Disarmament and International Security (DISEC)

Chair Letter

DEAR DELEGATES

Welcome to the Disarmament and International Security Committee (DISEC) at CNYMUN 2025!! With the presence of many issues facing the global community today, we look forward to productive debate and collaboration between delegates during the conference. Your chairs for the conference will be Claire McDonald and Connor Burke, aided by Yutaro Hirabayashi as their rapporteur.

ABOUT THE CHAIRS

Claire McDonald is a junior at Fayetteville-Manlius High School and has been participating in MUN since her freshman year. This will be her first time chairing. Outside of MUN she runs both cross country and track and enjoys baking, reading, and listening to music, particularly Taylor Swift and Noah Kahan. Claire is also a member of both the music and science honor societies.

Connor Burke is also a junior at Fayetteville Manlius High School and has been a part of CNYMUN since his freshman year. Coming back to MUN as a sophomore he also attended UNAR in addition to CNYMUN as delegates. This makes for his 4th conference with more soon to come. Outside of MUN, you can find Connor rowing with the rest of the FM crew team, or participating in the FM Mock Trial team preparing for "court." Connor also enjoys playing video games, hanging out with friends, and participating in Civil Air Patrol, the US Air Force Auxiliary.

ABOUT THE COMMITTEE

Your topics for the Disarmament and International Security Committee (DISEC) at CNYMUN 2024 will be:

1. Assessing the Weaponization of Gene Editing and its Effect on Cyber Technology
2. Prevention of Cyber Attacks On Government and Civilian Infrastructure

The United Nations Disarmament and International Security Committee (UN DISEC) was the first among the committees within the general assembly to be established following the signing of the United Nations charter in 1945, and is often referred to as the first committee. DISEC was founded to serve as an international body for the purpose of discussing peace and security issues among the international community, as well as the regulation of armaments. DISEC is also able to propose certain topics to be brought into consideration by the Security Council, however, the committee cannot interfere directly with the Security Council's decision-making process.

ABOUT THE CONFERENCE:

Following CNYMUN tradition, the debate will be conducted in Harvard style, meaning delegates will not be allowed to use pre-written clauses and/or resolutions during committee. Doing so will make a delegate ineligible for awards.

To be eligible for awards, delegates must submit a 1-2 page position paper via email that addresses both topics before the start of the conference. Position papers should outline the stance of your delegation, and display an understanding of the topics, demonstrating research and knowledge of your organization's goals. When deciding on awards, the chairs will look favorably upon delegates who have put significant effort towards research/preparation, collaborate with other delegates during committee sessions, stay within their nation's policies, and get their voice heard without being overbearing.

Furthermore, for the first time, CNYMUN is implementing a tiered structure of committees to ensure similar experience levels for all committee members. The Disarmament and International Security Committee (DISEC) is designated as an open committee. In turn, the Best New Delegate Award will be offered to a first-time delegate in this committee.

Please share position papers before the conference begins. Our emails are listed below for you to contact your chairs about any research, position papers, committee inquiries, or other questions. We also encourage you to scan our lengthy delegate preparation resources and award structure on www.cnymun.org. We wish you luck and look forward to what CNYMUN 2025 will bring!

Claire McDonald
26cmcdonald@fmschools.org

Connor Burke
26tburke@fmschools.org

TOPIC 1: ASSESSING THE WEAPONIZATION OF GENE EDITING AND ITS EFFECT ON CYBER TECHNOLOGY

Innovation in the sphere of biotechnology is increasing rapidly. The most notable recent development in this field is the development of CRISPR-Cas9. CRISPR works by targeting specific areas of DNA, and then "cuts" those targets, thereby editing the genome.[1] Using this technology, a genome can have new functions. CRISPR is employed in various industries, serving purposes ranging from the production of virus resistant yogurt bacteria, to the destruction of weeds and pests.[2] It also serves important purposes in the biomedical industry, being commonly used in the production of vaccines.[3] However, for the many beneficial applications of gene editing technology, its potential to change the state of international conflict cannot be understated. Many defense experts have begun to raise concerns about the biotechnology's possibility to create strong and inexpensive biological weapons.

The development of gene editing technology has rapidly accelerated in the past twenty five years. As early as the 1980s some progress had been made towards the modern state of gene editing.[4] A large breakthrough came in the form of the Australian Mousepox Experiment. In this experiment an immune system suppressing gene was spliced with the mousepox virus.[5] As a result, mice inoculated against mousepox developed the disease, and died. The experiment was reproduced using cowpox, which can infect humans.[6] In 2015, modern gene editing began to take shape. This was the first occurrence of the modification of the human germline. The editing of germline is done on the embryo of an organism, and the adjustments are carried onto the next generation of organisms.[7] The use of human germline editing called into question various ethical debates about gene editing, weighing the potential medical benefits versus the moral failings and potential dangers. China was one of the first nations to conduct experiments surrounding human germline editing, followed shortly by Russia. At this time, human germline editing is banned in the US and most of the European Union.[8]

The history of biological warfare is vast, and has had significant repercussions on 21st century security, with several notable incidents putting defense officials on alert. In 2001, the United States suffered one of the worst biological attacks in its history. In the months following the September 11th attacks, four letters laced with anthrax were mailed to multiple US senators and journalists.[9] Anthrax is a serious bacteria caused disease that results from contact with contaminated substances or inhalation of the disease-causing agent.[10] The letters resulted in five deaths, and seventeen people falling ill. Aside from the tragedy brought about by the victims and their families, this example of bioterrorism sparked public panic among the American people. Noting the severity of bioterrorism, it is also crucial to consider recent examples of governments utilizing biological and chemical warfare in times of crisis. A prominent example would be the use of chemical warfare by the Syrian government, led by President Bashar al-Assad, during the Syrian Civil War.[11] Beginning in 2013, reported widespread attacks included the use of mustard gas, and chemical nerve agents, such as Sarin gas. The actions of the Syrian government were a violation of the 1925 Geneva Protocol, launching a UN investigation. Results showed that chemical

[1] Kosal, Margaret E. "Emerging Life Sciences and Possible Threats to International Security." Orbis vol. 64,4 (2020): 599-614. doi:10.1016/j.orbis.2020.08.008
[2] Ibid.
[3] AyanoĞlu, Fatma Betül, et al. "Bioethical Issues in Genome Editing by CRISPR-Cas9 Technology." TURKISH JOURNAL of BIOLOGY, vol. 44, no. 2, 2 Apr. 2020, pp. 110-20. National Library of Medicine, https://doi.org/10.3906/biy-1912-52. Accessed 30 Aug. 2024.
[4] Ibid 2
[5] Ibid 2
[6] Ibid 2
[7] Ibid 2
[8] Ibid 2
[9] "Amerithrax or Anthrax Investigation." Federal Bureau of Investigation, www.fbi.gov/history/famous-cases/amerithrax-or-anthrax-investigation. Accessed 30 Aug. 2024.
[10] "About Anthrax." Center for Disease Control and Prevention, 14 May 2024, www.cdc.gov/anthrax/about/index.html. Accessed 30 Aug. 2024.
[11] Britannica, The Editors of Encyclopaedia. "Syrian Civil War". Encyclopedia Britannica, 17 Aug. 2024, https://www.britannica.com/event/Syrian-Civil-War. Accessed 30 August 2024.

warfare was present on a large scale in Syria, and victims were mainly civilians.[12]

Many governments and international security experts now share their growing concern about the looming impact of CRISPR and other gene editing and biotechnology softwares as it pertains to security. In 2016, then US Director of National Intelligence James Clapper explicitly included advances in gene editing in the list of threats posed by "weapons of mass destruction and proliferation", and was the only agent of biological warfare included on the list.[13] The cause of unique concern over these technologies is their ability to enhance the effects of existing biological agents. Specific possibilities include increasing the ease of transmission of microbiological agents, while also making them more lethal and longer lasting.[14] Furthermore, as observed in the Australian Mousepox Experiment, it is capable of making viruses and other pathogens immune to inoculation and treatment. Also to be considered is the possibility for the creation of novel delivery tactics, which would catch an enemy off guard in a way not previously seen in the history of warfare.[15] This ability, which becomes open to more governments and organizations as the technology develops, would cause biological warfare to become more effective and deadly than ever before. Enhanced biological agents possess the ability to destroy large amounts of people at once, similar to nuclear weapons. Additionally, considering the often transmittable nature of these agents, the spread of destruction could be difficult to contain, especially as gene editing is not fully understood by any military. Many defense experts especially consider the possibility of a new strain of smallpox being created. Smallpox, which has been eradicated since 1980, is highly contagious and deadly. While vaccines led to its disappearance from the globe, many experts believe that a near-smallpox-like pathogen, created via gene editing, could be one of the most destructive weapons proposed in recent times. In 2002, a group of researchers at The State University of New York at Stony Brook artificially synthesized live polio virus from scratch using the genetic sequence of the virus, which is readily available.[16] While polio cannot be used as a biological weapon, this method can be transferred to smallpox and ebola. Smallpox is particularly deadly because of its highly contagious nature, and the fact that since its eradication, the world's population has not been vaccinated against it or exposed to it, giving people no immunity against smallpox. There is no known treatment for smallpox, as it is generally a non-issue in modern society.[17]

The dangerous potential of gene editing, among other emerging biotechnologies, is extenuated by the ease in which it's becoming available. CRISPR is a relatively inexpensive and easy to use technology, compared to previous gene editing mechanisms. This allows biotechnology to be utilized by both wealthy governments and smaller organizations. Bioterrorism, as observed in 2001, could become even more of a possibility as this technology becomes increasingly widespread. Some terrorist organizations, such as the ISIL (Islamic State of Iraq and the Levant), have a history of using chemical and biological agents in their attacks.[18]

Currently, the majority of international debate surrounding these new forms of biological warfare surrounds CRISPR, but it is imperative to remember that this is not the only existing gene editing technology. Others, like Zinc Finger Nuclease, are actively being researched in their usage for somatic

[12] Kimball, Daryl, and Kelsey Davenport, editors. "Timeline of Syrian Chemical Weapons Activity, 2012-2022." Arms Control Association, Oct. 2023, www.armscontrol.org/factsheets/timeline-syrian-chemical-weapons-activity-2012-2022. Accessed 30 Aug. 2024.

[13] Ibid 2 Security." Orbis vol. 64,4 (2020): 599-614. doi:10.1016/j.orbis.2020.08.008

[14] Kosal, Margaret E. "Emerging Life Sciences and Possible Threats to International Security." Orbis vol. 64,4 (2020): 599-614. doi:10.1016/j.orbis.2020.08.008

[15] Ibid 2 Security." Orbis vol. 64,4 (2020): 599-614. doi:10.1016/j.orbis.2020.08.008

[16] Van Aken J, Hammond E. Genetic engineering and biological weapons. New technologies, desires and threats from biological research. EMBO Rep. 2003 Jun;4 Spec No(Suppl 1):S57-60. doi: 10.1038/sj.embor.embor860. PMID: 12789409; PMCID: PMC1326447.

[17] "Smallpox." Center for Disease Control and Prevention, 3 May 2024, www.cdc.gov/smallpox/clinicians/treatment.html. Accessed 30 Aug. 2024.

[18] Kosal, Margaret E. "Emerging Life Sciences and Possible Threats to International Security." Orbis vol. 64,4 (2020): 599-614. doi:10.1016/j.orbis.2020.08.008

gene editing. Somatic, unlike germline, is done on the body cells of an organism, rather than the embryo. The mutations are not passed onto future generations.[19]

When legislating limits on biotechnology, it is crucial to understand the many benefits of genetic engineering. First of all, according to the Nuclear Threat Initiative's biosecurity program, the EU had a bioeconomic turnover of 2.3 trillion euros and provided 18 million jobs in 2015.[20] Many nations have an economic incentive to support the unchecked growth of biotechnology. Second of all, these technologies are most widely used for public health. Gene editing is used in research for the treatment of HIV/AIDS, Parkinson's Disease, cancer, genetic disorders, and various other ailments.[21] Because of the contrasting potential for both treatment and destruction of humans, it is important to consider gene editing and biotechnology under a completely new lens. Most limitations regarding chemical and biological agents fall under Cold War-era nuclear proliferation agreements. Many defense experts argue that this is outdated and not applicable to these modern and different technologies. In particular, gene editing technologies are scarcely regulated by many governments. The National Library of Medicine suggests worldwide legislation to control genetic editing, but this action has not been taken by many nations.[22]

The nations with the most influential and well-endowed biotech industries are also nations with specific international policy and allies. For example, China is a global leader in biotechnology. From the years of 2015 to 2020 the Chinese government allocated $11.8 billion for the development of biotechnology.[23] Other global leaders in the biotechnology sphere are the US, UK, Denmark, and Singapore.[24] The international community has voiced extra concern in regards to the research that Russia is currently partaking in surrounding germline experimentation,[25] and its history of using nerve agents. This has been observed in the use of Novichok to poison former intelligence officer Sergei Skipral in 2018.[26] A 1925 and a 1972 convention prohibited the use of biological and chemical weapons in warfare, and while this has not been upheld by all nations, it has been an important step towards the limitation of these dangers.[27] However, global tensions are rising. Conflict is particularly prominent in Ukraine and the Middle East and the limitation of new superweapons has the potential to stop mass destruction before it becomes all-consuming.

[19] Kosal, Margaret E. "Emerging Life Sciences and Possible Threats to International Security." Orbis vol. 64,4 (2020): 599-614. doi:10.1016/j.orbis.2020.08.008

[20] Kavanagh, Camino. "Biotechnology." New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?, Carnegie Endowment for International Peace, 2019, pp. 23–30. JSTOR, http://www.jstor.org/stable/resrep20978.6. Accessed 31 Aug. 2024.

[21] AyanoĞlu, Fatma Betül, et al. "Bioethical Issues in Genome Editing by CRISPR-Cas9 Technology." TURKISH JOURNAL of BIOLOGY, vol. 44, no. 2, 2 Apr. 2020, pp. 110-20. National Library of Medicine, https://doi.org/10.3906/biy-1912-52. Accessed 30 Aug. 2024.

[22] AyanoĞlu, Fatma Betül, et al. "Bioethical Issues in Genome Editing by CRISPR-Cas9 Technology." TURKISH JOURNAL of BIOLOGY, vol. 44, no. 2, 2 Apr. 2020, pp. 110-20. National Library of Medicine, https://doi.org/10.3906/biy-1912-52. Accessed 30 Aug. 2024.

[23] Kavanagh, Camino. "Biotechnology." New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?, Carnegie Endowment for International Peace, 2019, pp. 23–30. JSTOR, http://www.jstor.org/stable/resrep20978.6. Accessed 31 Aug. 2024.

[24] Kavanagh, Camino. "Biotechnology." New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?, Carnegie Endowment for International Peace, 2019, pp. 23–30. JSTOR, http://www.jstor.org/stable/resrep20978.6. Accessed 31 Aug. 2024.

[25] Kosal, Margaret E. "Emerging Life Sciences and Possible Threats to International Security." Orbis vol. 64,4 (2020): 599-614. doi:10.1016/j.orbis.2020.08.008

[26] U.S. Mission Italy. "Putin's poisons: 2018 attack on Sergei Skripal." U.S. Embassy and Consulates in Italy, 11 Apr. 2022, it.usembassy.gov/putins-poisons-2018-attack-on-sergei-skripal/. Accessed 30 Aug. 2024.

[27] Kimball, Daryl, and Kelsey Davenport, editors. "Timeline of Syrian Chemical Weapons Activity, 2012-2022." Arms Control Association, Oct. 2023, www.armscontrol.org/factsheets/timeline-syrian-chemical-weapons-activity-2012-2022. Accessed 30 Aug. 2024.

QUESTIONS TO CONSIDER

1. What strategies could be used to both limit the potential destructive capabilities of gene editing biotechnology, while simultaneously promoting scientific development?
2. How do the competing interests of stakeholders impact the discourse surrounding the limitations of biotechnology?
3. How are lower-income nations, especially those struck by conflict, liable to the creation of these biotechnical weapons by more powerful nations? How would the development of these weapons impact their conflicts?
4. What strategies can be developed to keep the destructive nature of gene editing and other biotechnologies away from terrorist organizations as the technologies become more inexpensive and easier to handle?

HELPFUL SOURCES:

Chemical & Biological Weapons: Positions, Prospects and Trends
https://www.jstor.org/stable/42909302

The New Killer Pathogens: Countering the Coming Bioweapons Threat
https://carnegieendowment.org/posts/2018/04/the-new-killer-pathogens-countering-the-coming-bioweapons-threat?lang=en

Synthetic Bioweapons Are Coming
https://www.usni.org/magazines/proceedings/2021/june/synthetic-bioweapons-are-coming

TOPIC 2: PREVENTION OF CYBER ATTACKS ON GOVERNMENT AND CIVILIAN INFRASTRUCTURE

Cybersecurity is no new topic but is still one of any organization's biggest concerns. Since over an estimated two-thirds of the world's population has access to the internet, we all share a common concern over our identity online.[28] The world as we know it would not be able to function without the internet. Almost anything from medical services to critical infrastructure, government services, and private industries rely on the internet to stay connected. Cyber attacks have risen alongside the complexity of computer technology itself, growing from harmless intrusions to holding industries on the east coast of North America for ransom.

The first known malicious malware was a *worm*, which once installed to a computer could replicate itself and spread to other computers without human interaction. This refers to the Morris Worm which was developed by a 24 year old Cornell student in 1988.[29] This software slowed down affected mini computers, professional stations, and mainframes as it required processing power to function, but never hurt or stole from the station. Morris stated the purpose of the program was to count all connected computers to the internet, but he was still charged under the Federal Computer Fraud and Abuse Act of 1986. Morris was the first person to be charged under this act, and was served a $10,000 fine alongside 300 hours of community service, all for a seemingly harmless program. Another malware, which also seemed harmless, was released in 1999 and spread like wildfire called Melissa.[30] This type of malware is classified as *phishing*, which sends fake texts, emails, or messages trying to trick the victim into giving away personal information, money, or installing

[28] Petrosyan, Ani. "Worldwide Digital Population 2024." *Statista*, 19 Aug. 2024, www.statista.com/statistics/617136/digital-population-worldwide/. Accessed 30 Aug. 2024.
[29] Markoff, John, and Special To the New York Times. "Computer Intruder Is Put on Probation and Fined $10,000 (Published 1990)." *The New York Times*, 5 May 1990, www.nytimes.com/1990/05/05/us/computer-intruder-is-put-on-probation-and-fined-10000.html. Accessed 30 Aug. 2024.
[30] FBI. "The Melissa Virus | Federal Bureau of Investigation." *Federal Bureau of Investigation*, 25 Mar. 2019, www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519. Accessed 30 Aug. 2024.

malware. In this case, the scam known as Melissa sent fake emails promising explicit images that contained a virus-laced attachment of itself. Once downloaded, the malware would instantly send the same fake emails to the top 50 contacts listed on the device. Melissa didn't need to steal information or demand ransom to cause havoc. It simply flooded government, company, and personal email accounts with phishing scams that slowed internet communication to a crawl. It cost over 80 million USD to clean up the mess of messages the virus caused.

As computer technology developed, its applications in the private and government sectors evolved alongside it. In 2010 a worm virus called Stuxnet invaded Iranian industrial sites, most notably a uranium enrichment plant.[31] The worm exploited the Window software systems by presenting itself like a reputable program while avoiding malware detection. Then, it would check if the computer was a part of a targeted industrial control system called Siemens. If not, then the worm wouldn't do anything to the machine. However, if Siemens was detected, then the worm would exploit four *zero-day* vulnerabilities, and cause centrifuges to spin until failure while reporting false data that everything was operating as normal. A zero-day vulnerability is a weakness in a program unknown to the developer or antivirus software. The fact that four of these unknown exploits were discovered and used in a way to complement each other was revolutionary. Stuxnet was able to ruin a fifth of Iran's nuclear centrifuge while never revealing its developers. More unforeseen attacks happened in 2014, both Target and The Home Depot experienced security breaches which resulted in almost 100 million credit cards being stolen.[32] These breaches were reported as unrelated, The Home Depot claimed that the virus used against them was much more custom than the one used against Target. However, both attacks ultimately cost The Home Depot 62 million USD and Target 142 million USD. The virus also cost the companies in the eyes of the public, as they seemed untrustworthy, which was reflected as sales dropped.

Cyberattacks haven't been "cured" by any means and still happen every year. More recently, in 2021 a group of hackers referring to themselves as Darkside were able to illegally access Colonial Pipeline's network.[33] Darkside succeeded in stealing 100 gigabytes of data and shutting down the pipeline system in 2 hours. The hackers were able to accomplish this by using *ransomware*, which is a type of malware that restricts access on devices until a fee is paid. Colonial Pipeline is a pipeline system that carries gasoline and jet fuel from Texas to New Jersey, which is the east coast's main source of gas. After the Darkside group was able to steal gigabytes of data and infect much of the network, including billing and accounting, Colonial Pipeline shut down the entire system to stop the spread of the virus. At the same time, Darkside demanded 75 Bitcoin, equivalent to 4.4 million USD, for a tool to reverse the malware. This was quickly paid, but it took 5 days for the tool to restore the functionality of the pipeline. During this time, mass panic spread among the east coast of the US as gas shortages started and prices rose, all leading to United State's President Biden declaring a state of emergency. A month after the attack, the FBI was able to recover 63.7 Bitcoin, or 2.3 million USD, worth half of the ransom paid.

Each day an estimated 2,200 cyber attacks happen, or in other words a cyber attack occurs every 39 seconds. This is why it's critical to have security measures and fail safes put in place. With almost every process from purchasing to registering being streamlined online, having your online identity stolen becomes increasingly dangerous. There are many companies and services dedicated to cybersecurity for individual, national, international, and all other levels of private, commercial, and government use. These can come from personal digital advisors or from divisions of the European Union that are dedicated to maintaining international peace and stability online. Just some examples of government organizations

[31] Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 26 Feb. 2013, spectrum.ieee.org/the-real-story-of-stuxnet. Accessed 30 Aug. 2024.
[32] Vinton, Kate. "With 56 Million Cards Compromised, Home Depot's Breach Is Bigger than Target's." *Forbes*, 18 Sept. 2014, www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/. Accessed 30 Aug. 2024.
[33] Kerner, Sean Michael. "Colonial Pipeline Hack Explained: Everything You Need to Know." *TechTarget*, 26 Apr. 2022, www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know. Accessed 30 Aug. 2024.

dedicated to these goals are the European Union Agency for Cybersecurity and the Cybersecurity & Infrastructure Security Agency. Unfortunately, it can be much worse for governments, as almost every aspect of administration incorporates computers in some way. Anything from financial aid to emergency services, healthcare to critical infrastructure, all routed through machines that could be vulnerable to attacks. Government representatives have to exercise extreme caution while dealing with cybersecurity, because they protect their government, community, themselves, and everyone in every scenario in between from being exploited. Since cybersecurity poses such a large threat many countries take preparation very seriously, for instance the United States and United Kingdom spend billions of dollars per year on cybersecurity. Whereas Poland has been one of the most prepared countries to receive, mitigate, and exterminate cyber attacks.[34] Just as some countries see cybersecurity as a real threat that needs to be taken care of, they may see each other in a similar way.

There are many different types of malware besides worms and phishing scams, some examples are adware, Denial of Service (DoS), eavesdropping, keyloggers, sniffing, spyware, trojan, and much more. With all of these diverse options, there's almost a limitless amount of ways hackers can try to target people. Each one of these different systems can be used to exploit anyone with severe consequences. This is why it's imperative that delegates come together, ensuring that all populations of the world have safe and fair access to the most revolutionary concept in history. The proposals will lay the groundwork for other developing countries to follow as they grow and succeed, and just because some countries might not be at a level to focus on digital debates doesn't mean their ideas, values, and voices don't matter. As for governments that have been focusing on this matter, there are many benefits that come from encouraging cybersecurity like education, critical thinking, and increased security. Whereas some other countries might not value the benefits and opportunities that come alongside the risks. With all of these different perspectives and opportunities come tension that have to navigate and minimize as well. Keeping these considerations in mind, delegates will have to work with their own and foreign policies to prevent cyber attacks on civilians, companies, and governments alike.

[34] "The 10 Best (and Worst) Countries for Cybersecurity." *Www.sciencefocus.com*, www.sciencefocus.com/news/the-10-best-and-worst-countries-for-cybersecurity. Accessed 30 Aug. 2024.

QUESTIONS TO CONSIDER:

1. How much development has been made for safety precautions, how and who do your safety precautions protect?
2. How does your government protect critical infrastructure and emergency services?
3. How does your government maintain preparedness in the government, military, and civilian sectors?
4. What is your nation's policy on cooperation with other nations concerning cybersecurity?

Helpful Sources:

European Union Agency for Cybersecurity
https://www.enisa.europa.eu/

Cybersecurity & Infrastructure Security Agency
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Digital Divide In Developing Countries Article
https://ctu.ieee.org/digital-divide-in-developing-countries-why-we-need-to-close-the-gap/