Forum: Disarmament Commission Sub-Commission 2

Issue: Measures to ensure the creation and implementation of a new cyber disarmament treaty

Student Officer: Ashwin Utamchandani

Position: Deputy President of Disarmament Commission Sub-Commission 2

Introduction

Every day, the human civilization constantly develops, and with that development, both positive and negative outcomes arise, and it is important to distinguish the difference between one another. Cyber Disarmament is a long overdue issue that countries have been dealing with, and the sooner the issue is resolved, the better.

Years ago, militaries were well prepared to fight on land, at sea and even in the air, however, as we develop, a fourth face has arisen, and that is cyberspace. Cyber Wars are speedily becoming another way to combat, and with the dependency humans have towards the Internet, it is not hard to see how a disruption of computer infrastructure could easily cripple a society.

Definition of Key Terms related to the Issue

Ensure

Ensuring in this context is to secure or guarantee that a treaty will be created or implemented. It will be important to agree on practical, yet flexible solutions in order to create and implement a cyber-disarmament treaty.

Cyber War

A Cyber War is one of the upcoming ways to tackle a society, steal information or form a distraction. With the escalated levels of dependency toward the Internet, cyber wars, through the use of computers, have the goal to disrupt the activities of an enemy country, government or companies, especially the deliberate attacking of communication systems.

Cyber Disarmament

Cyber Disarmament is the current goal of most governments to try and combat the use of cyber war. It aims to stop the use of hacking, attacking of communication systems, sabotage and espionage.
General Overview

Methods and means of cyber warfare

Espionage and security breaches

Cyber espionage is the act of leeching private information from another person, company or government in order for military, political, economic, public or private benefit using illegal methods on the internet, through networks and software. Private information that has not been securely handled can easily be stolen through many different methods. Many attacks on the United States has occurred in the past, one of the most recent being Edward Snowden, using exploiting private information to the public.

Denial of Service attack (DoS) and Distributed Denial of Service attacks (DDoS):

Denial of Service attacks (DoS) and/or Distributed Denial of Service attacks (DDoS) are attempts of hacking with the aim to make a machine, network or website unavailable due to the extended number of “packets”, or fake users, on a network. Because of this, the network cannot handle the extended number of packets, and therefore shuts down, becoming unavailable. DoS and DDoS attacks have become increasingly common in the new age, and are normally used on high-profile website servers, such as banks, gaming companies and credit card companies.

Sabotage

Sabotage is a different means of cyber-attack, however is closely related to DoS attacks. The means of sabotage is to compromise military systems, government systems and even bank accounts to lead to the corruption and interception of classified material. Sabotage is mostly found with computer and satellite networks, being extremely hard to combat.

Terrorism

Unfortunately, Terrorism is one of the main means to start a cyber-war, normally between two opposing countries. Cyber-terrorism, as it is called, is the use of internet based attacks in terrorist activities, including acts of deliberate large-scale disruption, meaning government networks in the hopes of obtaining classified data in order to exploit a country. These are normally attached with means of tools, meaning Internet and computer viruses.

Civil and Private Sector

Civil and Private Sector cyber-attacks are mostly with the motivation of financial exploitation of another person or corporation, led by groups of people, sometimes on a larger scale than the average hacker. Computer hacking is a growing threat, and occurs in every aspect
of the internet, sometimes in the form of advertisements and free deals, or even a downloadable program targeted at companies and the average person.

The need for cyber disarmament

Cyber Disarmament is the act, or goal, of stopping or preventing the use of cyber-based attacks towards companies, persons or governments with the hopes of gaining information or blackmail in order for something in return.

However, as the Internet carries a borderless aspect, it is difficult for one international solution to be applied regarding cyber-security, and clearly unsurprising that the topic of cyber-security, cyber-warfare and cyber-disarmament has left a hole for international debate.

Since the election of President Obama, governments took a new approach to cyber discussions, and the final solution about cyber-disarmament. In previous years, diplomats focused solely on the need for countries to improve their own cyber-security, and cooperate in the fight against cyber-crime, however, there is not only one form of cyber-crime, therefore since then, and there has been no real solution.

Cyber-attacks can be crafted and manipulated by individuals and/or groups; furthermore, even without the involvement of a nation, cyber-attacks can make an impact on a very large scale. What must be taken into account is that the biggest and most innovating corporations today that have developed and deployed sophisticated defense systems are still breached, despite their efforts.

In order to stop cyber-terrorism, a treaty formed by the United Nations on the restriction of internet programming and other such related issues must be confronted head on, and thorough yet flexible suggestions must be made to ensure the creation and implementation of a cyber-disarmament treaty.

Timeline of Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of event</th>
</tr>
</thead>
<tbody>
<tr>
<td>23rd November, 2001</td>
<td>International treaty seeking to address internet and computer crimes taken was opened for signature by Budapest.</td>
</tr>
<tr>
<td>1st July, 2004</td>
<td>The treaty was taken into force and adapted by other countries</td>
</tr>
<tr>
<td>1st March, 2006</td>
<td>Additional Protocol to the Convention on Cybercrime was introduced.</td>
</tr>
<tr>
<td>November 2013</td>
<td>41 states officially ratify the convention, however leaving 11 states having not ratified the convention to address internet crimes.</td>
</tr>
</tbody>
</table>
UN Involvement, Relevant Resolutions, Treaties and Events

As stated by the United Nations Office for Disarmament Affairs (UNODA), the issue of information security has been on the United Nations agenda since the Russian Federation in 1998 first announced a draft resolution in the First Committee of the United Nations General Assembly. The relevant UN documents include:

- Report of the Secretary-General on the Developments in the field of information and telecommunications in the context of international security (A/68/156), (A/68/156/Add.1), (A/66/152), (A/66/152/Add.1),

Bibliography


