HIMUNC VII BACKGROUND GUIDE

WELCOME. BIENVENIDOS. أهلا بك. 欢迎. BIENVENUE. ДОБРО ПОЖАЛОВАТЬ

Special Political and Decolonization Committee (SPECPOL)

Dear Delegates,

Welcome to the seventh iteration of the Henrico Invitational Model United Nations conference! We would like to thank you for choosing to take part in our committee of the General Assembly, as delegates of the United Nations Special Political and Decolonization Committee. The Special Political and Decolonization Committee will provide delegates with the unique opportunity to explore the effect of imperative political matters in the world. As delegates, it is your responsibility to think critically and creatively to develop the most effective resolutions to these issues.

The two principal issues that this committee will be focusing on include safeguarding integrity and combating corruption during conflict as well as mitigating the effects of cybersecurity and hybrid attacks. There is much to discuss regarding the effect of conflicts created by political matters, cybersecurity, and hybrid attacks. A particular increase in territorial conflicts has stimulated a variety of additional political problems. The purpose of this committee is to develop comprehensive and innovative resolutions.

To learn more about the Special Political and Decolonization Committee, as well as the specific issues we will be addressing, make sure to refer to the background guide to gain a better understanding of how to develop your position. Any questions regarding the committee can be directed through email to either of the chairs or to the Undersecretary-General of General Assemblies. Those who actively participate, communicate with others and demonstrate their thorough understanding of these issues will be awarded for their performance as a delegate of our committee. We wish you the best of luck!

Regards,

SPECPOL

Gianna Aquino | Co-Chair | hcps-aquinogn@henricostudents.org

Sriya Jeereddy | Co-Chair | hcps-jeereddys@henricostudents.org

Krishita Muduli | Vice-Chair | hcps-mudulik@henricostudents.org

Arjun Beeravalli | Undersecretary-General of General Assemblies | himunc.genreg@gmail.com

Topic 1: Safeguarding Integrity and Combating Corruption During Conflict

Understanding War Time Corruption

Wartime corruption can have detrimental effects. In the context of the Russia-Ukraine conflict, it is essential to comprehend the intricate nature of corruption and how it is exacerbated during armed conflict. Wartime corruption involves the exploitation of power, resources, or authority for personal or group gain. Conflict environments, characterized by weakened governmental systems and a focus on immediate survival, create ripe conditions for corruption to skyrocket.

Wartime corruption can take many forms, each presenting unique challenges to the parties involved. Embezzlement and misappropriation of funds designated for humanitarian aid, military support, or infrastructure development are only some of the prevalent forms of corruption during armed conflict. Corrupt actors exploit the chaos and diversion of resources to siphon off funds for their gains, depriving the intended recipients of much-needed assistance.

Extortion and bribery are also rampant during times of war. The breakdown of law and order provides an environment in which armed groups or individuals demand payments in exchange for services. This form of corruption further victimizes the vulnerable population already grappling with the adverse effects of conflict.

Impact on Humanitarian Aid

Throughout the war, humanitarian aid has been given to Ukraine through a variety of methods. Currently, more than 17.6 million people[1] in Ukraine are in need of humanitarian assistance, and more than 3 million people are living in areas controlled

[1] “Ukraine.” 2023. OCHA. November 14, 2023. https://www.unocha.org/ukraine.

by Russian-backed separatists, where access is limited and conditions are dire. However, the delivery of humanitarian aid has been hampered by corruption, both within Ukraine and in the occupied territories. Such corruption severely hampers the delivery of vital humanitarian services intended to alleviate the suffering of those affected by conflict. This highlights the lack of transparency and accountability in the allocation and distribution of aid, as well as the challenges faced by civil society and independent media in monitoring and reporting on corruption.[2]

The impact of corruption on humanitarian aid extends beyond misappropriation. The skewed distribution of aid resources, influenced by corrupt practices, results in aid being diverted to individuals with political connections rather than reaching those in dire need. Recently, the National Anti-Corruption Bureau of Ukraine (NABU) and the Specialized Anti-Corruption Prosecutor's Office (SAPO) discovered that Ukraine's first deputy minister of agrarian policy and food, alongside the former deputy minister of economy, allegedly misappropriated approximately UAH 62 million (equivalent to about €1.5 million).[3]

Deterring the Risk of Illicit Arms Trading

Another aspect of the conflict that is affected by corruption is the arms trade, which involves the supply and demand of weapons and equipment by the warring parties and other actors. The war in Ukraine has created the conditions for the accumulation of weapons, often outside direct state control, and the potential for more serious levels of proliferation after the

[2] Falk, Thomas O. 2022. "How Much of a Problem Is Corruption in Ukraine?" Al Jazeera, June 16, 2022. https://www.aljazeera.com/news/2022/6/15/how-problematic-is-corruption-in-ukraine.

[3] Lutsevych, Orysia. 2023. "Ukraine Is Locked in a War with Corruption as Well as Putin – It Can't Afford to Lose Either." The Guardian, January 30, 2023. https://www.theguardian.com/commentisfree/2023/jan/30/ukraine-war-with-corruption-putin-resignations-russia.

the end of hostilities. As the current situation holds, Ukraine's battlefields[4] could become the new arsenal of anarchy, arming everyone from insurgents in Africa to gangsters in the streets of Europe.

The risk of illicit arms trading extends beyond the immediate conflict zone. The availability of weapons due to illicit trade heightens the potential for spill-over effects, impacting neighboring countries and possibly igniting new conflicts or exacerbating existing ones. There is evidence of illicit arms flowing from Ukraine to other conflict zones, such as Syria and Libya, as well as allegations of Russian involvement in the smuggling of weapons to the Taliban in Afghanistan.[5] The consequences of these arms finding their way into the hands of unauthorized entities can be devastating, hindering peace efforts and prolonging the suffering of affected populations. Moreover, the influx of illicit arms has implications for the safety and security of the civilian population. These weapons often end up in the hands of non-state actors, perpetuating violence and human rights abuses. This has led to cases of torture, abduction, and extrajudicial killings committed by some of the armed groups in Ukraine, who operated with impunity and often enjoyed political patronage. The widespread availability of arms not only intensifies the conflict but also obstructs efforts to establish peace, stability, and recovery in the region.

Questions to Consider

1. How can international cooperation effectively combat wartime corruption by addressing its various forms, including embezzlement,

[4] Global Initiative Against Transnational Organized Crime. 2023. "Peace and Proliferation: The Russo-Ukrainian War and the Illegal Arms Trade | Global Initiative." Global Initiative. September 6, 2023. https://globalinitiative.net/analysis/russia-ukraine-war-illegal-arms-trade/.

[5] "MSN." n.d. https://www.msn.com/en-us/news/world/putin-says-some-western-weapons-for-ukraine-are-ending-up-in-the-talibans-hands/ar-AA1jtEIH.

misappropriation of funds, extortion, and bribery, during the Russia-Ukraine conflict?

2. How might technology and transparency measures be employed to track and monitor the flow of humanitarian aid, thereby deterring corruption and enabling timely intervention to prevent aid diversion in conflict zones like Ukraine?
3. How can countries involved in the Russia-Ukraine conflict collaborate to enhance transparency and accountability within the supply chain, especially in critical sectors like defense and humanitarian aid, to mitigate corruption risks?
4. In what ways can comprehensive border control measures and international collaborations help in curbing the illicit arms trade and preventing the spillover effects that

Topic 2: Mitigating the Effects of Cybersecurity and Hybrid Attacks

Hybrid Warfare and Cyber Threats

Defined by NATO, hybrid war is "an interplay or fusion of conventional as well as unconventional instruments of power and tools of supervision… blended in a synchronized manner to exploit vulnerabilities of an antagonist and achieve synergistic effects".[6] In an effort to weaken the civil defenses of Ukraine and take over its population, Russia initiated "active measures" such as espionage, cyber-attacks, and internet-based information.

Throughout all of history, the war between Russia and Ukraine has been the largest military conflict of the cyber age. Before the war had begun, Russian Advanced Persistent Threat (APT) actors were infiltrating networks all over Ukraine

[6] Kong, Weilong, and Timothy Marler. "Ukraine's Lessons for the Future of Hybrid Warfare." RAND, November 28, 2022. https://www.rand.org/blog/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html.

such as government agencies, electoral processes, and critical infrastructure.[7] These cyber techniques hacked, intimidated, disinformed, surveilled, and disrupted the citizens, government, military, and infrastructure of Ukraine.[8] By August 2022, the Computer Emergency Response Team of Ukraine (CERT-UA) recorded over 1,123 cyber-attacks only in the first half of the war.[9] In January 2023, the CERT-UA reported 2,194 attacks during 2022.[10] Of 30 recorded cyber events between Russia and Ukraine, 28 were initiated by Russia.[11] Russian-initiated attacks negatively affected Ukraine in many ways such as the government and local authorities, defense and security, energy, financial services, IT and telecoms, and logistics sectors.

Mitigating Cyber War

Cyberwar mitigation is the "application of policies, technologies, and procedures to reduce the likelihood and impact of a successful cyber attack".[12] Cyberwarfare can be just as harmful as physical warfare by using many of the same tactics including disrupting power grids, gas lines, internet service, and water supplies, employing propaganda, spying, and disinformation. With Russia being a top cyber threat, mitigating cyber wars is crucial

[7] Schulze, Matthias, and Mika Kerttunen. "Cyber Operations in Russia's War against Ukraine." *SWP*. April 17, 2023. https://www.swp-berlin.org/10.18449/2023C23/.

[8] George, Jordana J. "Considering Cyberwar Efficacy: Is Mitigation Possible? | GJIA." Georgetown Journal of International Affairs, September 11, 2023. https://gjia.georgetown.edu/2023/09/11/considering-cyberwar-efficacy-is-mitigation-possible/.

[9] Державна Служба Спеціального Зв'язку Та Захисту Інформації України. "Enemy hackers attacked Ukraine more than a thousand times during the war," August 26, 2022. https://cip.gov.ua/en/news/bilshe-tisyachi-raziv-atakuvali-ukrayinu-vorozhi-khakeri-za-chas-viini.

[10] Scroxton, Alex. "Ukraine Cyber Teams Responded to More than 2,000 Attacks in 2022." *ComputerWeekly.Com*, January 18, 2023. https://www.computerweekly.com/news/252529292/Ukraine-cyber-teams-responded-to-more-than-2000-attacks-in-2022.

[11] Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. "Cyber Operations during the Russo-Ukrainian War," October 10, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#:~:text=Of%20the%2030%20recorded%20cyber,operations%20targeted%20government%20military%20targets.

[12] Balbix. "What Is Cyber Risk Mitigation? | Balbix," November 28, 2022. https://www.balbix.com/insights/what-is-cyber-risk-mitigation/#:~:text=Cyber%20risk%20mitigation%20is%20the,and%20achieve%20its%20business%20goals.

to minimize the attacks and reduce the damage that is being done in Ukraine.

There are many ways organizations in Ukraine can do this (“Cybersecurity and Infrastructure”). For instance, implementing and enforcing the use of multifactor authentication (MFA). With this method, there will be an increased amount of security that protects organizations from cyber-attacks. Ukraine has also been asking organizations to report any malicious activity to the Cybersecurity and Infrastructure Security Agency (CISA) to maintain the issue as quickly as possible. By monitoring and implementing these practices, Ukraine can decrease the risks of cyber threats.

Ukraine Cybersecurity Strategy

The amount of targeted countries from Russia has increased to over 300% in 2022 compared to only 250% in 2020.[13] Users in NATO countries have also been targeted during this same period. Countries often take a concealed approach when carrying out cyber operations, masking their identities through third-party servers cataloged among academic, government, and threat intelligence firms.

On February 15, 2016, Ukraine adopted a National Cybersecurity ‘Strategy’ in response to its large-scale attacks from prior years. Following the requirements of the Budapest Convention and taking steps in line with internet service providers, Ukraine has taken two steps in enhancing its cybersecurity. These activities have been strongly cooperated with other international partners across the cybersphere.[14]

[13] Huntley, Shane. “Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape.” *Google*, February 16, 2023. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/#:~:text=Russian%20government%2Dbacked%20attackers%20ramped,300%25%20in%20the%20same%20period.

[14] Tkachenko, Oleksii. “Cybersecurity in Ukraine: National Strategy and International Cooperation – Global Forum on Cyber Expertise.” GFCE, May 2017. https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/#:~:text=The%20Ukrainian%20experience%20demonstrates%20that,the%20necessary%20capacities%20and%20respond.

The Strategy (Ukraine) has focused on three axes; developing the national cybersecurity system, enhancing capabilities across the security and defense sector, and ensuring the cybersecurity of critical information infrastructure and Government information resources. Implementing this system required the collaboration of all government agencies including research/educational institutions, civil groups, and businesses and organizations involved with electronic communications and information infrastructure. Towards implementation of the Strategy, Ukraine has formed collaborations with numerous partners within the cyber domain. In joint with the European Union and Council of Europe Projects, CyberCrima@EaP II and CyberCrime@Eap III, provide mutual assistance in mitigating cybercrime, and fostering trust-building exercises to tackle public and private information.

Ukraine has been working with the NATO Cyber Defence Trust fund to further enhance the country's technical abilities to counter cyber threats. Establishing an Incident Management Centre, the Security Service of Ukraine, and collaboration with the NATO partners has allowed Ukraine to conduct cyber defense exercises and training to react to major cyber-attacks through a national defense infrastructure.

International Relations

As a partner country with NATO, Ukraine cooperates closely with its policies but is not guaranteed to be covered by its security measures. Following Russia's invasion in 2022, NATO and its Allies have provided support to Ukraine.[15] Cyber defense is part of NATO's core task of deterrence and defense, helping allies enhance their national resilience and providing a platform for political

[15] NATO. "Relations with Ukraine," July 28, 2023. https://www.nato.int/cps/en/natohq/topics_37750.htm

consultation and collective action.[16] NATO provides allies to consult, share concerns about malicious cyber activities, exchange national approaches and responses, and consider possible collective responses. The allies focus on enhancing mutual assistance in preventing, mitigating, recovering from, and responding to cyber-attacks.

Adopted by the Allies at the 2021 NATO Summit in Brussels, the Comprehensive Cyber Defense Policy supports the core tasks of NATO, reaffirming its defensive mandates employing a range of capabilities for defending against cyber threats in use with its political, diplomatic, and military tools. The impact of cumulative cyber activities may be considered an armed attack, leading the North American Council to invoke Article 5 of the North Atlantic Treaty. This requires unity of efforts through political, military, and technical levels. Along with the 2023 NATO Summit in Vilnius, Allies endorsed concepts focused on enhancing the contribution of cyber defense, further integrating cyber defense in political, militaristic, and technical aspects. The Alliance has been able to further enhance their shared situational awareness, strengthening their situational awareness and mitigating potential harm from cyber threats.

Implications

From the 2011-2013 Moscow protests, Russia recognized the strong influence of the media and its use in generating public unrest. Russia began to utilize information campaign capabilities exemplified by the Internet Research Agency, allowing them to influence audiences and facilitate the annexation of Crimea in 2014. Russian skepticism of the West has grown since NATO's enlargement, initiating aggression towards Russia's

[16] Cybersecurity and Infrastructure Security Agency CISA. "Russia Cyber Threat Overview and Advisories | CISA," n.d. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia.

"sphere of influence." Through militaristic and non-militaristic methods, Russia holds goals of achieving strategic effects and further expanding its superiority over its opponents. Cyber operations play an essential war technique in Russia's international influence, compensating for their loss of power from the upbringing of NATO alliances supporting Ukraine (Hakala and Melnychuk, 2021).[17]

Questions to Consider

1. How could NATO implement its policies and alleviate tensions with Russia's goal of maintaining its power?
2. What regulations could be agreed on between Ukraine and Russia without a high control of NATO's influence?
3. Are there alternate techniques Russia could use to assert its power within its nation without harming the cybersecurity of neighboring countries in conflict?
4. What are some possible techniques used to improve the cybersecurity of Ukraine?
5. How could the disabling of civil infrastructure compensate for cyber attacks, with consideration of ethical implications?

[17] Hakala, Janne, and Jazlyn Melnychuk. "Russia's Strategy in Cyberspace." *NATO*. June 202

Bibliography

NATO. “Cyber Defence,” September 14, 2023. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Державна Служба Спеціального Зв’язку Та Захисту Інформації України. “Enemy hackers attacked Ukraine more than a thousand times during the war,” August 26, 2022. https://cip.gov.ua/en/news/bilshe-tisyachi-raziv-atakuvali-ukrayinu-vorozhi-khakeri-za-chas-viini.

George, Jordana J. “Considering Cyberwar Efficacy: Is Mitigation Possible? | GJIA.” Georgetown Journal of International Affairs, September 11, 2023. https://gjia.georgetown.edu/2023/09/11/considering-cyberwar-efficacy-is-mitigation-possible/.

Hakala, Janne, and Jazlyn Melnychuk. “Russia’s Strategy in Cyberspace.” *NATO*. June 2021. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

Huntley, Shane. “Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape.” *Google*, February 16, 2023. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/#:~:text=Russian%20government%2Dbacked%20attackers%20ramped,300%25%20in%20the%20same%20period.

Kong, Weilong, and Timothy Marler. “Ukraine’s Lessons for the Future of Hybrid Warfare.” RAND, November 28, 2022. https://www.rand.org/blog/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html.

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. “Cyber Operations during the Russo-Ukrainian War,” October 10, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#:~:text=Of%20the%2030%20recorded%20cyber,operations%20targeted%20government%20military%20targets.

NATO. “Relations with Ukraine,” July 28, 2023. https://www.nato.int/cps/en/natohq/topics_37750.htm.

Cybersecurity and Infrastructure Security Agency CISA. “Russia Cyber Threat Overview and Advisories | CISA,” n.d. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia.

Schulze, Matthias, and Mika Kerttunen. “Cyber Operations in Russia’s War against Ukraine.” *SWP*. April 17, 2023. https://www.swp-berlin.org/10.18449/2023C23/.

Scroxton, Alex. “Ukraine Cyber Teams Responded to More than 2,000 Attacks in 2022.” *ComputerWeekly.Com*, January 18, 2023. https://www.computerweekly.com/news/252529292/Ukraine-cyber-teams-responded-to-more-than-2000-attacks-in-2022.

Tkachenko, Oleksii. “Cybersecurity in Ukraine: National Strategy and International Cooperation – Global Forum on Cyber Expertise.” GFCE, May 2017. https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/#:~:text=The%20Ukrainian%20experience%20demonstrates%20that,the%20necessary%20capacities%20and%20respond.

Balbix. “What Is Cyber Risk Mitigation? | Balbix,” November 28, 2022. https://www.balbix.com/insights/what-is-cyber-risk-mitigation/#:~:text=Cyber%20risk%20mitigation%20is%20the,and%20achieve%20its%20business%20goals.

Falk, Thomas O. 2022. “How Much of a Problem Is Corruption in Ukraine?” *Al Jazeera*, June 16, 2022. https://www.aljazeera.com/news/2022/6/15/how-problematic-is-corruption-in-ukraine.

Global Initiative Against Transnational Organized Crime. 2023. “Peace and Proliferation: The Russo-Ukrainian War and the Illegal Arms Trade | Global Initiative.” Global Initiative. September 6, 2023. https://globalinitiative.net/analysis/russia-ukraine-war-illegal-arms-trade/.

Lutsevych, Orysia. 2023. “Ukraine Is Locked in a War with Corruption as Well as Putin – It Can’t Afford to Lose Either.” *The Guardian*, January 30, 2023. https://www.theguardian.com/commentisfree/2023/jan/30/ukraine-war-with-corruption-putin-resignations-russia.

“MSN.” n.d. https://www.msn.com/en-us/news/world/putin-says-some-western-weapons-for-ukraine-are-ending-up-in-the-talibans-hands/ar-AA1jtEIH.

“Ukraine.” 2023. OCHA. November 14, 2023. https://www.unocha.org/ukraine.