Research Report | XXV Annual Session

Special Conference 2 on International Cooperation

Combating the growing threat of cyber terrorism

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Tega Akati-Udi

Forum: Special Conference 2 on International Cooperation

Issue: Combating the growing threat of cyber terrorism

Student Officer: Tega Akati-Udi

Position: Deputy President

Introduction

"Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." – National Academy of Sciences Report 1990

The Internet since its creation has gradually become a bigger part of our everyday lives as humans. Most people did not really see any insecurity in the use of cyberspace till the year 2000 which ushered in "The Year 2000" software problem or the millennium bug. This was a problem that simply arose from the abbreviation of 4 digit years (e.g. 1998) to 2 digit years (e.g. 98). The problem from this was that computers working like this could only work in one century; was "00" an abbreviation for 1900 or 2000? And although this problem did not turn out to be as disastrous as speculated, it did arouse a new fear in people: a question of the true safety of the internet. It became obvious that software and cyberspace could be very susceptible to manipulation and mishandling. And although cybercrime and cyber terrorism had been spoken of (although not to great extent) before, these became more pressing issues in politics and even social lives.

And the recognition of cybercrime was only heightened by the 2007 Estonian cyberattacks, which affected the Estonian parliament, banks, ministries, newspapers. The denial of service attacks targeted government and corporate sites crippling numerous services in Estonia. There were 128 unique denial of service (DoS) attacks. These attacks called international attention on cybercrime; the North Atlantic Treaty Organization (NATO) was prompted to establish their cyber defence research centre in Tallinn in 2008, Estonia called on the European Union to criminalise cyberattacks and the Federal Bureau of Investigation (FBI) announced in 2009 that it would permanently base a computer crime expert in Estonia to help fight international threats against computer systems.

Other attacks such as the Titan Rain made it obvious that cyberspace was not 100% secure and that any country could be targeted. This calls on the need for international cooperation to combat cyberterrorism, a recent option for terrorists over traditional terrorist

methods. The internet connects countries worldwide in a network and the possibility of terrorist groups exploiting the weaknesses of cyberspace calls for certain alarm. Cyberterrorism, although not given as much attention as traditional terrorism, must not be ignored but must be fought to prevent a worldwide cyberattack like that in Estonia in 2007.

This research report aims to discuss cyberterrorism and suggest possible ways to combat it. Whilst this research report is a good starting point for research, it should be, by no means, the only source of research. Delegates are therefore urged to research beyond this research report.

Definition of Key Terms

Cyberterrorism

There is no internationally accepted definition of cyberterrorism as terrorism itself is a highly subjective word to define. Many organizations have their own definitions of cyberterrorism. For the purpose of this research report, D. Denning's (a renowned professor of computer science) will be used: "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives." Some people also believe that since cyberterrorism is a convergence of terrorism and cyberspace, it includes propaganda and recruiting carried out on the internet. There is, however, significant debate on this.

Cybercrime

This is another term that is used interchangeably with cyberterrorism. Although very similar, the two are not the same. Cybercrime is simply a crime committed through the use of information technology. Some people include cyberterrorism under cybercrime.

Cyber warfare

Cyber warfare is a planned attack by nations on other nations using cyberspace. The Estonian 2007 attacks could be classed as cyber warfare.

Note: The three aforementioned terms should not be confused with each other. According to a report "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", if a person hacks into a bank account, it is a cybercrime because "the attacker's intention is neither political nor social." If this is done to several accounts and "the

attacker declares that he is going to continue attacks until the government accepts his demands," then it is cyberterrorism. If this is done by "agents of a foreign power," and "if all the banking system of a nation is targeted," then it is cyber warfare.

Denial of Service Attack

Denial of Service attacks are a type of cyberattack where the user or organization attacked is denied access to online resources. In most cases, it is done by flooding a network with traffic.

Hacktivism

As the word suggests, hacktivism is the use of hacking for political activism. Unlike hackers, hacktivists have a political agenda. This is often confused with cyberterrorism but hacktivists aim to bring about political and social awareness with no violence or serious damage. With cyberterrorism, the damage caused is much more serious.

General Overview

Overtime, the growth of technology has not eased lives of many but has also made us heavily dependent. And therein lies the very basis of cyberterrorism: exploiting this weakness to the advantage of several terrorists.

The convenience of cyberterrorism

Ironically, the success of the "war on terror" after 9/11 may have encouraged terrorists to look at unconventional means of terrorism such as cyberterrorism. Cyberterrorism offers numerous advantages to terrorists.

One of the appeals of cyberterrorism is the fact that it is cheaper than traditional terrorist methods. All a terrorist needs is a computer and a connection which is significantly cheaper than weapons. Added to this is the cost of training and hiring recruits. Cyberterrorism entails less physical danger and risk of mortality than traditional terrorism enabling terrorists to keep their recruits for longer. The benefit to cost ratio is, therefore, extremely high. The internet offers numerous advantages in that is has little or no regulation, easy access, the potential of huge audiences, anonymity and the fast flow of information.

Also, cyberterrorism is more anonymous than traditional terrorism making it harder to track down the terrorists. Moreover, the variety of targets is also significantly more. The terrorist can target governments worldwide from one position just with a computer. The

effects of cyberterrorism are also much more significant than those of traditional terrorism. Due to the high dependence on technology, cyberterrorism has a wider effect than traditional terrorism. As seen in Estonia, a cyberattack has the potential to cripple an entire country. When a cyberattack is, therefore, carried out by a terrorist group, the effects can be much worse. Furthermore, cyberterrorism is easier than using a bomb or other weapons as the terrorist is not limited by distance. There are no physical barriers or checkpoints that they have to cross. This is why cyberterrorism so dangerous. Rather than being a danger to one specific country or organization, it is a threat to countries worldwide, which is why stopping cyberterrorism requires international cooperation. As dangerous as cyberterrorism sounds, a combination of traditional terrorism and cyberterrorism could have more disastrous effects increasing the need to combat cyberterrorism.

Growing fear of cyberterrorism

There is great fear of cyberterrorism: a survey of 725 cities conducted in 2003 by the National league of Cities discovered that cyberterrorism ranked alongside biological and chemical weapons at the top of a list of city officials' fears. These fears are reasonably placed. The risks of cyberterrorism are vast including the fact that many critical infrastructure are at risk such as transportation and power supply, the fact that numerous cyberattacks have already been conducted such as the Estonian attacks and due to future forecasting that our dependence on technology is most likely to increase.

The fear of cyberterrorism may, however, have been exaggerated. Despite the fact that there is increasing possibly of cyberterrorism, no real cyberterrorist attack has been recorded. This may be due to the ambiguity of the definition of cyberterrorism but may also be that no terrorist groups have staged any serious cyberattack. Terrorist groups lack the required IT skills to successfully conduct a severe cyberterrorist attack. There is, however, a possibility that terrorist groups recruit people who are capable of doing so.

Furthermore, it is possible that the fear may have been heightened by the mass media. Mass media fail to distinguish hacking from cyberattack from cyberterrorism. This promotes ignorance of the true danger of cyberterrorism and may be a reason why fear of cyberterrorism is greater. However, this may also constitute another problem as lack of understanding of cyberterrorism increases the alarm of the issue.

Nonetheless, cyberterrorism does pose a threat although this threat may be unclear or different according to different views. Cyberterrorism must, therefore, be combatted internationally.

Major Parties Involved and Their Views

United Nations Office on Drugs and Crime

The UNODC has a major role in assisting member states in implementing a successful crime fighting legal system. Since terrorism counts as a crime, the UNODC aids in combatting cyberterrorism in member states. The UNODC aids in the fight against cybercrime (which includes cyberterrorism) by promoting long-term and sustainable capacity building in the fight against cybercrime through supporting national structures and action of member states. It provides technical assistance, prevention and awareness raising, international cooperation and data collection.

The United Nations Counter-Terrorism Implementation Task Force (CTITF)

The UN CTITF has a working group that aims to "identify and bring together stakeholders and partners on the issue of abuse of the Internet for terrorist purposes, including through radicalization, recruitment, training, operational planning, fundraising and other means." The working group aims to identify the United Nation's role in combating cyberterrorism, quantify the threat that cyberterrorism poses and examining the options in combating cyberterrorism at local, national and global levels. This working group has produced several reports on cyberterrorism informing on its progress towards combatting cyberterrorism.

North Atlantic Treaty Organization (NATO)

NATO is also involved in the fight against cyberterrorism. It has been advancing its efforts to confront cyberterrorism. Cyber defence is now a part of NATO's core task of collective defence. NATO approved its first cyber defence policy in January 2008 following the cyber-attacks against Estonia in 2007.The alliance is enhancing its cooperation with industry as well as increasing its capability for cyber education, training and exercises. The NATO Computer Incident Response Capability (NCIRC) protects NATO's own networks by providing centralised and round-the-clock cyber defence support to the various NATO sites.

Council of Europe

Cyberterrorism and use of the Internet for terrorist purposes have been identified by the Council of Europe as priority focus areas. The council has worked towards addressing this through the Cybercrime convention (2001) and the Council of Europe Convention on the Prevention of Terrorism (2005). It has been surveying the situation in member states to

evaluate whether existing international instruments are sufficient to respond to this emerging threat. It made a database on cyberterrorism containing national contributions.

Al Qaeda

Al Qaeda is a terrorist group which uses the internet as a tool for many of its terrorist activities. Terrorist internet sites are a danger as they can serve as virtual training grounds, offering tutorials on building bombs, firing surface-to-air missiles, shooting at U.S. soldiers, and sneaking into Iraq from abroad. They also host messages and propaganda videos which help to raise morale and further the expansion of recruitment and fundraising networks. For Al Qaeda, As Sahab is its media arm that uses technology to relay Al Qaeda's views to the world. Al-Qaeda operatives are known to have taken training in hacking techniques but the risk of cyberterrorism still remains relatively low.

Islamic State in Iraq and Syria (ISIS)

ISIS is increasingly using social media to recruit, radicalise and raise funds. The terrorists are able to hide their identities using encryption tools. Although the groups use of internet is primarily for propaganda and making the world aware of their views, their use of several social media such as Twitter and YouTube shows the sophistication in their use of social media. Unlike Al Qaeda, ISIS has taken a more direct approach especially in uploading videos of invasions and beheadings. These activities, however, run far from cyberterrorism and hacking. A growing competence in use of the internet by these terrorist groups increases the alarm of the possibility of cyberterrorism.

Timeline of Events

The timeline below shows some of the key events that have occurred in recognizing and combating cyberterrorism. It is significant to note that the conferences listed below whilst including several countries are not entirely global (involving all countries).

Date	Description of event
November 23rd, 2001	Convention on Cybercrime
May 16th, 2005	Council of Europe Convention on the Prevention of Terrorism treaty concluded
April 27th, 2007	Beginning of Estonian cyberattacks
July 20th, 2008	Cyberattacks on Georgian government, business websites and network infrastructure
March 23rd – 26th,	The Council of Europe "Octopus Interface " Conference on " Cooperation

2010	against Cybercrime ”
April 12th-19th, 2010	United Nations Congress on Crime Prevention and Criminal Justice
May 12th -19th, 2010	United Nations Session on Crime Prevention and Criminal Justice in Vienna
June 17th – 19th, 2015	Octopus Conference 2015: Cooperation against Cybercrime

UN involvement, Relevant Resolutions, Treaties and Events

Not many resolutions discussing cyberterrorism specifically have been discussed in the United Nations. Cyberterrorism is usually an issue that is brought up under discussion of terrorism. The resolutions below, therefore, only highlight the need for more international cooperation relating to cyberterrorism.

- The United Nations Global Counter-Terrorism Strategy, 8 September 2010, **(A/RES/64/297)**
- Measures to eliminate international terrorism, 9 December 2011, **(A/RES/66/105)**
- Technical assistance for implementing the international conventions and protocols related to counter-terrorism, 19 December 2011, **(A/RES/66/178)**
- The United Nations Global Counter-Terrorism Strategy Review, 29 June 2012, **(A/RES/66/282)**

Evaluation of Previous Attempts to Resolve the Issue

The Convention on Cybercrime was the first international treaty hoping to tackle cybercrime. It was drawn up by the Council of Europe and aimed to: foster international cooperation on tackling cybercrime, harmonizing laws against cybercrime and providing for domestic criminal procedural law powers necessary for the investigation and prosecution of cybercrime. Although this was signed by 50 countries and ratified by 46 encouraging international cooperation, there are many more countries who are not included in this treaty and so international cooperation was not completely accomplished. Cyberterrorism could potentially affect countries worldwide and if it is to be successfully tackled, all countries must join up to battle it. Furthermore, this treaty aimed to tackle cybercrime which incorporates not just cyberterrorism possibly but also computer-related fraud and child pornography. For a

treaty to be more effective in combatting cyberterrorism, it should more specifically pertain to cyberterrorism. Likewise, the Council of Europe Convention on the Prevention of Terrorism treaty aimed to “increase the effectiveness of existing international texts on the fight against terrorism” and although terrorism includes cyberterrorism, cyberterrorism is not mentioned in the treaty and the lack of work specified towards battling cyberterrorism is an issue that needs to be corrected.

The Council of Europe “Octopus Interface ” Conference on “ Cooperation against Cybercrime ” was more effective in that it involved over 300 cybercrime experts from all continents and so was more international than the Convention on Cybercrime treaty. This interface was successful in that it encouraged discussion on how to tackle cybercrime with effective solutions. Key messages were highlighted including the need for “measures against cybercrime” to “follow principles of human rights and the rule of law” and the fact that “security and the protection of rights is the responsibility of both public authorities and private sector organisations.” However, this interface involved cybercrime experts and not government officials which might have had a better impact. Again, cybercrime is a broad term and more attention needs to be paid to cyberterrorism specifically.

The United Nations Congress on Crime Prevention and Criminal Justice also discussed many issues relating to cybercrime and called on numerous UNOs such as UNODC to address cybercrime but there was no specific mention of cyberterrorism in the report. The UNODC recognises that more international cooperation is needed to tackle cyberterrorism and while few countries liked the UK have effective laws in place to tackle cyberterrorism, the issue as Ban Ki-Moon said is “transnational” and requires that all member states “to think and function in an equally transnational manner.” The report suggested ways in which policymakers can combat the growing threat of cyberterrorism through ways such as regulating Internet Service Providers (ISPs).

Possible Solutions

In order for solutions to tackle cyberterrorism, they must tackle the problems associated with cyberterrorism. These problems include: the lack of a universal definition of cyberterrorism, little international cooperation and lack of international treaties or conferences relating specifically to cyberterrorism rather than cybercrime. A good resolution will contain clauses touching on all these problems.

There is need for countries to consider the guidance offered by the UNODC 2012 report as it calls out the key issues concerning cyberterrorism. Countries who have not already done so need to ensure that there exists a legal framework highlighting cyberterrorism as a crime and punishing it. This is a logical starting point for any other solutions. There also needs to be international law resulting from international cooperation concerning cyberterrorism. It is critical that these laws seek to investigate into any acts of cyberterrorism and punish the crime doers. This will act as a deterrence, hopefully, to others.

Obtaining a universal definition of cyberterrorism, however, entails problems in itself as defining terrorism is very difficult. Differences among countries may be difficult as someone might be a terrorist to one and a freedom fighter to another. The universal definition must be decided in a way that is acceptable to all countries.

A prevention method is to routinely check information infrastructures for any signs of cyber activity that is suspicious. Systematic and routine checks can be successful as prevention methods to avoid cyberterrorism.

Although technology is the means through which cyberterrorism is carried out, it could also be a solution to cyberterrorism. Developments in technology may well provide solutions to the weaknesses of information infrastructure. It is, therefore, a viable option to invest into research and development concerning technology to counter cyberterrorism although this would involve money and infrastructure and thus may not be an option for developing countries.

Education is also needed as a reason why cyberterrorism is potentially dangerous is the lack of valid information of what actually constitutes cyberterrorism and much of the fear arousing (as discussed earlier on) is from speculation on what constitutes as cyberterrorism.

Bibliography

"Action against Cybercrime." - Council of Europe. N.p., n.d. Web. 05 July 2015. <**http://www.coe.int/en/web/cybercrime/home** >.

Compendium, Working Group. "Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects." (n.d.): n. pag. Web. 5 July 2015. <**http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf** >.

Convention on Cybercrime: Budapest, 23 November 2001. London: Stationery Office, 2012. Web. 5 July 2015. <**https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/238194/8309.pdf**>.

"Council of Europe." Cyberterrorism. N.p., n.d. Web. 05 July 2015. <**http://www.coe.int/t/dlapil/codexter/cyberterrorism_EN.asp**>.

"Counter-Terrorism Implementation Task Force, CTITF." UN News Center. UN, n.d. Web. 05 July 2015.

"Cybercrime & Cyberterrorism: Inducing Anxiety & Fear on Individuals." IconOf.Com. N.p., n.d. Web. 05 July 2015.

Cyber Crime. Digital image. *The Modern Network*. N.p., n.d. Web. 6 Sept. 2015. <**http://themodernnetwork.com/government/weekly-news-round-up-cyber-threats-on-the-rise/**>.

"Cyberwar Timeline." The Christian Science Monitor. The Christian Science Monitor, n.d. Web. 05 July 2015. <**http://www.csmonitor.com/USA/2011/0307/Cyberwar-timeline**>.

"Defending against Cyber Attacks." NATO. N.p., n.d. Web. 05 July 2015. <**http://www.nato.int/cps/en/natohq/75747.htm**>.

"Developing New Strategies to Combat Cyber-Terrorism." IDEA GROUP PUBLISHING, n.d. Web. 5 July 2015. <http://www.irma-international.org/viewtitle/32381/>.

"The History of Cyber Attacks - a Timeline." NATO Review. N.p., n.d. Web. 05 July 2015. <**http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm**>.

"Octopus Conference 2015: Cooperation against Cybercrime." Octopus Conference 2015: Cooperation against Cybercrime. N.p., n.d. Web. 05 July 2015. <**http://giplatform.org/events/octopus-conference-2015-cooperation-against-cybercrime**>.

Rd. Page. Any Other Reproduction or Transmission Requires Prior Written Permission. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism (n.d.): n. pag. Web. 5 July 2015.

Reporters, Telegraph. "How Terrorists Are Using Social Media." The Telegraph. Telegraph Media Group, n.d. Web. 05 July 2015.

<**http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html**>.

"The Role of the United Nations in Fighting Terrorism." (2002): n. pag. Center for Strategic and International Studies. Web. 5 July 2015. <**http://csis.org/files/media/csis/pubs/roleofun.pdf**>.

TERRORIST USE OF CYBERSPACE COURSE REPORT (n.d.): n. pag. Web. 5 July 2015.

"Terrorists and the Internet." Council on Foreign Relations. Council on Foreign Relations, 08 Jan. 2009. Web. 05 July 2015. <**http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p6**>.

"UN: More International Cooperation Needed to Fight Cyberterrorism." Computerworld. N.p., n.d. Web. 05 July 2015. <**http://www.computerworld.com/article/2492864/cybercrime-hacking/un--more-international-cooperation-needed-to-fight-cyberterrorism.html**>.

"United Nations, Main Body, Main Organs, General Assembly." UN News Center. UN, n.d. Web. 05 July 2015. <**http://www.un.org/en/ga/66/resolutions.shtml**>.

Ward, Mark. "Cyber Terrorism 'overhyped'" BBC News. BBC, 14 Mar. 2003. Web. 05 July 2015.

Weimann, Gabriel. Cyberterrorism: How Real Is the Threat? Washington, D.C.: United States Institute of Peace, 2004. Web. 5 July 2015.

"What Is Cyberterrorism? Even Experts Can't Agree." The Harvard Law Record -. N.p., n.d. Web. 05 July 2015.

"What Is Cyber-terrorism?" What Is Cyber-terrorism? N.p., n.d. Web. 05 July 2015.

Appendices

Appendix I

Source giving detailed look into cybercrime and its global response:

https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Russia_1_Cybercrime_EGMJan2011.pdf

Appendix II

Report by the CTITF on cyberterrorism:

http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf

Appendix III

Key messages from the Octopus Interface of 2010:

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1s%20provisional%20_24%20Apr%2010.pdf

Appendix IV

Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice:

https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

Appendix V

Report from UNODC calling on International Cooperation:

http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf