BACKGROUND PAPER:

Disarmament and International Security Committee (DISEC)

Cyber Warfare

“I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We’ve created life in our own image.” – Stephen Hawking

Introduction:
As our world becomes increasingly digital, many amazing developments have occurred. We’ve mastered smart phones, created electronic currencies, and been connected through countless forms of social media. Computers have become integral parts of not just our everyday lives, but also the ways in which our country is both run and protected. However, with all these new changes come new risks as well. “Cyber-attacks” are now commonplace in international wars and as means of aggression in general. Computers are becoming the most important weapons and hackers the most menacing soldiers. Anything online can be accessed if hackers try hard enough, including international security information. The United Nations has not yet set any regulations for “cyber warfare” and “cyber terrorism”, but we encourage you to use this committee to make strides in creating a safer digital global landscape.

Background & History: Cybercrime has existed for as long as the internet. “trolls,” troublemakers, and others have attempted to hack everything from retail stores to banks, all the way to the pentagon. The internet is becoming an increasingly “hactive” place, attacks are now more prominent than ever, the pentagon reports that it alone has 10 million hacking attempts a day. Since 2006 we have seen a massive increase in “hactivist” groups and international security breaches. Beginning with the most famous of them all, Anonymous, the hacker activism, or “hacktivists” who in the past have leaked government documents to the popular site WikiLeaks, taken down the CIA website, and gone head to head with the church of scientology. On an international scale we see the constant cyberwar that china wages on the U.S. government and business. With an ever expanding amount of information available on the internet, and an expanding consumer size the internet is larger, more sophisticated and more dangerous than ever before.

Current Situation: Small-scale cyber-attacks are waged every day, but some larger operations and aggressions have received more media attention in recent years. One of the largest cyber-attacks was the Stuxnet virus, which infected at least 14 industrial sites in Iran in 2010, including a uranium-enrichment facility.
(Spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet) Since then, Stuxnet has spread across the globe, infecting well over 50,000 computers. Iran has not only been on the receiving end of cyber-attacks, though. The country has been responsible for hacking into the US Navy’s computer network in early 2014, and during feuds with Israel this summer; Iran launched a huge attack on Israeli computers that included hacking the Israeli Defense Force’s twitter account.

China is also a major aggressor, having been accused of hacking into Google’s corporate infrastructure in 2010. And of course, the United States has planned many cyber-attacks of its own, including the infiltration of Huawei, a premier Chinese telecommunications company.

**Committee Mission:**
The committee recognizes that cyber-attacks and international cyber warfare are daily occurrences, and attacks ranging from hacking online games, to cyber espionage are an internet norm. We encourage you to define the difference between hactivism and cyber terrorism. We as a committee feel that there are many ways to approach this issue; we encourage you to consider different legislations for times of war (cyber warfare) and domestic disputes. Establish whether cyber-attacks on private citizens of a nation, or corporations within the nation are attacks on the nation itself. If the committee decides that attacks on private citizens or corporations are attacks on the nation itself, this could lead to a more sensitive cyber and international landscape which comes with its own complications. We encourage you to consider creating an international body that keeps track of and helps countries deal with international cyber terrorism and crime.

**Questions to Consider:**
1.) Is recognizing that cyber warfare and cybercrime is an ongoing international issue, what can the UN as an international legislative body does to limit the toll it takes.
2.) Is it practical to enforce cybersecurity laws internationally? if so how?
3.) Should the UN recognize attacks on individual citizens and corporations of a country as an attack on the country itself?

**Sources for Further Research:**

4. International Telecommunications Union:
   [http://www.itu.int/en/Pages/default.aspx](http://www.itu.int/en/Pages/default.aspx)