
Cyber Espionage and Warfare after the Second World War

Following the end of the Second World War, the U.N general assembly formed various committees to deal with different issues. One such committee was the disarmament committee. However since the end of the Second World War and following the build up to the cold war a shift in warfare has appeared. Warfare relied less on artillery and weaponry and more on espionage and cyber warfare. Despite the fact that the cold war virtually ended with the dissolution of the U.S.S.R in 1990 Cyber warfare has reached a pinnacle in modern times and is a pertinent issue now more than ever, with technological advancements the growth of the internet and the world wide web. Committee's main agenda is to tackle the downsize cyber warfare and malware as well as draw clear distinctions between information gathering and exploiting information.

Cybercrime has not been restricted to the U.S and Russia. Instances of cybercrime could be seen on Estonia, when many of her vital services were rendered useless for harmful periods of time after the removal of soviet memorial. Instances of Cybercrime can also be seen by the Assad regime in the Middle East with the use of the Syrian electronic army, it can also be seen in Iran with its FEPs being attacked by the American-Israeli efforts. The global cybercrime threat doesn't end there. Various hacking incidents in South Korea have been said to be orchestrated by North Korea, however due to a lack of tracing technology the hacking could only be traced to China, which also is infamous for its behavior with regards to hacking and cybercrime under Ji Jin Ping. China has been implicated in various Hacking scandals. The change in warfare and increase in technological capabilities of countries has even allowed economically poorer countries to target financially better off countries, such as the Pakistani hacking of the state bank of India. However the most prolific amounts of espionage can be seen between the U.S and Russia, this is despite the fact, the post the Cuban Missile Crisis a hotline installed between the pentagon and the Kremlin. The most recent U.S Russia Espionage crisis can be seen with the "alleged" hacking of the democrat national convention and prior to that there was the incident more commonly known as the Snowden files. Wherein ex American NSA and CIA I.T worker Edward Snowden became the world's most infamous whistle blower as he leaked classified information with regards to the U.S government's secret espionage campaign on her citizens as well as other nations and their leaders. The implications of the Snowden case were serious as Snowden seek refuge in Russia once again displaying that the U.S-Russian rivalry exists in post-Cold War times. To this day Snowden is living in Russia under asylum

Whilst Bolivia hasn't been as seriously impacted by the growth of cybercrime as the U.S or Russia, Bolivia does have gripe with the U.S and her NATO and western European allies. This is following an incident where in the Bolivian resident, Evo Morales' plane was grounded after

Need help with the assignment?

Our professionals are ready to assist with any writing!

[GET HELP](#)

the U.S had suspected that Snowden was on board. Furthermore, The French had said it was grounded for technical difficulties, this was a humiliating moment for Bolivia who is unwilling to comply with the U.S and her western allies till a formal apology is delivered. Bolivia is facing major internal problems, mass amount of crime through homicides and drug trafficking, as well as disease such as diarrhea and hepatitis A claiming large amounts of lives. This coupled with a negative migration rate, means that Bolivia has various internal problems to solve before it can extend itself with international help. This being said, Bolivia will still try to fight cybercrime while improving its cyber security and IT departments. Bolivia is looking to improve technology and telecommunications within Bolivia such that There can be an improve in medicine to help fight mass disease as well as an increase in security could help in the fight against petty crimes, homicides and drug trafficking in Bolivia.

There will have to be two steps taken before possible solutions can be drawn out. Firstly, the line between intelligence gathering and use of intelligence for malicious purposes has to be defined as, as of now it is a grey area, furthermore a sure fire way of tracing the cybercrime or hacking needs to be sought as it is necessary to identify the guilty party. Only once this is solved can a means to appropriately take action against the culprit be devised, thus Bolivia looks to aid in finding a way to solve these in committee as well as better her own cyber security and advance her technology.

While Bolivia looks to help in the war against cybercrime she will need a formal apology from the U.S and her west European allies before she can work alongside them, although Bolivia is willing to extend herself, her struggling economy and domestic issues could mean that her help is limited and she will always have to look to work toward her own best interests.

Need help with the assignment?

Our professionals are ready to assist with any writing!

[GET HELP](#)