ODUMUNC 2015
Issue Brief for the
GA First Committee: DISEC

Cyber Security: Defining Cyber Terrorism and Permissible Responses

By: Robby Townsend
Old Dominion University, Model United Nations Society

What is it all about? The use of the Internet and information technology to cause harm is an issue of great concern and difficulty. Although terms like cyberwar are widely used, there is little agreement on what they mean, or whether a cyberwar would cause enough human suffering to be worthy of the name. Cybercrime is much more accepted. The impact on companies is usually very quick—network managers have gotten much better at responding to hacking and viruses—but often quite costly. Is the threat to state security, to people, or mostly to business? How should the international community respond?

The cyber security problem: The first major cyber-attack came in 2007, when several networks in Estonia were shut down by a massive Distributed Denial of Service attack (DDoS). This blocked access to government websites for several hours and stopped some banking for a full day. The attacks were associated with a political confrontation over removal of a statue commemorating Soviet re-conquest of Estonian during World War Two. Whether the attacks were officially sanctioned by the Russian government or the work of Russian activists remains unknown. Smaller attacks were directed against Georgia during its three-day war with Russia in August 2008.

The best known and most effective cyber-attack of all time came in 2009-2010, when the United States launched a virus against Iranian nuclear enrichment centrifuges at its fissile material facility at Natanz, south of Tehran. The Stuxnext attack destroyed or shut down ten percent of Iran's uranium enrichment capabilities for a full year.[1] Stuxnet reportedly was a virus targeted through flash drives, not the internet. Other major attacks have been focused on specific companies, often penetrating their security systems in search of credit card numbers.

In May of 2010 the Dow Jones Industrial Average plummeted nearly 1000 points (8 percent of its value) after a trading algorithm malfunctioned. This proves that stock exchanges are highly vulnerable to cyber glitches and hackers. Less than a year later, NASDAQ revealed that its servers had been broken in to and hackers had access to confidential corporate documents. It is unknown what the cause for the hacking was; it is known that the hackers were able to plant malware inside the Director's Desk web application. While the trading platform wasn't breached, it raises questions about just how secure financial markets are. NASDAQ accounts for almost 19 percent of the American stock market, and a breach to its trading platform could be disastrous, especially in the short-run. Weather an attack would have long-term consequences is more speculative.

In early 2012 a virus now known Flame virus was discovered. Like Stuxnet, Flame attacks windows operating systems and was believed to be made by a group of nations, including those involved in Stuxnet. Unlike Stuxnet, it was used for espionage purposes. Several major laboratories including CrySyS and Budapest University for Technology and Economics deemed

[1] Sanger, David E., "Obama Order Sped Up Wave of Cyberattacks Against Iran", *New York Times*, 1 June 2012; 'How cyber-warfare really started—and where it will lead', *The Economist*, 13 December 2014.

it the most complex malware they had ever encountered and possibly the most complex malware ever made. According to estimates by Kaspersky in May 2012, Flame had initially infected approximately 1,000 machines, with victims including governmental organizations, educational institutions and private individuals. At that time 65 percent of the infections happened in Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt, with a "huge majority of targets" within Iran.

The dilemma of cyber vulnerabilities: A major problem with cyber security is the speculative nature of the threats. The range of possible threats is quite broad. Well-known possibilities include:

- Attacks interfering with internet related installations, server parks, major firms
- Attacks on financial industries such as banking and security trading
- Attacks denying access to defense ministries
- Energy industries, electricity generation and distribution, including oil refineries and oil and gas pipelines
- Interference with equipment at critical infrastructure such as emergency services, hospitals, energy generation and distribution, transportation
- Information access of criminal and terrorists
- Information access of revolutionaries
- Violation of commercial and individual privacy

The contradictory nature of cyber security means that efforts to protect any of these (government, industry or critical infrastructure) or block their access (such as revolutionaries, criminal and terrorists) usually affects others in unpredictable and often counterproductive ways. Cyber security, the, is always about tradeoffs between possible security and likely disadvantages of slower of blocked internet access and limits of freedom and entrepreneurship.

Wikileaks founder Julian Assange speaking from his haven in the Ecuadorian embassy in London, October 2012

International Action: Cyber security is an issue relevant to all UN organizations an bodies, either as users of on-line services or because they are responsible for issues related to insuring access and protecting state interests. Cyber security has been considered by the UN General assembly, the Economic and Social Council, and specific attacks by the UN Security Council.[2]

The Geneva-based International Telecommunications Union (ITU), an independent international organization affiliated with the United Nations, has emerged as the center for international coordination on these issues.[3] By setting standards for all telecommunications, it provides essential benchmarks for governments, establishing what is universally accepted as permissible and where limits are for governments. UN General Assembly and ECOSCO relations usually mandate the ITU as the center for further consideration and action.

In May of 2012 a UN committee charged with helping member nations secure infrastructure plans issued a warning to member nations of the UN regarding the Flame virus. Marco Obiso, cyber security coordinator for the U.N.'s Geneva-based International Telecommunications Union said that it was the "most serious cyber warning they had ever issued." "The confidential warning will tell member nations that the Flame virus is a dangerous espionage tool that could potentially be used to attack critical infrastructure," he said in an interview.

Considering the growing popularity and necessity of internet usage in the highly developed countries of the world, places such as China and the United States will likely by very keen to see a functional definition for cyber-attacks established, and some ideas for what the proper recourse after such an attack might be. Most of world can likely stand and agree that cyber-attacks with kinetic effects similar to an armed attack can be treated as an act of war, but considering that Stuxnet could have been considered an act of war under such definitions, it is likely that the US and Israel, along with many of their NATO allies, would stand together in denouncing the possibility of making armed retaliatory responses a viable option, while nations like China, Iran, and Russia would likely feel that cyber-attacks should be punishable by initiation of a full-fledged war to deter any possible attacks on their financial markets or military industrial complex.

It is largely within the interests of all nations to establish a basis for what is acceptable in the cyber world and what exactly can be considered a cyber-attack. If a virus such as Stuxnet or Flame were to infect a major stock market, the resulting economic fallout could be disastrous and cause suffering for many millions of people in the affected country beyond even those that trade on the infected market.

Leading countries and positions: A major international division pits the United States, who charges China with widespread internet malfeasance, and many other countries, who see activities like Stuxnet and conclude the United States is greatest source of danger in the international system.[4] This has led some countries, such as India, to fear being caught in a cyber war between Beijing and Washington, and leads them to search for international restrictions on offensive attacks.[5]

The United States emerged as the pace-setting country for cyber security issues, both as the best known source of cyber security innovations and the most ambitious use of cyber-attacks.

[2] "Cybersecurity: A global issue demanding a global approach", *United Nations News*, 12 December 2011
[3] International Telecommunications Union (ITU)
[4] "Cyber Security: China Most Threatening Cyberspace Force, U.S. Panel Says", *Bloomberg*, 5 November 2012
[5] "Cyber security: India, UK to conduct talks bi-annually on cyber security", *DNA India*, 8 November 2012

American leaders have been among the loudest warning of threats of cyber attacks.[6] The United States has established a military command (Cybercom) dedicated to making its military more secure against hacking and disruption. It has aggressively prosecuted hackers and leakers, such as Bradley Manning, the American soldier accused and held in prison awaiting trial for providing 250,000 classified documents to Julian Assange who made them public through Wikileaks. On the other hand, the United States also is the source of the most ambitious cyber-attacks, most notably Stuxnet, a virus used to temporarily disable uranium enrichment centrifuges in Iran in 2010. The United States believes that private enterprises, businesses and individuals, should be responsible for their own on-line security and leaves private security to those actors.

The United States demands that other countries establish clear polices to stop cyber crime and maintain cyber security, but it does not have clear national law regulating its own domestic activity. The paralysis of its government means it now lags far behind most other countries in this regard, except failed states like Democratic Republic of Congo (DRC), Somalia and Yemen.[7] While the United States government is very active in this area, its contradictory positions and lack of domestic law weaken its international leadership. It is a massive force in international deliberations on these issues, but often seeks contradictory goals, leading other countries to work around its initiatives.

The European Union and member European countries have emerged as leading advocates of individual on-line privacy and freedom. They are among the most creative and original source for innovative solutions to perplexing internet and telecommunications issues. European's strongly maintain that the states and international organizations have no legitimate role interfering with the on-line activities of individuals or private firms. While European countries work assiduously to protect official networks and help business maintain their security, they reject any right of the state to spy on-line domestically without probable cause and court-ordered search authority. Several European countries have major political parties dedicated to assuring internet access and privacy: notably the *Pirate Parties* of Germany and Sweden.

European governments are more inclined to be suspicious of the massive corporations that control much of the internet, pioneering prosecutions of firms like Facebook, Google and Microsoft for violating customer privacy and forming illegal monopolies. European governments seek to protect the internet and other telecommunications from all disruptions, including official disruption.

China and Russia believe the internet should be controlled by governments and states to serve to goals of national policy. They appreciate the creative advantages made possible by the internet, but also express concern with its ability to weaken the state and interfere with its ability to set national policy. They are extremely concerned at the way on-line telecommunications have been used by revolutionaries to undermine governments, as in the 2004 Orange Revolutions in **Georgia** and **Ukraine**, and the attempted revolution in **Iran** in 2009.[8] Their response has been to channel all on-line communications through official gateways, screening content. The so-called Great Firewall of China is a well-publicized example. China is routinely accused of being the origin of hacking efforts against foreign governments. Russian hackers or its government are suspected to launching denial of service attacks against

[6] **"**Panetta Warns of Dire Threat of Cyberattack on U.S**."** *New York Times, 11 October 2012.*
[7] "Cyber security: US Senate likely to revisit cyber bill when Congress returns", *Chicago Tribune*, 31 October 2012

[8] "Iran rejects UN criticism of its cyber security rules," *Reuters*, 25 October 2012

Since the American Stuxnet attacks, countries that previously overlooked cyber security have become heavily engaged. **Australia, India** and **Indonesia**, for example, have established domestic cyber security agencies and begun working to insure the security of government activity, commerce and vulnerable firms. They see the state as the guardian of private enterprise and work with businesses to insure their security.

Estonia has been a world-leader in on-line policy reform since the early 2000s, when it put all government activity on-line, including voting. After the 2007 denial of service attacks, Estonia emerged as a center for cyber security. It hosts the Cybersecurity Center of the North Atlantic Treaty Organization (NATO). It stresses individual freedom and privacy, with state activism to insure system stability and safety.

Similarly, **Ecuador** emerged in 2012 as a leader for free internet access and activity, championing the freedom and work of Wikileaks founder Julian Assange, harboring him in its London embassy against British efforts to send him to Sweden where he faces rape charges.

Non-governmental organizations and prominent individuals often take a completely different direction, arguing that the role of the UN should not be to protect states and their interests, but to serve humanity. They maintain that the best use of the UN is to restrain states and their freedom of action to protect private interests. Their inspiration comes in part form the state-defying work of individuals like Julian Assange and Edward Snowden, who in revealed the existence o massive cyber spying by the United States. For this perspective to be effective in the UN, it would have to be advocated by major states, the members of the UN.

Bibliography

General:

‘A special report on cyber-security: Defending the digital frontier’, *The Economist*, 10 July 2014

Cyberspace Governance: The Next Step, Council on Foreign Relations, March 2011

"Cyberwar: War in the Fifth Domain," *The Economist*, 3 July 2010.

“Marching off to cyberwar,” *The Economist*, 4 December 2008.

Sanger, David E., “Obama Order Sped Up Wave of Cyberattacks Against Iran”, *New York Times*, 1 June 2012.The best background article on the 2009-2010 Stuxnet attack.

“UN warns member nations on risk of Flame virus”, *Chicago Tribune*, 29 March 2012

“Why the Financial World Is Spooked by Nasdaq Cyber Attack”, *The Atlantic*, 7 February 2011

Sample positions:

Australia: "Cyber security a top priority for Australia", *PC Advisor*, November 2012

Canada: "Canadians lax on cyber-security: Experts 'Regulations may be necessary'", *Windsor Star*, 1 November 2012

India: Enter the cyber dragon , *India Today*, 5 November 2012

India: "Cyber security: India, UK to conduct talks bi-annually on cyber security", DNA India, 8 November 2012

India: "Indian Government to invest $200 mn in 4 yrs on Cyber Security Infrastructure", *Government of India*, November 2012

Indonesia: "Indonesia's cyber defense strategy and its challenges", *Jakarta Post*, 1 November 2012

Iran: "Iran rejects UN criticism of its cyber security rules," *Reuters*, 25 October 2012

United Nations: "Cybersecurity: A global issue demanding a global approach", *United Nations News*, 12 December 2011

United Nations: http://www.itu.int/cybersecurity/

United Nations: International Telecommunications Union (ITU)

United States; "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*, 11 October 2012.

United States; "Cyber security: US Senate likely to revisit cyber bill when Congress returns", *Chicago Tribune*, 31 October 2012

United States: "Cyber Security: China Most Threatening Cyberspace Force, U.S. Panel Says", *Bloomberg*, 5 November 2012