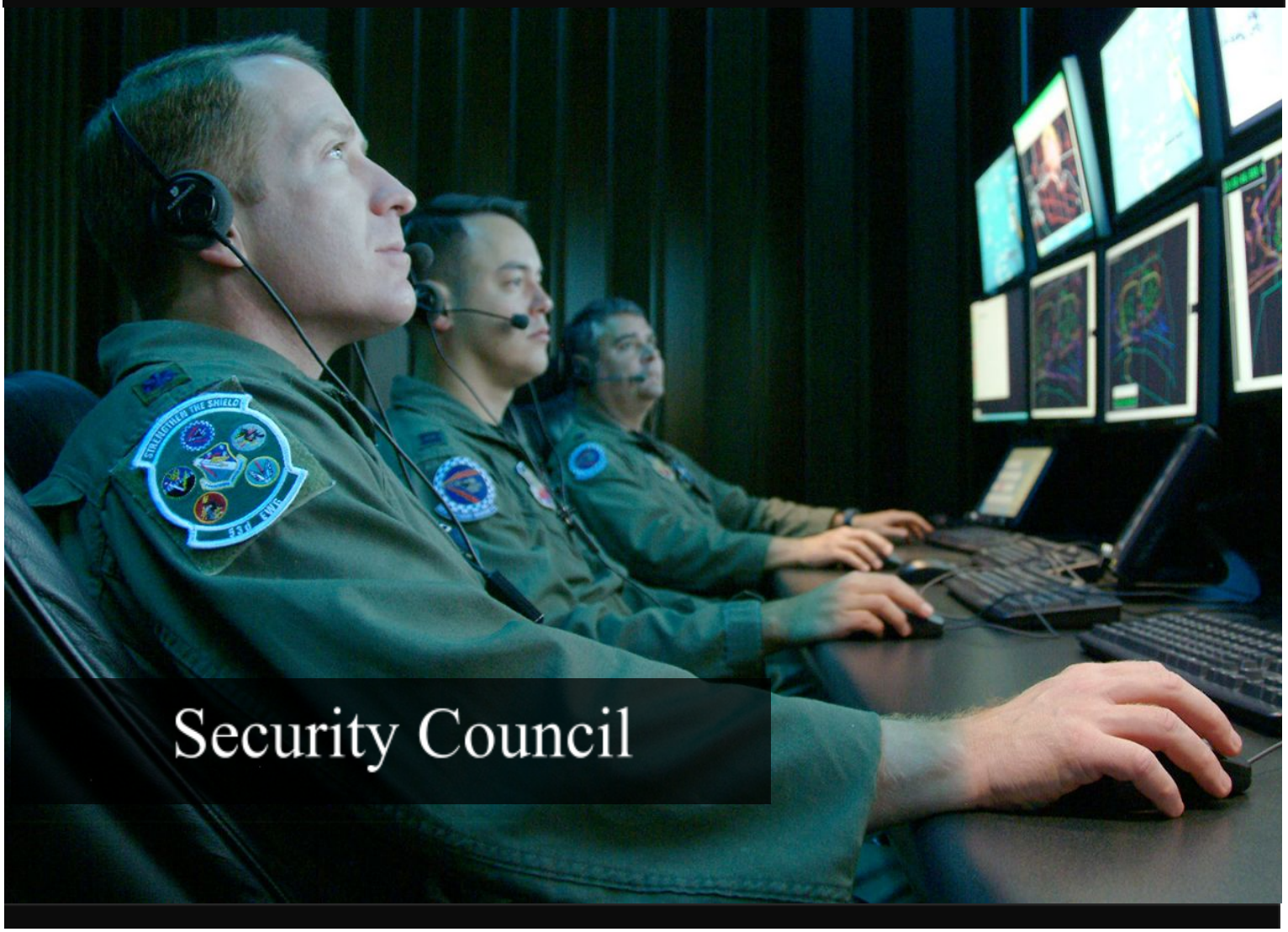
Surf City XVIII

Huntington Beach High School



Security Council

Topic A: Cyber Warfare

&

Topic B: Militarization of the Arctic

Mark Heine

Michael Rubly

Sam Shaw

Welcome Letter

Dear Delegates,

On behalf of the Huntington Beach High School Model United Nations Program, we would like to welcome you to our Surf City XVIII advanced conference!

Our annual Surf City conference upholds the principles and intended purpose of the United Nations. Delegates can expect to partake in a professional, well-run debate that simulates the very issues that those at the United Nations discuss every day. Both novel and traditional ideas will be shared, challenged, and improved.

It is our hope that all delegates will receive the opportunity to enhance their research, public speaking, and communication skills as they explore the intricacies of global concerns through various perspectives, some of which may be very different from their own. We hope their experiences here give them new insight and values that they can apply outside of the realm of Model UN for the betterment of the world community.

Although we will be entertaining a new style of a virtual conference, we hope all delegates will experience a fruitful and enhancing debate. Please do not hesitate to approach our Secretariat or Staff Members with any questions or concerns that you may have throughout the day. We wish the best to all our participants and hope that they may share a fulfilling experience with us! Enjoy the conference.

Sincerely,

Summer Balentine
Secretary-General

Jenna Ali
Secretary-General

Kayla Hayashi
Secretary-General

Hailey Holcomb
Secretary-General

Meet the Dias

Michael Rubly

Hello Delegates! My name is Michael Rubly and I will be your head chair for Security Council, Surf City 2021.This is my Senior year in high school and fourth year in MUN. I've been spending my past four years surfing our beautiful coastline, beating Mark Heine in MUN (by a landslide), and playing guitar in Huntingon's performing arts program: MMET. I also enjoy listening to and playing music, especially from songs by Pink Floyd. Over my past 13 conferences, I've spent five of them in Security Council and even chaired this committee last year. I wouldn't say that I have fallen in love with those three minute speeches, but the topics do speak for themselves. Security Council gives everyone an opportunity to speak on some of the world's most pressing and intriguing issues. With that being said, I am very excited to be your chair in Security Council and cannot wait for committee!

Mark Heine

Hola delegates! My name is Mark Heine, and I am a commended MUN delegate with four years of success to my name. Aside from MUN, I enjoy spending my time taking long walks on the beach, playing the drums, and singing in APA's MMET program. You may also recognize me as the libero on Huntington's varsity volleyball team. I am quite a man of the community, participating in National Honor Society, the Spikeball club, and the critically-acclaimed HBHS "Campus Update" team. If I have any advice for delegates, I would recommend not wearing glasses because we can see you're reading off your speeches if you do. I can already smell the raw potential of you delegates, so I can't wait to see what you have to offer!

Sam Shaw

Hello everyone! I am Sam Shaw and this is my 3rd year of MUN. My current hobbies include running, purchasing an unhealthy amount of either Postmates, Doordash or UberEats, drinking an ungodly amount of coffee, procrastination, playing lots of Amongus, and being a horse girl...well kind of. I enjoy listening to all kinds of music (except country...do not even get me started) ranging from Destroy Boys to Frank Ocean, and cannot wait until concerts come back! I also love to cook however I hate doing dishes, hence my Postmates addiction. I fell in love with the Security Council my freshman year, and have been in it 3 times since! I am beyond excited to chair this debate and see what you guys can do!

All Papers are due on January 2, 2021 by 11:59pm to surfcity.sc@gmail.com

TOPIC 1: Cyber Warfare

BACKGROUND

In 1988, Robert Tappan Morris, a student at Cornell University, created the first computer worm transmitted via the internet. Initially intended to simply test the expanse of cyberspace, the worm mutated into a virus, replicating rapidly and enacting denial of service (DoS) errors on every device it reached. In the end, the damage was devastating. Although no harm was meant, up to $100 million in repairs became necessary due to the worm, and the world suddenly became aware of potential dangers that a world connected by the internet could initiate.

The following decades saw similar stories. The 1999 "Melissa" virus caused $80 million in damages, infecting Word documents and sending itself to unsuspecting users. In the same year, 15 year-old Jonathon James installed a backdoor into the Department of Defense servers, and later NASA, giving him the ability to intercept emails and confiscate software. It soon became clear that the threat of cyber attacks were not limited to personal computers and devices- the privacy of large corporations and national security was at stake.

Some of the most common examples of cyber attacks include espionage, DoS, sabotage, and propaganda. Cyber espionage is not necessarily an attack on a nation, but occurs when a nation uses technological means to gain intel on a populous or foreign country. There have been numerous cases of cyber espionage in recent times, including Chinese hackers targeting United States-based businesses, Russia's espionage attack against Montenegro in 2017, and Vietnemese group APT32 performing surveillance on ASEAN nations. Hackers performing cyber espionage gain access to emails, contacts, and internet activity. Cyber espionage is not limited to between nations, but also can be used by a nation to keep tabs on its own citizens. In 2013, Edward Snowden leaked classified NSA information on the U.S. government's PRISM program, which allowed legal government access to all American Yahoo and Google accounts. Hundreds of other documents were released, demonstrating the amount of control and influence the NSA, along with Australia's ASD, the UK's GCHQ, and Canada's CSEC programs, had unbeknownst to the public. Despite this discovery, nations around the world continue to spy on citizens in foreign nations as well as their own, and it may never be known the extent which others can access our personal information.

A denial of service error (DoS) or a distributed denial of service (DDoS) is an attempt to disrupt a server or network by overloading it with Internet traffic.[1] DDoS attacks utilize compromised devices to contribute to internet traffic, preventing legitimate users from visiting the site or server. Hackers typically use DDoS attacks on high profile sites, such as credit card payment gateways and banks.[2] In 2019, the Chinese government resumed use of the "Great Cannon," a DDoS tool, against a Hong Kong forum used for organizing Beijing protests. Their goal was to prevent protesters from accessing the tool, and discouraging dissent. Although DDoS attacks do not cause overall harm to the victim in the long run, it can be detrimental to privacy and digital freedom.

Sabotage in terms of cyber warfare refers to the interruption of essential systems such as power, water, fuel, and military operations. In military operations, communication is commonly targeted, aiming to disable, intercept, or alter transmitted information. One of the most famous examples of cyber warfare as means of sabotage is Stuxnet, a computer worm allegedly

developed by the U.S. and Israel to derail the Iranian nuclear program.[3] Stuxnet targeted Microsoft Windows in Iranian nuclear systems, monitoring the gas centrifuges used to make nuclear materials and offsetting them so they would essentially destroy themselves. Alongside nuclear systems, electrical grids have been identified as potential targets of attacks. Almost all societies run off electricity, making electrical grid disruption an effective way to impact a wide population in a single attack.[4] In June of 2019, the United States targeted Russian power lines in retaliation to voting intervention. A similar situation occurred in Ukraine, with power cut in Kyiv, commonly believed to be enacted by Russian hackers.[5]

In response to the growing threat of cyber warfare, many different defense systems have been established. Groups such as NATO and other world powers are developing their own protective measures, as the question is no longer *if* a cyber attack will occur, but when. The European Union (EU) has recently adopted their EU Security Union Strategy for 2020 through 2025, aiming to protect their citizens as well as firms.[6] The United States Department of Defense offers informational programs and courses for individuals and businesses to learn how to protect themselves online alongside their own guidelines.[7] Under Chinese cybersecurity law, all citizen information is made available to the government, allowing China enhanced control on what comes in and out of its cyberspace.[8]

International frameworks regarding cyber security have been established as well. In 2007, the International Telecommunications Union (ITU) launched the Global Cybersecurity Agenda (GCA), with the goal of encouraging international collaboration and protection.[9] It has fostered numerous initiatives including Child Online Protection, and assists member states to create their own legislation regarding cyber warfare and security. Under the Tallinn Manual Process, it has been established that international law does apply in cyberspace, and therefore so do regulations of war and retaliation.[10]

UNITED NATIONS INVOLVEMENT

The United Nations, as a whole, has recognized specifically that the rise of technology in our modern era can be both a benefit to society and an enabler of asymmetrical technological threats. Seeing the increase of this issue over the past decade and the expanded use of advanced technology in military and security systems, the UN has made it their priority to work towards managing this issue through international cooperation.

In the case of the General Assembly, they have made their mark in the terms of combating cyber warfare by implementing resolution 55/63 in 2001.[11] This was the first official step towards bringing this issue into light because the UN recognized that informational technology was being misused by criminals and fought to stop that action. But, it wasn't until 2010 that the GA took a huge step towards combating this threat when they implemented resolution 64/11.[12] Titled “Creating a Global Culture of Cybersecurity and Taking Stock of the Nation's Efforts to Protect Critical Information Infrastructures”, this resolution marked the GA’s goal of working towards global cooperation of cybersecurity. Also, it recalled their earlier resolutions of the 2000s due to a prodigious increase and change of technology over that decade. This change refocused the UN’s concerns towards combating the misuse of Information Communication Technology (ICT).[13] Discussions and resolutions combatting the misuses of ICTs are what heavily dominate the discussion of cyberwarfare today. But, as the Security

Council (SC), it is important to focus on this specific actions and history of the Security Council towards the topic of cyberwarfare.

It wasn't until 2017, at the "Hit the Ground Running" workshop in Finland, that UN Secretary-General Antonio Guterres specifically called for the Security Council to consider and prevent the many modern threats of cyberwarfare.[14] Before 2017, only one discussion had been held by members of the Security Council at the 2016 Arria-formula meeting in which council members were only encouraged to further their research and consideration of the misuse of ICTs.[15] But, today, the topic has only expanded in the scope of consideration for Security Council members. In 2019, the SC Panel of Experts discussed the major violation of cybersecurity and cyber attacks committed by Democratic People's Republic of Korea (DPRK).[16] This was marked as a vital incentive for the Security Council to further their discussions on the topic as the threat was only seeming to increase. Since then, the Security Council has worked tirelessly to prevent and counter cyberwarfare. It is important to note that the SC mainly focuses on issues that pose a large threat to our modern world. Seeing that this branch of the UN barely even considered this topic in 2016 and now it is at the top of their priority list; there is no question that the threat of cyberwarfare is only getting worse.

Technology is what our world so vitally uses for its most important aspects of communication and development. The Security Council has now decided that this threat needs to be put under control and that it is an obligation for framework to be put in place to further secure our world. The threat is increasing and the council is in action.

CASE STUDY: STATE-SPONSORED CYBER ATTACKS IN THE MIDDLE EAST

State-Sponsored cyber attacks, or cyber attacks that are led by countries against other private corporations or governments, have increasingly become a threat in the Middle Eastern region due to attacks from larger world powers such as North Korea and China, as well as a series of attacks centered around the actions of Iran. Cybersecurity firms such as FireEye cite these attacks as a major security concern for the Middle East and state that the most at risk nations are the UAE and Saudi Arabia. In July of 2019, Microsoft reported that ten thousand users had been attacked by state-sponsored hackers; they were later able to connect one out of ten of these affected users to an Iranian state-sponsored hacker.[17]

In late April 2020, Israeli media reported on a probable cyber attack on the water treatment and sewage facilities throughout the nation. Israel's Water Agency initially described this as a technical malfunction, but would later revise it to affirm that it indeed was a cyber attack. With the current state of the pandemic, there was little media coverage, besides that Israel would blame this attack solely on Iran. What appeared to be a counter-cyber attack from Israel would take place on May 9, 2020 on the Shahid Rajaee Port, a maritime trading hub near the Strait of Hormuz. This cyber attack was not directed at security systems, but instead was targeted at private corporations' operating systems. This attack caused substantial delays in traffic and shipping amongst the crowded maritime hub. While Israel did not take responsibility, the Israeli Defense Minister alluded that the attack on Iran could have very well been their doing.[18] A similar attack on Israel was initiated by the Iran-sponsored Islamic Revolutionary Guard Corps in May 2020, when Iranian hackers attacked Israelis websites that belonged to political organizations, corporations, and individuals.[19]

As state-sponsored terror attacks grew in popularity, another incident would take place involving Iran, in which Iranian hackers focused on the high profile Munich Security Conference in October 2020. During this attack, hackers targeted 100 extremely high profile German and Saudi individuals that were highly ranked in their corresponding nations for security. The hackers attempted to hack into these individuals' emails through fake invitations. According to the Microsoft Security Chief, this attack was committed with the intent to collect intelligence, and would affect several individuals who were responsible for shaping foreign policies within their nations.[20]

State-sponsored cyber attacks from the Middle East have had negative implications internationally as seen in the United States as well. Iranian hackers working for the Islamic Revolutionary Guard Corps reportedly attempted to interfere with the 2020 election by sponsoring a cyberattack in which they would hack into governmental voter registration records to launch a series of intimidating emails at voters. In retaliation, the US General of Cyber Command, Paul Nakasome, finalized a defense strategy coordinated between social media companies, private sectors, as well as foreign allies.[21]

The overabundance of Iranian state-sponsored cyber attacks has been cited by cybersecurity firms such as BAE Enterprise as an Iranian assertion of military domination.[22] Military dominance is perceived as vital in Iran, as evidenced by the fact that Iran has the largest standing military in the Middle East.[23] The cyber dominance displayed by Iran could have severe implications on the Middle East. As many of these attacks have been motivated by the desire for increased geopolitical influence, there arises the probable reality of Iran corruptly influencing the legislation and stability of nations globally.

With internal threats to the cyber stability of the Middle East on the rise, there is also substantial concern of external threats from world powers. This was seen as early as January 2020, when Turkey attacked 30 organizations across Europe and the Middle East including embassies, governmental ministries, security forces and private corporations. Hackers sought to intercept internet traffic in order to obtain access to specific information found on classified governmental websites. Although unconfirmed by Turkey, British and US officials stated that this attack was characteristically similar to state-sponsored cyber espionage missions created in order to further the state's interests.[24]

Additionally, in August 2020, Israel would thwart a cyber attack from North Korean hackers that posed as Boeing officials on Linkedin messages to a senior official of a corporation that produced weapons and intelligence for the Israeli government. After these initial Linkedin messages, hackers proceeded to ask for emails and phone numbers, and to connect through WhatsApp while continuing to mimic aerospace companies like Boeing. The hackers would finalize their operation by sending the Israeli targets files containing spyware. Concerns were raised by Israeli officials that this attack could have been motivated by the alliance held between North Korea and Iran, and was made to provide Iran with classified information on Israel.[25]

QUESTIONS TO CONSIDER

1. Think about cyber warfare in terms of your own country. How does this topic affect your country and the security of your citizens? What measures will you take to stop it?
2. Seeing that this crime can take place anywhere, has your nation been involved with breaching the security of others?
3. Should cyber warfare be an issue addressed by international groups such as the UN, or solely at the domestic level?
4. Has your country specifically sponsored any cyber attacks? If so was it justified, and how would this affect your country's stance?
5. Consider cyber security on a governmental level as well as a civilian level. What different things can be done to ensure the security of both areas?
6. What have technology companies done on their own to enhance cyber security, and how can countries add on to these efforts?
7. Where does cyber warfare fall in terms of existing legislation regarding warfare? Does this need to be redefined to adapt to the expanse of cyberspace?

TOPIC 2: Militarization of the Arctic

BACKGROUND

When the term "militarization" is brought up in today's day and age, many relate its definition to the harsh standpoint of the South China Sea, the increase of armed forces in the Middle East, and even the proliferation of weapons in the DPRK. But one of the most pressing and concerning topics having to do with our world's increase of national security does not occur in the far east nor the west. This militarization occurs in the Arctic. Today, the increased militarization of the Arctic as a result of newly founded resources in the region has captured the interests of nations who have claimed territory in the Arctic Ocean. The Arctic Five consists of Canada, the United States, Russia, Norway, and Denmark, as well as Finland, Sweden, and Iceland. These nations in which all have had involvement in militarizing the desolate north have now sparked the dilemma we are experiencing today. Although their actions upon this region do date back to post World War II, it wasn't until the fall of the Soviet Union in which the militarization of the Arctic began to take its place as a discussion topic for the international community.[26]

The increase of military personnel throughout the 20th century caused the formation of the Arctic Council in 1996.[27] With the purpose of regulating this region regarding concerns such as the environmental effects, indigenous reservations, and wildlife conservation, the Arctic Council acted as the first ever official treaty towards the conservation of the Arctic. Although the council was enacted in 1996, it wasn't until 2007 that the Arctic became immensely accessible to the Arctic Five as a result of the opening of Northwest Passage. As an effect of global warming, the Arctic has lost over 70% of its ice within the past 30 years, providing an influx of new territory and resources that have a calculated worth of over 17 trillion dollars.[28] The interests of the Arctic Five were then changed from not only militarization, but now to the utilization of the Arctic's many newfound resources.

The increased exploration in the Arctic by its bordering countries has led to tension between the Arctic Five due to the vast demand for territory in the region. This tension has caused countries to make controversial and threatening moves. Russia, accounting for 53% of the Arctic coastline while acting to be the most prolific on militarizing the region, announced its plans in 2017 to implement 100 new bases within the region over the next 10 years.[29] Furthermore, the dominant nation has also incentivized its oil and energy corporations to further extract resources in the north by offering 40 billion dollar tax cuts to any company willing to expand its facilities into the Arctic.[30]

Seeing the actions of its former enemy, the United States, arguably containing the smallest stretch of coastline in the Arctic, has also joined the race towards gaining territory in this newly discovered region. In 2015, Shell confirmed its plans to invest over 15 billion dollars into drilling and searching for oil in undiscovered deposits.[31] With its main focus revolving around the collection of resources amid the early 2010s, the U.S. made a daring move. After 30 years of minimal military action in the Arctic, the United States Navy began to patrol the Barents Sea (a Russian exclusive economic zone) with the carrier Harry S. Truman in 2018 and a surface action group patrol in 2019.[32] These actions by the U.S. were seen as both an infringement upon

clearly slated territory and a threat to the security of not only Russia, but the rest of the Arctic Five.

Seeing that global warming is only getting worse and opportunities to gain land in the Arctic are increasing, it can be predicted that this issue will only exacerbate. The concerns and actions of the Arctic Five have been purely based around gaining land, increasing security, and utilizing the Arctic's resources for their own good. Unfortunately, the significant increase of action in the Arctic, especially the use of the Northwest Passage, has proven to have crucially harmed the many indigenous groups who have formerly occupied the region. As of today, over 10,000 members of the Sami tribe in Norway have been forced to relocate due to climate-induced melting of ice and increased military action in the Arctic. Even worse, Russia's militarization efforts have shown their very own Yakut tribe "strong opposition by the authorities [and] manifested in complete disregard for indigenous peoples and violation of their lawful rights and interests" (Lothe 13).[33] Tribes that used to reside in the Arctic Region for hundreds of years are now being infringed upon by the aggressive moves of their so-called neighbors.

In the end, the militarization of the Arctic has proven to be a very prevalent and violent issue. Over the past ten years, the culmination of personnel in the north has multiplied from when it began decades ago. This prideful expedition into the unknown has now turned into a violent expression of proliferation and power. Although the Arctic Council has been hard at work to control the actions of the Arctic Five, there has been little evidence that any considering efforts have been shown by the most active nations. Furthermore, this issue will only get worse in the coming years, and the addition of any military actions will add on to the detrimental environmental effects in the Arctic. The modern militarization of the Arctic has proved to be more effective than predicted and is nowhere close to coming to a halt.

UNITED NATIONS INVOLVEMENT

Due to the increasingly prevalent nature of the topic, the United Nations has been extremely attentive towards militarization in the Arctic Regions. The UN regulates the Arctic through Exclusive Economic Zones (EEZ's) originally established by the United Nations Convention on the Law of the Sea (UNCLOS). The EEZ's are contained to 200 nautical miles from the coast of an Arctic nation, giving the country exclusive rights to exploring and exploitation of resources.[34] Nations can file for a re-evaluation of their EEZ with the UN, which has led to some ambiguity as to exactly where the 200 miles begins. In order to do so, nations must create a three-dimensional map of the ocean territory that they wish to add and gather data on the resources it provides. Currently, the UNCLOS does not outline clear guidelines regarding disputed territory, leaving it up to the nations themselves to resolve issues.

Another of the main shortcomings of the UNCLOS is its lack of legislation regarding indigenous peoples in the Arctic. Under the current legislation, nations are granted the power to completely control indigeneous populations, consequently leading to controversial issues of land ownership and human rights. An estimated 10% of all Arctic land is occupied by indigenous people, and as nations look to expand further, more conflict will occur.[35]

The UNEP has also been very involved in the Arctic region in order to address the increasing industrialization. The General Assembly document A/63/25 addresses the escalating impact of climate change on the issue and works to encourage research in the Arctic Circle.

Additionally, the Protection of the Arctic Marine Environment (PAME) was established as an Arctic Council working group which collaborates with UNEP to identify major environmental issues. This group has created regulations regarding protected marine zones and shipping routes to help ensure that the environment is not degraded due to increased use.[36] Indigenous peoples are also greatly affected by climate change as they have learned to live off the land and are facing major consequences due to expansion in the Arctic region. It is clear that the current international legislation in place has been somewhat effective in the initial stages of Arctic development, yet the future holds much uncertainty.

CASE STUDY: EFFECTS OF CLIMATE CHANGE ON MILITARIZATION OF THE ARCTIC

Since 1980, the rate of global warming has gone up to 0.18 (degrees Celsius) per year, twice as much as the previous rate.[37] In the Arctic specifically, it has become extremely evident that a crisis is bound to occur, as the Arctic sea ice is disappearing at a rate of 13.1 percent per decade.[38] Sea levels continue to rise, thus inciting an international sovereignty crisis, as the very claims people and countries have to this land are being eroded away before their eyes. With less ice, there becomes more of an incentive for larger ships to come to the Arctic for trade and likely proliferation of militarization to follow. In fact, it is predicted that with the melting of ice in the Arctic, trade routes will decrease by 3,000 to 4,000 miles for European and Asian nations.[39]

Russia, a vast majority of the Arctic Circle, has reportedly been warming at a rate 2.5 times greater than the rest of the world since the 1970s. With effects of climate change expected to increase exponentially by 2030, international agencies such as the CSIS have reported on how Russia plans to use these freer waterways for their own agendas. Currently, the Northern Sea Route (NSR) is viewed by Russia as a domestic route, while the rest of the international community views this as a route for the whole world.[40] With melted ice, Russia plans to use the waterway solely as a domestic waterway, despite the prospect of increased and better international trade through the expansion of trade routes.

Opposing Russia's view, China has unveiled plans for a "Polar Silk Road" to be utilized as more ice melts in the Northern Sea Route. Currently, China utilizes trade routes that are inefficient and go through the Indian Ocean in order to deliver products to Europe. With the freeing up of trade routes throughout the Arctic Circle due to melted ice, China plans to launch large infrastructure projects through the Belt and Road Initiative to facilitate a trade route like the Silk Road and further connect Europe and Asia. [41]

Despite this project's opposition to Russia's view of the Arctic as a Russian entity, China and Russia have worked together on furthering infrastructure that could have detrimental implications for the sensitive environment, especially after more ice melts. These have included the development of the Payakha oil field in 2019.[42] While profitable, climate change poses a severe threat to the pressurized tubes found in this intricate, five billion dollar infrastructure project. With the melting of permafrost severely increasing, oil spills have become a severe threat. An example of this is the oil spill in Norilsk that spilled 17,500 tons of diesel oil due to melting permafrost. This oil spill specifically is estimated to take over 30 years to clean, and the further environmental implications of others with increased infrastructure could have severe international consequences. Additionally, larger nations have long held dependencies on Russia

for their natural gas and oil trade, most of which they would achieve from the Arctic's rich resources. With infrastructure projects such as these, the potential for increased military tensions with Russia in the Arctic arises.[43]

Another area for concern is the proximity of Russia's nuclear arsenal to the NSR. With more and more ice melting, ships taking the enlarged NSR could come into close contact with Russia's Novaya Zemlya arsenal. Contained within this arsenal include the Soviet nuclear powered submarines with ballistic missiles. Although the United States has created hypersonic technology with the capabilities of tracking these submarines, the effects of melting ice have not been fully researched.[44] Much of Russia's military activity involves protecting its nuclear reserves on the Kola Peninsula within the Northern Sea Route, which could pose a serious threat as the extent of the NSR broadens due to melted ice. Protecting the Novaya Zemlya nuclear arsenal specifically is the Northern Fleet, a group specifically from Russia's Navy.[45] In recent times, this fleet has worked to assert Russia's claims to this area through tests of hypersonic missiles and nuclear underwater drones. As more ice melts, the Northern Fleet can likely take advantage of the GIUK-N(Greenland-Iceland-United Kingdom) Gap in order to intercept NATO communication.[46]

To further assert Russia's dominance, Russia has given nuclear weapon company Rotacon claims to the NSR. Larger powers, including senior US military officials, have expressed utter concern over Russia's increased nuclear presence in this area.[47] With 39 nuclear powered vessels and 62 nuclear reactors, numbers that are only expected to increase, the Arctic Circle is projected to be the most nuclearized waters in the world by 2035, topping even the South China Sea where active territorial disputes are occurring currently. Not only has this raised concerns for possible military conflict similar to the Cold War in this region, but also has elevated environmental concerns. This is due to the fact that Russia has a poor history with managing nuclear products, as seen in the Chernobyl meltdown in 1986.[48]

With Russia claiming their control of the Arctic sea passages, tensions are bound to occur as the region is shaped into an international waterway, as previous boundaries held by glaciers are melted away. With that said, the positive possibility of allowing a restart to relations over control of the Arctic is provided with the reshaping of the current landscape.[49]

QUESTIONS TO CONSIDER

1. Should the United Nations Convention on the Law of the Sea continue to dictate the actions of the Arctic Five? If not, what other body does your nation see as a qualified alternative?
2. What can your country, or the international community as an entity, do to prevent the issue of militarization and industrial proliferation in the Arctic Sea?
3. Overall, what is your country's stance on the infringement indigenous properties by countries who onced vowed to protect them?
4. Even if your country is not a major player or near the Arctic region, how do the actions and demands for resources by the Arctic Five affect your country socially, politically, and economically?
5. Does your country have any claims to the Arctic? If not, how could your country's relationship with other nations that do have claims affect your perspective?
6. Arctic nations are under attack for the invasion of indigenous rights. What more could countries do to satisfy the needs and preserve the culture of the indigenous Arctic communities?

Endnotes

1. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
2. https://en.wikipedia.org/wiki/Denial-of-service_attack
3. https://en.wikipedia.org/wiki/Stuxnet
4. https://energycentral.com/c/iu/how-and-why-power-grid-cyberattacks-are-becoming-terrorists-go
5. https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/
6. https://ec.europa.eu/digital-single-market/en/cyber-security
7. https://business.defense.gov/Small-Business/Cybersecurity/
8. https://www.chinalawblog.com/2020/10/china-cybersecurity-no-place-to-hide.html
9. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
10. https://ccdcoe.org/research/tallinn-manual/
11. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
12. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211
13. https://www.un.org/disarmament/ict-security/
14. https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php
15. https://www.securitycouncilreport.org/un-security-council-working-methods/arria-formula-meetings.php
16. https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf
17. https://www.thenationalnews.com/iran-led-state-sponsored-attacks-remain-a-major-threat-to-middle-east-stability-1.906752
18. https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/
19. https://www.timesofisrael.com/cybersecurity-groups-iranians-targeted-top-israeli-firms-in-ransomware-attack/
20. https://apnews.com/article/germany-hacking-iran-email-saudi-arabia-807fe633c5388341f19a050414f65669
21. https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html
22. https://www.mei.edu/blog/cyber-conflict-middle-east-considerations-future
23. https://www.mei.edu/blog/cyber-conflict-middle-east-considerations-future
24. https://www.reuters.com/article/us-cyber-attack-hijack-exclusive/exclusive-hackers-acting-in-turkeys-interests-believed-to-be-behind-recent-cyberattacks-sources-idUSKBN1ZQ10X
25. https://eurasiantimes.com/north-korea-cyber-attacks-israel-steals-classified-data-which-could-be-sold-to-iran/
26. https://thediplomat.com/2013/10/the-creeping-militarization-of-the-arctic/

27. https://2009-2017.state.gov/e/oes/ocns/opa/arc/ac/establishmentarcticcouncil/index.htm
28. https://www.theguardian.com/world/2012/jul/22/arctic-ice-melting-oil-drilling
29. https://www.thearcticinstitute.org/russias-arctic-military-and-security-part-two/#:~:text=In%20August%202007%2C%20Russia%20resumed,Russian%20military%20in%20the%20Arctic.
30. https://www.cnbc.com/2019/12/27/russias-dominance-in-the-arctic.html
31. https://www.bbc.com/news/business-31034870
32. https://www.defensenews.com/naval/2020/05/11/the-us-navy-returns-to-an-increasingly-militarized-arctic/
33. http://www.arctis-search.com/Indigenous+Peoples+Rights+in+the+Arctic
34. https://www.un.org/Depts/los/convention_agreements/texts/unclos/part5.htm
35. https://www.arcticcentre.org/EN/arcticregion/Arctic-Indigenous-Peoples
36. https://www.unenvironment.org/explore-topics/oceans-seas/what-we-do/working-regional-seas/regional-seas-programmes/arctic-region
37. https://www.bloomberg.com/graphics/climate-change-data-green/temperature.html
38. https://climate.nasa.gov/vital-signs/arctic-sea-ice/
39. https://www.fraserinstitute.org/article/meeting-russias-arctic-aggression
40. https://climateandsecurity.org/2020/08/emerging-threat-as-the-arctic-melts-russian-plans-to-militarize-could-create-a-nuclear-hotspot/
41. https://www.interactioncouncil.org/media-centre/polar-silk-road
42. https://www.maritime-executive.com/editorials/china-s-arctic-silk-road
43. https://www.maritime-executive.com/editorials/china-s-arctic-silk-road
44. https://warontherocks.com/2019/11/the-icebreaker-gap-doesnt-mean-america-is-losing-in-the-arctic/
45. https://jsis.washington.edu/news/the-impacts-of-climate-change-on-arctic-security/
46. https://www.csis.org/features/ice-curtain-russias-arctic-military-presence
47. https://www.fmprc.gov.cn/mfa_eng/topics_665678/xjpfwzysiesgjtfhshzzfh_665686/t1076334.shtml
48. https://www.planetarysecurityinitiative.org/news/nuclearisation-russian-arctic-new-risks
49. https://outrider.org/climate-change/articles/new-arms-race-arctic/