Cyber Terrorism
High School General Assembly
2026 St. Mary's County Model UN Conference

Background

With nations' increasing reliance on technology, a new system of warfare has developed. It is called Cyber terrorism. The FBI defines cyber terrorism as "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." This would include the NSA, CIA, and MI6 hacking other countries. This has been used countless times over the past decade between countries. Examples include China and the U.S., Israel and Iran, etc.

Current Issue

Cyber terrorism is a very heated topic. The U.S. and China have been going head to head with cyber attacks. China has been hacking U.S. computers, stealing classified documents, and copying U.S. weapons development. According to the recent leaks by Edward Snowden the U.S. has also been hacking China and Hong Kong for years. This has put pressure on the already strained relationship between the U.S. and China.

Another country famous for utilizing cyber terrorism is Israel. They have developed several computer viruses to attack Iran, including Flame and Stuxnet. They were used against the Iranian Nuclear Weapon Program. They were very effective, however it has spread all over the world causing problems for everyone. The U.N. originally found it when they were asked to find out what was wiping data from machines. Iran has blamed the U.S. and Israel for developing it and has created an anti-cyber unit to combat such viruses.

The U.N. has created charters on dealing with Cyber terrorism. They have created several small steps in order to try and control it. One of these steps is the Counter Terrorism Implementation Task, which is creating working groups to combat cyber terrorism. They have also created the International Telecommunications Union (which was the agency that founded Flame) to develop a baseline against which network operators can access their security. The ITU has tried to train people to counteract computer viruses as well. Despite these efforts, there has been no major breakthrough in the fight against cyber terrorism.

A huge aspect of cyber terrorism is extradition. If Country A hacks Country B, Country B would want to try the hacker in its own courts. It would typically want to be harder on that person than on an individual from their own country. Country A would want to try the hacker as well and it would typically be more lenient on the hacker. This issue becomes even more complicated when the issues of human rights are considered. The U.S. is unwilling to send any person to China or North Korea, because they fear the person would be tortured. If extradition is demeaned by China or North Korea the U.S. will give the excuses about concerns with human rights as grounds for saying no.

Role of the United Nations

The U.N. states that countries need to have more cooperation in order to successfully counteract cyber terrorism. As stated before, countries have successfully used cyber terrorism to accomplish global security goals. Countries like China and the U.S. have veto power in the

Security Council, and have opposite ideas about what should be done. Both sides want it to still be possible to use cyber terrorism.

Guiding Questions*:*

- Has your country been a victim in any major cyber attacks
- Has your country conducted any major cyber attacks
- Does your country have an active agency that deals with cyber attacks
- What is your countries stance on cyber terrorism

Resources:

- UNODC. “Cybercrime Module 14 Key Issues: Cyberterrorism.” *Www.unodc.org*, June 2019, www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html.

- Matamis, Joaquin. “The UN Security Council Discusses Cyber Threats to International Security • Stimson Center.” *Stimson Center*, 15 Apr. 2024, www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/.

- “Cyber Clash with China (NSC).” *CFR Education from the Council on Foreign Relations*, 2024, education.cfr.org/learn/simulation/cyber-clash-china-nsc/background.

- Weimann, Gabriel. *Cyberterrorism: How Real Is the Threat?* United States Institute of Peace, Dec. 2004.