SUSQUEHANNA VALLEY MODEL UNITED NATIONS
2015-2016
Mr. Adam Titter, Chairman, Lampeter-Strasburg High School
Mr. Jason Perkowski, Vice-Chairman, Conestoga Valley High School
Mrs. Sallie Bookman, Treasurer, Penn Manor High School
Ms. Gretchen Ripple, Secretary, Garden Spot High School

General Assembly
CYBER WARFARE, TERRORISM AND CRIME

A SUMMARY OF THE ISSUE AS IT STANDS TODAY:
Increased numbers of cyber attacks are being launched by and against state and non-state actors (organizations, institutions and individuals). This has included the destruction of scientific equipment (like the computerized cenrifuges in Iran), the theft of personal and national security information, gaining control over infrastructure systems (like electrical grids, internet satellites, fuel systems, and water systems), and attacks against corporations. And increasingly the technology would allow a nation to go to war by shutting down their enemy's national infrastructures, destroying their enemy's weapons control systems, using blackmail techniques based on info garnered from cyber-espionage, etc. Using these techniques could allow a nation to force their enemy into submission with the limited use of conventional weapons (guns, missiles, tanks, etc.). However, there are limited regulations that dictate the rules of this type of warfare—and what constitutes cyber war versus cyber crime.

GOAL:
The General Assembly will decide on the rules of cyber warfare—building on the earlier work of the Geneva Conventions. They will define what constitutes cyber warfare versus cyber terrorism and cyber crime. Acknowledging that while warfare is never ideal it may sometimes be necessary, they will also determine the regulations of when and how cyber warfare may be conducted in order to minimize casualties—especially civilian casualties. Additionally, they will determine the legal responses that may be taken in response to cyber terrorism and cyber crime.

KEY CONSIDERATIONS OR ELEMENTS TO BE FOCUSED ON BY THE COMMITTEE:
Be sure to write your resolutions to clearly answer some or all of the following questions. Ensure that your research explores these question from an international perspective grounded in the background of the country which you are representing.

- **Cyber Warfare**
  - What constitutes legitimate scenarios in which a nation may declare cyber war against an enemy nation, organization, institution, and/or individuals?
  - In a world in which we are increasingly seeing non-state actors (organizations, institutions, and individuals) involved in conflicts, how can the international community (and the UN specifically) manage conflicts and hold actors accountable for their actions in order to minimize damage and protect civilians?
  - What process should be required for "declaring" war (keeping in mind state and non-state actors) acknowledging the desire that an actor may have for secrecy about their actions.
  - What are legitimate acts of cyber warfare that could be utilized in a conflict that would allow a nation to neutralize an enemy nation?
  - What are legitimate preventative measures that can be taken to investigate and thwart potential cyber attacks? And what are the limits to these actions—particularly in relation to acts of espionage that may be perceived to violate national, corporate and individual sovereignty?
  - What boundaries should be established that limit cyber attacks and strategies that may be limited—with the goal of saving civilian lives and minimizing unnecessary military casualties.
- **Cyber Terrorism & Cyber Crime**
  - What actions and behaviors by a state, organizations, institutions, and individuals constitute cyber terrorism? And what actions would constitute cyber crime that may not rise to the level of cyber terrorism?

- What are legitimate responses that can be taken in response to acts of cyber terrorism?
- What are legitimate preventative measures that can be taken to investigate and thwart potential cyber attacks? And what are the limits to these actions—particularly in relation to acts of espionage that may be perceived to violate national, corporate and individual sovereignty?

- **Oversight**
  - Keeping in mind that technology is rapidly changing, how can regulations be established that are flexible and accurate enough to be useful for an extended period of time?
  - Additionally, is there a mechanism / organization that could be implemented in order to monitor and update regulations as needed?
  - What institutions (extant or in need of creation) should be responsible for monitoring cyber conflicts and holding actors accountable for illegal acts, damage to property, and harm to citizens?

BACKGROUND:

Cyber Terrorism Background Guide – from Edison Model UN

Background:

The FBI defines cyber-terrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents."1 In 2013 the motivational statistic behind cyber attacks was shown to be 50% Hactivism. Hactivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. This was only seconded by cybercrime which accounted for 40% of cyber attacks in 2013. As for the distribution of different attack techniques that cyber terrorists use, the most popular is the use of DDoS. This number stood at 50.6% simply because of this attack's efficiency. DDoS is a denial of service tactic in which one can aggressively spam email blasts to someone or something or even temporarily shut down services anywhere in the entire world.

Due to the potential power and danger of cyber terrorists and their increasing affinity for becoming a worldwide issue, "[international] business IT budgets devoted to security nearly doubled from 7% in 2007 to an estimated 14% last year."2 By 2016, the world wide spending on data-security technology is projected to rise to over $10 billion. Cyber terrorism also created emergence among entire countries as well. In 2010, the US left aside its traditional policy of rivaling against the draft resolutions of Russia when it co-sponsored the Russian Federation's draft on cyber-security which Russia had proposed continually since 1998. In September 2011, the Russian Federation and China, along with Tajikistan and Uzbekistan, formed the International Code of Conduct for Information Security. This draft resolution aimed at clearly stating State's rights and promotes international cooperation in countering cyber terrorism.

Landmark incidents of cyber terrorism can be taken from the US's experience after 9/11. From then on, cyber attacks on the US became prevalent. For example, in 2006, a Romanian hacker, Victor Faur, disrupted over 150 US government computers. These cyber attacks on these computers led to the disruption of the NASA systems which created cyber damages costing up to $1.5 million. In other ways, cyber terrorism can create actual physical consequences. In 2001, Chinese hackers developed a way to intercept American surveillance planes with Chinese fighter planes. For days, these Chinese hackers were able to continually harass American surveillance planes. The Unmanned Aerial Vehicles (UAVs) were physically attacked and the damages cost over $100 million.

UN Involvement:

In September 2006, the Working Groups of the United Nations Counter-Terrorism Implementation Task Force (CTITF) were created in order for Member States to pledge their cooperation in international and national counter terrorism measures on the internet. Through this pledge the CTITF formed the Global Counter-Terrorism

Strategy, which detailed the aims of this working group including the countering of financing toward terrorism. In October 2009, the CTITF published a "report containing 36 findings and 45 recommendations that are intended to help Member States increase the effectiveness of efforts to combat the financing of terrorism." The general areas that were covered include value transfer systems, non-profit organizations; and the freezing assets. This specific report even led to an Action Plan prepared by the International Monetary Fund (IMF) which undertook the recommendations of the CTITF.

Besides that, this working group has pooled together certain reoccurring issues among the international community and two nations noted cyber terrorism as their top issue. In response, the working group created a solidified version of all possible motives of cyber terrorism via internet. By examining the reasoning behind the hackers, the CTITF developed possible solutions and goals for 2009 including building a database of research into use of the Internet for terrorist purposes. In 2011, the CTITF shifted their focus on the aim to "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."3

Specialized agencies such as the ITU, International Telecommunication Union, work toward supporting a cyber-peace initiative by decreasing the prospect of countries engaging in a cyber war. The ITU also tracks and records statistics in a UN database for the UN Secretary General in case of a cyber attack. They use the Global Cybersecurity Agenda as reference during attacks in order to quickly and politically handle a cyber attack. While the ITU is an agency that promotes the use of Information and Communications Technology (ICTs) it holds regulations on ICTs through its Global Cybersecurity Agenda which it uses as an international framework. By modeling its international policy after the Global Cybersecurity Agenda it thus promotes its main goals of using model legislation such as that of the Budapest Convention on Cybercrime for Member States and creating a Cybersecurity Readiness Index.

The UN Economic and Social Council adopted a 2004 resolution, 2004/26 titled "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes." This resolution detailed the illegitimacy and classification of identity theft or fraud. In recognizing this, the resolution urges certain regulations such as the prevention, detection and punishment of frauds and hackers. It also states that countries should use bilateral and multilateral systems in order to pool information including through the United Nations Convention against Transnational Organized Crime. While ECOSOC does relate to some specific aspects of cyber crime, it generally stays flexible to account for different resolutions across the board. ECOSOC is responsible for either adopting or denying draft resolutions from several committees, sub committees and agencies such as the Commission on Crime Prevention and Criminal Justice and the ITU.

The General Assembly adopted resolution A/RES/64/211 titled, "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures." This resolution focused on determining the cyber security of Member States. It urges the precaution of a round-the-clock Cybercrime Point of Contact Network, bilateral partnerships, and international evaluations of how prone a nation is for cyber terrorism. It also emphasizes the responsibilities of governments to protect their citizens against these crimes. It notes that governments should create national and international strategies for cyber crime and report issues with the Secretary General in order to have an accurate and efficient pool of information against hackers.

Under the UNODC, the NGO, Society For The Policing of Cyberspace (POLCYB) uses its international network to influence public and private organizational levels in aspects such as prevention, research and anti-corruption of cyber crime. Specifically they enforce their three main goals which are to increase bilateral and multilateral partnerships against cyber terrorism, establish a permanent international network for cybersecurity, and provide public education on cyber security.

BACKGROUND LINKS:

- **Geneva Conventions and other Protocols -- https://www.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp**
- **"Here is how cyber warfare began — 50 years ago" --** http://wtvr.com/2015/03/12/here-is-how-cyber-warfare-began-50-years-ago/
- **"Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment" -- http://www.un.org/press/en/2014/gadis3512.doc.htm**
- **Towards Cyberpeace: Managing Cyberwar Through International Cooperation -- http://unchronicle.un.org/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation/**
- **"Watch out world: North Korea deep into cyber warfare, defector says" --** http://www.cnn.com/2014/12/18/world/asia/north-korea-hacker-network/
- **"Cyberwar: CyberCaliphate targets U.S. military spouses; Anonymous hits ISIS" --** http://www.cnn.com/2015/02/10/us/isis-cybercaliphate-attacks-cyber-battles/
- **General Assembly Resolution on Cyber Security --** https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf
- **"These 5 Facts Explain the Threat of Cyber Warfare" –** http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/
- **"NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar" --** http://www.wired.com/2013/06/general-keith-alexander-cyberwar/
- **"Cyberwar Ignites a New Arms Race" --** http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128
- **"U.S. Team and Israel Developed Iran Worm" -** http://www.wsj.com/articles/SB10001424052702304821304577440703810436564http://www.wsj.com/articles/SB10001424052702304821304577440703810436564

ADDITIONAL REFERENCE GUIDES ON THE ISSUES:

- http://www.un.org/ - The U.N. website's homepage
- **http://www.un.org/sc - Security Council Home Page**
- http://www.un.org/documents/ - Access to search for UN Documents – including press releases and resolutions
- http://www.un.org/members/ - For a listing of all member states, observers, NGOs, etc.
- **http://www.un.int/missions/webs.html Links to the websites of all permanent missions.**
- **http://www.un.org/largerfreedom/contents.htm - "In Larger Freedom" Text**
- http://www.un.org/cyberschoolbus/ - U.N. Education Website with materials on various issues
- http://www.unausa.org/ - The association that helps with public awareness of the UN in the USA.
- **http://www.globalpolicy.org/security/reform/index.htm - Watchdog website on global policy**
- **https://www.cia.gov/cia/publications/factbook/index.html - A great source of statistical data on various nations**
- **See various links listed in text throughout this document**

BOLDED hyperlinks are especially recommended as first stops in your research. Of course a plethora of information can be found by utilizing databases such as GALE or AP sources, Googling news releases, or browsing documents on the websites of the State Departments or Executive branch of specific countries. Also be sure to make use of the search features on the UN Website. Just be sure to select reputable sites. Much of Wikipedia's information is listed on the other sites—so stick with the reputable ones to ensure accuracy.

Respectfully Submitted,
Jason Perkowski & Gretchen Ripple
Chairpersons, General Assembly – SVMUN