Leiden University

What factors explain why there is not a common and comprehensive global response to cyber threats?

Global Response to Cyber Threats

By Saulius Pakalniškis
(s1154788)
1st reader (supervisor): Dr. A. W. Chalmers
2nd reader: Prof. Dr. M. O. Hosli

6/11/2012

Word Count: 14,717

TABLE OF CONTENTS

INTRODUCTION

With the dawn of the information age and the pervasive introduction of digital and network enabled elements to so many, if not all, of our activities such as government, business, military and even our personal lives there is a wealth of information accessible at our very fingertips. Yet as we keep finding out with the growing importance of information technology these digital networks are increasingly under serious threat.

From the rise of extensive cybercrime, fears of terrorists exploiting digital infrastructure, state and corporate cyber espionage, crippling disruption by cyber activists and even suggestions of cyberspace becoming the fifth element of warfare (along with land, sea, air and space) the issue of cyber security has become extraordinarily important global issue (Zanders 2009: 2).

Despite this exponentially growing importance there has been no overarching and comprehensive global agreement or a set of agreements aimed at combating different types of cyber threats. While most states have introduced national measures and legislation pertaining to cyber security (cybercrimelaw.net), this is seldom enough to appropriately address and curb cyber threats that are inherently global and borderless in their very nature, therefore requiring a global response.

There nonetheless have been some attempts to provide a global framework for dealing with cyber threats, for example through the Council of Europe's Convention on Cybercrime, various resolutions and actions in the United Nations, as well as the Organization for Security and Co-operation in Europe and nearly all major international organizations, groupings or alliances (from the OECD to NATO). Yet most of these efforts have been moderately successful at best in accomplishing any of their goals of greater cyber security and all of them fall short of a truly universal, effective agreement on par with deals such as the Chemical Weapons Convention.

Thus with the potential risks posed by cyber threats to nearly all aspects of our lives, with the exponential digitalization and ever increasing use of networks it is a very urgent societal, governmental and business issue that we identify what is preventing a comprehensive and adequate global response to cyber threats. Because only upon identification of hurdles faced in developing a comprehensive global cyber security agreement, it is possible to find solutions for the appropriate ways of dealing with or circumventing these issues.

Therefore in this thesis I ask just that:

"What factors explain why there is not a common and comprehensive global response to cyber threats?"

This question is important because cyber threats are global and borderless in nature and cannot be effectively addressed on a national or even a regional level. Cyber attacks can come from anywhere in the world and target any system on the globe. Therefore close and systematic international cooperation is essential for monitoring, tracking, curbing and apprehending perpetrators of undesirable and illicit cyber activity. There simply is no other way to effectively address these threats.

Therefore in order to answer my research question I will examine what factors explain the lack of a global response to cyber threats by looking at mechanisms (such as agencies or task forces), initiatives (missions, programs) , agreements (resolutions, conventions, treaties, etc.) and problems (the issues that prevent the development of agreements, mechanisms and initiatives) in various international organizations that have stressed the importance of cyber security and that have attempted to address the problem of existent and emerging cyber threats. More specifically I will focus my efforts on two international organizations, namely the United Nations and Council of Europe, though I will briefly examine the activity of some other actors such as the Organization for Security and Co-operation in Europe, etc. I have chosen to closely examine these two organizations in particular for several reasons.

Firstly, I think it is essential to look at the United Nations because it is the flagship global organization for addressing international issues that truly affect nearly every nation in the world. In addition it has had great successes with various arms control conventions and agreements in the past. It is also the most inclusive organization in the world, uniting all recognized states in a large forum.

Secondly, I wanted to look at the Council of Europe despite it being a fairly regional organization largely because of the relative success it has had in building foundations for addressing a specific set of cyber threats, namely those emanating from cybercrime. In fact the Council's Convention on Cybercrime has become the prime agreement in the world dealing with this issue as well as the only binding one.

Lastly I will briefly look at the efforts of several other organizations such as the Organization for Security and Co-operation in Europe because it will provide a better picture of the cyber security efforts being undertaken globally and provide a better understanding of the challenges faced as well as show that the United Nations and the Council of Europe are the most substantial international forums in addressing cyber threats.

Upon examining these two organizations and their efforts of combat cyber threats and introducing any international cyber security agreements in more detail, as well as briefly going over the efforts of other important organizations, I identify the major reason that has led to, at best, a patchwork global response as being differing political and societal values of various states from which different laws and approaches to dealing with matter such as cyber security emerge. Thus in this thesis I argue that varying state values as expressed through priorities, objectives and approaches to international relations, ultimately create differing and difficult to reconcile positions on the issue of cyber threats, thus preventing a comprehensive global response. This reason while extrapolated mainly from only two international organizations is a general problem in attempting to combat cyber threats that are faced by most, if not all actors in the world.

While the scope of this paper is quite extensive, covering cyber security efforts of two major organizations and briefly looking at others, it is however not without its limits. I will in turn not be examining in any depth various anti piracy, copyright infringement and protection of intellectual property initiatives or agreements (such as the Anti Counterfeiting Trade Agreement or ACTA). While they have been numerous of these initiatives and they do somewhat impact upon cyber security, the sheer complexity of the issues faced cannot be done justice in this paper and would in my opinion require a separate research question.

Thus I will begin by briefly reviewing existing literature on the topic of cyber security, outlining my variables, hypothesis and indicators. I will go on to explain what exactly cyber threats are and give examples of the variation that exists amongst them for purposes of clarity. Finally I will examine both of my selected international organizations, briefly review the activity of others and at the same time I will identify the common problems faced in developing a comprehensive global response to cyber threats.

LITERATURE REVIEW

Most of the existing academic and policy related literature on cyber security starts out by underlining the rise of the Information Age and thus the centrality of information and communication technologies in nearly all sectors of society from government, to business and even to the individual level. Of course information has always been important but now in post industrial society information is more paramount, pervasive, accessible and vulnerable than ever before. In fact the dependence of society on information systems is simply overwhelming with so many activities having a network enabled capacity (Ganuza 2011: 11).

Needless to say the potential damage of cyber attacks therefore is quite large. One of the greatest threats is attacks targeting various critical infrastructure assets, such as telecommunications, transportation, power, financial services and defense. While such attacks may not likely be the scope of what some contributors call a “Digital Pearl Harbor”, nonetheless attacks can be very economically damaging and disruptive. In fact cyber attacks on critical infrastructures are now quite common. Perhaps one of the most famous ones is the Estonian case in 2007. After the decision to move a Soviet World War II memorial to a different location, which inflamed the Russian public as well as a significant Russian minority in Estonia, a wave of cyber attacks hit various Estonian government sites and businesses. With 98% of Estonian banking done electronically the disruption of bank sites paralyzed banking activity in the country. Even basic government communications were significantly affected by these attacks (Geers 2009: 5).

With there being a plurality of attacks such as espionage, disruption and/or destruction of critical information systems and statistics pointing to an exponential rise in malicious cyber activity, the desire for a secure cyberspace if growing amongst governments and non-state actors alike (Schmitt 2005:14).

In fact some contributors on the topic of cyber security have already boldly declared that the cyber arms race has begun. There might be good reason for such statements as well because many nations have stated in their strategic doctrines the importance to develop offensive cyber capabilities and amongst them some of the major global powers, such as the United States, Russia and China (Goel 2011: 132). In addition the US has already established its Cyber Command with the goal of protecting its military and defense networks form a continuous barrage of many thousands of attacks (Glenny 2011: 18).

Yet despite the development of offensive cyber capabilities by states and the seriousness of cyber threats in general, they have not been fully addressed in international forums or on a truly global level (Maurer 2011: 20 - 21).

It has been widely recognized that the lack of clear and widely excepted definitions on concepts relevant to cyber threats has been one of the main hurdles in developing global agreements on cyber security. In addition clearer definitions on various types of cyber attacks and international norm setting is important even when dealing with already existing international agreements. It is not clear now if cyber attacks should be viewed as aggression that is covered under Article 51 of the UN Charter or possibly under the solidarity clause in the Lisbon Treaty or even by Article 5 of the NATO treaty (Zanders 2009:2). If cyber space can be seen as the fifth domain of defense (along with land, sea, air and space) then cyber attacks could possibly be considered the same as kinetic attacks and therefore possibly even merit a physical response.

In addition there has been virtually no literature directly relating the implications of cyber security to international relations theory. Most of the literature on cyber threats has been written by or aimed at policy makers and therefore has not gone over any major theoretical considerations. This is somewhat of a loss because of the potential explanatory power theoretical considerations might bring to the table (Eriksson 2006).

Thus in conclusion, the literature on cyber security is still largely dominated by policy makers and professionals in the field rather than political scientists, though the amount of academic work done on it is growing at a significant rate due to the importance of the issue. As a result of this most literature is very pragmatic in nature with little to no theoretical considerations. Yet there is a large consensus concerning the types of threats faced, even though the scale and severity of the threats might still be subject to debate. Additionally there seems to be a great and in fact a near universal agreement about the need for a global response in order to adequetly combats these threats.

THEORY, VARIABLES AND HYPOTHESES

I approach the question of a global response to cyber threats through a somewhat realist perspective as I focus my examination on the actions of states in the main forums of bilateral cooperation on cyber security. There are a couple of reasons for me choosing such an approach. Firstly I define a global response to cyber threats as the existence of an inclusive global convention, agreement or treaty framework. These sort of global agreements are negotiated and ultimately entered into voluntarily by states, therefore when trying to asses why such an agreement has not been successfully developed it seems quite natural to look at states. Secondly it is less relevant to look at the impact of other actors such as international organizations when examining the topic of cyber security due to a virtually uniform support for greater global cooperation in tackling cyber threats from all major international organizations. I will further elaborate on this support when examining activity in the United Nations and the Council of Europe as well as briefly looking at other influential international organizations. Therefore with this nearly uniform support from other major actors I am lead to suggest that the problems in formulating a global response to cyber threats lie with states.

Therefore my independent variable in examining global cyber threats is the differing political and societal values of various regimes. More specifically values, expressed through preferences as stated priorities, support, opposition or concern in relation to certain issues or potential agreements on cyber security. These values usually differ noticeably between more liberal democratic states and more authoritarian states, and as a result considerably influence national priorities on the domestic and international stages. As I will later show more authoritarian states tend to lean to towards a more realist state centric values of military power and state sovereignty, whereas more liberal democratic states tend towards values coupled with economic advancement and individual freedoms. These values to a large extent shape state approaches to global responses to cyber threats.

Thus my dependent variable is that there is no common and comprehensive global response to cyber threats. As previously stated I define this concept more specifically as the lack of a common and comprehensive global response as the lack of a treaty, binding agreement or convention with significant global participation from all continents and regions, that provides a global framework for combating cyber threats.

Therefore I will show that differing values of regimes (IV) are the direct and most substantial cause of the lack of a common and comprehensive global response to cyber threats (DV).

Consequently the main and fundamentally overarching hypothesis that I will be working on in this paper is that the greater the similarities are of the political and societal values of states the greater the chance for agreement on a common, comprehensive global response to cyber threats.

DATA AND CASE SELECTION

Firstly I will briefly examine some of the different types of cyber threats that exist as well as their relative effects and severity. I will briefly identify and examine a few particular cyber incidents, to illustrate the diversity of cyber attacks possible. Next I will provide some important and relevant statistics from various sources pertaining to the quantity of cyber incidents, their trends over time as well as their financial implications, both globally and locally. This is important in order to better show the magnitude as well as prevalence of the cyber threat problem and to show that it is ultimately in the interest of all global actors to have a secure cyberspace. In addition this section will also show how important it is to find out what inhibits an adequate global response to cyber threats, which is ultimately the purpose of this thesis.

Furthermore as previously stated I will be looking primarily at cyber security attempts by the United Nations and the Council of Europe due to their central status as forums in the global cyber security debate.

I will be using several different data sources in answering my research question. While examining the UN, I will primarily be looking at various resolutions (or the lack of them), their content (how much they are geared at progress towards a global agreement or convention), support for them (or lack of support), statements (expressing concerns or support in relation to various initiatives), work being done by various UN agencies concerned with cyber security and strategic considerations of some states.

Furthermore, when looking at the Council of Europe I will focus on the number of participants of the Convention on Cybercrime, the level of participation (just signing or full ratification and accession of the convention), geography of participation (where are most participant states located, whether they are primarily from one region, a particular continent or are they well dispersed across the globe), the reasons given for not participating in the convention or its additional protocol by various states, concerns expressed by participants on the content and or specific requirements of the treaty and possible hurdles to future participation of some states.

Finally I will briefly outline the efforts and positions in relation to the combating of cyber threats of several other prominent international organizations. I will do this mainly to further emphasize the point of uniform support for global cyber security by all major international organizations and therefore reinforce my method of looking for the major factors preventing such an agreement lie at the state level, or more specifically are driven by the values of particular states that are often correlated with specific regime types. In addition this section will also help to reaffirm my decision of focusing my examination of global cyber security efforts within the framework of the United Nations and the Council of Europe by showing that they are the most advanced on the issue relative to other major organizations.

Lastly since differing values of regimes are important to my overall argument I will use Democracy Index data to classify regimes either as more liberal democratic or more authoritarian leaning.

CYBER THREATS

In this section I will outline some of the different types of cyber threats, give several real world examples of them and present some relevant statistics concerning malicious cyber activity. I will do all of this in order to provide some basic understanding that is vital for a further and deeper examination of the topic and show how these threats fundamentally affect the whole globe. This is vital for showing the apparent paradox that despite a global response to cyber threats being seemingly beneficial to nearly all states as well as many other global actors (such as businesses and even private individuals) no comprehensive and substantial response exists.

Firstly though, it should be noted that cyber threats are fundamentally different from any other because they usually do not involve any kinetic, or in other words physical, effects or actions. Yet they nonetheless have a huge potential for damage because digital and networked enabled elements permeate our governments, infrastructure, businesses and even private lives.

Secondly cyber threats are fundamentally borderless and global in nature. They can originate from absolutely any place in the world and target virtually any other place. In addition some attacks may originate in one country, use a botnet (a group of voluntarily or involuntarily remotely controlled computers, used to increase the effect of some types of cyber attacks) of computers in another (or even several other) country and target a server or website in a third. Thus effective solutions for such global threats have to in turn also be truly global.

For a start it might be helpful to split cyber threats into two very broad categories, namely cyber warfare and cybercrime. Cyber warfare is malicious cyber activity directly threatening the security, defense capabilities, vital infrastructure or societies of a particular state or region. An act of cyber warfare can include espionage (acquisition of sensitive information), disruption or destruction of critical infrastructure (such as communications), manipulation of defense or other vital systems. These attacks are generally taken to be perpetrated by states, terrorist or other militant organizations or by proxies acting on behalf of the afore mentioned. Cybercrime (often referred to as computer crime in legal matters) on the other hand refers to criminal act perpetrated using computers and their networks. Cybercrimes often can include personal information theft by various means in order to use it to gain access to bank accounts. Other examples might include corporate espionage through cyber means. Yet not all cybercrimes are committed for financial gain. Hacktivism and so called recreation hacking are great examples of this. The former is done for political values, ideals (such as freedom, self determination, etc.) or on the behalf of particular causes and latter is done for the “lulz” (basically for fun or for recognition amongst peers, namely others in the hacker community).

Secondly it might be useful to identify some of the most prominent methods used to commit various cyber attacks. One of the most pervasive ones and probably one of the easiest to commit is called a denial of service attack (DoS) or more commonly a distributed denial of service attack (DDoS). These attacks are very common because of their relative ease of execution and significant impact upon the target. To put it simply perpetrators of these attacks often use computer programs called network stress tools, such as the Low Orbit Ion Cannon (LOIC) to target a particular website or network. These stress tools work by bombarding the target with very large numbers of requests, therefore overloading servers, consuming all the bandwidth and at least temporarily making the network or webpage inaccessible (DoS Attacks - CERT). DDoS attacks use the exact same principle but on a larger scale by enlisting multiple computers in a botnet (voluntarily or not) to amplify the effect of the attack. Network stress tools like LOIC can be easily downloaded on the internet and used by anyone with even minimal computer knowledge because they do not require any programming or coding skill. For these reasons DDoS attacks are very popular with hacktivists such as Anonymous, though they are also frequently used by other actors.

However the most popular method of committing cyber attacks is by way of malware which is catch all term that describes all malicious software or pieces of code. In fact malware attacks account for as much as 67.1 per cent of all committed cybercrimes according to recent surveys (CSI Comp Crime Survey 2010/2011). Malware probably most notably includes attacks with computer viruses or worms. These are types of malicious self replicating programs that infect computers and spread through networks and the internet. Worms specifically are a subset of computer viruses that spread by making copies of themselves in every infected computer or system. Viruses in general can be programmed to perform many different actions, from just spreading and replicating oneself, to deleting or altering programs in target computers, granting remote access to third parties to an infected computers, stealing or spreading data from computers or servers and performing other pre programmed actions. Thus their effects can range from the relatively benign to the very dire (Moir 2003).

While there are other means of committing various cyber attacks, they are all based on the same principles of exploiting vulnerabilities and finding system loopholes to achieve desired effects. Those effects can be anything from, disruption or destruction of information, to control or access of a system. Moreover in recent years there have been many different well publicized cyber attacks committed using various different methods, targeting a lot of different entities and ranging in scale and severity.

Many well publicized denial of service attacks were perpetrated during the Arab Spring uprisings by the hacktivist collective and internet grouping called ‘Anonymous’. One of the first of these was the so dubbed *“Operation Tunisia”* by the Anonymous collective, targeting several websites of the Tunisian government during the mass protests that took place in the country in the beginning of January 2011. The websites taken down by the DoS attacks included those of the ministry of foreign affairs, the stock exchange, the ministry of industry, the president and the prime minister (Hill 2011). While these attacks were considered by many to be commendable and positive, they nonetheless were at least formally criminal acts. Yet cyber attacks can be a lot more severe than just the disruption of websites which is usually simply a basic tactic employed by hacktivists.

This brings us to an example of probably the most famous cyber worm attack in recent times, namely that of the worm known as ‘Stuxnet’ that primarily affected the Natanz nuclear facility in Iran in June 2010. The worm had been called the most sophisticated cyber weapon to date and is credited by some with temporarily paralyzing the Iranian nuclear program; though the Iranian government has repeatedly denied that it caused any severe damage or disruption. Therefore it is hard to know the true scale of the impact of the attack. What is known is that the worm works by infiltrating and gaining remote control of the target system in turn reprogramming it. Stuxnet in particular target centrifuges used in uranium enrichment by changing the frequency of the electric current to them, thus disrupting their normal operation and potentially sabotaging the enrichment process. While the source of the Stuxnet worm is unknown, it was referred to by some as a military grade cyber weapon, which has lead to speculation that it has been created by some state trying to interfere with Iran’s nuclear program (Farwell 2011). Yet whatever its origin the Stuxnet attacked proved that cyber weapons can potentially cause not only damage in cyberspace, but can be used to manipulate processes that transfer in to kinetic effects, possibly inflicting physical, real world damage.

There have also been many prominent attacks that targeted corporations and other private entities. A good example of this is an intrusion in June 2011 by unidentified hackers into Citigroup (one of the largest financial services companies in the world) servers saw the mass theft of the credit card as well as other personal information of more than 200,000 of their customers (Kravets 2011). Another good example are the attacks that occurred in May 2011 on the US defense and aerospace company Lockheed Martin, which produces several fighter jets such as F-16 and F-22 for the US armed forces. While official reports suggested that the damage from the attacks was minimal and quickly responded to, it is reported that restoration of normal employee access to its systems took at least several days following the incident (BBC News 2011).

Besides the above stated specific examples of various cyber incidents it is also important in understanding the effect of global cyber threats on all types of global actors to take a look at broader trends and statistics to do with cyber threats to really get a clearer picture of the gargantuan scope of the problem.

For example a recent report on cyber threats in the United States provided a shocking insight into the exponential growth of these incidents every year. The report stated that cyber security incidents in US federal agencies have increased by a staggering 680 per cent over a period of six years. This huge rise in attacks is said to be especially due to the increased activity of hacktivists and state sponsored actors (Freedberg 2012). Furthermore a report done by Symantec has valued global losses due to cybercrime in 2011 at 388 billion USD with 441 million people worldwide being affected by them. As the report points out, cybercrime globally costs the world a much greater amount than the global illicit trade in marijuana, cocaine and heroin combined, which is valued annually at 288 billion USD (Norton Cybercrime Report 2011).

Additionally in 2010 the *"Second Annual Cost of Cyber Crime Study"* done by the Ponemon Institute based on a representative sample of 50 sizable companies from different industry sectors in the United States revealed that the costs incurred from cybercrime for them ranged from 1.5 million up to 36 million USD per annum, with the median cost being incurred standing at 5.9 million USD. These loses represented a staggering 56 per cent increase from the results of the same study conducted the year before. The study noted that the 50 organizations in the sample sustained about 72 successful cyber attacks per week, averaging out at more than one per week per company. This also showed an increase from the 2010 study by 44 per cent. Moreover it was also found that some of the most costly attacks for these companies were actually basic denial of service attacks that severely disrupted business (Ponemon Institute 2011).

Thus it is not difficult to see that cyber threats have severe security and financial implications to the public and private spheres. Due to the global nature and prevalence of information systems with network enabled capabilities cyber threats do not leave any state, business or private individual safe from their adverse effects. In addition cyber attacks are no longer rare occurrences, but very common, pervasive and at times extraordinarily damaging events. Furthermore, precisely the global nature of these threats once again leads to the inevitable conclusion that any significant solution to them has to be global as well. Yet despite the nearly universally harmful nature of cyber threats there has not been a comprehensive global response. I will begin examining the reasons for this by looking at cyber security efforts and actions in the United Nations.

UNITED NATIONS

The United Nations has on multiple occasions expressed the importance of cyber security and its support for global solutions to existent and emerging cyber threats. The UN Economic and Social Council (ECOSOC) on December 9th, 2011 held a special event on Cyber Security and Development in which it was stressed that

> *Cyber security is one of the greatest issues of our time, and will continue to grow in importance. As more and more people use mobile phones and the Internet, it is our collective duty to ensure that ICTs [information communication technologies] are safe and secure so that the 7 billion people of this planet can reap the benefits of ICTs. Today, everything is dependent on ICTs and we are all vulnerable – cyber security is a global issue which can only be solved with global solutions* (ECOSOC Special Event 2011).

Furthermore concerns with cyber threats have been similarly reiterated by the UN Secretary General Ban Ki-Moon, while stressing the importance for global solutions and international cooperation in addressing them due to their both interconnected and trans-national nature (UN News Center 2010).

These or similar sentiments have been echoed across many UN institutions and agencies therefore there can be little doubt of that the UN recognizes the ever growing importance of cyber security or is very committed to helping facilitate appropriate and comprehensive global responses to cyber threats.

Yet perhaps the most important body in addressing security concerns within the UN framework, namely the UN Security Council, has largely been silent on the question of cyber threats and security. It has not made any resolutions pertaining to cyber security despite their being significant cases in which they were possible. Examples of these cases include the 2007 Estonian and 2010 Iranian cyber attacks. In addition the 2008 resolution on Georgia failed to mention the pressing cyber aspects of the conflict. In fact the UN SC involvement in cyber security matters seems to be solely limited to the Counter-Terrorism Implementation Task Force (Maurer 2011: 17).

Nonetheless cyber security is being discussed in other parts of the UN, most notably the General Assembly. In fact, cyber security focus in the United Nations GA can largely be split up into two somewhat separate fields, namely that of the economic and the politico-military (Maurer 2011: 15). The economic sphere as the name would suggest is primarily concerned with issues of cyber crime, i.e. cyber attacks perpetrated usually by non state actors that in one way or another are committed for financial gain or possibly to directly obstruct certain economic activity, business and perpetrate other criminal activities. The politico-military field on the other hand is concerned with attacks that threaten national, regional or global security and defense; these are usually taken to be committed by states, terrorist organizations or proxies of either.

The GA Third Committee and ECOSOC are the primary intergovernmental bodies concerned with the economic sphere of cyber security. They are supported by the United Nations Office on Drugs (UNODC) and Crime and the United Nations Interrogational Crime and Justice Research Institute (UNICRI) (Maurer 2011: 15).

The UNODC is mandated to help UN member states combat narcotics, crime and terrorism. It focuses on research into these areas, international treaty implementation assistance for member states and technical cooperation assistance (UNODC.org). It engages in many projects relevant to cyber security such as the launching, in partnership with Microsoft, of the *"Advanced*

Forensic Training on Cyber Crime and Computer-facilitated Crimes against Children" program to train law enforcement officials (G. Lewis Speech 2006) and the effort to establish a 'Virtual Forum Against Cyber-crime' (Kemp 2007).

UNICRIs main function is to help governments and various organizations to implement and improve policies concerning crime prevention and justice. It aims to improve the efficiency of criminal justice systems and further the understanding of various criminal problems. It has been quite active in the area of cyber crime by conduction various research into cyber crime and hacker profiling. It has also accumulated valuable information on cybercrime activity, as well as malware and botnets. In addition UNICRI has been engaged in training policy makers, judges and prosecutors on various aspects of cyber crime and electronic evidence (UNIRI Cybercrime Initiatives).

The GA First Committee is the primary intergovernmental body dealing with the politico-military sphere with assistance from International Telecommunications Union (ITU), United Nations Institute for Disarmament Research (UNIDIR), Counter-Terrorism Implementation Task Force (CTITF).

The ITU is the UN agency responsible for information and communication technologies (ICT). It develops technical standards for ICTs and promotes greater access to them. In terms of cyber security the ITU has developed the Global Cyber security Agenda (GCA) with which it promotes greater international cooperation in developing global cyber security measures. This agenda offers a five pillar approach to cyber security that includes legal measures, technical and procedural measures, organization structures, capacity building and international cooperation (GCA brochure 2007). The ITU has also made numerous resolutions within its framework reiterating its commitment to enhancing security in cyberspace, helping to build confidence in the use of ICTs, as well as training and awareness-raising on cyber security (ITU Resolution 130).

The United Nations Institute for Disarmament Research (UNIDIR) provides independent research on various disarmament issues and promotes cooperation in finding solutions for them. The institute primarily functions as an advisory body and international forum for discussion.

Cyber threats in particular are covered by the institute under the heading of emerging threats, with various reports and numerous articles available on the topic (UNIDIR.org).

The CTITF's primary role is to "enhance coordination and coherence of counter-terrorism efforts of the United Nations system", thus its scope for addressing cyber threats is quite limited (UN Global Counter Terrorism Strategy). Its focus is largely on terrorist use of the internet and its primary concerns are currently largely not about terrorist organizations launching cyber network attacks against critical infrastructure or engaging in other types of cyber terrorism, but rather on the use of the internet as a communication, propaganda, financing, training, recruitment, radicalization and data mining tool (CTITF 2011: 1). Therefore the work done by it is not directly focused on cyber security matters.

Therefore the issue of cyber security has got more direct attention from the UN General Assembly. In fact primary efforts in response to the emergence of cyber threats within the United Nations began with a resolution titled *"Developments in the field of information and telecommunications in the context of international security"* introduced by the Russian Federation and adopted without a vote in the 53rd session of the General Assembly in 1999 (A/RES/53/70).

The resolution firstly noted the rapid development of information and communication technologies and their great benefit to all of humanity but also expressed concern that these emerging technologies can also be used for malicious purposes (possibly by terrorists or criminals) that would potentially threaten global security and stability.

The resolution was encapsulated in four key points:

1) [The General Assembly] Calls upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;
2) Invites all Member States to inform the Secretary-General of their views and assessments on the following questions:
    (a) General appreciation of the issues of information security;
    (b) **Definition** of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

(c) Advisability of developing international **principles** that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality;

3) Requests the Secretary-General to submit a report to the General Assembly at its fifty-fourth session;
4) Decides to include in the provisional agenda of its fifty-fourth session an item entitled "Developments in the field of information and telecommunications in the context of international security".

(UN General Assembly A/RES/53/70)

The broad goal of this resolution was to spark a dialog amongst member states on the issues of information security with the rapid development and proliferation of information technologies. The development of widely internationally recognized, clear definitions and principles concerning cyber security is an essential precursor for the development of any truly global and comprehensive agreement or treaty on cyber security. This resolution was to be reviewed and a report on it was to be submitted by the Secretary General to the General Assembly during the next (54th) session. The resolution was also entered into the next session agenda as it has been done continuously every year thereafter.

The resolution kept being readapted every year without any significant changes to the actual text being made. Yet there were some significant changes made to the original text of the resolution in the 60th session in 2005. The new resolution (A/RES/60/45) most notably changed the invitation for member states to inform the Secretary General on their views and assessments on the *"Definition of basic notions related to information security…and information resources"* (A/RES/53/70 - 3(b)) to *"Efforts taken at the national level to strengthen information security and promote international cooperation in this field"*. It can be argued that this **somewhat weakened** the resolution by no longer making a direct call focusing on developing internationally recognized definitions that are essential to the development of comprehensive agreements or conventions but rather focusing on more practical, easier and less politically controversial aspects of cyber security such as national efforts to address cyber threats. This is somewhat at odds with numerous statements by the UN emphasizing the global nature of cyber threats and the insufficiency of national responses.

Nevertheless the changes to the text of the resolution were only one problem. Efforts by Russia to push for the development of a cyber arms control agreement were viewed with suspicion by some European nations and even more so by the United States. It was largely thought that Russian efforts were more aimed at limiting the perceived or real dominance and superiority the US possessed in cyber space. In addition US official were concerned that the Russian Federation efforts to secure their cyber space would lead to censorship of political dissent on the internet and other means electronic communication under the guise of security (Maurer 2011: 17).

Thus the 60th session also marked the first time the resolution - *"Developments in the field of information and telecommunications in the context of international security"* was voted on in the General Assembly as all previous times it was adopted without a vote. A total of 177 nations voted in favor, with one voting against and zero abstaining from the vote, thereby adopting the resolution. The only member to have voted against was the United States citing reasons such as the unwillingness to support a 'global instrument' [a reference to clause 4(b) -*"Possible measures that could be taken by the international community to strengthen information security at the global level"*] and another group of governmental experts on the subject in the future (UN Disarmament Yearbook 2005).

The United States continued to be the only one to vote against the resolution every year up to 2009, even as the resolution gained ever more sponsors from 2006 onwards, complimenting the initial sole sponsorship of the Russian Federation. In 2006 the resolution (A/RES/61/54) was sponsored in total by 14 members – Armenia(hyb), Belarus(a), Chile(flwd), China(a), Ethiopia(a), Kazakhstan(a), Kyrgyzstan, Madagascar(a), Mali(flwd), Myanmar(a), Russian Federation(a), Tajikistan(a), Turkmenistan(a), Uzbekistan(a) (UN Disarmament Yearbook 2006: 455). It should be noted that all of these states except for Armenia, Chile and Mali are classified as authoritarian regimes according to the 2011 Democracy Index. In addition Armenia is considered to be a hybrid regime, which is leaning more towards authoritarian regime than a liberal democracy, while Chile and Mali are considered to be flawed democracies (Democracy Index 2011). The following year the resolution (A/RES/62/17) had 13 sponsors (the same ones as last year with the exception on Turkmenistan which became a co-sponsor) and 4 co-sponsors – Cuba, Japan, Nicaragua and Turkmenistan (UN Disarmament Yearbook 2007: 14). Out of the new co-sponsorships, Japan is considered to be a democracy while, Nicaragua – a hybrid regime and Cuba an authoritarian regime (Democracy Index 2011). By 2008 the resolution (A/RES/63/37) already had 24 sponsors and 4 co-sponsors, with new sponsors including India, Serbia, Democratic People's Republic of Korea (and many others), and a new co-sponsorships by Brazil, Vietnam and Fiji (UN Disarmament Yearbook 2008: 6). This year again included more support from authoritarian regimes such as Fiji, North Korea and Vietnam, but also included increased support from flawed democracies like Brazil, India and Serbia (Democracy Index 2011). By 2009 the *"Developments in the field of information and telecommunications in the context of international security"* resolution (A/RES/64/25) was once again adopted without a vote, with sponsors and co-sponsors increasing yet again to 29 (UN Disarmament Yearbook 2009: 12). Finally in 2010 (A/RES/65/41) the sponsorship and co-sponsorship increased to 36 members, including for the first time developed countries such as Canada, Germany, Australia and probably most notably of all the United States, after its former long standing suspicion and opposition to the resolution (UN Disarmament Yearbook 2010: 8-9). Thus only in 2010 did the resolution receive greater support from liberal democracies such as Canada, Germany, Australia and the US (Democracy Index 2011). Despite this in 2011 the support in terms of sponsorship and co-sponsorship decreased to 32, with the US and several of the developed nations no longer sponsoring the resolution (A/RES/66/24), yet it was once again adopted without a vote (UN Disarmament Yearbook 2011: 16-17).

Therefore we can see that the support for this important resolution on cyber security has generally been growing and even has at one point received the sponsorship of several developed, liberal democratic countries and even the US, which harbored the most doubt, suspicion and opposition towards it. Nonetheless the significant revision of the original text, to a **less committal and arguably more practically based** one in the 60th General Assembly session in 2005 can be seen as important drawback in developing a comprehensive global cyber security agreement. In addition, the overall support in the form of sponsorship for the resolution has come overwhelmingly from authoritarian or authoritarian leaning regimes, showing a significant divide and lacking of western liberal democratic support. Furthermore the decrease in active support for the resolution, especially by the US as well as other developed countries is a worrying sign to say the least and a hint of old doubts resurfacing. Ultimately there seems to be a disparity between the values and perhaps urgency concerning the need of securing cyber space between developed, western liberal democracies and more eastern, developing, more authoritarian regimes.

Both western liberal democracies and eastern authoritarian or semi-authoritarian regimes seem to comprehend and acknowledge the seriousness of cyber threats and the need for global cyber security measures. Yet the semi-authoritarian eastern regimes seem to give more primacy to security above most other considerations (especially to security in military cyber arms sphere) while the western liberal democracies are not willing to sacrifice some of their core values like freedom of expression (as well as dissent) or individuals right to privacy. Therefore the push for a cyber security or a cyber arms treaty largely supported by authoritarian regimes is viewed with great suspicion in the west. So we can see clearly just by looking at this resolution on *"Developments in the field of information and telecommunications in the context of international security"* and its varying support that a significant obstacle to a comprehensive and widely supported cyber security treaty, agreement or convention is a differing conception of cyber security priorities and methods possibly based on somewhat differing values.

Furthermore the US has several other considerations somewhat more specific to it when considering the possibility of a global cyber arms or cyber security agreement. Firstly provided that the US would be able to withstand and deal with external cyber attacks on it by being probably the most advanced nation in the field, it might not be a good strategic move entering into such an agreement and therefore possibly limiting its own valuable cyber offensive capability (Elliott 2009). While it is still hard to gauge if a cyber arms control agreement would be more detrimental to the US than positive, it is reasonably fair to predict that active US support for such an agreement will be hard to come by. Furthermore the push from Russia and other authoritarian regimes for a cyber arms control treaty can be seen as an attempt to limit US superiority and positional advantage in the field. This is quite a significant suspicion because of Russia's stated goals of maintain its regional power and seeing NATO eastern expansion as one of the primary threats to its security (Gudkov 2009). This may be even more emphasized in relation to cyber security with the opening of the NATO Center of Excellence on Cyber Defense in Estonia. In addition the US had expressed concerns about verification mechanisms in a possible cyber arms control treaty. There would seem to be no concrete ways of verification of compliance to such an agreement (Elliott 2009).

Nonetheless the *"Developments in the field of information and telecommunications in the context of international security"* is not the only significant resolution series in the United

Nations General Assembly to do with cyber threats and security. While this resolution was more concerned with general cyber security with possibly a greater emphasis on the politico-military (in other words, cyber warfare/terrorism) sphere of cyber security, there is a string of resolutions focusing more on the economic or in other words, cybercrime sphere.

The first of these resolutions is called *"Combating the criminal misuse of information technologies"* and it was adapted without a vote during the 55th session of the General Assembly in 2001. This resolution (A/RES/55/63) in particular expresses the fact that with the advancement of information communication technologies there has been a growing threat of criminal misuse and manipulation of these technologies. In addition the resolution notes that the growing, though unequal, reliance of these information technologies by states which has resulted in greater international cooperation which might be seriously threatened by cyber misuse of these technologies. The resolution also acknowledges work done and effort put into the draft Convention on Cybercrime done by the Council of Europe. Finally the resolution takes note of the worth of some broad measures aimed at combating criminal misuse of ICTs:

(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

(b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

(h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

(i) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

(j) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse;

(UN General Assembly A/RES/55/63)

The resolution goes on to invite states to take into account these measures when combating criminal misuse of ICTs and also reintroduces this resolution as an agenda item for the next UN GA session.

This resolution outlines broad strategies to combat cybercrime, putting paramount emphasis on the need for international cooperation in addressing instances of cyber crime. Legal cooperation and quick access to data pertaining to criminal investigations is stressed. It also explicitly states that the combating of criminal misused of ICTs, or to put it simply, cybercrime, should not be done at the expense of individual freedoms or privacy.

Building of this resolution (A/RES/55/63) and the afore examined *"Developments in the field of information and telecommunications in the context of international security"* (A/RES/53/70) the 57th session of the UN GA adopted without a vote a resolution titled *"Creation of a global culture of cyber security"* (A/RES/57/239). As the title entails, this resolution focuses on the need to create a global culture of cyber security. It notes that this can only be accomplished if all participants address 9 elements necessary for this: *awareness* of the need of security, *responsibility* for security of ICTs, *response* to security incidents in a timely fashion, *ethics* pertaining to the rights and concerns of others, *democracy* in the sense that security should be executed while taking into account democratic values, *risk assessment* done periodically to identify security vulnerabilities and manage the risk of potential harm, *security and design implementation* to the design and planning process for information systems and networks, *security management* that includes all aspects of operations and that is based on risk assessment, and finally *reassessment* to evaluate new arising risks, threats and vulnerabilities.

Therefore the resolution also asks member states (as well as relevant international organizations) to take these elements into account when creating a culture of cyber security in their respective societies. In addition it stresses the importance of transferring information technology to developing states as well as helping them in the introduction of cyber security measures.

This resolution is in turn modified in the 58th UN GA session and renamed *"Creation of a global culture of cyber security and the protection of critical information infrastructures"* (A/RES/58/199). The significant changes in this resolution include parts stressing the importance of reducing risk from cyber threats to critical information systems in addition to just societies in general. The resolution invites and encourages states as well as relevant international or regional organizations to develop strategies to protect their critical information infrastructures and to do so by taking into account the 9 elements presented in the annex of this resolution (A/RES/58/199) as well as the past one (A/RES/57/239).

In 2010 during the 64th session of the General Assembly a similar yet distinct resolution was adopted, titled *"Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures"* (A/RES/64/211). This resolution primarily sets out a brief as well as voluntary self assessment tool for member states and international organizations that are well in the process of implementing or have just begun to implement measures to protect their critical information infrastructures against various cyber threats. This self assessment tool consists of several brief points. Firstly it recommends to assess the role of ICTs in the state's own economy, security, civil society and critical infrastructure as well as suggesting determining the cyber risks to these areas that need to be managed and creating a comprehensive national cyber security strategy that takes account of vulnerabilities of the networks in use as well as the current progress of the implementation process. Secondly it advises to determine the key stakeholders in the process along with their respective responsibilities and to indentify or develop key venues for government and private sector cooperation in efforts of cyber security. Finally the resolution urges to develop effective cyber incident monitoring, warning, response and recovery capabilities in addition to appropriate, up to date legal frameworks and law enforcement agency capabilities. In the last note the resolution also invites member states who have already implemented functioning and successful critical information protection programs to share their experience and best practices with others.

Thus it can be said that the above discussed UN GA resolutions 57/239, 58/199 and 64/211 have been basically a set of pragmatic recommendations for member states and relevant organizations in the development of adequate national measures for the protection of critical infrastructure, national economies, civil society and national defense capabilities against cyber threats. These resolutions in turn do not in any significant way build towards the widely acknowledged (by the UN as well) and much needed comprehensive global response to cyber threats.

Therefore with this concise yet largely all inclusive analysis of United Nations efforts to promote and instill greater cyber security globally we can identify several relevant points and draw some significant conclusions about why there is no comprehensive global response to cyber threats. Firstly the United Nations recognizes cyber threats as major security concerns and also acknowledges that since they are global threats, they only way to full address then is by way of a global response.

Secondly while the UN does seem committed in advancing global cyber security, for example through its many organizations and institutes (such as the UNODA, UNIDIR, CTITF, ITU etc.), their work has been largely advisory or research focused with little development in way of a global agreement or convention. In addition, arguably the United Nations most powerful and significant body dealing with security, namely the Security Council has been completely inactive on the issue of cyber security. This is of course despite having ample chances to include cyber threats in resolutions with events such as the 2007 cyber attacks in Estonia, the 2010 Stuxnet attack in Iran as well as the 2008 cyber attacks in Georgia that accompanied its brief armed conflict with Russia.

Therefore the most significant forum for discourse on cyber threats and security has been the UN General Assembly having adopted several resolutions on the subject. Yet a lot of these resolutions (such as 57/239, 58/199 and 64/211) have focused on more pragmatic advisory measures for member states in relation to implementing national strategies and means of national security, despite them not being an adequate remedy to cyber threats.

Perhaps the most promising resolution attempting to address (at least in a preliminary way) the issue of cyber arms control was the *"Developments in the field of information and telecommunications in the context of international security"* (A/RES/53/70) introduced by the Russian Federation. Its initial call for the development global of definitions relevant to cyber threats was an important step towards the future development of a potential cyber arms treaty, yet the change in the text the 2005 version (A/RES/60/45) replaced this significant part. Additionally resolution faced opposition from the US that later morphed in a sponsorship in 2010, yet in 2011 the sponsorship was not renewed by the United States as well as some other western democracies.

Differing perspectives on the way cyber security should be executed and what concerns are primary in this execution have lead to suspicion from the west of the eastern states agenda. From this we can say that liberal democratic values like privacy and freedom of expression have become somewhat cleavages preventing the facilitation of a global agreement. In addition strategic considerations, especially those of the United States may make the possibility of a cyber arms control treaty even fainter. The suspicions are high that a cyber arms control agreement pushed for by Russia is little more than an attempt to limit the superiority of the cyber resources of western liberal democratic states, in particular the United States and its NATO allies. Furthermore concerns about the lack of verification mechanisms for such a treaty have often been voiced, yet this seems to be somewhat of scapegoat reason for not supporting a cyber arms control agreement because there are of course examples of such agreements being highly successful without any formal verification mechanisms. In fact one such example is the biological and toxin weapons convention, which lacks any verification mechanism, yet it is arguably one of the most successful arms control agreements of all time.

Nonetheless cyber arms control and in general concerns about cyber warfare or terrorism are only half of the picture. The other significant set of cyber threats are those of cybercrime. There has been relatively little direct action in the UN concerning cybercrime aside from the *"Combating the criminal misuse of information technologies"* resolution (A/RES/55/63) which most notably recommended a set of measures to be considered when addressing cyber crime. Yet the UN has expressed great support and to some extent worked with the Council of Europe on this issue. I will examine this work more detail in the following section.

COUNCIL OF EUROPE

The Council of Europe (CoE) unlike the United Nations is a regional rather than a global organization. It has 47 member states, which includes nearly all European states, except for Belarus and also includes member extending beyond the geographical borders of Europe such as Turkey and Russia (CoE.int). Despite being a regional organization the Council of Europe has developed probably the most significant international cyber security agreement to date, namely the Convention on Cybercrime and for this reason it is important to consider it when looking at global efforts to combat cyber threats.

The purpose of the 2001 Convention on Cybercrime is to facilitate greater cooperation between states in fighting cybercrime. One of its main tenets is the synchronization of national cybercrime laws in participant states. In addition the convention also provides procedures for investigating and prosecuting cybercrime offences through the setting up of an efficient international cooperation regime. Oddly enough the convention does not explicitly provide a strict and formal definition of cybercrime, but rather operates under the looser understanding that cybercrimes are simply offences committed using computers and computer networks, that target other computers as well as the data stored within them. It recognizes that cybercrimes can also target individuals and data transferred by computers (EM Convention on Cybercrime 2010).

It is important to note that the Convention of Cybercrime is open for signature to all states and not only member states of the Council of Europe. Currently there are 46 parties to the CoE Convention on Cybercrime, 30 of them have both ratified and acceded to the convention, while 16 have only signed it without ratifying. Most of the parties to the convention, 42 out of the total 46, perhaps unsurprisingly are CoE member states, with only four CoE non member states participating. These four external participants are Canada, Japan, South Africa and the United States. Aside from the US which has both ratified and acceded to the convention, the three other external participants have only signed the convention without ratifying or acceding to it. Out of the CoE member states five have not participated in the treaty even by signature. These states are Andorra, Monaco, San Marino, Turkey and Russia (Convention Status 2010).

Consequently we can straight away identify a couple major flaws of the CoE convention. While it is significant that it is the only binding international agreement dealing with cybercrime, its membership is very limited and primarily regional. With only four external non CoE member participants and with only one of them to have fully ratified and acceded to the convention it is hard to see it as a truly global and inclusive agreement. Major non CoE world powers are such as India, China, Brazil and others are not participants of the agreement. Thus the Convention on Cybercrime seems a lot more like a regional agreement rather than a global one, which it aspires to be. Yet even on a regional level it cannot boast universal participation because not all member of the CoE are participants, with the most notable exceptions being Turkey and the Russian Federation. In addition to all of this 16 of the participating states have only signed the convention without moving toward full ascension and ratification.

The United States Congressional Research Service report on the Convention on Cybercrime noted that while the convention is an important step in combating cybercrime it can only be useful if more states become signatories to it. It also note that most of the participants in the convention are not problem states in cyber security and that many cybercriminal route their attacks through countries like Yemen and North Korea which are not parties to the convention. Thus the convention does not significantly impede cyber attackers, because they can operate with significant freedom in some non party states. Additional internal concerns are cited in relation to civil liberties and opposition in the US from groups like the American Civil Liberties Union which argue that the convention grants the US government powers not enshrined in domestic law. Concerns were also expressed about the fact that foreign government would be able to request the US to investigate cyber activity that is not seen as criminal under US law. The report also cites concerns expressed by some European parties to the convention about the transfer of personal data to countries outside of Europe such as the US which has less protective laws concerning such sensitive data. However many of these concerns have been denounced by the CoE as unfounded, stating that there are sufficient provisions in the Convention on Cybercrime to protect the civil liberties in states participating in the convention (Archick 2006).

The convention has been promoted to try and get more participant but with relatively little success. While African countries were urged to become participants to the convention, little headway has been made on this. As previously stated South Africa is the only participant from the whole continent and it has only signed the convention without ratifying or acceding to it. A significant hurdle to the progression of the convention is the legality of different activities according to national law. Examples of varying national legislation include the legality of pornography or of the whistle blower websites like Wikileaks. While these differences exist the required harmonization of cybercrime legislation to participate in the convention can become a very difficult and controversial task (Mbuvi 2011).

Besides this there are several reasons that can be identified for this underwhelming success of the convention. A lot can be gauged from Russia’s primary objection to the Convention on Cybercrime which is that it allows criminal investigations to be conducted in relation to cybercrime incidents in foreign states without prior warning to local authorities (Markoff 2009). This objection seems point to a broader concern for more autocratic regimes such as China. Unreported investigations within other countries could be seen by some as an infringement of state sovereignty, i.e. something that China, Russia and similar regimes often find highly objectionable. China especially has often taken a very hard line to what it perceives to be meddling in its internal/domestic affairs. Case and point of this stance could be the recent rhetoric around the incident of the Chinese dissident and asylum seeker Chen Guangcheng who hid out in the US embassy in Beijing after escaping house arrest. Chinese officials portrayed the involvement of the US embassy as interference by the US in China’s internal affairs (Blanchard 2012). This is largely because China, similarly to Russia and other authoritarian regimes pursues a realist policy paradigm on the international level that makes it weary of open and inclusive cross border cooperation that functional cybercrime agreements ultimately entail (Pei 2006). Ultimately cybercrime conventions or treaties will require stable international cooperation based on mutual trust which is incompatible with the realist anarchical view of international relations that most authoritarian regimes still subscribe to.

Another important reason for the limited success of the convention is that it was fundamentally negotiated and developed in the regional forum of the CoE, therefore non member states had little to no say in the drafting of the agreement. This can cause specific concern of various states to have not been taken into account in the convention, therefore leading to little enthusiasm to participate in an agreement drafted primarily by western states. This perspective was in fact expressed during the 12th *"UN Congress on Crime Prevention and Criminal Justice"* in 2010 by some of the delegates. While all of the delegates agreed global cooperation is essential some acknowledged the utility of the CoE Convention on Cybercrime as an important platform for international cooperation while others felt that a completely new global cybercrime convention would be a more positive way to move forward (Com II meeting report 2010).

Furthermore the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, has received even less support in terms of participation. The goal of the protocol was to include provisions that criminalized racist and xenophobic acts that are committed through the internet. Just 34 states participated in this protocol, with only 20 fully ratifying and acceding to it while the remaining 14 only signed it. Only two of the signatories were not CoE member states (Canada and South Africa) and they have not ratified or acceded to the agreement (Protocol Status 2011). In addition in the United States an objection has arisen to the signing of the additional protocol on constitutional grounds, because of a perceived limitation of freedom of expression that is enshrined in the first amendment, so it is reasonable to suspect that the US will never become a signatory of this protocol (Rollins 2005).

It therefore possible to conclude that while the Council of Europe's Convention of Cybercrime has been touted by some to be a major international step in combating cybercrime, its many flaws, such as limited participation (especially by great powers such as Russia and China as well as many problem states in terms of cyber security) and various clashes with the domestic legal frameworks of various states have made it far from a success. Like in the case of the United Nations efforts to move towards a cyber arms control agreement fundamental issues concerning values seem to be underlining the difficulties. The western versus eastern, or the liberal democratic versus the authoritarian paradigm seems to play a big part. While cybercrime seems to be the most important issue concerning cyber security for the United States and European nations (in other words – liberal democracies) it is somewhat secondary to eastern and more authoritarian regimes such as Russia or China. Suspicion concerning cybercrime agreements seems to be coming from the eastern side, where concerns over sovereignty and intrusion into internal or domestic affairs that result from greater cross border cooperation seem to be the primary causes of opposition or unwillingness to participate in these efforts.

While these concerns might not be as strong in all eastern states as they are in great powers such as China and Russia due to their somewhat direct competitiveness with great western powers, they are nonetheless usually located in the regional influence zones of either China or Russia. Many authoritarian regimes in central Asia for example have strong links with Moscow that can be traced back to the times of the Soviet Union. Therefore a sort of opposition block can be created.

Yet even on different scale there seems some concern between the US and Europe on issues of freedom of expression and privacy. With some Europeans voicing unease over the transfer of personal data to the US which they view has lax laws concerning such delicate information. On the other hand some in the United States raising concerns about protection of freedom of expression in the convention and especially in the additional protocol (Rollins 2005).

Various similar concerns of incongruent national laws have arisen or are bound to arise between different regions and states. However these differences are often rooted deeper than just in simple laws. They often the expression of the values of particular regions or nations and therefore can be extraordinarily difficult to change or amend to comply with global agreements.

OTHER INTERNATIONAL ORGANIZATIONS

As I have previously indicated many international organizations have made commitments and pushed for responses to cyber threats within their own capacity, power and mandate. Most of them primarily encouraged international cooperation when dealing with matters of cyber security. I will briefly describe the commitments and actions towards greater global cyber security by some of the most prominent organizations in order to show their nearly uniform position on the issue, so that there can be little doubt left that obstacles to a comprehensive global response to cyber threats come almost solely from differing values of states (most significantly along regime type lines). In addition it will become evident that the United Nations and the Council of Europe have made the most substantial progress out of all major international organizations on the issue of global cyber security, therefore reaffirming my choice of focusing my examination primarily on them.

A good example of this is the **Organization for Security and Co-operation in Europe** and the effort it has put in to advancing goals of cyber security. Being the largest regional security organization in the world it has a membership of 56 states, from North America to Central Asia.

Since 2005 the OSCE has made cyber security one of its priorities. The OSCE Action against Terrorism Unit (ATU) has organized various workshops training law enforcement officials on handling cyber threats and has a goal to set up a framework to allow cross border searches in member state pertaining to illicit cyber activity, though this goal has not yet been fulfilled. In addition the OSCE Strategic Police Matters Unit has assisted the ATU in training law enforcement officials how to deal with cybercrime, with a particular focus on the Balkan region. It has also cooperated with academics and private sector entities to facilitate easier prosecution of cybercrimes (OSCE Cyber Sec).

Furthermore during the *"OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role"* it has recognized the importance developing clear definitions and terminology relating to cyber security and has committed to becoming a forum for this goal (OSCE Closing Remarks 2011).

Another organization that has actively been promoting cyber security initiatives is the **Organization for Economic Co-operation and Development**. Most of OECDs work had focused on promoting greater co-operation in building up the internet economy and encouraging the spread of ICTs to developing countries. But it also has come out with recommendations for governments on how to protect their critical infrastructure from cyber threats (OECD Recommendation 2008) as well as producing comprehensive reports on cyber security issues. One of the most recent of these is called "Reducing Systemic Cyber Security Risk" and it covers in great detail the nearly everything to do with cyber threats, from describing the various different types of them, to providing descriptions of technical, educational and legislative means of lessening the negative impact of cyber attacks, as well as providing a whole host of recommendations for securing cyber space on all levels, from the individual to the global (Brown 2011).

Thus the OECDs input to efforts of cyber security had been largely in an advisory capacity, providing recommendations, reports, statistics, and promoting best practices for dealing with cyber threats.

Some international organizations however have work to more primarily to secure their members with promotion of global security goals being somewhat secondary. The prime examples of this are the **European Union** and the **North Atlantic Treaty Organization**.

In 2005 the EU opened its Network and Security Agency, the purpose of which is to react to cyber security problems of the EU itself as well as its constituent member states. Its activities include advising and assisting member states in dealing with software and hardware security issues, gathering data on emerging security risks in Europe, promoting risk management and assessment strategies within member states to improve their ability to respond and deal with cyber threats, and promoting cooperation between the public and private sphere in working to secure European cyberspace (ENISA Activities).

The EU also extensively cooperates with the United States in attempting to secure its cyberspace. A good example of this is the joint cyber readiness initiative, dubbed “Cyber Atlantic 2011”, in which the US and EU simulated two hypothetical cyber attack scenarios. The goal of the exercise was to simulate the cooperation methods between both sides of the Atlantic during severe cyber incidents (Cyber Atlantic 2011).

Similarly NATO recently confirmed a revised cyber defense policy that focuses on improving the alliances defensive capability against external cyber threats. The new policy incorporates cyber defense into the overall NATO Defense Planning Process and centralizes cyber protection within the organization (NATO Policy 2011).

Thus it is quite evident that despite the problems in addressing cyber security issues through the United Nations and the Council of Europe, they still have achieved the most progress. Cyber security efforts by most other international organizations are either minimal due to their limited capacity and mandates, or they are specifically focused on primarily addressing the cyber threats of their member states with global initiatives taking a back seat on the agenda. This is why analyzing global responses to cyber security it is sufficient to look at the activity and processes surrounding the activities of the United Nations and the Council of Europe as I have done. Yet even with the relatively minor achievements of these organizations in addressing cyber threats it is evident that their support for greater global cooperation on this issue is uniform and unwavering.

CONCLUSION

From the examination of global efforts to combat the new and rising cyber threats through major international forums several patterns and cleavages seem to arise that are the causes of great difficulty in agreeing to a comprehensive global response.

There is much and near unanimous agreement throughout the international community about the severity of cyber threats and the great urgency that is present to deal with them. In addition nearly all states, significant international organizations, experts and academics agree that only global solutions can be effective in attempting to curb cyber threats with because of their fundamentally global nature.

Yet most of the international efforts to combat cyber threats so far have been pragmatic, by which I mean they have aimed at raising awareness, providing recommendations on best practices, urging the development of national legislation, monitoring cyber activity, producing reports and examining trends. While these initiatives have enjoyed various levels of success they ultimately do not attempt to develop a comprehensive global framework or agreement for dealing with cyber threats, but rather attempt to promote small solutions for the national, governmental, corporate or individual level that ultimately do not address the issue head on. All of these efforts have been within the limited scope of various international organization mandates, without any powerful multilateral and comprehensive inter-state agreement.

This seems to be primarily due to the difficulty, complexity of achieving truly global agreements. A host of measures need to precede any feasible, significant and workable cyber security agreement. Most basically clear, global and widely excepted definitions concerning cyber threats need to be established, yet this has proven difficult. When looking at the two major international forums in attempting to address cyber threats we clearly see such difficulty. In the United Nations the *"Developments in the field of information and telecommunications in the context of* *international security*" General Assembly resolution (A/RES/53/70) introduced in 1999 that encouraged states to begin the process of developing global definitions relating to matters on cyber security was modified in 2005 (A/RES/60/45), thereby excluding the call for definition development. In addition the Council of Europe's Convention on Cybercrime in general lacks a formal and explicit definition of what cybercrime actually is. The convention operates more based on a loose understanding and implicit operations definitions.

The United Nations could be considered the prime forum for cyber security in the sense of cyber warfare and clear efforts by the Russian Federation (with later support from other, primarily eastern and more authoritarian states) to push for a cyber arms control agreement. Yet this was met with suspicion and caution by western states, namely Europeans and even more so the United States. One of the main concerns was over possible use of such agreement for greater government control and even censorship over information by some more authoritarian regimes (and specifically Russia). In addition it is suspected that for the US in particular such a cyber arms control might have limited their relative advantage of cyber capabilities for military purposes, which was thought by many to be one of the primary motivations for Russia's push for such an agreement, since it seems to operate with a more realist conception of international relations like many authoritarian regimes. Conversely the opposite was seen in attempts to address issues of cybercrime, most notably with the Council of Europe's Convention on Cybercrime; while western, liberal democratic nations largely were supportive and the most notable participants, eastern nations largely shunned the convention. Russia especially expressed concern that the convention was at odds with state sovereignty, allowing unreported investigations pertaining to cybercrime into other states. Thus we see a rift between authoritarian states approaching the issue of cyber security on the international level with a more realist manner, while liberal democratic states seem to be taking a more liberal view. The former being more concerned with politico military aspects of cyber threats and being suspicious of open cross border cooperation due to its perceived incompatibility with the value of sovereignty. While the latter being more concerned with the economic aspects of cyber threats and being suspicious efforts to control cyber threats by possibly at the expense liberal democratic values such as privacy and freedom.

Yet this is not just an east and west, authoritarian and liberal democratic divide. Differing legislation and approaches to cyber security can exist on smaller levels due to varying state or regional values. An example of this is the concerns expressed by some Europeans about sharing of information pertaining to cybercrimes as is required by the Convention on Cybercrime, fearing that same legal protection of it might not be awarded to it in other states, even the United States. In addition tensions arisen in the US over the Additional Protocol to the convention relating to freedom of expression enshrined in its constitution have led to the US refusing to become a participant of it.

Therefore it can be concluded that fundamental divisions existing between the laws and priorities of various states, arising from fundamental values of particular societies and governments are the primary obstacles that have prevented effective cooperation and the development of a comprehensive global response to cyber threats.

BIBLIOGRAPHY

“15th Annual Computer Crime and Security Survey 2010/2011” Computer Security Institute

“About UNODC” United Nations Office on Drugs and Crimes; URL: (http://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop), last accessed: June 10th, 2012

“About UNIDIR” United Nations Institute for Disarmament Research; URL: (http://unidir.org/html/en/about.html), last accessed: June 10th, 2012

“Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems: Status as of: 28/8/2011” Council of Europe; URL: (http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=28/08/2011&CL=ENG), last accessed: June 10th, 2012

Archick, K. “Cybercrime: The Council of Europe Convention” Report for Congress, Congressional Research Service, September 28th, 2006; URL: (http://www.au.af.mil/au/awc/awcgate/crs/rs21208.pdf), last accessed: June 10th, 2012

Blanchard, B. and Quinn, A. “China denounces U.S. as dissident Chen leaves embassy” Yahoo! 7 News, May 2nd, 2012; URL: (http://au.news.yahoo.com/world/a/-/world/13584206/china-denounces-u-s-as-dissident-chen-leaves-embassy/), last accessed: June 10th, 2012

Brown, I. and Sommer, P. “Reducing Systemic Cyber Security Risk” Multi-Disciplinary Issues International Futures Program, Organization for Economic Co-operation and Development, January 14th, 2011; URL: (http://www.oecd.org/dataoecd/57/44/46889922.pdf), last accessed: June 10th, 2012

“Combating the criminal misuse of information technologies” United Nations General Assembly resolution 55/63 – 2001

“Convention on Cybercrime: Status as of Status as of: 28/10/2010” Council of Europe, URL: (http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG), last accessed: June 10th, 2012

“Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects” Working Group Compendium, United Nations Counter-Terrorism Implementation Task Force, May 2011; URL: (http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf), last accessed: June 10th, 2012

“Council of Europe in brief” Council of Europe, URL: (http://www.coe.int/aboutCoe/index.asp?page=47pays1europe&l=en), last accessed: last accessed: June 10th, 2012

“Creation of a global culture of cyber security” United Nations General Assembly resolution 57/239 – 2003

“Creation of a global culture of cyber security and the protection of critical information infrastructures” United Nations General Assembly resolution 58/199 – 2004

“Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures” United Nations General Assembly resolution 64/211 – 2010

“Cybercrimes - UNICRI's Initiatives” United Nations Irrigational Crime and Justice Research Institute; URL: (http://www.unicri.it/emerging_crimes/cybercrime/initiatives/), last accessed: June 10th, 2012

“Cybercrime laws from around the world” Cybercrime Data AS; URL: (http://www.cybercrimelaw.net/Cybercrimelaws.html), last accessed: June 10th, 2012

“Cyber security: virtual threats, real responses” Organization for Security and Co-operation in Europe; URL: (http://www.osce.org/home/76011), last accessed: June 10th, 2012

“Democracy index 2011: Democracy under stress” Economist Intelligence Unit, The Economist, 2011

“Denial of Service Attacks” Cyber Security Engineering Team, Software Engineering Institute, Carnegie Melon University; URL: (http://www.cert.org/tech_tips/denial_of_service.html#1), last accessed: June 10th, 2012

“Developments in the field of information and telecommunications in the context of international security” United Nations General Assembly resolutions 50/70 – 1999, 60/45 – 2005, 61/54 – 2006, 62/17 – 2007, 63/37 – 2008, 64/25 – 2009, 65/41 – 2010, 66/24 – 2011

“Digital Agenda: EU & US conduct readiness tests for cyber attacks in "Cyber Atlantic 2011"” Press Release, European Commission, November 3rd, 2011; URL: (http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1305&format=HTML&aged=0&language=EN&guiLanguage=en), last accessed: June 10th, 2012

Elliot, D. (November 2009) “Weighing the Case for a Convention to Limit Cyber Warfare” Arms Control Today, Arms Control Association; URL: (http://www.armscontrol.org/act/2009_11/Elliott), last accessed: June 10th, 2012

Eriksson, J. and Giacomello, G. (July 2006) “The Information Revolution, Security, and International Relations: (IR) Relevant Theory” International Political Science Review, Vol. 27, No. 3, 221 – 224

“Explanatory Memorandum on the Council of Europe Convention on Cybercrime” Foreign and Commonwealth Office, August 12th, 2010; URL: (http://www.fco.gov.uk/en/publications-and-documents/treaty-command-papers-ems/explanatory-memoranda/explanatory-memoranda-2010/050Cybercrime), last accessed: June 10th, 2012

Farwell, J. P. & Rohozinski, R. (January 2011) “Stuxnet and the Future of Cyber War” Global Politics and Strategy, Vol. 53, No. 1, 23 – 40

Freedberg, S. J. “Cyber Attacks on Feds Soar 680% In 6 Years: GAO” AOL Defense, April 24th, 2012; URL: (http://defense.aol.com/2012/04/24/cyber-attacks-on-feds-soar-680-in-6-years-gao/?a_dgi=aolshare_twitter), last accessed: June 10th, 2012

Ganuza, N., Hernandez, A. and Benavente, D. (June 2011) “An Introductory Study to Cyber Security in NEC” NATO Cooperative Cyber Defense Center of Excellence - Tallinn, Estonia

Geers K. (January 2009) “The Cyber Threat to National Critical Infrastructures: Beyond Theory” Information Security Journal: A Global Perspective; 18 (1):1-7

"Global Cyber security Agenda brochure" Corporate Strategy Division, International Telecommunications Union, 2007; URL: (http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf), last accessed: June 10th, 2012

Goel, S. (August 2011) "Cyber warfare: Connecting the Dots in Cyber Intelligence" Communications of the ACM; Vol. 54, No. 8, 132 - 140

Glenny, M. "The Cyber Arms Race Has Begun". Nation, October 31, 2011; 293 (18): 17 - 20

Hill, E. "Hackers hit Tunisian websites" Aljazeera, January 3rd, 2011; URL: (http://www.aljazeera.com/news/africa/2011/01/201113111059792596.html), last accessed: June 10th, 2012

Gudkov, L., Klyamkin, I., Satarov, G. and Shevtsova, L. "False Choices on Relations with Russia" Washinton Post, June 9th, 2009; URL: (http://www.washingtonpost.com/wp-dyn/content/article/2009/06/08/AR2009060803496.html), last accessed: June 10th, 2012

Kravets, D. "Citi Credit Card Data Breached for 200,000 Customers" Wired Magazine, June 9th, 2011; URL: (http://www.wired.com/threatlevel/tag/citibank/), last accessed: June 10th, 2012

Kemp, W. "Korean company helps UNODC fight cyber-crime" United Nations Office on Drugs and Crime, December 3rd, 2007; URL: (http://www.unodc.org/unodc/en/press/releases/2007-12-03.html), last accessed: June 10th, 2012

Maurer, T. (September 2011) "Cyber Norm Emergence at the United Nations – An Analysis of Activities at the UN Regarding Cyber-Security" Explorations in Cyber International Relations Discussion Paper Series, Belfer Center for Science and International Affairs, Harvard Kennedy School

Markoff, J. and Kramer, A. E. "U.S. and Russia Differ on a Treaty for Cyberspace" New York Times, June 27th, 2009; URL: (http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=2&pagewanted=all), last accessed: June 10th, 2012

Mbuvi, D. “African states urged to ratify Budapest Cybercrime Convention” Computerworld Uganda, October 10th, 2011; URL: (http://www.computerworlduganda.com/articles/2011/10/10/african-states-urged-ratify-budapest-cybercrime-convention), last accessed: June 10th, 2012

Moir, R. (October 2003) “Defining Malware: FAQ” Tech Net, Microsoft Corporation; URL: (http://technet.microsoft.com/en-us/library/dd632948.aspx), last accessed: June 10th, 2012

“NATO Defense Ministers adopt new cyber defense policy” North Atlantic Treaty Organization, June 8th, 2011; URL: (http://www.nato.int/cps/en/natolive/news_75195.htm?selectedLocale=en), last accessed: June 10th, 2012

“Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually” Norton Cybercrime Report, Symantec, September 7th, 2011; URL: (http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02), last accessed: June 10th, 2012

“OECD Recommendation of the Council on the Protection of Critical Information Infrastructures” Committee for Information, Computer and Communications Policy, Organization for Economic Co-operation and Development, June 18th, 2008; URL: (http://www.oecd.org/dataoecd/1/13/40825404.pdf), last accessed: June 10th, 2012

“Only global cooperation can thwart security threats, both old and new, Ban warns” UN News Center, UN News Service, October 5th, 2010; URL: (http://www.un.org/apps/news/story.asp?NewsID=36346&Cr=terror&Cr1=), last accessed: June 10th, 2012

“OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role - Closing Remarks by H.E. Ambassador Norkus, Chairperson of the OSCE Permanent Council” Organization for Security and Co-operation in Europe, May 11th, 2011; URL: (http://www.osce.org/cio/77481), last accessed: June 10th, 2012

Pei, M. “China's political evolution: implications for Beijing's foreign relations” Canadian Institute of International Affairs, Toronto, October 6th, 2006; URL: (http://www.thefreelibrary.com/China's+political+evolution%3a+implications+for+Beijing's+foreign...-a0155824547), last accessed: June 10th, 2012

Rollins, J. Wilson, C. “Terrorist Capabilities for Cyberattack: Overview and Policy Issues” Report for Congress, Congressional Research Service, October 20th, 2005; URL: (http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL33123_10202005.pdf), last accessed: June 10th, 2012

Schmitt, B. (editor), Esterle, A. and Ranck, H. (March 2005) “Information Security – A new challenge for the EU” Chaillot Paper No. 76, European Union Institute for Security Studies

“Second Annual Cost of Cyber Crime Study – Benchmark Study of US Companies” Ponemon Institute, August 2011

“Special Event on Cyber Security and Development – Informal Summary” ECOSOC, United Nations, December 9th, 2011; URL: (http://www.un.org/en/ecosoc/cybersecurity/summary.pdf), last accessed: June 10th, 2012

“Speech by Mr. Gary Lewis, Representative, United Nations Office on Drugs and Crime (UNODC) at the launch of the Advanced Forensic Training on Cyber Crime and Computer-facilitated Crimes against Children” United Nations Office on Drugs and Crimes, October 9th, 2006; URL: (https://www.unodc.org/india/speech_gary_lewis.html), last accessed: June 10th, 2012

“Strengthening the role of ITU in building confidence and security in the use of information and communication technologies” Resolution 130, International Telecommunications Union, 2010

“Subsidiary Body Divided over Whether To Expand Existing Convention or Start Negotiations on New Treaty” UN Congress on Crime Prevention and Criminal Justice, Committee II, 2nd & 3rd Meeting Report, News and Media division, Department of Public Information, April 13th, 2010; URL: (http://www.un.org/News/Press/docs/2010/soccp349.doc.htm), last accessed: June 10th, 2012

“The United Nations Disarmament Yearbook” United Nations Office for Disarmament Affairs, Volume 30 – 2005, Volume 31 – 2006, Volume 32 (Part 1) – 2007, Volume 34 (Part 1) – 2008, Volume 35 (Part 1) – 2009, Volume 36 (Part 1) – 2010, Volume 37 (Part 1) – 2011

“United Nations Global Counter Terrorism Strategy” Counter Terrorism Implementation Task Force, United Nations; URL: (http://www.un.org/en/terrorism/ctitf/index.shtml), last accessed: June 10th, 2012

“US defence firm Lockheed Martin hit by cyber-attack” BBC News, May 30th, 2011; URL: (http://www.bbc.co.uk/news/world-us-canada-13587785), last accessed: June 10th, 2012

“What does ENISA do?” European Network and Information Security Agency; URL: (http://www.enisa.europa.eu/about-enisa/activities), last accessed: June 10th, 2012

Zanders, J. P. (2009) “Cyber Security: What Role for the CFSP?” Institute Report - seminar organized jointly by General Secretariat of the Council of the EU & the EU Institute for Security Studies in cooperation with Estonia held in Brussels on 4 February 2009, European Union Institute for Security Studies