Research Report

Special Conference 1: Security and Globalization

Countering cyber security attacks and establishing cyber security strategies in the digital age

MUNISH '14

Forum	Special Conference 1: Security and Globalization
Issue:	Countering cyber security attacks and establishing cyber security strategies in the digital age
Student Officer:	Abhash Bhattacharya
Position:	Deputy President

Introduction

"Hacking" can be traced back to the 1960s, when the large artificial intelligence laboratories present at universities were unprotected and became prime targets because of the precious data they contained. The term 'hacking' had a positive connotation, linked to "the mastery of computers, pushing programs beyond what they were designed to do" (St. Petersburg Times, Robert Trigaux). Within a couple of years, the first online connection started in 1969, and twenty years later Tim Berners-Lee developed the world wide web, the window that opened a world of online connectivity, known as cyber space. This became the perfect platform for cyber-interactions: social, political and financial. However, soon after, issues arose with respect to cyber security i.e. the protection of the platform itself, its users and its content. Hackers, who came to be known as cyber-criminals, used their computing skills to carry out security breaches, resulting in the theft of information. More recently there have been attacks on national security systems, which are considered cyber warfare.

In today's world, nearly 3 billion people (40%) have access to the Internet. The endless possibilities coupled with the vast amount of users have made the Internet a perfect place for cybercrime. The scope of hacking attacks can range from small scale personal websites to national security information. The United Nations defines two streams of Cyber Attacks: the political and military stream known as Cyber Warfare; the economic stream known as Cybercrime. Access to the Internet needs to be controlled, so as to make it a more secure and safe network for information, while protecting rights to information and controlling the risks of Cybercrime and Cyber Warfare. In order to achieve this, several measures must be taken by the United Nation with respect to cyber security. UN action on the issue of cyber security started in 1998, when Russia submitted a resolution to the First Committee. However, as hackers and hacking software have since become more developed, the security standards need to be uniform across nations and advanced in keeping with new developments.

Definition of Key Terms

The Internet

A global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide.

World Wide Web

A platform for online communications through the Internet, allowing people to share and access information from all over the world.

Digital Age

The Digital Age is an era of human history based on information computerization. The Digital Age is associated with the Digital Revolution, which refers to the growing number of people connected online in the world.

Hacking

The act of using technology (most often computers) to gain unauthorized access to data in a system belonging to a person, company or country.

Virus

A type of computer code, which has the ability to copy itself and spread on the computer, corrupting the system or destroying data.

Malware

Computer software or programs designed to damage or block computers.

Firewall

A protection system for computers to prevent unauthorized access.

Cyber Security

“Information security as applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the Internet as a whole.” (Wikipedia)

Cyber Security Attacks

Breaking into the cyber security systems to acquire private information. This action can happen on a personal level up to on a macro level, and is illegal in most places.

Cyber Security Strategies

Strategies and methods used to prevent and limit the number of cyber security attacks and breaches. This consists of a wide variety of methods, security concepts, policies and tools, to be discussed later.

Cyber Security Standards

Security standards that enable organizations to practice safe security techniques to minimize the number of successful cybersecurity attacks. These guides provide general outlines as well as specific techniques for implementing cybersecurity.

Cybercrime

Hacking into servers with the intent to gain economic benefits, i.e. bank account, monetary funds, etc.

Cyber Warfare

Hacking into servers with the intent of acquiring political information, i.e. confidential government information, access to weaponry.

General Overview

The nature of the debate on cyber security protocol is created when attempts are made to compromise between freedom and privacy of Internet usage and data access on the one hand, and the security and safety of the information, the users, and national policies on the other. Citizens and nations alike want to have freedom of expression, as well as having their privacy and data protected. The ability to use the internet freely without being constantly identified, monitored or tracked is desired, along with a plea for safety and security in cyber space. This dichotomous situation has resulted in a lot of debate, as trying to find a balance between the two aspects as well as having international cooperation on the issue is difficult to attain. Cyber space extends beyond national boundaries and geographies, thus calling for one international code to be followed by all. Thus, the role of the UN and its member states is critical to arrive at a consensus and urge urgent adoption of an international strategy to combat cyber security issues.

Past UN Involvement

Governance of cyberspace is developing, and is moving towards the establishment of feasible norms. Since the debates have been present in the General Assembly's first committee for more than a decade, at least half a dozen UN organizations have become involved in the issue most notably in the last five years, and in the latest proposals for a code of conduct. There was a lot of debate about cybercrime in the UN between 1998 up until 2004, when the Budapest Convention on Cybercrime came into force. There have been several standards or norms on cyber warfare emerging at the UN and related forums in the past decades. The speed with which the strategies are being proposed, discussed and adopted about cyber space has increased since the year 2006. With reference to appendices I and II, the graphs illustrate the norm emergence and sponsorship of resolutions in the first committee respectively. From the trend line it can be concluded that the norm emergence and sponsorship of resolutions increased significantly in 2006 when there was support from China, and eventually the US in 2008.

Russia submitted a resolution in the First Committee in 1998 to resolve international issues concerning Internet security. Initially, the United States of America never supported the attempts of the Russian Federation to attain cyber security. However, later in 2009 the U.S. changed their earlier stance by co-sponsoring the draft resolution on cyber security that had been introduced by the Russian Federation in 1998.

In 2010, a Group of Governmental Experts (GGE), consisting of diplomats from several powerful member states, stated that "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century". This was followed by Russia proposing an "International Code of Conduct for Information Security" in September 2011 (together with China, Tajikistan and Uzbekistan). In October 2013 the UN approved a Russian proposal titled: "Development in the field of information and telecommunications in the context of international security", a draft intended to keep the internet and mobile communications secure. The approval of the draft is dependent on the US's stance on the issue concerning Edward Snowden, who leaked confidential information from the US's national security agency. The UN General Assembly will debate this resolution this year.

Most recent UN Action

In 2013, a resolution to the General Assembly was submitted by Brazil and Germany calling for all countries to extend internationally guaranteed rights to privacy to the Internet and other electronic communications. The resolution also calls for more transparency to make the surveillance operations more conceivable.

Recent cybercrime incident

The biggest cybercrime case in U.S. history is a great example of the possibilities and effects of the activity. In July of the year 2013, a specialized hacking team consisting of five people from Russia and Ukraine hacked into various networks, and acquired access to the bank account details of several individuals and companies. The team hacked into networks, mined them for data, masked their activities through anonymous web hosting services, sold the stolen data (including at least 160 credit card numbers) and distributed the profits. According to the Inside Counsel, “The hacked companies include Nasdaq, Visa Inc., J.C. Penney Co., JetBlue Airways Corp. and Carrefour SA”, showing the vulnerability of large corporates with sophisticated protection tools. The total expense of recovery from the data breach cost the targeted companies more than 300 million dollars, and an attorney concluded that people with the ability to hack are one of the greatest dangers to national security. This large-scale recent incident further proves the urgent call for the need to recognize the threat, invest in sophisticated expertise and equipment, and above all, international norms to govern and police the cyber space.

Major Parties Involved and Their Views

The Russian Federation

Russia was the first country to take action addressing cyber security, submitting a resolution to the First Committee in 1998. In 2010, along with the USA and China, Russian delegates considered the issue of cyber-attacks the most serious of challenges in the 21st century, and followed up in 2011 by publishing a convention on International Information Security. On the other hand, Russia has been accused of conducting several cyber-attacks, such as the ones between 2007 and 2008 on several eastern European countries. More recently, the incident sparked by Edward Snowden has brought the Russian stance into the limelight regarding the formulation of cyber warfare policies.

The United States of America

The mission statement of the USA with respect to cyber security is the following: "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defence of specified Department of Defence information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." This mission statement shows the USA's full support of freedom in cyberspace, and allows for operations to take place.

A recent controversial case from the USA started when Edward Snowden hacked into the US servers and published confidential information of the US government surveillance plans on the public website WikiLeaks. He was accused for property theft, however people argue in his defence that what he did was correct as he was just informing the citizens of what their country is doing.

Organisation for Security and Cooperation in Europe (OSCE)

In December 2013 the OSCE participating states in the Permanent Council (decision No.1039, 26 April 2012), decided to step up individual and collective efforts to address the security of and in the use of Information and Communication Technologies (ICTs). They further decided to elaborate a set of draft Confidence Building Measures (CBMs) to enhance interstate cooperation, transparency, predictability, stability, and to reduce the risk of misperception, escalation, and conflict that may stem from the use of ICTs. The OSCE role as a regional arrangement under chapter 8 of the UN Charter confirms that the CBMs complement UN efforts to promote CBMs in the field of security of and in the use of ICTs.

European Commission

The European Commission established a Communication on a European Cybercrime Centre in 2012 which has four main aims:

1. Serve as the European cybercrime information focal point;
2. Pool European cybercrime expertise to support Member States;
3. Provide support to Member States' cybercrime investigations;
4. Become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

People's Republic of China

There is a lot of controversy around the People's Republic of China concerning cyber security and cyber warfare. China was one of the first countries to support Russia with respect to cyber security, supporting the resolutions and suggested conventions. On the other hand, China has allegedly been accused of conducting cyber warfare on countries including Australia, India, Canada and the USA. Most recently, China has suspended the Cybersecurity Cooperation with the USA after being charged with cybercrime.

International Telecommunications Union (ITU)

The ITU is the only UN organization working on issues related to cybercrime. It is a treaty organization that joined the UN under article 57 of the UN Charter. This union is run by large and specialized technical staff with the role of setting technology standards. The main role of the ITU, following the World Summit on Internet Security (WSIS), and the 2010 ITU Plenipotentiary Conference, is to improve security and safety, as well as build confidence in the use of Information and Communication Technologies (ICTs). The Global Cybersecurity Index (GCI) is an ITU-ABI research joint project which ranks the cybersecurity capabilities of member states.

Timeline of Events

Several cases of hacking have occurred in various countries over the course of the last three decades. Significant international attacks and viruses, as well as significant UN actions regarding this topic have been brought up.

Date	Description of event
1960s	First computers "hacked" by students in universities.
1982	First three viruses that attack Apple computers, making computers crash or leak information
1985	First virus that attacks PCs
1998	First resolution submitted to the UN by the Russian Federation
November 23rd 2001	Budapest Convention on Cybercrime
2004	Adoption of the Budapest Convention on Cybercrime
2008	Proposal for an International Cybercrime Convention from several member states
2009	Google China hacked into

April 2010	Proposal for a global treaty on cybercrime rejected due to stalemate between LEDCs and MEDCs
September 14th 2011	Russia and China propose an International Code of Conduct for Information Security
December 2011	ECOSOC event on cyber security and development
June 2013	Edward Snowden leaks confidential NSA information

UN involvement, Relevant Resolutions, Treaties and Events

International Telecommunications Union (ITU)

ITU is the United Nations specialized agency for ICTs. It is the single global organization including the 193, ICT regulators, leading academia, and 700 private companies all related to the IT sector. Of the 9 key areas of action, the ITU has a special thrust on cyber security activities as the facilitator of Action Line "Building confidence and security in the use of ICTs". Another key action area of the ITU is internet policy and governance, and its role is mandated in various resolutions regarding international public policy issues on the internet and its management.

International Multilateral Partnership Against Cyber Threats (IMPACT)

- First UN action with respect to cyber security
- Founded in 2008
- 149 Members

Resolutions

- 12th United Nations Congress on Crime Prevention and Criminal Justice, 21 December 2010, **(A/RES/65/230)**

  The resolution called for "technical assistance and training to States to improve national legislation and build the capacity of national authorities in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks".

- ECOSOC Draft Resolution 20/7 "deals with promotion of activities relating to combating cybercrime. Including technical assistance and capacity building".

Evaluation of Previous Attempts to Resolve the Issue

Several different approaches have been taken in attempts to resolve the various types of cybercrime. On an individual basis, many antivirus and computer security firms such as Norton and Avast have flourished trying to prevent cyber-attacks on an individual's computer or Internet server. By installing firewalls and educating users about safe internet conduct, these companies try to significantly reduce the amount of cyber-attacks at the unit level computer. Large corporations such as Facebook and Google, which depend on the cyber space for their services, are known to employ hackers to test out their security systems. This is an indication of the sophistication required to protect online systems which transact commercially or use private data. Unfortunately, none of these systems have a 100% success rate, however they are still developing and improving by the day. Efforts of the organizations mentioned above, coupled with private individuals, corporates and governments, all have recognized the need for adopted strategies for protection against cybercrime, however standardization and to some extent mandatory requirements and policing is required by a unified international authority to ensure efficiency and efficacy of these measures, while maintaining the right to freedom of information, expression, and access. At the micro level, the attempts to protect the cyber space have been many and there seems to be an adequate awareness for the need to combat cybercrime. With respect to privacy norms, some more standardization between the countries would help in unifying access rights thereby enhancing the possibility of protection.

On the macro level, governments have similarly adopted new security measures. However, the development of hackers has unfortunately progressed too. Some countries have tried to submit resolutions to combat the issue, however there is rarely collective support. Some parties want strong security measures, whilst others do not want to compromise freedom and privacy. National level security on one hand, and espionage on the other hand remain within the boundaries of governments, whereas the internet supersedes such boundaries. This makes it critical for such organizations like the UN and related bodies to adopt a single strategy for monitoring internet access and preventing cybercrime and cyber warfare.

There is large-scale awareness of the risks of cybercrime, particularly when related to economic considerations. The threat of cyber warfare and the underlying issues around the freedom of access and expression, the citizens' right to knowledge, and the risk of leaking national security data make it more difficult to arrive at a consensus or adopt international norms. The UN intervention is at this stage much needed to address the needs of cyber security and combat cybercrime. Despite all the security measures that have already been implemented, there are still large-scale security breaches happening frequently. The frequency and effects of these incidents call for new and more effective international norms to control cyber space.

Possible Solutions

The main problem at hand is balancing security and safety, whilst safe keeping freedom and privacy. Member nations have different views on the topic, and attending to all views would be the ideal solution to the problem at hand. This however would not be easily achieved so it is necessary for international organizations such as the UN to provide intervention, guidance and a common strategy to be adopted by all organizations, individuals and nations.

In order to combat cybercrime on a micro level, netiquette (basic guidelines of internet etiquette) could be incorporated into the educational systems so that Internet users are made aware of the dangers and respect codes. The need to step up research and training in security aspects of cyberspace are urgently required alongside the development of sophisticated software and hardware solutions. This aspect of managing cybercrime attacks the edit of the problem and is not yet a part of the international agenda

All personal computers could have malware prevention systems installed as standard to prevent viruses and hackers, and to prevent malware from spreading from computer to computer. Public and private networks could also have standard protection against malware and hackers. Public networks could notify all users of the risks of using the public network, despite the safety features. Data protection and secured access systems would help prevent cybercrime while maintaining the freedom to use and access cyberspace freely

Cyberwarfare and threats to national security need serious attention and should be regarded as part of international protocol. Cybersecurity should be treated as border security, transfer of arms or defense matters are given utmost importance while respecting international norms.

All security systems should constantly be updated to protect computers to the ever-developing computer hackers. Policies should be formally agreed upon and implemented to ensure regular updates over a given time period. Solutions to ensure this can be made possible just like patents and intellectual property rights are adhered to in the computer industry. The need for legislation to this effect is a necessary part of the solution.

It is important to understand that improving security will require more transparency in the systems. Nations need to find methods of implementing security methods without breaching the privacy of the users too severely. Honesty may be the best way forward, informing the users every step of the way.

The main issue at the moment in the UN is that not all member nations agree with the discussions. Unions and treaties have been established, however are seldom successful. If all countries were to see eye to eye and collaborate, the issue would be solved much more efficiently and effectively. The UN therefore needs to adopt a resolution that is binding on all its member states, taking into consideration the rights to information and data privacy, whilst protecting sensitive data. A unified approach to prevention of cybercrime and minimizing possibilities of cyber warfare is vital.

Bibliography

Post, Ashley. "Five Hackers Charged in Biggest Cyber Crime Case in U.S. History." Five Hackers Charged in Biggest Cyber Crime Case in U.S. History. Inside Counsel, 26 July 2013. Web. 17 June 2014. <http://www.insidecounsel.com/2013/07/26/five-hackers-charged-in-biggest-cyber-crime-case-i>.

"Computer Security." *Wikipedia*. Wikimedia Foundation, 13 June 2014. Web. 17 June 2014. <http://en.wikipedia.org/wiki/Computer_security>.

"Cyber Security Attack." *Wikipedia*. Wikimedia Foundation, 15 June 2014. Web. 17 June 2014. <http://en.wikipedia.org/wiki/Cyber_security_attack>.

"Cyber Security Standards." *Wikipedia*. Wikimedia Foundation, 06 June 2014. Web. 17 June 2014. <http://en.wikipedia.org/wiki/Cyber_security_standards>.

"Cybercrime." *DGs*. N.p., n.d. Web. 17 June 2014. <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm>.

"Cybersecurity: A Global Issue Demanding a Global Approach | UN DESA | United Nations Department of Economic and Social Affairs." ***UN News Center*****. UN, n.d. Web.**

17 June 2014. <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>.

"Developing an Effective Cyber Security Strategy." *PA Consulting Group*. N.p., n.d. Web. 17 June 2014. <http://www.paconsulting.com/our-thinking/developing-an-effective-cyber-security-strategy/>.

"Digital Age." *Wikipedia*. Wikimedia Foundation, 06 Oct. 2014. Web. 17 June 2014. <http://en.wikipedia.org/wiki/Digital_age>.

"ECOSOC Draft Resolution 20/7: Promotion of Activities Relating to Combating Cybercrime, Including Technical Assistance and Capacity-building."*Council on Foreign Relations*. Council on Foreign Relations, n.d. Web. 17 June 2014. <http://www.cfr.org/cybersecurity/ecosoc-draft-resolution-207-promotion-activities-relating-combating-cybercrime-including-technical-assistance-capacity-building/p28130>.

"Germany, Brazil Present UN Resolution on Cyberprivacy | Al Jazeera America."*Germany, Brazil Present UN Resolution on Cyberprivacy | Al Jazeera America*. N.p., n.d. Web. 17 June 2014. <http://america.aljazeera.com/articles/2013/11/7/brazil-and-germanydraftunresolutiononcyberprivacy.html>.

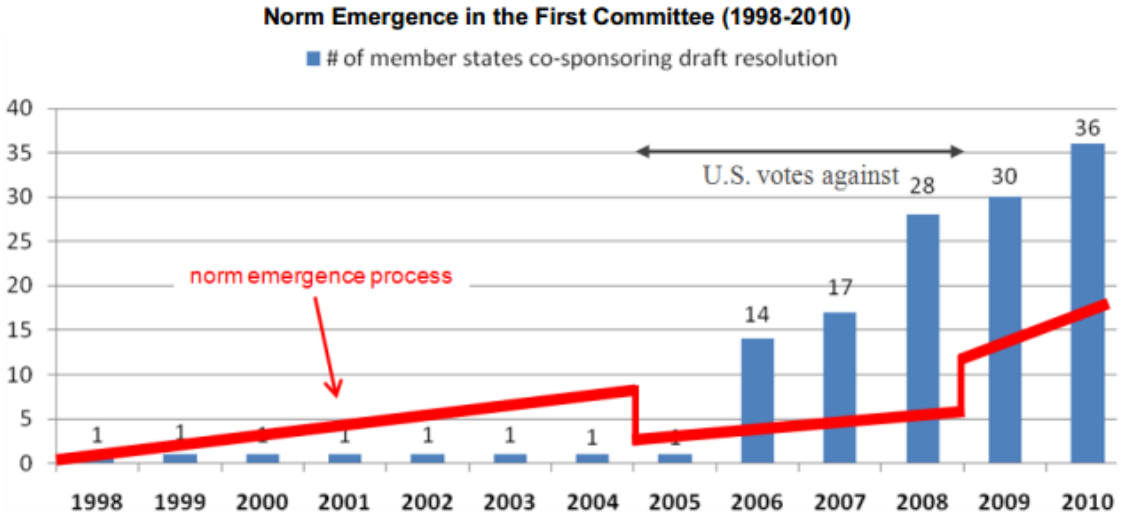
"Global Cybercrime Treaty Rejected at U.N." *SC Magazine*. N.p., n.d. Web. 17 June 2014. <http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/>.

"Google." *Google*. N.p., n.d. Web. 17 June 2014. <https://www.google.com/#q=define+hacking>.

Robert Trigaux. "A History of Hacking." A History of Hacking. St. Petersburg Times, n.d. Web. 17 June 2014. <http://www.sptimes.com/Hackers/history.hacking.html>.

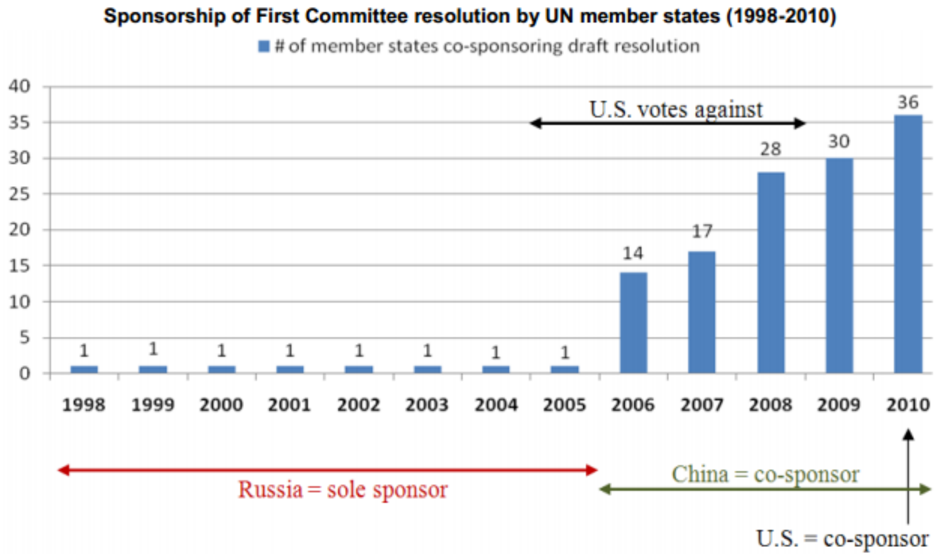
Appendices

I) The following graph shows the norm emergence in the UN First Committee



Science, Technology, And Public Policy Program, and Explorations In Cyber International Relations Project. "Cyber Norm Emergence at the United Nations." *Cyber Norm Emergence at the United Nations* (n.d.): n. pag. Harvard Kenedy School, 2011. Web. 17 June 2014. <http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf>.

II) The following graph shows the sponsorship of resolutions on cybercrime in the UN First Committee



Science, Technology, And Public Policy Program, and Explorations In Cyber International Relations Project. "Cyber Norm Emergence at the United Nations." *Cyber Norm Emergence at the United Nations* (n.d.): n. pag. Harvard Kenedy School, 2011. Web. 17 June 2014. <http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf>.