall Street Journal*, 15 December 2017. Accessed 23 June 2018. www.wsj.com/articles/guilty-pleas-in-canada-drugs-counterfeit-medicines-cases-1513383756?mg=prod/accounts-wsj.

This news article explores the guilty verdict on Canadian online pharmacy counterfeit medicine scandal and its effect on the United States fraudulent medicine market.

"What is Parallel Distribution?" *European Association of Euro-Pharmaceutical Companies.* www.eaepc.org/about-parallel-distribution/what-is-parallel-distribution.

This source explains how parallel distribution functions.

Wyld, David. "Genuine Medicine? Why Safeguarding the Pharmaceutical Supply Chain from Counterfeit Drugs with RFID is Vital for Protecting Public Health and the Health of the Pharmaceutical Industry." *Competitive Review: An International Business Journal* 18, no. 3 (2008). www.emeraldgrouppublishing.com/learning/management_thinking/articles/pdf/medicine.pdf.

The source examines the impact of the global epidemic of counterfeit drug sales on pharmaceutical companies.

Yadav, Sankalp and Gautam Rawal. "Counterfeit Drugs: Problem of Developing and Developed Countries." *International Journal of Pharmaceutical Chemistry and Analysis* 2, (2015): 46-50. Accessed 20 May 2018. www.researchgate.net/publication/277301823_Counterfeit_drugs_problem_of_developing_and_developed_countries.

This source examines how development status and access to healthcare affects the types of drugs that are counterfeited and trafficked, with developed countries involved primarily in illegal lifestyle medicines.

Zezima, Katie. "Counterfeit Opioid Pills are Tricking Users — Sometimes with Lethal Results." *The Washington Post,* 19 November 2017. Accessed 10 July 2018. www.washingtonpost.com/national/counterfeit-opioid-pills-are-tricking-users--sometimes-with-lethal-results/2017/11/19/d34edb14-be4b-11e7-8444-a0d4f04b89eb_story.html?noredirect=on&utm_term=.83b35c799e21.

This news report details the dangerous result of two lethal public health crises, fake medicine and the opioid epidemic, intersecting with one another in

the United States.

Topic B

UN Sources

"A New Sustainable Development Agenda," United Nations Development Programme, accessed 13 July 2018, www.undp.org/
         content/gcp/en/home/2030agenda/.
Outlines the goal of the Sustainable Agenda set forth in 2030.

"CCPCJ Mandate and Functions." *United Nations Office on Drugs and Crime.* Accessed June 25, 2018. www.unodc.org/unodc/en/
         commissions/CCPCJ/CCPCJ_Mandate-Functions.html.
Official mandate and scope for CCPCJ that gives a clear and concise blurb on how the committee should be run and what it is responsible for.

"Chapter I." United Nations. Accessed July 15, 2018. www.un.org/en/sections/un-charter/chapter-i/index.html.
This source recites the UN Charter.

"Global Programme on cybercrime." UNODC. Accessed 26 June 2018. www.unodc.org/unodc/en/cybercrime/global-pro-
         gramme-cybercrime.html.
*Great overall breakdown of the issue as it explains the overall mandate, types of cybercrime, and issues related such as geographic scope. This will give
a great starting point, so we can best write a solid introduction.*

"Goal 16.:. Sustainable Development Knowledge Platform." United Nations. Accessed July 18, 2018. sustainabledevelopment.
         un.org/sdg16.
Directly highlights the importance of SDG 16 in the agenda.

"Strengthening Capacity to Counter Terrorism in Nigeria." *United Nations Office on Drugs and Crime.* Accessed June 26, 2018. www.
         unodc.org/unodc/en/commissions/CCPCJ/index.html.
Gives complete overview of CCPCJ activities to help better guide delegates in its future goals.

Non-UN Sources

Ben-Meir, Elad. "Cyberwar, US, Russia and the Non-State Actors: Frenemies with Benefits?" Our Favorite Examples of How
         CEOs Respond to Cyber Breaches. February 27, 2017. Accessed May 29, 2018. blog.cyberint.com/cyberwar-us-russia-
         and-the-non-state-actors-frenemies-with-benefits.
*Article that does really well to outline the most prominent case study in this topic, the 2016 US elections and the subsequent Russian hacking. But
more importantly it talks about how the U.S. contracted a non-state actor, a Ukrainian hacking group to hack Kremlin emails. Would give delegates
an opportunity to debate something that isn't very binary thus allowing for a need for creative and innovative solutions.*

Buchanan, Ben, and Michael Sulmeyer. "Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity." Harvard
         Kennedy School, October 2016. Accessed June 25, 2018. www.belfercenter.org/sites/default/files/files/publication/
         hacking-chads.pdf.

Addresses the hackability of voting machines and does an in-depth international analysis of voting infrastructure.

Calabresi, Massimo. "Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say." *Time.* 22 June 2017. Accessed 30 September 2018. time.com/4828306/russian-hacking-election-widespread-private-data/.
The events of the 2016 Russian hack into the American Presidential election are the backdrop for much information on this topic. This source reports on such events.

Chan, Sewell. "Fearful of Hacking, Dutch Will Count Ballots by Hand." The New York Times. December 22, 2017. Accessed June 26, 2018. www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html.
Shows an example of what the Dutch did when fearful of hacking, also shows a possibility of a non-sustainable solution. Delegates will have to decipher the longevity and simultaneous stability of these solutions.

"Cybersecurity and National Elections." Internet Society. September 13, 2017. Accessed June 25, 2018. www.internetsociety.org/blog/2017/03/cybersecurity-and-national-elections/.
Outlines the domain and elections issue when new and innovative solutions arise.

"Cybersecurity in the European Digital Single Market." *European Commission: High Level Group of Scientific Advisors.* No. 2 (2017). Accessed June 25, 2018. ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf.
Infographic outlining the logistical overview of a public private partnership to stop cybercrime.

"Declaration on Free and Fair Elections." *Women in Parliaments: World Classification.* Accessed June 26, 2018. archive.ipu.org/cnl-e/154-free.htm.
Important declaration on fair and free elections across the globe.

Eichernssehr, Kristen E. "The Cyber-Law of Nations." Georgetown Law, 317th ser., 103, no. 1 (2015): 317-80. 2015. Accessed May 23, 2018. www.law.georgetown.edu/cle/materials/CybersecurityLawInstitute/2015/Sessions/09/Eichensehr - The Cyber-Law of Nations.pdf.
Outlines the issue of the cyberworld as it progressed through time and who holds what domain in regard to governance and sovereignty. The way this would be framed in an election sense is regulation. A very contentious topic within the committee is who is responsible to regulate this almost infinite domain, using this subtopic as a starting point would provide delegates with a great backdrop as to the problem of the internet and allow them to debate how and where to regulate it going forward.

"Electoral Violence Prevention: What Works?" Taylor & Francis. Accessed June 26, 2018. www.tandfonline.com/doi/full/10.1080/13510347.2017.1365841.
Article that outlines how NSA's can be used to stop electoral violence in troubled regions.

Elewa, Aboubakr Ebrahim et al. "Challenges of Electronic Voting - A Survey." *Advances in Computer Science: An International Journal.* [S.l.], p. 98-108. ISSN 2322-5157. 2015 November. Accessed 1 October 2018. www.acsij.org/acsij/article/view/379.
A thorough explanation of the structure and function of electronic voting is presented in this source. The difficulties of such technologies are also examined in detail.

Fung, Brian. "FCC net neutrality process 'corrupted' by fake comments and vanishing consumer complaints, officials say."
The Washington Post. 24 November 2017. Accessed 30 September 2018. www.washingtonpost.com/news/the-switch/
wp/2017/11/24/fcc-net-neutrality-process-corrupted-by-fake-comments-and-vanishing-consumer-complaints-offi-
cials-say/?utm_term=.a7bc897ae63a.
*An example providing insight into how impersonation through cybercrime can influence policy, this source highlights the importance of honest online
forums and identity fraud protection.*

"GovData360: Free and Fair Elections." GovData360 - Governance Data. Accessed May 29, 2018. govdata360.world-
bank.org/indicators/h7a147898?country=BRA&indicator=28751&countries=MEX,VEN,ARG&viz=bar_
chart&years=2016#table-link.
Shows how a prominent country in this bloc is placed its emphasis on an environment needed to foster fair and free elections.

Hautala, Laura. "Voter fraud and dead people: How tech sets things right." *CNET.* 19 October 2016. Accessed 1 October 2018.
www.cnet.com/news/how-tech-eases-trump-election-rigging-voter-fraud-concerns/.
This source explains technology failures which could lead to compromised elections and incorrect vote totals.

Hennessey, Susan. "Cybersecurity of Voting Machines." Brookings. December 04, 2017. Accessed June 25, 2018. www.brook-
ings.edu/testimonies/cybersecurity-of-voting-machines/
Outlines the actual issues with infrastructure and how to solve them when infrastructure is concerned.

"Human Development Report 2015: Work for Human Development." *United Nations Development Programme.* Accessed 30 Sep-
tember 2018. hdr.undp.org/sites/default/files/2015_human_development_report.pdf.
*This source is useful in determining the qualities of the countries which compose each bloc. This index indicates circumstances of each bloc, which allows
for extrapolation regarding approaches to discussing cyberattacks.*

"Internet Voting." *National Democratic Institute.*17 December 2013. Accessed 26 June 2018. www.ndi.org/e-voting-guide/internet-
voting.
Outlines all important facets online voting and its susceptibility to change in upcoming elections.

"Internet Voting in Estonia." National Democratic Institute. November 25, 2013. Accessed June 26, 2018. www.ndi.org/e-
voting-guide/examples/internet-voting-in-estonia.
*Highlights an important example of online being used and being successful all while shining light on the important issue of relative infrastructure as
well.*

Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New
York Times. December 13, 2016. Accessed June 26, 2018. www.nytimes.com/2016/12/13/us/politics/russia-hack-
election-dnc.html.
Timeline of the DNC hacking and the U.S. immediate response.

Maluk, Holly, Myrna Perez, and Lucy Zhou. "Voter Registration in a Digital Age: 2015 Update." Brennan Center for Justice at
New York School of Law. 2015. Accessed June 26, 2018. www.scribd.com/document/286672575/Voter-Registration-

in-a-Digital-Age-2015-Update.

Outlines the importance of online voter registration and how it plays a very overlooked role in addressing the legitimacy of elections as hackers use this data to base their target audience off of.

"Measuring the Information Society Report 2016: Key Findings," *International Telecommunication Union,* accessed 30 September 2018, www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-KeyFindings.pdf.

This source is instrumental in determining the divisions between countries and how they may fall into blocs based on level of technological development.

Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Nicaragua), 1986 I.C.J. 14, ¶ 205 (June 27).

Summary of important precedent of sovereignty and territorial disputes.

"Online Voting." *Parliamentary Office of Science and Technology.* May 2001. Accessed 30 September 2018. www.parliament.uk/documents/post/pn155.pdf.

This source is a detailed report on voting technologies. It provides a detailed explanation of the components of voting technologies, which provides the background for better overall understanding.

Plinkington, Ed. "Hanging chad redux? US heading for 2000-style election catastrophe, report finds." *The Guardian.* 15 September 2015. Accessed 30 September 2018. www.theguardian.com/us-news/2015/sep/15/2016-election-old-voting-machines-hanging-chad.

This source provides the historical background of the events from the 2000 American presidential election. The events of the past are compared to the current situation to gauge election integrity in the United States.

"Recommendation of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-voting." Search.coe.int. Accessed May 29, 2018. search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dbef8.

Recommendation that outlines a recommendation by the Council of Europe to make elections completely electronic. This would be a very contentious point of debate between the blocs that is also extremely interesting!

Reiter, Svetlana. "What the Arrest of the Russian Intel Top Cyber-Crime Expert Has to Do with American Elections." The Bell - Eng. January 30, 2018. Accessed May 29, 2018. thebell.io/en/arrest-russian-intel-top-cyber-crime-expert-american-elections/.

Interesting piece how a very prominent country in this bloc deals with the issue of cybercrime, and how it is dealing with it today.

Rodriguez, Andrea. "Ahead of Mexico's presidential election, fears and warnings over possible fraud." Chicago Tribune. 29 June 2018. Accessed 6 October 2018. www.chicagotribune.com/news/nationworld/ct-mexico-election-fraud-warning-20180629-story.html.

This piece elaborates on election security in Mexico. This source is valuable since it is from only a few months ago and lends insight into recent developments and the current situation.

Rodriguez, Juan. "The Benefits and Disadvantages of P3." The Balance Small Business. March 28, 2018. Accessed July 19, 2018. www.thebalancesmb.com/public-private-partnership-pros-and-cons-844713.

This is a source defining PPPs.

Serhan, Yasmeen. "Italy Scrambles to Fight Misinformation Ahead of Its Elections." The Atlantic. February 24, 2018. Accessed
        29 May 2018. www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/.
Excellent article that outlines Europe's troubles with misinformation in elections that has spread across the world with the rise of populist and nationalist groups and political movements.

Shackelford, Scott, Bruce Schneier, Michael Sulmeyer, Anne Boustead, Ben Buchanan, Amanda N. Craig Deckard, Trey Herr
        & Jessica Malekos Smith, "Making Democracy Harder to Hack," 50 U. Mich. J. L. Reform 629 (2017). repository.law.
        umich.edu/mjlr/vol50/iss3/3,
Excellent article outlining the need and importance for strong internal voting systems and offers a comparative lens of introspection through the comparison of numerous states in different regions such as South Africa, Estonia, and Germany.

Stark, Harold. "How Russia 'Hacked' Us In 2016 [And What We Did Wrong]." Forbes. April 29, 2017. Accessed June 26, 2018.
        www.forbes.com/sites/haroldstark/2017/01/24/how-russia-hacked-the-election/#2c5030684a9f.
Concrete mistakes and steps taken that led to the Russian hacking and how it can be avoided for all states in the future.

The United States District Court for the District of Columbia. Case 1:18-cr-00215-ABJ. 13 July 2018. Accessed 30 September
        2018. www.justice.gov/file/1080281/download.
*This is the indictment of the Russians accused of interfering with the 2016 Presidential election in the United States. This case study is valuable
because it explains the real events of cybercrime without any hypotheticals.*

Waldrop, M. Mitchell. "News Feature: The Genuine Problem of Fake News." PNAS. November 28, 2017. Accessed June 25,
        2018. www.pnas.org/content/114/48/12631.
Offers a solution and real mathematical analysis of the fake news dilemma.

Ward, Alex. "Russia Hacked Voting Systems in 39 States before the 2016 Presidential Election." Vox. June 13, 2017. Accessed
        June 26, 2018. www.vox.com/world/2017/6/13/15791744/russia-election-39-states-hack-putin-trump-sessions
A basic overview of how the Russian hacking of the U.S. Presidential election came to be and how wide spread it was.

Willis." Willis - Global Risk Advisor, Insurance and Reinsurance Broker. Accessed July 19, 2018. www.willis.com/Client_Solu-
        tions/Services/PPP-PFI_(Public_Private_Partnerships_and_Private_Finance_Initiative)/.
Describes and gives examples of the pros and cons of PPP's

"Universal Declaration of Human Rights (Article 21)." Minority Rights Group. Accessed June 26, 2018. minorityrights.org/law-
        and-legal-cases/universal-declaration-of-human-rights-article-21/.
Article 21 of the UNHDR states that all people have the right to participate in elections, this will be a building of all actions taken.

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