History of the Security Council

The Security Council, first created in 1946, is one of the six major bodies of the United Nations. The Security Council is responsible for maintaining international peace and security. The Security Council is also special in that it is the only UN council with the authority to enforce their decisions, including peacekeeping operations, sanctions and other punishments, and military intervention.

The Security Council has 15 nation-state members at any given time: 5 are permanent, while 10 are temporary. The 5 permanent Security Council members--China, Russia, USA, UK, and France--all have the ability to veto resolution, which completely removes that resolution from consideration. The 10 other nation-states rotate every two years to give the Security Council a more diverse perspective. The current temporary members of the Security Council are Angola, Chad, Chile, Jordan, Lithuania, Malaysia, New Zealand, Nigeria, Spain, and Venezuela.

"Security Council, SC, UNSC, Security, Peace, Sanctions, Veto, Resolution, President, United Nations, UN, Peacekeeping, Peacebuilding, Conflict Resolution, Prevention." UN News Center. UN, n.d. Web. 28 Mar. 2015.

Topic I: Drugs and Weapons Trafficking by Terror Groups

The issue of Drug Trafficking has grown significantly worse over the last 20 years despite many attempts to stem the illegal drug trade. While much of the attention towards drug trafficking has been concentrated on the Americas, the situation has greatly worsened in Africa, the Middle East, and the surrounding regions.

There are two primary areas of drug production. South America is the primary source for the world's supply of illegal cocaine, and Central Asia is the primary source of opium/heroin. Many African countries such as Nigeria, Somalia, Tanzania, Ethiopia, Uganda, and many others in the region have become major stops for smuggling drugs into the European and North American markets. The growing trend with this illegal drug trade is the involvement of local terrorist groups controlling the trade and using it as a source for financing of terror plots.

Weapons trafficking has also become a significant source of financing for terror groups in Africa and the Middle East including Boko Haram, ISIS, and Al Qaeda. The main sources of illegal arms in the world today is include Libya, which has struggled since the collapse of the Gaddafi regime to keep arms out of the hands of extremists in the region, Eastern Europe, where many weapons used in the Balkan War remain unaccounted for, and the United States, whose lax gun laws have made it easy for groups to make "straw" purchases to stockpile weapons for export.

Regardless of the sources of the weapons, terror groups and organized crime groups play a major role in the trafficking of weapons. Many of the weapons end up in the hands of these groups who then use them for training and terror attacks, or turn around and sell them at a profit to other groups.

The sale of illegal weapons is a developing enterprise, the illicit sales is valued at more the US $1 billion ("arms"). The beginning of the illegal trade can to a degree be traced back to the developing countries founding this industry through the developed countries discreetly supplying these struggling countries ("arms"). In several instances, the UN has been able to trace the origin of weapons used in African conflict to countries in Europe and Asia, including: Albania, Bulgaria, China, Germany, Hungary, India, Iraq, North Korea, Poland, Romania, Russia, Serbia, and Venezuela ("arms"). When the International Action Network on Small Arms (IANSA) surveyed collected weapons in the 2002-2003 Disarmament, Demobilisation, and Reintegration (DDR), and collected weapons by international

peacekeepers in Ituri, only a small percent of them were manufactured in Africa. Most of the weapons being provided to rebel groups are being supplied by the developed states outside of Africa. Furthermore, United Nations experts investigated violations in Somalia when an Ethiopian truck delivered arms to Somali militias (“arms”).

However, with states largely intertwined with supplying illegal arms to rebel groups within developing countries, it is impossible to say they achieved it on their own without the help with Government officials and private companies. These “middlemen” have been arms brokering, which is not illegal; however, brokers often create loopholes and weak regulations in order for small arms to be bought by somebody legally but then sold to a second owner (“arms”). International reports demonstrate how state-owned small arms leak into the illegal market through corruption, theft, and other diversions from the military and other police stockpiles (“arms”).

The economic impact from the illicit trade have been a dangerously threatening risk in Africa. Not only does this lead to direct medical, military and reconstruction costs, but it also diverts money away from production and drops income from tourism (“arms”). Africa has suffered from inflation, debt, reduced investment, unemployment, lack of social benefits, trauma, and death (“arms”). Africa has lost at least US $2.2 billion dollars in arms and ammunition, which has been imported by other countries between 2000 and 2010 (“arms”). Some of these consequences are not only damaging Africa’s economy, but the international community as well who suffer from the corruption of the sale of illegal arms and the violence that corresponds with it.

Works Cited

"Arms for Alms: Africa and Its Story of Illicit Trade in Small Arms." *Arms for Alms: Africa and Its Story of Illicit Trade in Small Arms*. Web. 28 Mar. 2015.
"Libya Is Epicenter of Illicit Arms Trade â€ “ UN." - *RT News*. Web. 28 Mar. 2015.
"Mikhail Kalashnikov, Inventor of AK-47, Dies at 94." *CNN*. Cable News Network. Web. 28 Mar. 2015.

Topic II: Combating Cyber Warfare and Cyber Terrorism

What is Cyber Warfare?

Cyber warfare is politically motivated hacking in order to conduct sabotage or espionage. U.S. government security expert Richard A. Clarke, in his book *Cyber War* defines "cyberwarfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. As a more subtle type of offensive, it is used in a widespread manner throughout the world.

Be careful to find the distinction between cyber warfare and cyber terrorism. Cyber warfare is strictly engagements between countries, whereas cyber terrorism is distinguished as unidentified attacks from non-affiliated groups.

Currently, many countries throughout the world have seen various forms of cyber warfare. Cyber warfare in the United States has been recognized. The United States has itself used cyber warfare in various relationships, and has taken measures to take defensive stances. China, who has been held responsible for a variety of cyber attacks, has used its capabilities to obtain valuable information, such as high-performance computers, nuclear weapon design, cruise missile data, and more. South Korea, in response to attacks from North Korea, has raised concerns and has taken measures to protect themselves. North Korea is known to have powerful cyber attack capabilities, and has displayed its power in various instances.

Cyber warfare is a global concern because of its relatively subtle mechanics and its widespread influence. It has the power to damage nations across the world almost instantaneously, and is a pressing issue for the United Nations.

It is not easy to predict what will occur with the war on cyber terror, but with the advancement of new technology, the threat of invasion of privacy, security, and sovereignty has been an international issue. Many people believe the threat is only within developed countries, but this invasion can pocket out from all developing and developed countries. The business and political world have seen a rise in digital attacks, and now there is international concern for the state's infrastructure, which if threatened, could cripple a country's ability to function. With unlimited information and communication offered online, the opportunities for cyber hackers and terrorism is endless. One of the many major infrastructures at risk through this cyber threat is power plants and telecommunications, which if out of commission can cause a domino effect for the rest of functional operations. If security measures are not issued on an international scale through state's budgets and policies, the problems the international community faces with cyber terrorism is boundless.

The UK has spent over US $1.3 million on programs going towards the country's cyber security capabilities within the Cyber Security Programme (NCSP), because the government is weighing the problem with much consideration on the potential damage it can cause ("beware"). However, the one UK Cabinet Office noted that there needs to be stronger cooperation from the international community including the "share of information in order to warn ahead of potential attacks"("beware").

Both the UK and USA have pledge to move forward with the issue, and are much aware of the risk since the issue continues to grow larger with the threat of the ISIS terrorist group growing and attacking through the use of computers ("beware"). Furthermore, E.J Hilbert, the heads of Kroll's cyber unit for Europe, the Middle East, and Africa, reported that hundreds to thousands of attacks have already been occurring in that area ("beware").

Cyberterror attacks have been frequently known in the USA for the alleged attacks on Sony from North Korea, but there has also have been international hacking if international news agencies by the "Syrian Electronic Army". Furthermore, in January of 2015, Malaysian Airlines claimed that its website by the "Cyber Caliphate", which claims to be affiliated with the Islamic State (ISIS) ("brutal").

With the UK and US's attempts to contain the issue, the two countries have developed "cybercells", which involves intelligence agents staging attacks against each other in order to test the resistance of certain sectors ("brutal"). For example, the first of these sectors tested was the financial sector, which tested the resistance of the City of London, Bank of England, and Wall Street ("brutal"). However, only to some degree can preparation be made without knowing the terrorist's intentions. Testing resistance will not be suitable for predicting future cyber attacks when loopholes can always be found by these hackers.

Works Cited

"Beware: A National Cyberterrorism Attack May Loom." *CNBC*. 27 Jan. 2015. Web. 29 Mar. 2015.