General Assembly, First Committee
Disarmament and International Security (DISEC)

Background Guide

Written By: Colby Saxton, Madeline Myers, Rishik Hombal, & Jon Arms, Case Western Reserve University

The United Nations puts the Disarmament and International Security Committee (DISEC) as the first committee. With being the first committee the focus is on dealing with disarmament, challenges on a global scale, and threats to peace that jeopardize the the balance of peace within the international community. The goal of the committee is then to find solutions to problems that threaten any aspect of the international security stage. The committee specifically reviews all disarmament and threats to international security, that are within the scope of the Charter of the United Nations, or any other body within the United Nations. The committee when faced with an issue it will be guided by the principles of cooperation and as well as maintaining security and peace on the international stage. The committee will also regulate armaments, promote cooperative arrangements, and aim at finding stability in the lower levels of armaments ("UN General Assembly - First Committee - Disarmament and International Security").

Topic A: Restricting the Use of Cyber Warfare

Statement of the Issue

As a continuously developing world we are faced with the problem of technological development and our interconnectedness with each other. The software of the camera in our computers can be hacked, our bank accounts, and worst of all our Netflix accounts. While modernization in technology, has brought so many benefits to the military such as better sensing systems for incoming attacks, or new guns who have better aim that, it has also introduced a new method of warfare. We are use to conventional means of warfare that uses guns, cannons, that are used man to man with little to no sure barrier in between. With the modernization of technology, new warfare has taken effect where weapons are easier to use and are more lethal at the same time. The push of a button can shutdown an entire sensor system and cause a country to be unprepared for attack. The absence of the individual allows for it to be easier to kill, by not being in the presence by using the technologies of cyber warfare. According to RAND Corporation a nonprofit, nonpartisan organization who specializes in military
research, cyber warfare, “involves the actions by a nation-state or international to
attack and attempt to damage another nation’s computers or information network”. Cyber warfare can happen anywhere from a desk to a couch to a bed. It is so easy
to do and can be done anywhere, which is why restrictions need to be put in place. It is the duty of the United Nations to put forth restrictions on the use of cyber
warfare to prevent the remorseless massacre of humanity.

History

Any attack on a country, virtual or in reality, that causes harm on another
country allows for the victim to respond in defense. However, with cyber warfare
since there is not always lethal damage when attacked, how does someone protect
themselves. By knowing when it is appropriate to react to a cyber attack,
preemptive wars can be prevented. Since the internet has been a creation in the
last two decades, cyber warfare has become a more recent issue with little
legislation, despite the atrocities that it can cause. The United Nations, within its
own charter took a stance on the issue of defense way before the internet when it
passed in 1945, with Article 51. Article 51 states that a nation can defend itself, if
an attack reaches a level of force that requires an “armed response”. With this in
mind if a cyberattack reaches a level where arms are necessary to diffuse the
attack, then they can be used. The United Nations, in 2012 appointed 15 experts to
regulate cyberspace law, that resulted from the report called, “On the
Developments in the Field of Information and Telecommunications in the Context of
International Security”. These experts were very unhappy with the vagueness of
Article 51, and kept the investigation going on how to further restrict such warfare.
In 2013, the United Nations worked to further prevent the use of cyber warfare in a
report from the committee of 15 experts called, “ who insisted on the creation of a
“peaceful” environment of Information and Communication Technology (ICT) (Arms
Control Association).

The reason for such a creation came out of the rise of cyber attacks that
began in the last decade, that started back in 2006. In 2006, the United State’s
National Aeronautics and Space Administration had to block a hack attempt from an
unknown server who had found their launch codes. In 2007, China’s Ministry of
State Security found 42% of foreign hackers came from Taiwan, and 25% were
from the United States who were stealing confidential information of the
government. There would be a jump in the lethality in cyber attack, which can be
seen in 2010 when the Stuxnet attack occurred, which was when Siemens had a
virus that shut down all of the control systems in Iran and Indonesia. It was
believed to be a program started by the United States government in order to
interfere with Iran’s nuclear program. Fast forward to October 2012, one of the
largest worldwide cyber attacks called, “Red October” was discovered which was
when government agencies, embassies, military institutes, and energy producers all
over the world had been hacked. The information was collected through Microsoft’s
Word and Excel programs, with the majority of victims being in Russia and Asia, with victims also being reported in western European countries and the United States (NATO). Even though the world looked grim 6 years ago with the technology of then, technology has only gotten more complex and caused more tragedy. It is time to make deadly cyber warfare a fad of the past.

Current Situation
Currently, cybersecurity has undergone growing pains over the advent of emerging technologies and the growing attack capabilities of Nation-state actors. First is regarding the emergence of new technologies such as the Internet of Things and Artificial Intelligence. The Internet of Things is defined as the interconnectedness via the internet of computing devices in everyday objects, enabling them to send and receive data. Ranging from all aspects of military devices to home appliances, many things have become “smart” and can now send data to one another. This interconnectedness leaves many new avenues in which hackers can breach the confidentiality of systems. Since the small computers transmitting data in new devices have limited processing power, this leaves the systems equally limited in their defense capabilities to prevent breaches. Thus hackers are able to observe data which they are not authorized to view, delay transmissions, obstruct processes and even alter data in magnitudes never seen before.

Artificial Intelligence has equally obstructed the current status of cybersecurity in recent years. In the past, cybersecurity professions have been able to hold back hackers by putting in place mechanisms which require time consuming human interaction. However, with increasing processing power and the prospect of Quantum Computing as well as the growing intelligence of computer systems, hacking into previously un hackable systems has become more frequent. The combination of quantum computing in association with Artificial Intelligence allows potential hackers to overrun systems through sheer processing power and adjustments made by artificial intelligence. Cybersecurity systems and policies put in place by countries will have to account for the growing vulnerabilities of their current infrastructure.

Emerging hacking attacks by nation-state actors have increased the need of modern cybersecurity policies. A recent study has shown that the majority of cyber attacks completed against companies of all sizes are done by nation-state actors. These actors are cited as either direct state employees or government hired contractors. Recent countries under fire for alleged state-sponsored cyber attacks are Turkey, North Korea, United States, Russia, China and Iran. These countries have been lambasted for roles in cyber attacks recently, however the global response has been cited as having an unproportionally staunch response as stated by cybersecurity policy experts. Attacks have been targeting various sectors: intellectual property, malicious digital traffic, black markets, financial data, political
information and user data. Current repercussions of attacks are limited as it is
difficult to gather enough information for formally connect attacks to nation-states.
Thus attacks may incur millions or up to billions of US dollars in cost, however may
never yield an International response through the UN under current law. With the
financial cost of cyber attacks expected to rise along with the growing connected
environment and hacking capabilities of computer systems, cybersecurity has
reached a time of paramount importance for the UN to address.

Works Cited
"Cyber Warfare." RAND Corporation Provides Objective Research Services and
Public Policy


Review, NATO. "The History of Cyber Attacks - a Timeline." NATO Review,

"UN General Assembly - First Committee - Disarmament and International
Security." Welcome

"The UN Takes a Big Step Forward on Cybersecurity | Arms Control Association." Arms Control

Association | The Authoritative Source on Arms Control Since 1971,
www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cy
bersecurity

“Nation-State Actors Responsible for Most Cyber Attacks.” ComputerWeekly.com,
-for-most-cyber-attacks.

Browne, Ryan. “Weaponized Drones. Machines That Attack on Their Own. 'That Day
Is Going to Come'.” CNBC, CNBC, 25 July 2018,
bersecurity.html.

BaigMar, Anas. “Top 5 Countries Where Cyber Attacks Originate.” Security Today,
securitytoday.com/articles/2017/03/03/top-5-countries-where-cyber-attacks-originate.aspx.

Fruhlinger, Josh. “What Is a Cyber Attack? Recent Examples Show Disturbing
Trends.” CSO Online, CSO, 7 Mar. 2018,
www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cybe
r-attack-recent-examples-show-disturbing-trends.html.

Teplow, Lily. “Empowering Your MSP Business to Grow and Prosper-One Post at a
Time.” 6 Important OS Hardening Steps to Protect Your Clients,
www.continuum.net/blog/the-financial-consequence-of-a-cyber-attack-is-wor
sening-chart.
Topic B: Protecting Trade from Somalian Pirates

Statement of the Issue

As a young child many of us are taught not to steal, whether it be from family, friends or even neighbors. The idea of stealing was one that was to see consequence with very little benefit, almost making an “Axis of Evil” cameo. However, what if stealing was used as survival so that people could have something to eat, and provide for their family? Is it still wrong? Unfortunately, as much as we want to see humanity thrive we must face the harsh reality that stealing is still wrong. Especially when stealing is going to affect the economies of two countries who are trading goods with each other. It may seem impossible to do, but Somalian Pirates have managed to get it down to a science. Somali Pirates will attack ships who are amidst trading with each other to steal goods, that they can sell elsewhere to make money as well as take hostages to make negotiations with local governments. According to the non-governmental organization Oceans Beyond Piracy (OBP), the Somali pirate hijackings have increased over the past few years. This can be seen in the jump from 54 attacks in 2015 to 95 attacks in 2016. The report also showed that the amount of hostages taken in 2015 and held for ransom, was 44 whereas in 2016 the amount had jumped to 96 (Kieron Monks). Unfortunately, these attacks are getting deadlier, and more frequent. Thus it is the duty of the United Nations to put forth restrictions to protect trade and the high seas from Somali Pirates.

History

Pirates have often been a myth of our favorite tales fighting in Neverland or even being portrayed by the hot Johnny Depp. As much as these stories invoke our imagination, pirates have created a miserable reality for many over time. Pirates have been attacking the Straits of Malacca, the Caribbean, and many other high seas for centuries. Stories of pirating have dated back to, first century AD, in *Periplus of the Erythrean Sea* as well as in *Geographia*, by Claudius Ptolemy in 150 AD (“Pirates of Puntland, Somalia”). Unfortunately the United Nations was not created until 1947, so it could have not been able to help stop and prevent these attacks. However, no since it is a world governing body it can get involved. The United Nations has passed legislation fighting piracy on the high seas in the 1982 *United Nations Convention on the Law of the Sea*. This convention set up the legal framework for combating piracy as well as put a system in place on how to assist nations facing piracy. Since the crisis in Somalia has been very rampant, the United Nations has been working with the Contact Group on Piracy off the Coast of Somalia to help find an appropriate response. This group has been extremely helpful in
advising the Security Council when it the attacks of the Somali Pirates has raised international security concerns. The efforts made by the Contact Group on Piracy off the Coast of Somalia as well as the United Nations and Security Council all have been regulated by the United Nations Assistance Mission in Somalia (“Piracy”). This is just the institutions that have been put in plan to regulate, now let’s look at what processes have been put in place to combat these pirates.

There have been several resolutions specifically passed by the United Nations in order to combat Somalian Pirates. The first piece of legislation that was passed was Resolution 2077, that secured the support of military forces to help fights against the pirates. Resolution 2077 also set in place prosecuting measures for pirates that are captured. However, since the status quo was new for the United Nations to help support fight against the Somali Pirates, Resolution 2077 was set up to only last a year. Once that year was up the United Nations Security Council would again renew their support of ground troops to help fight the pirates with passing Resolution 2125. The next resolution to be passed in order to support the fight against the Somalian Pirates would be in 2017, which was Resolution 2383. Resolution 2383, would again commit ground troops to fighting the Somali Pirates, but would also expand support to naval forces for combat as well (“UN Documents for Piracy”). This resolution was also set to be up in one year, so it will be interesting to see what the United Nations does going forward. This is a great chance for you to make a difference in policy, and we cannot wait to see what solutions you come up with. The United Nations needs your help to fight the Somali Pirates and protect the high seas! Good luck everyone!

Current Situation

Currently, Somali Pirate attacks have been on the upswing. The number of attacks on merchant and commercial vessels peaked in 2007 with 8 attacks. The number of attacks since has been decreasing, such that between 2013 and 2017 there were no recorded attacks. However, since then, there has been two attacks in 2017 and one attack in 2018.

The first attack in 2017 was a hijacking of a large commercial vessel off the coast of Somalia. The commercial vessel was boarded by 24 pirates and subsequently anchored where they remained demanding ransom. However, after intervention by powerful Somali business people, the pirates departed from the ship and left the crew unharmed.

The second attack in 2017 was another hijacking led by 3 Somali pirates. This attack triggered a security alert in the area, where Indian and Chinese navy ships were nearby. The commercial vessel was boarded and retaken by Chinese navy personnel.
The most recent attack occurred in 2018 where two pirate vessels opened fire on a commercial ship. After a brief firefight, the pirates escaped without any further engagement.

Although the nature of the attacks listed above are not as serious as in previous years, this problem still remains at the forefront of International Security.

Analysis

At the core of these attacks, lies many different factors playing into this increase in attacks. The first of those reasons is lower adherence to international safety standards. The first of which complacency by commercial vessels. Between 2013 and 2017 when there were no large commercial attacks, many companies began to roll back many of the safety measures that they had used to put in place. For example, in the first attack of 2017 described above, the targeted vessel was sailing slow and close to the shore, which makes it an easy target for attacks. Had the ship followed the industry’s Best Management Practices, the attack might have been avoided. In addition to this, there needs to be greater coordination between International Security Forces, individual countries’ Navies and security forces aboard Commercial Vessels. Greater coordination may lead to better prevention measures as well as faster response times to incidents.

The second main issue causing the increase in attacks is the deteriorating condition of the Somalian Government. To be more specific, this issue has manifested in reduced policing of the Somalian Coast Guard off their coasts. Additionally, the government is in need of modern pirating prevention legislation as well as greater coordination with other navies and security forces to create a comprehensive security policy.

Additional socio-economic problems have been continuing to fuel pirating. Famine, poverty and illegal fishing in Somali water by international parties has caused more pirating activity. Although Somalia has been dealing with high poverty rates for decades, more recent famines have been exacerbating current conditions.

Conclusion

With growing frequency of Somali Pirate attacks in the recent years, the UN is designated to attempting to curb this growing problem. With limited coordination and legislation to effectively combat modern Somali Piracy, it is up to this committee to determine the proper course of action.

Questions To Consider

- How can we create greater coordination between the Somali Government and International Actors?
- How can we reduce illegal fishing in Somalian waters?
- What are the ways in which we can create better collaboration between vessel security crew, state navies and International bodies?
- How can the UN mitigate long term poverty and famine issues in Somalia?

Works Cited


"Pirates of Puntland, Somalia | Origins: Current Events in Historical Perspective." Front Page |
Origins: Current Events in Historical Perspective, origins.osu.edu/article/pirates-puntland-somalia.


