ODUMUNC 2011

Issue Brief for the

GA First Committee: Disarmament and International Security (DISEC)

The Prevention of Cyberterrorism and Cyberwar

By: Son Thanh Dang

These days, when the Internet is virtually indispensible in people's lives, the risk of cyber-attacks has become one of the most alarming threats to the world. Cyber-attacks can range from slowing down a website's operations, to hacking into a computer to steal data, to disrupting a network system. But when a cyber-attack is considered to be a terrorist or warfare crime it's still a disputable issue since there is not a consistent international treaty in this regard yet.

Cyber terrorism is often interpreted as unlawful actions conducted via computer network that may cause violence against or generate fear among people, or lead to serious destruction for political or social purposes. This interpretation of cyber terrorism is not clear enough. In case terrorists do not directly attack computers or networks but use them as part of their preparation for their physical attacks, just like terrorists in the disastrous 9/11 attacks making travel plans and booking flight tickets via public library computers in Delray Beach, Florida, it raises questions whether these actions are considered to be cyber terrorism or not. Similarly, cyberwars are currently mentioned as computer-based attacks accompanying physical military operations to destroy an enemy's military forces or deriving from political conflicts between nations. However, distinguishing military from civilian networks is not simple, as it is impossible to attack a military computer system without affecting civilian uses. Another main obstacle in defining cyberwar is that attackers can initiate their action from any territory, and there is no way to trace their identity. Even when we have known the nation where the attacks originate from, determining whether its government is involved in the crime is another challenge.

It is because of the ease, low cost, speed and anonymity of the Internet, in addition to the current lack of an international convention on cyber-crime, that the number of cyber-attacks as well as the degree of destruction increases very rapidly. In Columbia, the names of 65 young people have just been found on facebook as a supposed death list since three of those were killed, which poses concerns about terrorism and requires protection from the Colombian government. According to a recent survey of 1,580 private businesses in critical infrastructure industries conducted by Symantec—the world leader in Internet security technology—about half of the respondents said they suspected or were "pretty sure" they had been the subject of an attack with a specific political goal in mind, among which banking and financial sectors reported the most attacks, and 80% of the respondents thought the frequency of attacks would remain the same or increase.

ODUMUNC 2011
Issue Brief for the
GA First Committee: Disarmament and International Security (DISEC)

The Prevention of Cyberterrorism and Cyberwar

By: Son Thanh Dang

Specific examples of cyberwar and cyber terrorism between nations are numerous. In the wake of the United States (U.S.) spy plane incident in April 2001, the escalating political tension between the U.S. and China led to attacks by U.S. and pro-Chinese hackers upon important websites and mail servers of the other side in several weeks. Another more obvious example is a series of denial-of-service attacks from Russia on Estonia in 2007 right after the latter relocated a statue deemed to be sensitive to Russians. Since the Estonian government relied heavily on the Internet, the attacks substantially crippled Estonia's banking and targeted government systems, including telephone access to the emergency services. In the following year, another series of attacks again from Russia crashed Georgia's website system just before and during the former's physical invasion in the latter's territory. In all these cases, it cannot be proved that the governments were behind the attacks, but they also did not make any attempt to stop them. Less seriously, under more international pressure following its second nuclear test last year, North Korea organized attacks to disable many computers from offices of the President, Defense and Foreign Ministries, leading banks and the top selling newspaper of South Korea, and slow down several U.S. websites. The most recent cyber-attack was relevant to Stuxnet virus detected last month targeting Iran's nuclear facilities. This is a complex and carefully designed malware that can infect computers and then automatically look for a particular model of Programmable Logic Controller made by Siemens to reprogram and even provide dangerous commands. Many experts claim that this sophisticated "spy" virus could have been written by a nation state, and Israel and the U.S. are now the most common suspected due to their political conflicts with Iran.

In its position, the United Nations (U.N.) has already published charters on war and terrorism, but formulating laws and conventions on cyberwar and cyber terrorism will be a much more complicated process. The U.N. has responded to the issue with slow and minor actions. To illustrate, one of the actions taken by the Counter-Terrorism Implementation Task established in 2005 is to pursue efforts collectively through working groups on many terrorism-related issues including "Countering the Use of the Internet for Terrorist Purposes". At present, the only specialized U.N. body directly dealing with cyber attacks is the International Telecommunications Union (ITU), which has been trying to create a focus group to develop a baseline against which network operators can access their security. Apart from that, the U.N. has developed various workshops to train and teach diplomats about cyber attacks, making necessary

preparations in case of emergency situations. The U.N Institute for Training and Research's senior editor Ahmad Kamal wrote the book "The Law of Cyber-Space: An Invitation to the Table of Negotiations", offering solutions for further work and calling for negotiations leading to an international law on cyberspace. He points out that if the U.N. were to hold these negotiations, the discussions could not just be intergovernmental, but all stakeholders including the private sector and civil society have to fully participate. More officially, resolution A/RES/2321 on cyber terrorism adopted in 2008 by the U.N. General Assembly was focused on enhancing public awareness and calling for a standard punishment of this kind of attacks. Also, early in 2010, the General Assembly adopted a resolution on "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures", which encourages its member states to share best practices and measures in cybersecurity. Indeed, the international community has petitioned the U.N. to come up with a plan or a special task force to stop a potential cyberwar or cyber terrorism; however, many governments are, at the same time, not willing to share their knowledge, as they possess advanced cyber-fighting applications and want to preserve their advantage in this domain. This lack of cooperation, in addition to the previously discussed challenges, causes extreme difficulty in expanding the existing law of war and terrorism to the cyberspace.

Worried about the issue, the U.N. Secretary-General Ban Ki-moon revealed last year that cyber-weapons are to be added to the list of arms falling under the remit of the U.N.'s Advisory Board on Disarmament Matters, which develops policy on weapons of mass destruction. More recently, Hamadoun Touré, who has been Secretary-General of the ITU for 11 years and is up for reelection in a few weeks, has targeted cyber security issues in his electoral pledges. Touré said that he had been proposing for an international cyber peace treaty and would continue with it in spite of resistance. In addition, he would settle for a "common code of conduct against cybercrime" in which each country would make a commitment to protect its citizens against cyber criminals, and not to harbor terrorists or criminals in their territory nor attack another country first. As such,

the upcoming session of the U.N. General Assembly will be much more likely to feature debate over controversial legal and ethical issues around cyberwar and cyber terrorism. Currently, the only international treaty against cybercrime is the Council of Europe's Cybercrime Convention, signed by 43 countries, most of which are technically advanced. Meanwhile, many other countries have begun to take this issue into consideration for their own legal framework. In the U.S., President Bill Clinton created in 1996 the Commission of Critical Infrastructure Protection, which found that the combination of electricity, communications and computers are necessary for the survival of the U.S. and can be threatened by cyber-warfare. After that, President George Bush established the National Security Agency with a large cybernetics strike force. Several U.S. agencies created their own cyber-security groups such as the Information Warfare Center of CIA, the Electronic Security Engineering Teams of the Air Force, and the Cyber Command of the Pentagon. Likewise, Israel has the Unit 8200, devoted to cyberwarfare, which is often accused of supporting attacks against this state's enemies. Facing increasing threats of cyberwar and cyber terrorism, Brazil and Panda Security have recently signed an agreement in which the latter will support the training of the Brazilian Army's operational agents to fight against Internet-based crime and prevent cyberwar. In a similar context, the U.N. launched the African Center for Cyber Law and Cybercrime Prevention in August to monitor cyberspace and cybercrime in Africa. In Asia, Singapore announced the first cybersecurity training and accreditation program last month with view to teaching cybersecurity professionals how to defend the country from hackers.

In sum, until the U.N. issues an effective international treaty to combat cybercrime, states, businesses and individuals have to protect themselves from cyber-attacks. This is nearly impossible as cyberspace is too large, too sophisticated and too interconnected to be dealt with alone without cooperation. Therefore, it is time for governments to sit together and formulate a single solution to this top concerning problem at the international level.

Bibliography

1. Clarke, Richard and Robert K. Knake (2010). The Growing 'Cyberwar' Threat. Available WWW: http://www.npr.org/templates/story/story.php?storyId=126097038

2. Collin, Barry C. (2001). The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. Available WWW: http://afgen.com/terrorism1.html

3. Conway, Maura (2005). Terrorist Use of the Internet and Fighting Back. Available WWW: http://www.oii.ox.ac.uk/research/cybersafety/extensions/pdfs/papers/maura_conway.pdf

4. Denning, Dorothy E. (2000). Cyberterrorism Testimony before the Special Oversight Panel. Available WWW: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

5. Frauenheim, Ed (2002). IDC: Cyberterror and Other Prophecies. Available WWW: http://news.com.com/2100-1001-977780.html?tag=fd_top

6. Galley, Patrick (1996). Computer terrorism: What are the risks? Available WWW: http://www.iwar.org.uk/cyberterror/resources/risks/index.html

7. Grabosky, P.N. (1998). Crime and Technology in the Global Village. Available WWW: http://www.aic.gov.au/crime_types/cybercrime/onlinevictimisation/~/media/conferences/internet/grabosky.ashx

8. Kerr, Kathryn (2003). Putting Cyberterrorism into Context. Available WWW: http://www.auscert.org.au/render.html?it=3552

9. Lewis, James A (2002). Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats. Available WWW: http://www.csis.org/tech/0211_lewis.pdf

10. Masko, Dave (2010). Cyber-War Underway with Citizenry Targeted. Available WWW: http://www.huliq.com/10282/cyber-war-underway-citizenry-targeted

11. Noble, Johan J. Ingles-le (1999). Cyberterrorism Hype. Available WWW: http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm

12. Palmer, Shelly (2010). Cyberterrorism vs. Cyberwarfare: Defending the United Networks of America. Available WWW: http://www.shellypalmermedia.com/2010/02/07/cyber-terrorism-vs-cyber-warfare-defending-the-united-networks-of-america/

13. Pollitt, Mark M. (1997). Cyberterrorism - Fact or Fancy? Available WWW: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

14. Shahar, Yael (1997). Information Warfare. Available WWW: http://www.iwar.org.uk/cyberterror/resources/CIT.htm

15. Shelley, Louise I. (2003). Organized Crime, Terrorism and Cybercrime. Available WWW: http://www.crime-research.org/library/Terrorism_Cybercrime.pdf

16. Snyder, William (2010). Thresholds for Cyberwar. Available WWW: http://blog.cybersecuritylaw.us/2010/10/thresholds-for-cyberwar-center-for-strategic-and-international-studies.html

17. Spencer, Vikki (2002). Cyber Terrorism: Mass Destruction or Mass Disruption? Available WWW: http://www.crime-research.org/eng/library/mi2g.htm

18. Sproles, Jimmy and Will Byars (1998). A Student Paper on Cyber-terrorism. Available WWW: http://csciwww.etsu.edu/gotterbarn/stdntppr/

19. Thomas, Timothy L. (2003). Al Qaeda and the Internet: The Danger of "Cyberplanning". Available WWW: http://www.iwar.org.uk/cyberterror/resources/cyberplanning/al-qaeda.htm

20. Vivero, Richard J. (2001). Revenge of the Nerds: Cyber-terrorism Poses New Threats to National Security, and U.S. Defense Policy Must Anticipate the Menace. Available WWW: http://www.iwar.org.uk/cyberterror/resources/harvard-review/vivero-cyberterror.htm

21. Wilson, Clay (2005). Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Available WWW: http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf

Author's Biography: Son Thanh Dang is from Vietnam and a second-year Masters Student of the Graduate Program in International Studies at Old Dominion University.