Introduction

The evolution of the Internet changed the way that individuals, businesses, and organizations gather, share, and process information. Nowadays, the mere action of typing and clicking on websites like Google can gather more information than searching at a local library and looking through printed sources. People can interact and communicate with others who are thousands of kilometers away. News stories from the opposite side of the globe are transmitted almost simultaneously and are received by the people. The development of the Internet can thus be called the epitome of modern technological revolution.

However, the increased use of the Internet made us vulnerable to the threats of malicious activities, such as targeted attacks, hacktivism, identity theft, and malwares. The Internet has also provided a new battleground for the world's superpowers as well. Today, states vie to hack other states to obtain confidential information, as proven by the revealed NSA (National Security Agency) scheme of the USA that extensively delved into the state secrets of USA's rivals and allies. Furthermore, the emergence of independent hacker groups such as Anonymous aggravated the already unpredictable nature of threats on the cyberspace. Delegates must keep in mind that the Internet and the information communication technology (ICT) are potent tools, yet they are prone to be misused by any party with malicious intentions. They must come up with pragmatic and apt solutions that can protect both the individual states' and the international community's cyber space.

Definition of Key Terms

Hacktivism

"The act of hacking, or breaking into a computer system, for a politically or socially motivated purpose" (Rouse). An individual who engages in the act of Hactivism is called a "Hactivist." A hactivist often disrupts normal service to bring attention to a certain social or political cause. Whether Hactivism is a crime or not is still being debated.

Denial-of-Service Attack
Also abbreviated as "DoS attack" or "DDoS attack." It is an attempt to make a machine or a network become unavailable to their users. Most perpetrators of DDoS attack use it as a form of expressing dissent and protesting. Sometimes a nation could use it to attack another nation's vital facilities (e.g. North Korea's July 27 DDoS attacks against South Korean government networks and websites).

**National Security Agency (NSA)**

It is an American intelligence organization primarily tasked with collecting, decoding, and analyzing information and data for counterintelligence purposes, as well as conducting surveillance on specific individuals on American land. It is authorized to acquire information through covert methods, including but not limited to bugging electronics and engaging in sabotage.

**Planning Tool for Resource Integration, Synchronization, and Management (PRISM)**

It is a mass surveillance data mining programme, used by the NSA since 2007. The PRISM collects information and data based on demand to internet companies, like Google Inc. Its existence was revealed by Edward Snowden last July, who described extent of its operation as "dangerous" and "criminal-like." The US government officials disputed some of Snowden's claim, stating that the PRISM helped the US prevent terrorist activities.

**Government Communications Headquarters (GCHQ)**

It is a British intelligence organization tasked with providing signals intelligence and information assurance to the British government and armed forces. According to The Guardian which exposed Edward Snowden's revelation, GCHQ is alleged to produce more metadata ("basic information on who has been contacting whom, without detailing the content") than the NSA.

**Tempora**

It is another mass surveillance data mining programme used by the GCHQ since 2011. Tempora extracts data from fibre-optic cable communications and processes it. Tempora is alleged to have acquired recordings of phone calls, content of e-mails, Facebook entries, and the personal internet history of users. According to Snowden, there is no distinction between targeted subjects and innocent civilians in information acquisition. The NSA also has access to this programme.

**Background**

Since the Second World War and the Cold War, information security has been a crucial sector for the nations. As the new millennium approached, the fear of the alleged Millennium Bug and attacks by cyber terrorists intensified among people. Although the Bug was found to be a hoax, it nonetheless became an early example of the public's fear of a large-scale cyber attack.
This issue is crucial in determining relations between nations. With no set precedent, it is critical for member states to peacefully come to terms to not exacerbate the problem into an unprecedented global cyber war. Nations have recognized that the misuse of Internet communications technology can potentially harm not only their internal security but also tarnish their international reputation. The recent events proved that preemptive measures are needed to hinder the escalating threat of cyber terrorism and cyber warfare. Nations would have to establish firm, practical, and definitive guidelines on how to reduce collective risk and protect critical national and international infrastructure, and a set of protocols and standards for information intelligence.

2000 Israel-Palestine cyber war

The Israel-Palestine Cyber War in 2000 was one of the first cases of politically-motivated cyber attacks perpetrated by a national authority. The crisis involved the defacing and denial-of-service attacks against Hezbollah-related websites by Israeli hackers and several Israeli Ministry websites and the Tel Aviv Stock Exchange by Arab hackers. Later, the conflict escalated into a cyber war, where foreign organizations linked to Israeli interest were also attacked. This was proven to be very successful. This also demonstrated that innocent third parties that are located many kilometers away can be affected by the cyber warfare. Cyber warfare may be the new form of warfare between nations, the one without guns and bullets.

2007 Attacks on Estonia

Estonia, a nation on the Baltic Sea and a former constituent state of the Soviet Union, was subject to multiple denial-of-service attacks in spring 2007. All Estonian cyber infrastructure remained offline for three weeks, from online banking to government websites. Estonia was especially hit hard by the attacks because it is one of the most advanced European nations in its internet usage; it is thus highly vulnerable to such attacks. The attacks coincided with Estonia's removal of a Soviet World War II memorial statue in Tallinn, in which several ethnic Russians were arrested after protesting the action. As Estonia was a member of the North Atlantic Treaty Organization (NATO), NATO officials were dispatched to Estonia to advise on strengthening Estonian cyber security. Estonia and the NATO blamed Russia for the attacks, but the Russian government denied any responsibility. This is known to be the first incidence in which one state targeted another state by cyber warfare.

WikiLeaks and Anonymous

The activities of organizations like WikiLeaks and Anonymous also created controversy. WikiLeaks is an organization that publishes secret information and classified media from anonymous sources. It was founded in 2006 in Iceland. In 2010, the organization surfaced in the mainstream media by the publication of the Afghan War Diary, the Iraq War Logs, secret files about the Guantanamo Bay detention camp, and the US State Department diplomatic cables. This created a huge backlash, with several companies ending their association with WikiLeaks and Julian Assange, its creator, being forced to live in exile in the Ecuadorian Embassy in London. The American Private Bradley Manning, indicted of releasing the secret documents to WikiLeaks, was sentenced to 35 years of prison and dishonourably discharged. Meanwhile, the world was shocked once again by the revelations of Edward Snowden, a former system administrator for the NSA, who divulged the existence and the scope of several American and British surveillance programmes, including PRISM and Tempora, to the reporters from The
Guardian in Hong Kong. Snowden was charged with theft of government property by the American government and was forced to seek temporary exile in Russia after staying in Sheremetyevo Airport for months. His revelations of the existence of a mass surveillance programme attracted criticisms from the EU nations which were spied on by the American intelligence.

**Major Parties Involved**

**United States of America (USA)**

The USA claims that many of its surveillance operations have protected their citizens' security and prevented terrorist acts. It has successfully prosecuted Private Chelsea (previously Bradley) Manning under the Espionage Act of 1917. After the revelation of the existence of NSA programmes, President Obama and other officials ordered for the review of intelligence and communications technology. Most of the government officials continue to maintain harsh stance against "hactivism" and other activities that may jeopardize its intelligence operations. The US Army blocked its employees' access to The Guardian website to prevent further spreading of classified information.

**United Kingdom (UK)**

The UK maintains a close relation with the USA especially in terms of intelligence cooperation. In a speech on June 10, William Hague, the British Foreign Secretary, assured the House of Commons that the GCHQ and other intelligence agencies uphold and practice the common UK law. He mentioned that in order for the agency to intercept an individual's electronic records, it needs a warrant signed by a cabinet-level official in the British government. However, Mr Hague denied to confirm or deny the accuracy of any leaked information.

**China**

China is another major player in the area of intelligence. In 2009, a group of Canadian researchers found out that China's global cyber-espionage network GhostNet managed to infect dozens of computers in more than 100 nations, infiltrating ministerial and diplomatic communications. However, the details and the validity of this programme have not been acknowledged by the Chinese government. After Edward Snowden disclosed the mass surveillance programmes, the Hong Kong SAR administration let him board the airplane to Russia, despite the American government's effort. China refuted USA's allegation that it was involved in Snowden's departure from Hong Kong. In addition, China expressed grave concern about Snowden's allegations that the USA hacked into many broadband and mobile networks in Hong Kong and mainland China.

**European Union, except the UK**

Many European nations reacted angrily upon the news of Snowden's revelation. German chancellor Angela Merkel and French president Francois Hollande designated the spying as "unacceptable." The EU Parliament
adopted new rules and protocols to fight cyber-crime on July 4, 2013, which was described by Cecilia Malstrom, EU Commissioner for Home Affairs, as "an important step to boost Europe's defences against cyber-attacks."

Democratic People's Republic of Korea (DPRK)

The Democratic People's Republic of Korea (DPRK) maintains a cyber warfare cell called Bureau 121. Defectors from North Korea claim that Bureau 121 is staffed by talented computer technology experts. They also testify that it is part of the General Bureau of Reconnaissance, an elite spy agency run by the DPRK military, and it has been involved in state-sponsored hacking incidents to sabotage its enemies. Members of Bureau 121 operate secretly, but they receive enormous financial incentives for their services. Bureau 121 has been blamed several times for targeted attacks on South Korean cyber infrastructure and finance systems. When the Sony hacking scandal broke out in December 2014, many, including the US Federal Bureau of Investigations (FBI) blamed DPRK for the hacking. The North Korean government denied any involvement and even offered to cooperate in the American investigation. However, the North Korean National Defense Commission, headed by the North Korean Supreme Leader Kim Jong-un, warned that should the US counteract on the DPRK, it will fight the USA both militarily and in the cyberspace.

Previous Attempts to Resolve the Issue

There have not been many attempts to resolve the issue through the passing of resolutions. After the collapse of the Soviet Union in 1991, the threat of cyber terrorism and cyber warfare grew. The United Nations managed to adopt a resolution in the General Assembly without vote in 1998 regarding "Developments in the Field of Information and Telecommunications in the context of international security" which was sponsored by Russia. This resolution was remarkable in that the UN recognized the use of ICT both beneficial toward mankind and "possibly inconsistent with the objective of maintaining international stability and security and may adversely affect the security of States." However, this draft only managed to outline the very issue of ICT and the collective security, without providing any further details. It failed to achieve or execute any practical solutions or protocols, for the resolution (and its subsequent updates) only "called upon" or suggested the member states to promote the consideration of existing and potential threats in international security.

Since then, this agenda has been annually debated in the United Nations General Assembly. In particular, the First Committee has been actively examining this topic. Other regional bodies such as the African Union (AU) and the European Union (EU) published conventions and strategies related to cyber security. The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organization that focuses on cyber security. Its mission is to promote and enable the cooperation and information sharing between the NATO, member nations, and partner states. NATO CCD COE sponsors a real time network defence drill called Locked Shields, helping the member states to practise and test the skills in order to be able to fend off a real cyber attack. It also conducts research on the applicability of the international law in cyber space. However, these
regional groups did not succeed in producing a multilateral treaty, which at the current stage seems to be the most effective tool in combating cyber warfare and terrorism.

- Developments in the Field of Information and Telecommunications in the context of international security, 4 January 1999 (A/RES/53/70)
- Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General, 30 June 2014 (A/69/112)

**Possible Solutions**

- To effectively combat cyber terrorism and prevent further cyber warfare, member states need to build a framework upon which all of them can agree. There would be a multinational forum for states to exchange their national views on the right use of ICT. The forum would work as a mediator between contentious states.
- The culmination of this framework would be a multilateral treaty that clarifies the exact definitions of the currently vague terms of cyber terrorism and cyber warfare. The multilateral treaty should also include a binding agreement regarding the extent the existing international laws can be applied to the cyberspace. Furthermore, member states would have to come to a conclusion on to what extent states can use the cyberspace for their national defense and international defense. In addition, it will enable the cooperation between states to combat hacktivism and mal-intentioned cyber attacks. Finally, it will strive to promote the clean and safe usage of the cyberspace between nations.
- Such framework is designed to build up a follow-up to the several passed UN General Assembly resolutions. General Assembly resolutions succeeded in raising awareness of the importance of ICT in terms of global security and identifying the core tasks, as stated in the following:

  3. Invites all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

  (a) General appreciation of the issues of information security;
  (b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;
  (c) The content of the concepts mentioned in paragraph 2 above;
  (d) Possible measures that could be taken by the international community to strengthen information security at the global level; (from UN GA Resolution 64/25)

  The aforementioned forum and the framework should be built on these points.
• An international inquiry should be conducted as to measure how sovereign nations have engaged in cyber warfare, to be investigated within the maximum parameter allowed by those nations' national security.

• Assistance should be given to the less technologically developed nations by the more technologically developed nations, to prevent a similar situation to the 2007 Estonia attack.

• There would need to be a binding force or an incentive for nations to proactively take up this issue. It may also be necessary to consider this issue in the Security Council as well, in order to establish negative consequences for those states that do not follow the multilateral treaty as prescribed above.

• The existing regional cooperation should be expanded for all the member states.

Bibliography


