JHUMUNC

Johns Hopkins Model United Nations Conference

Special Political and Decolonization Committee (SPECPOL)

Chair: Peyton Blackstock

JHUMUNC 2018

Special, Political, and Decolonization Committee

Topic A: Threats to Cybersecurity

Topic B: Deconstructing Neocolonialism in Africa

Committee Overview

The Fourth Committee of the General Assembly of the United Nations is the Special Political and Decolonization Committee, commonly referred to as SPECPOL. The Committee was established in 1993 when the Decolonization Committee and the Special Political Committee (formerly the Seventh Committee) merged. SPECPOL broadly encompasses a variety of subjects, including those related to decolonization, refugees and human rights, peacekeeping, outer space, public information, the University for Peace, as well as any special political issues that are not directly assigned to any of the other UN General Assembly committees.

The General Assembly is the main deliberative, policymaking and representative organ of the United Nations. Created in 1945, the assembly is responsible for reviewing reports of the Security and Economic Councils; making recommendations on international political cooperation; fostering collaboration in economic, social, cultural, educational, and health fields; encouraging peaceful settlements of hostile situations amongst nations; as well as appointing leaders of the UN, itself. During the time of our committee, the 72nd session of the UN General Assembly will be taking place with 193 member states in New York City.

One of the topics that is broadly discussed by SPECPOL is peacekeeping of all kinds. Strategies for peacekeeping must evolve as technologies and strategies of attack evolve themselves. Today, one of the most prominent means of illicitly gaining information is through the act of cyber terrorism, which makes cybersecurity one of the most important means of keeping peace between nations. Despite its importance, and though the topic has been previously discussed, cybersecurity, and its accompanying transparency, has not yet been mandated by any of the committees of the UN.

Topic A: Threats to Cybersecurity

Introduction

Why Is Cybersecurity Important?

The topic of Cybersecurity has already gained an enormous amount of significance, and as technology continues to race forward, so does the importance of a globally secure cyber network. Cyberspace is an asset in connecting the international community. However, the more connected countries – and the people in them – become, the easier it becomes to target large groups of people and large blocks of countries simultaneously. It has even been noted by previous UN assemblies that if cyber warfare goes unchecked it could "topple [the] entire edifice of international security." [1]

Cybercrimes fall into two broad categories that are detrimental to the stability of the international cyber community: data breaches and sabotage.[2] Data breaches are a risk for

[1] United Nations, Meeting Coverage and Press Releases, *Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment*. GA/DIS/3512, 28 October 2014, https://www.un.org/press/en/2014/gadis3512.doc.htm.

[2] Detlev Gabel, "Cyber risk: Why cyber security is important," *White & Case*, 1 July 2015, accessed 1 July 2017.

everyone from the common person to international organizations, as these can come in the form of stealing personal identification information to state secrets. Often these breaches occur to steal money in some form or another, and it has been estimated that cyberattacks "cost the global economy over $400 billion per year."[3] Sabotage, on the other hand, can be in many forms but generally aims to disable systems for whatever purpose. The real threat of these attacks lies in that most cyberattacks go unnoticed until it is too late, if they are ever noticed at all.

Currently, while there have been discussions regarding the necessity of combatting and preventing cyberattacks, there is no singular, international effort to bolster cybersecurity. It is imperative that a united effort is decided upon, as all countries need to be held to certain standards not only to combat attacks, but to prevent more from occurring in the future.

Major Issues the Committee Must Address

There are several major issues that must be addressed in order to combat the existing and future threats to cybersecurity. First, there is the issue of transparency. The UN has spent its history creating a cooperative international community. As means of attack advance, it is important that cooperation efforts advance as well. The issue of transparency is directly tied into the need for some measure of checks and balances on UN members, which must be addressed by the Committee as well.

Second, threats as they have previously been identified must be addressed. As previously stated, cybercrimes broadly fall into two categories: data breach and sabotage. These attacks can be further divided into identified categories of cybercrime, cyber espionage, cyber terrorism, and cyber war. To fully understand these categories, definitions have been provided:

1. Cybercrime is "the use of computers or related systems to steal or compromise confidential information for criminal purposes, most often for financial gain,"
2. Cyber espionage is "the use of computers or related systems to collect intelligence to enable certain operations,"
3. Cyber terrorism is "the use of computers or related systems to create fear or panic in a society," and
4. Cyber war "consists of military operations with cyberspace to deny an adversary. . . the effective use of information systems and weapons." [4]

Please note, that while these definitions are widely used, they have not been agreed upon by the UN member states and variation in the definitions across states allows for the acceptance different activities.

A main goal of this Committee is to create a feasible way to combat these cyber attacks, if not to stop them altogether.

It is also imperative that the Committee address ways to deal with emerging threats. Technology advances at an incredibly fast pace, and so it is necessary to stay up-to-date with combatting new types of attacks as soon as possible once they have emerged. Additionally, the platforms that are at risk and thus necessary to be included in cybersecurity needs to be discussed.

Historical Background

Notable Past Cybersecurity Threats

The Morris Worm

In 1988, Robert Tappan Morris created the first computer worm ever to be transmitted through the internet, aiming not to harm but to determine exactly how vast cyberspace is.[5] Unfortunately, the worm mutated and ended up infecting over 600 computers in an estimated $100 million dollars of damage.[6] While it may have been unintentional, this denial of service to those computers via the Morris Worm is the first documented case of cyber sabotage and has inspired many contemporary attacks.

Solar Sunrise

Ten years after the Morris Worm, in what was originally thought to have been an Iraqi effort to seize US government and private computer systems, over 500 systems running on the Sun Solaris operating software were seized by the hackers.[7] The culprits were later found to not be Iraqi operatives, but rather three teenagers from California. While this revelation did halt any backlash that may have been caused on the international scale, the attack itself was able to cripple the entire country's software

[3] Ibid.
[4] Harry, Katzan, Jr., "Contemporary Issues in Cybersecurity," *Journal of Cybersecurity Research,* June 2016, accessed 1 June 2017.
[5] "Top 10 Most Notorious Cyber Attacks in History," *ARN,* accessed 1 June 2017.
[6] Ibid.
[7] Ibid.

infrastructure. This highlighted exactly how extensive a collaborative effort could be on both the private and public sector, particularly because the attack had been an effort by three rookie hackers.

Teen Hacks NASA and the US Department of Defense

Only one year later, another teen by the name of Jonathan James was able to penetrate both the US Department of Defense and, using the information stolen, he was able to steal part of a NASA software program, shutting down systems for three weeks.[8] This event highlights both data breach and sabotage crimes, showing that the two are not mutually exclusive. As the software stolen was also related to the International Space Station, the attack also showed that one crime could affect not just one nation, but many all at once.

Internet Attacked

In 2002, the largest attack on the internet of the time occurred, shutting down the internet for an hour.[9] Although the average user was unable to notice any changes in service due to safeguards, the hackers were able to attack and shut down 13 of the main root servers that provide internet. Had the attack lasted for longer, even the average user would have been able to feel the attack. This attack brought this issue to the forefront of global attention. The problems boiled down to money and vulnerability. Experts on the issue stated that the "only way to stop such attacks is to fix the vulnerabilities on the machines . . . There's no defense once the machines are under the attacker's control."[10] It was also noted by the same experts that only those with money would even be able to protect themselves, and even then, it would be unlikely that their systems would be able to withstand a concerted attack.[11] This attack was a much-needed wake-up call to exactly how vast threats could be and how very little could be done to combat them. Years later, money and vulnerabilities in machines and software are still some of the largest problems in combatting attacks. It also remains a problem that most attacks can only be prevented, and if one is able to be launched, it is much, much more difficult to stop the attacks and can cost the targets millions of dollars, mainly because it would shut down the servers of important banks, stock exchanges, corporations, etc. The ramifications of this attack in regards to information are also vast, as the servers would have been left unguarded, making it that much easier to steal valuable information from individuals, corporations, governments, and international organizations.

Google China hit by Cyber Attack

In 2009, Google China was hit by a cyber attack in which hackers infiltrated Google's corporate servers in order to steal intellectual property – main Gmail accounts owned by Chinese human rights activists.[12] This crime was later also found to be tied to unauthorized access to private Gmail accounts of users in the US, China, and all over Europe. China is known to be rather stringent in its internet policies and censorship and this is yet another example of a nation targeting those who are a threat. It also shows that a corporation that is used worldwide is not impenetrable, despite many using it to send and share private information.

July 2009 Cyber Attacks

In a series of coordinated attacks, hackers were able to infiltrate thousands of computers belonging to US and South Korean government agencies, media agencies, and banks. The attacks were done with a botnet, or group of hijacked computers. The assumed aim of the attack was to cause disruption, rather than steal information.[13] Despite not having that large of an impact on the computers, if the attack had gone as planned, the estimated cost associated with the websites being down would have been huge, as it would have prevented business transactions from being carried out as planned and halted government work. The troubling aspect of these attacks came from the unknown perpetrator. It was largely assumed by Korean Intelligence agencies that the attack stemmed from North Korea. However, it was also found that the hijacked computers hailed from all over the globe, making it difficult to pinpoint those at fault.

Canadian Government Hacking

[8] Ibid.
[9] Ibid.
[10] David McGuire and Brian Krebs, "Attack On Internet Called Largest Ever," *Washington Post,* 23 October 2002, accessed 30 July 2017.
[11] Ibid.
[12] "Top 10," *ARN.*
[13] Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *The New York Times,* 8 July 2009, accessed 15 June 2017. http://www.nytimes.com/2009/07/09/technology/09cyber.html

In February of 2011, Canadian government officials became aware of a cyber attack being performed by foreign hackers. The IP address of the hackers was traced back to China, and before the attack was noticed, the hackers were able to penetrate three government departments.[14] The hackers were able to transmit classified information back to themselves, and in the end, Canada had to cut the internet access off for those departments to stop the transmission of information.[15] This further highlighted what had been stated previously, that attacks, once started, are hard to stop.

Flame

Noted as one of the "most complex threats ever," Flame was a malware attack targeting countries in the Middle East, including Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt.[16] The malware was suspected of having operated since August 2010, despite it not being discovered until mid-2012, and its origins were hard to trace, like the previous attack on the US and South Korea. The reason it was able to go undetected for so long is that the target of this malware was not to damage the system, but instead to collect massive amounts of sensitive information from over 600 targets, including individuals, businesses, and government institutions.[17] Because of the size and sophistication of Flame, experts theorized that it would have to have been a government-backed operation, as the only known organizations to have that kind of software are cyber criminals, hacktivists, and government organizations; when this knowledge was paired with the geographic location of the target states and that the attack was not designed to steal money, the only possible culprit left was a government organization, although which one or ones are still a mystery.[18] This attack was far superior to those known prior—rather than just siphoning information existing in cyberspace, Flame was capable of "recording audio via a microphone. . .take screenshots of on-screen activity, [and] automatically detecting when "interesting" programs – such as email or instant messaging – were open."[19] Flame showed the world that what preventive and protective measures were in place against known attacks were already too far behind what had been further developed. Flame highlights the need for technologies that counter cyber attacks to advance as quickly as the technologies that perform them. However, it also revealed another issue of how technologies advance is not always easy to predict, and thus is not always easy to guard against.

India Government Hacking

Despite being a technology powerhouse, India was still hit by a large-scale cyber attack, which left the email accounts – and the sensitive information inside them – of over 10,000 government employs compromised.[20] The attack seemed to try to obtain specific information, rather than simply disrupt system use or steal funds. In fact, of the information stolen, a large part of was of troop deployment plans, especially of the Indo Tibetan Border Police, whose plans were compromised.[21] This attack was a very real example of how the information being stolen could not only affect cyber information, but could have very tangible real-world repercussions that could be detrimental to the safety of many.

#opIsrael

Israel is one of the most contested and volatile regions in the world, and on April 7, 2013, it also became the target of a vicious cyber attack. The coordinated attack, known as #opIsrael, aimed to erase Israel from the internet on the eve of Holocaust Remembrance Day. [22] The attacks targeted both the public and private sector. Because the attacks had been known prior to occurrence because of the use of the hashtag, #opIsrael is widely regarded as a failure. However, it calls into focus the use of social media platforms, which continue to this day to advance and take over the common person's day, to perform cyber crime. It also showed a case of a long-standing fight being taken out of the real world and placed into cyberspace, a trend that continues to grow.

Contemporary Conditions

[14] Syed Balkhi, "25 Biggest Cyber Attacks in History," *List 25,* 11 May 2014, accessed 1 June 2017, http://list25.com/25-biggest-cyber-attacks-in-history/.
[15] Ibid.
[16] Dave Lee, "Flame: Massive cyber-attack discovered, researchers say," *BBC News,* 28 May 2012, accessed 1 June 2017, http://www.bbc.com/news/technology-18238326.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Phil Muncaster, "10,000 Indian government and military emails hacked," *The Register*, 21 December 2012, accessed 15 June 2017. https://www.theregister.co.uk/2012/12/21/indian_government_email_hacked/
[21] Ibid.
[22] Balkhi, "25 Biggest Cyber Attacks."

In Spring of 2017, two cyber attacks occurred that "the World [wasn't] ready for" in the form of a breach of IDT Corporation[23] and the subsequent WannaCry breaches that seized power of English hospital computers, Chinese universities, German railways, Japanese auto plants, and other organizations in over 100 countries.[24] While the demands for ransom and the temporary loss of power were devastating enough, it later became apparent that the attack had had a goal other than money in mind: it had also taken the information on the employees of IDT, allowing the hackers access to sensitive information, as well as other sensitive information gained from the hospitals, universities, and other breaches, putting lives at risk both immediately, like those in the hospitals and railways, and in the future.[25] Experts claim this is a new type of cyber attack the world simply is not prepared to face, as the attacks are becoming virtually undetectable until it is almost too late, or even until after the point of no return, especially because there is no leading force in securing cyberspace.[26]

Thus, that leaves cybersecurity as it currently stands today: with technology racing ahead, cybersecurity is scattered and falling increasingly behind. Starting even at the root of the problem, there is not even an agreed upon definition of cybercrime around the world and many countries still feel that it is an IT issue, rather than one of international concern.[27] Countries are reluctant at best to show transparency regarding cybersecurity and activities in cyberspace with even the closest of allies; attacks are also developing into hybrids that affect not only cyberspace but are very real dangers in the real world, whether it be in significant financial loss or the loss of lives.

Therefore, despite the fact that "the UN has been trying to implement meaningful guidelines on international cybersecurity for the better part of the last 15 years," no consensus is able to be reached, and all security measures continue to fall further and further behind the unpredictable and virtually undetectable attacks.[28]

Past UN and International Action

While there has been no consensus or successful hardline defense against cybersecurity on the international stage, there have been several notable efforts to secure cyberspace:

1. UN Resolution 57/239, passed in 2003, called for more awareness of capable nations "to prevent, detect, and respond to cybersecurity threats;"
2. One year later, Resolution 58/199 invited member nations to share cybersecurity strategies with other member nations, as they saw fit.[29]

While both of these resolutions were optimistic, they did little in creating actual transparency between member nations, as neither were enforced strictly, and cybersecurity threats continue to be among the most notable type of attack of the 21st century. [30]

Questions a Resolution Must Answer

1. What, by definition, is considered a cybercrime?

Before it can be determined how to prevent cybercrime, a universal definition is needed. Without one, all countries will not be held to the same standards and will not be targeting the same activity, thus making any combined efforts against cybercrime inefficient.

2. How is cyber warfare going to be defined from this day forward?

Similarly to cybercrime, cyber warfare also needs a universally, acknowledged definition that distinguishes it from cybercrime. This is necessary as cyber warfare is often more extreme and will warrant a more severe punishment, and a line needs to be drawn between the two types of attacks.

3. Is an act by a non-governmental individual against another nation's organization considered an act by the state or by the individual?

While the aggressor will be dealt with regardless, it is a matter of international peace

[23] United Nations News Centre, *In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet safety,* 19 May 2017.
[24] Nicole Perlroth, "A Cyberattack 'the World isn't ready for,'" *New York Times,* 22 June 2017, accessed 17 June 2017. https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html
[25] Ibid.
[26] Ibid.
[27] UN News Centre, 17 May 2009.
[28] Michael Beaver, *The United Nations and Cyber Warfare,* Global Risk Advisors, 28 September 2016, accessed 20 June 2017. https://globalriskadvisors.com/blog/united-nations-cyber-warfare/
[29] Ibid.
[30] Ibid.

whether or not an individual acting without government consent is considered a state act or not. Without this acknowledged, every attack by an individual can be used as a reason to retaliate against an entire state, which may have had no responsibility for it in the first place.

4. What measures will be taken in the event of a cybercrime against the aggressor?

In order to dissuade aggressors from attacking in the first place and to punish those who still decide to attack, the appropriate repercussions need to be in place. Ideally, several measures of varying degrees of severity, as in normal crimes, so that the punishment may fit the crime.

5. What type of preventive measures need to be taken?

One of the biggest problems with cybersecurity is that it is developing at a much slower rate than the technology being used to attack. Some sort of committee or similar organization needs to be set up in order to keep up to date with the attacks and develop the preventive measures as quickly as possible. Ideally, this organization would reach a point that it is able to predict the next step in attacks advancing and be proactive, rather than continually stay a reactive measure.

6. What parameters need to be set to decide what platforms need to be included in cybersecurity?

Cyberspace is a large place, encompassing many different types of information, media, and other various things. In order to protect and defend accurately, the different parts of cyberspace need to be assessed for risk and then decided which ones are covered by cybersecurity and to what degree.

7. In addition to cybersecurity encompassing the world wide web, what social media platforms will it cover?

Social media platforms are a growing way that information about persons is accessed. It needs to be decided which, if any, of the social media platforms fall under cybersecurity.

8. In what legal and transparent ways will the dark web be covered by the measures against cybercrime?

Cyberspace does not just include the platforms used by the everyday person. Rather, many crimes begin on the dark web, where trading of information and tangible goods is done illegally. The dark web is harder to monitor, however, so it necessary to create measures regarding the legality of this as well.

Bloc Positions

United States and Developed Nations

The US has been the target of the many of the attacks in cyberspace. As one of the leaders of the world, it has made a habit of condemning the attacks and under the Obama administration, began making more concerted efforts to reach international cooperation.[31] Currently, the US is trying to create an international community willing to share in transparency and defense efforts. At the same time, the US also aims to build a tech savvy workforce that is able to spot and defend against attacks when necessary. The US acknowledges that "the economic prosperity, national security, and personal liberties depend on [its] commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet."[32]

Similarly, developed nations in both Europe, the British Commonwealth, and Asian countries, like South Korea and Japan, among other nations, have had similar experiences with cyber attacks and tend to hold similar views to the US in terms of securing cyberspace.

China

China has been a target of much criticism for its harsh and restrictive policies regarding cyberspace for its citizens, and because of the fact it was one of the last developed world leaders to release its cybersecurity plan.[33] The plan that China did eventually release, articulated plans to overcome the digital gap, digital economy, and cybersecurity, among other issues. However, the Chinese plan must be heavily scrutinized in regards to its discourse with Chinese internet policy. China has also been found as both a victim and a perpetrator of cyber attacks over the years, both on its own citizens and allies and on its biggest competitors. However, in its recent moves to address cyberspace, China is opening up space so that it may build trust with the US and other countries in hopes of building a cyber community

[31] The White House, "Foreign Policy: Cybersecurity". accessed 1 August 2017
[32] Ibid.
[33] Lu Chuanying, *China's Emerging Cyberspace Strategy,* The Diplomat, 24 May 2016, accessed 1 August 2017

that they, too, are included in.

Russia

Russia is another country that has been both a victim and, often, a perpetrator in cyber attacks. Notably, there was the recent scandal of whether or not Russia had hacked into the US election to choose the outcome they felt would be most favorable for them. Their views as a whole differ entirely from the Western point of view. While most Western countries acknowledge a need for a certain degree of transparency, Russia believes that all cyber information should be accessible and does not think that physical borders exist in cyberspace, thus taking information from those they see fit.[34] Russia continually tries to submit proposals along these ideals and to normalize their viewpoint, which has made it difficult to come to agreements with Western countries and those of the same viewpoint.

North Korea

While North Korea has not issued an official statement on their position regarding cybersecurity, it is of concern to many nations. North Korea has begun moving more and more to cyberattacks, which are unpredictable and difficult to detect, making them even more dangerous. The greater North Korea's cyber capabilities, the bigger of a threat they become, which leaves its opposition even more on edge and wishing to reach an agreement.

Underdeveloped and Developing Nations

While cybersecurity is not the biggest of concerns to nations whose access to such platforms is limited, it is important these countries are included in the planning of such structures. They also should be included in participating in the structures that are set in place as to have more of a chance to get involved in cybersecurity.

Middle East

Like most other countries, those of the Middle East have been both victim and perpetrator in cyberattacks. The target in the Middle East tends to arise from the lucrative businesses in the area, such as the oil industry, as well as the unrest that plagues the area. Despite many of the countries attempting to bolster cybersecurity, the tensions in the area, which involves many more countries than just those in the Middle East, have made cybersecurity a goal of utmost importance. However, as the countries have a history of clashing against each other and a history of bad blood, it is going to be difficult to achieve levels of transparency between these countries, who are going to be eager to hear what their opposition will say, but want to keep their secrets hidden.

Conclusion

Cybersecurity has emerged as one of the most important issues in the 21st century, while still managing to be one of the most underdeveloped areas of defense. Like, security in real time, it is important that states are able to identify and stop attacks, or even prevent them altogether. However, as technologies advance much more quickly than plans of defense, many attacks go unnoticed until it is entirely too late.

In order to secure one of the most important platforms of information storage and communication, several big issues need to be addressed, including transparency between states, defense, and preventive measures. While there have been efforts by smaller groups of states, there needs to be a general consensus carried forth by member nations, so as to finally stand a chance against the issue.

Topic B: Deconstructing Neocolonialism in Africa

Introduction

Another topic heavily discussed in SPECPOL is the decolonization of Africa. This dilemma comes at a crucial time of economic globalization and development in third world countries. Even though African nations gained their independence in the 1950s following the end of World War II, many people still believe that the imperialistic nature of their governments prior to the war still haunts them and is even present today. Immediately after the war, European nations deserted the continent and left the African people with a lack of political experience and arbitrary political boundaries that placed many diverse ethnic people under the same government. Therefore, decolonization after the war only materialized on paper. These countries have simply become subjects of political and

[34] Kier Giles, *Russia's Public Stance on Cyberspace Issues,* Conflict Studies Research Center, 2012., accessed 2 August 2017.

economic exploitation over the past few decades. Under the guise of economic aid and neoliberal growth, the US, China, and many developed European countries have grasped at opportunities to take advantage of the abundance of natural resources on African land. However, is this form of economic and political intervention really beneficial for both sides? Or will the current dealings between African and first-world nations re-entrench the controversy of colonial Africa?

Why Deconstructing Neocolonialism in Africa Matters?

In order to protect the sovereignty of African nations, it is of utmost importance to deconstruct neocolonialist structures in their modern political system. To help better understand the premise of the issue being discussed, a few terms will be defined. First off, neoliberalism is an economic philosophy that rose in popularity in the late 1900s focused around deregulation and unrestricted free trade, leading to economic globalization. Meanwhile, neocolonialism is the form of economic and political control which has been enabled by the coming age of neoliberalism. It is a form of global power in which transnational corporations and global and multilateral institutions combine to perpetuate colonial forms of exploitation of developing countries. This allows capitalist powers (either nations or corporations) to dominate subject nations through operations of international capitalism rather than direct rule. Africa is the birthplace of neocolonialism, making it the starting point of deconstructing neocolonialism before moving on to the rest of the world. Neocolonialism began when European policies were created as schemes to maintain control of African and other dependencies after World War II at the European Summit in Paris in 1957. Neocolonalism still continues today – the latest addition being China's "no-strings attached" development assistance and promises of growth in exchange for African oil and metals. These billion-dollar plans and contracts can either bring economic success to African countries and partner nations, or they can lead to Africa's unending dependence on foreign countries.

Major Issues that the Committee Must Address

There are multiple issues that the committee must address that deal with the deconstruction of African neocolonialism. First, there is rampant economic exploitation in many African regions culminating in many human rights abuses. Most notably, the blood diamond trade in South Africa. Diamonds from African soil are worth billions of dollars, with wealth concentrated mostly in the US, Europe, Israel, and the white population of South Africa. African people labor in the mines under slave-like conditions for pennies a day.[35] Hundreds of miners die every year from tunnel collapses that are so seldom reported because they happen so often. Kids, 15-year-olds and sometimes even younger, shovel and sift through gravel daily for the opportunity to eat. On the other hand, profits from these diamond mines end up funding conflicts such as the civil wars of Angola and Sierra Leone. The UN and other bodies have tried to alleviate the issues associated with the diamond trade, such as the popularized "Kimberly Process," which is hailed as a major step towards ending diamond fueled conflicts. Even with these changes, the harsh working conditions and modern-day slavery of African workers still remain.[36]

Other major issues to address include the economic aid programs and assistance between the governments of Africa and developed countries. While the blood diamond trade deals with transnational corporations, there are instances of neocolonialism between governmental institutions themselves. Since the 1970s, Africa has received mountains of developmental assistance totaling over $300 billion. As stated above, China has recently ramped up its trading and foreign aid to Africa, with over $200 billion worth in goods traded in 2014 alone, as well as over half of its foreign aid distributed in Africa.[37] In exchange, African nations have began to support China on many UN issues. In 2014, South Africa denied entry to Dalai Llama. In early 2016, Kenya deported 50 Taiwanese nationals to China. Is this just a partnership? Or is it outright colonialism and control over another country?

Meanwhile, western countries (US and Europe) also want a piece of the African pie. However, instead of economic assistance, these countries approached Africa with a new "war on terror." AFRICOM is the US military operations command for 53 African nations created in 2007 giving a reason for the west to go in and protect

[35] "Blood Diamonds," *African People's Solidarity Committee*. http://apscuhuru.org/analysis/diamonds/page2.xhtml
[36] Ibid.
[37] Manero, Elizabeth, "China's Investment in Africa: The New Colonialism?," *The Harvard Political Review*. 3 February 2017. http://harvardpolitics.com/world/chinas-investment-in-africa-the-new-colonialism/

Africa.[38] Despite military officials claiming that operations are miniscule and only one admitted base in Djibouti, there is detailed proof of scant and hidden military outposts in at least 49 African countries. Ironically, since the start of AFRICOM, instability has actually increased in Africa, as shown in the conflicts in Somalia, South Sudan, and the breakout of Boko Haram.[39]

The International Monetary Fund (IMF) and the World Bank have not helped. African nations have been accumulating debt over the past few years because corruption and international pressure put upon African leaders have forced them to take out massive international loans with the purpose of infrastructure development.[40] Though this sounds beneficial, the reality is that corporations receive massive contracts to build infrastructure, profiting the elites and government officials, while the public gets stuck with a debt that can never be paid back. Overall, many issues need to be addressed regarding the deconstruction of neocolonialism in Africa.

Historical Background

Scramble for Africa

The colonization of Africa began in the 1870s with 3 notable conquests: Algeria was colonized by the French, Cape Colony was held by the United Kingdom, and Angola was held by Portugal. At the time, less than 10 percent of the continent was under the control of Western nations. Those three initial conquests led to the period known as the Scramble for Africa—the occupation, division, and colonization of African territory by European powers between 1881 and 1914. By the end, nearly 90 percent of Africa was controlled by Europe.[41] The starting point of the Scramble for Africa was the Berlin Conference of 1884. During this conference, European diplomats partitioned Africa and laid down the rules of competition by which the great powers were to be guided in seeking colonies.[42] European countries were driven by competition for preeminence and power struggles to control as much of Africa as they could. Additionally, Africa was a cheap and open market for selling their goods in exchange for virtually free raw materials. Furthermore, they believed that they could export "surplus population" during this age of industrialization to establish these colonies. The treaty, known as the Berlin Act, signed at the Berlin Conference, was drawn up without African participation, and subsequently led to the rapid invasion and colonization of Africa.[43]

Decolonization of Africa Following World War II

Rebellions against colonial rule increased after 1900, when Europe began implementing changes that took African land and forced Africans to work for Europeans in order to pay taxes.[44] During World War II, African leaders realized that European powers were loosening their grip on African colonies and focusing their troops on the war. This resulted in a surge of movements that gained momentum among the colonized people. These revolts were no longer about reform, but demanded independence. In August of 1941, President Roosevelt and Prime Minister Churchill came together to draft an unofficial document called the Atlantic Charter. This was a draft for plans of postwar reconstruction for the United States and Britain, which included support for restoring autonomy to all colonized countries during the war.[45] Following World War II, Europe faced pressures from the United States and Africa to follow the actions of the Atlantic Charter and grant self-government to African states. However, much of Europe's actions in African colonies to build self-determination were masks for attempting to regain control. Ironically, it was the expansion of Western education among the African colonies that strengthened the ideas of independence and spurred leaders to rise up and fight for the decolonization of Africa.[46]

---

[38] Bryant, Tim, "The Hidden Truths of Africa: Neocolonialism and the Modern Age of Slavery," *Wake Up World*. https://wakeup-world.com/2016/05/08/the-hidden-truths-of-africa-neocolonialism-and-the-modern-age-of-slavery/

[39] Ibid.

[40] Ibid.

[41] "Scramble for Africa," *New World Encyclopedia*. 10 October 2017. http://www.newworldencyclopedia.org/entry/Scramble_for_Africa

[42] Ibid.

[43] Iweriebor, Ehiedu E., "The Colonization of Africa," *Africana Age*. http://exhibitions.nypl.org/africanaage/essay-colonization-of-africa.html

[44] "Impact of WWII: how the nature of political quest for independence changed after 1945," *South African History Online*. 8 May 2017. http://www.sahistory.org.za/article/fight-against-colonialism-and-imperialism-africa

[45] Sullivan, Nate. "The Roots of African Independence Movements," Lesson 14 Transcript. http://study.com/academy/lesson/changes-in-africa-after-world-war-ii.html

[46] "Impact of WWII."

Neocolonialism Replaces Colonialism in Africa

One of the most notable national leaders educated in a Western university was Kwame Nkrumah. Nkrumah strived for independence and believed in pan Africanism.[47] He joined the United Gold Coast Convention before forming the Convention People's Party in 1949, where he supported nonviolent protests and strikes, gaining support through newspapers, schools, and organizations. The Gold Coast gained independence in 1957 and was renamed Ghana, where Nkrumah became the Prime Minister before Ghana became a republic and was elected President.[48] Nkrumah continued as an active advocate of economic and political success. He coined the term "neo-colonialism" to refer to states that have the semblance of independence but are still economically and politically dependent on colonial powers.[49] Because African states exported large amounts of raw material in order to generate revenue, their economies remained underdeveloped. Many African governments also sought foreign aid, which often came with high interest keeping African peoples impoverished.[50] Neocolonialism reach extended past the powers directly involved in the original colonialism of Africa. New powers, such as the United States, began playing a role in African national economies.

Contemporary Conditions

China's Rush for Energy and Mineral Resources in East Africa

Many countries see Africa as a continent abundant with untapped natural resource potential. Because Africa itself is not in a position to extract much of its own resources, other more politically and economically sound countries take advantage of the post-colonial, post-apartheid countries. To illustrate this point, between 2003 and 2011, the continent's Foreign Direct Investment amount increased from $491 million to $14.7 billion.[51] China in particular has significantly increased its investment in Africa's economy, specifically for its natural resources. As China continues with Foreign Direct Investment in various Sub-Saharan African countries, it is not yet clear whether this venture will affect broad-based growth in Africa. [52] Moreover, over half of China's foreign aid is currently distributed within Africa. With 60 percent of its agricultural land uncultivated and 40 percent of the world's reserve of natural resources, Africa seems like China's perfect target economy. While African countries such as Algeria, Nigeria, South Africa, Sudan, and Zambia are the top exporters of oil, gas, metals, and mineral to China, China mostly exports manufactured goods to the continent. The United Nation's main concern about this relationship is whether or not it is truly beneficial for both sides or if this is merely a neocolonial exploit. Additionally, because of the opportunities for cheap labor, this problem also brings ethics into question.

Blood Diamonds and Neoliberal Globalization in South Africa

Antwerp and Debeers: De Beers Diamonds, the world's leading diamond company, originated in Kimberely, South Africa. Here, the founder of the original diamond mining company created a monopoly. By the early 20th century, diamonds were essentially all supplied in a single channel system to distributors by De Beers, a corporate mega-giant.[53] When diamonds broke into the American market, De Beers marketed diamonds as everlasting, equating the minerals to love. This was the beginning of diamond engagement and wedding rings that couples still value in the 21st century. For countries around the world, diamonds became a symbol of love and luxury, but in the African continent itself the diamonds had a very different meaning. In 2010, Liberian President Charles Taylor was accused of using diamonds to fund the Revolutionary United Front, a rebel group in Sierra Leone. An unspoken fact of the case is that neither Taylor nor any African leader actually owns any of Liberia's diamond industry. There are diamond-producing firms within Liberia, but they are all owned by corporations outside of Africa. However, rebel-held mines have used un-cut diamonds to raise billions to fund rebel insurgencies in Angola, Democratic Republic of Congo, and Sierra

[47] The Editors of Encyclopedia Britannica, "Kwame Nkrumah," *Encyclopedia Britannica:* Encyclopedia Britannica, Inc, 21 April 2017. https://www.britannica.com/biography/Kwame-Nkrumah
[48] Ibid.
[49] Ibid.
[50] Halperin, Sandra, "Neocolonialism," *Encyclopedia Britannica:* Encyclopedia Britannica, Inc, 23 March 2016, https://www.britannica.com/topic/neocolonialism
[51] Manero, "China's Investment."
[52] Ibid.
[53] Baker, Aryn. "Blood Diamonds," *Time*. time.com/blood-diamonds/

Leone.[54] The blood diamonds provide rebels with funds for weapons which enables them to fight civil wars within their countries.

Past UN and International Action

Targeted Conflict Diamonds through Security Council (Civil Wars)

Resolution 55/56--Kimberly Process--Flawed?

In December 2000, Resolution 55/56 that limited the sale of conflict diamonds was officially adopted by the UN General Assembly.[55] Despite UN efforts to target conflicts in each country on an individual basis, the common thread they found was the sale of the blood diamonds. In order to halt this illegal and dangerous mode of gaining weapons, the UN placed a ban on the conflict countries in Africa. However, in recent years the embargoes have been lifted due to a decline in conflict diamond trade. The exact reason for the decline are unclear, but some factors that may have contributed to the decline include ending civil wars in the conflict countries as well as establishing the Kimberley Process to certify diamonds were not produced in the conflict zones. It is still unclear whether the Kimberley Process of certification was well-regulated or flawed. Some critics argue its monitoring was weak and ineffectual, urging the UN to create stronger mechanisms to prevent illegal blood diamond trading.

UN/China Development in Africa; UN-led initiatives

China has recently embraced a multilateral diplomacy despite its earlier inclination to deal bilaterally with Africa. Its efforts contributing to UN peacekeeping and building are developing immensely. Additionally, China has proposed the Belt and Road Initiative, an infrastructure-driving investment proposition. The plan will hopefully connect Asia to Europe and Africa with an unparalleled trade and infrastructure network. The UN strongly approves of this initiative because it sees it as a chance for a general betterment of the continent, economy, and alleviation of inter-continental conflict. Additionally, UN Secretary-General Antonió Guterres believes the initiative may deepen the connectivity of infrastructure, trade, and finance across regions.[56]

The UNESCO-China-Africa Tripartite Initiative aims to connect universities in order to integrate a strong mutual knowledge and understanding between Africa and China.[57] The 20+20 Cooperation Plan of higher education institutions in China with those in Africa is an integral part of the initiative.

Questions a Resolution Must Answer

1. How can countries or large corporations aid an African nation's development without causing neocolonialism?

As discussed, one of the main proponents of neocolonialism is the dependency caused by nations or corporations providing developing nations with aid. Underdeveloped nations will often become reliant on these loans and eventually unable to operate without the assistance of other developed countries or corporations.

2. How can we maintain trade agreements but still give African nations enough autonomy so as to prevent neocolonialism?

Although many trade agreements between developed nations and underdeveloped African nations are exploitative in nature, many others are fair and beneficial to both parties. In order to be able to prevent the former, we need to be able to guarantee that these agreements don not jeopardize the autonomy of the underdeveloped nations.

3. What can be done to prevent neo-liberalist policies from inviting neocolonialism?

Many nations implement neo-liberalist policies that invite free trade and globalization in order to better their economy. These policies, however, often are the gateway to neocolonialism, as underdeveloped nations fall prey to exploitative trade agreements and eventually neocolonialism.

---

[54] Ibid.

[55] United Nations General Assembly. *Resolution 55/56*. 29 January 2001. http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Sanc%20ARES%2055%2056.pdf

[56] Ibid.

[57] United Nations. "UNESCO-China-Africa Tripartite Initiative on University Cooperation." http://www.unesco.org/new/en/education/themes/strengthening-education-systems/higher-education/international-university-cooperation/unesco-china-africa-tripartite-initiative-on-university-cooperation/

4. What can we do to prevent the human rights abuses that often accompany neocolonialism?

Human rights abuses often go hand in hand with neocolonialist policies and simply addressing the political and economic aspects of neocolonialism is not sufficient in aiding the problem.

5. How can we address the blood diamond industry in South Africa?

The blood diamond industry is one of the largest and most obvious examples of corporate neocolonialism. As previously mentioned, it is also one of the biggest perpetrators of human rights violations and must be addressed specifically.

6. In what ways can a nation recover after neocolonialism and exploitation?

Even after a nation has freed itself from the economic and political control of another country/corporation, there are many steps that must be taken in order for it to regain its autonomy and stability.

7. How can those that are living off of the production of blood diamonds be supported without the trade?

It has been proven that without the diamond trade many people would not have the means to survive. However, given that that the diamond trade is damaging to many people, how can this be factored in so that many more people do not end up in even more severe poverty?

Bloc Positions

United States

Historically, the United States has often been the perpetrator of neocolonialism or exploitation and in Africa it is no different. While recently the United States has made noticeable attempts to take a more measured and controlled approach to aiding development in these countries, many nations still are incredibly reliant on U.S. aid, creating a system of dependency that opens the doors for neocolonialism. Although the United States and other developing nations condemn neocolonialism, many of their actions, especially in African nations, echo imperialist policies of the past. The United States, however, has tried to avoid these practices by requiring political, economic, and social reform before providing a nation with aid because if a nation is unstable it is much more susceptible to exploitation and neocolonialism.

Developed European Nations

Developed European nations are in a similar situation as the United States. While they try to aid developing nations and try to help them maintain their autonomy, many still become dependent on European Nations for funds and support, and many European nations are still heavily involved in the social, political, and economic affairs of these countries. Specific countries such as Britain and France have been significant actors in many African Nations in many debatably neocolonialist ways. In 2012, British platinum company Lonmin sent aid to South African police at one of their bases to stop a miners' protest.[58] This intervention ended in violence when 39 miners were killed.[59] France has aided in similar endeavors by sending troops into both Mali and the Central African Republic to guarantee that their mining interests were safe and secure.[60] Although many of these European nations advocate for the development of these African Nations, their own economic well-being and access to African resources jeopardize this progress. The European Union as a whole has also implemented similar neocolonialist trade agreements with African Nations. Their Economic Partnership Agreements (EPAs) with African Nations were created to safeguard the access of EU markets but there is now controversy over whether or not these agreements are actually bettering the economic situation of African Nations. Many claim that these trade deals are unfairly benefiting the European Union by fostering economic tensions between these different nations and unjustly catering the trade agreements to each specific nation.

China

China is currently Africa's largest trading partner and has been since 2009. Each year, China authorizes billions of dollars in loans to African governments in order to build infrastructure, aid in development, and gain land. Chinese companies such as China Henan International Cooperation Group and the Chongquing Foreign Trade and Economic Cooperation Group dominate many industries in Africa, bringing in their own cheaper labor forces and stripping the areas of resources. In nations

[58] Ibid.
[59] Ibid.
[60] Ibid.

where the political climate is more unstable, Chinese run companies have broken their country's longstanding non-interventionist policies and involved themselves in political. In South Sudan, China deployed peacekeepers to secure their ties with their oil companies and in Ethiopia, Chinese diplomats intervened to help African mediators attain peace in times of domestic conflict. But despite their actions, Chinese officials deny that their policies promote neocolonialism and adamantly deny any claims of exploitation in the area.

South Africa

When South Africa transitioned out of Apartheid in 1994, international organizations such as the World Bank Group and International Monetary Fund stepped in to aid with their economic and political development. Although these development agencies had good intentions, they created a state that is now dependent on their loans. According to the African National Congress, "The World Bank and IMF are promoters of what can certainly be called a hegemonic ideology in economic policy," and this hegemonic policy in South Africa has caused a nearly neocolonialist situation. Aside from the IMF and WBG, many multinational corporations also capitalized on South Africa's fragile state post 1994. Many of these corporations exploited South Africa's raw resources while setting up trade systems that unfairly disadvantaged their economy. Recently, South Africa has tried to launch new trade unions to break away from these neocolonialist bonds, but there is still much improvement to be made.

Underdeveloped/Developing Nations

Underdeveloped and developing nations are often forced to decide between receiving the financial aid that they need with the risk of exploitation, or turning down the much needed assistance to maintain their autonomy. As previously mentioned, organizations such as the World Bank Group and the International Monetary Fund are often some of the first to offer loans to developing nations, but often this assistance will drive nations into debt and leave them completely dependent. In Africa, many nations are forced to pay more in debt service payments than they receive in loans from the WBG and IMF, stripping them of their own economic independence and allowing these organizations to manipulate their economies with structural adjustment plans that are rarely beneficial in the long run. This dependency is found in underdeveloped and developing nations globally and leads to an exploitive and neocolonialist relationship between these nations and organizations.

Conclusion

Colonialism in Africa has begun to take a new form in neocolonialism, but is no less damaging to the citizens of African countries. The power is still tilted in favor of the countries colonizing, and the manual labor and other damaging effects of systems, like the blood diamonds need to be addressed in order to actually propel Africa into a time of freedom from colonizing forces, rather than continuing the trend of passing Africa from one ruling country to another.