Created by **Connor Markus.**

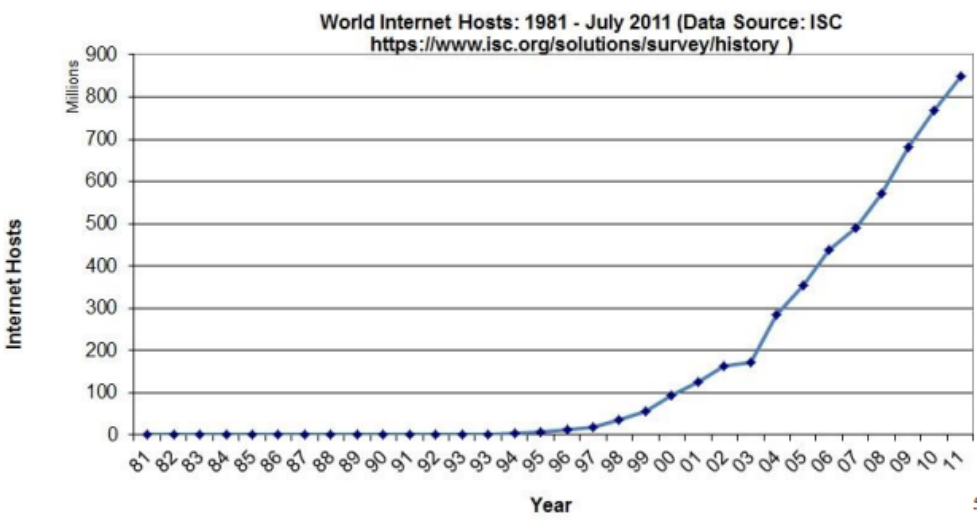
Background Information

Terrorists take advantage of the internet to organize themselves into terrorist organizations and learn how to create and acquire weapons, but also pose a risk to global privacy in their goals to hack into the information of foreign governments and people. In many nations, the prevalence of highly skilled organized hackers is becoming a threat to national privacy and even the security of politically opposing groups. This level of terrorist involvement in the internet cannot go unnoticed as the threat is more concerning and present than ever. The growth of internet-based terrorism is correlated with exponential growth in gross Internet users which has created a greater threat level to our internet synced population. Businesses are now also extremely dependent on internet use and data, and with malicious interference, attacks can deeply affect market stability and endanger sales, profits, leadership and employee reputations. Failure to address the problems of this scale in cyberterrorism can have the potential to destabilize a business or capital of a good beyond recovery.

Terrorist organizations have ambitious goals for internet sourced attacks, such as controlling systems that support the electricity industry, but measures have been put in so they have been sealed off through government intervention. But in some cases, many protections that created isolation have become weaker with the introduction of automated controls based through advanced online networks. With automation growing, the opportunities to hack into industrial control systems through a cyber-attack increase yearly. The dark web is based on the internet but needs software configurations to access, making it very challenging for governments to police. Improvised Explosive Devices (IEDs), which were used in the 1996 Olympic Park Bombing and the 2005 London Bombings are usually made with many commonly available materials, such as fertilizer, gunpowder, and hydrogen peroxide; one of our committee's main concerns will be combatting the spread of information regarding the making of IEDs. This poses the concern of information censorship and whether the

justification of blocking the malicious content is reasoned for global security.

Terrorist organizations also often use the internet to recruit new members, collect and transfer funds, organize terrorist acts, and as a weapon for cyberattacks. Facebook and Twitter have become direct sources of recruitment and have approached this by mass blocking of these pages, but dark web site still exist to maintain the publicity of the terrorist organizations. Our committee's Topic #2 will be split into **two primary parts**: the creation of terrorist groups from the use of online platforms and the acquiring of weapons and the supplies to make them from the dark web.



The exponential growth of the Internet that starts in the late 1990s as shown to the left. The year 1995 is often considered to be "year zero" of the internet. This growth is connected with the rapid growth in the number of Internet users which created greater interdependence and an increased threat level.

Terms/Topics to be familiar with:

- Cybercrime
- Cyberterrorism
- Sami Omar Al Hussayen
- ISIS and the internet

- How terrorists groups use the internet
- White Hat Hackers
- Hacktivism
- Legality of Hacking

UN Involvement

https://undocs.org/en/A/RES/64/211(2009)

This resolution from 2009 addressed the creation of a global culture of cybersecurity and advancements in taking stock of national efforts to protect critical information infrastructures.

https://undocs.org/en/A/RES/64/168(2009)

A resolution to reference the UNs terms of protection of human rights and fundamental freedoms while countering terrorism.

https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf

https://www.un.org/ga/search/view_doc.asp?symbol=A/68/164

List on nations involvements in combating terrorism

https://www.un.org/en/ecosoc/cybersecurity/summary.pdf

A commission on cyber security and the development of internet based terrorism from UN.

Questions to Consider

- How can we track down and limit the use of terrorist-specific websites?
- How can we police the dark web in a more effective way?
- How can we detect and take down informational pages about IED creation?
- Does your nation have an effective framework to tackle cyber terrorism?
- Has your nation or any of its allies been a victim of cyber terrorism in a big way?
- How open is the Internet in your country?

- Are various sites restricted in your nation? Example: Various social media sites are banned in China
- Is your nation a signatory to any international conventions related to cyber
- security?
- Most importantly, how can our nations work to combat terrorism while protecting the national sovereignty and specific laws of each other?

Sources

https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html
This Source contains a large database of definitions with examples and the global legality of policing cybercrimes and the prevention of cyberterrorism.

https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html
“The nature of the terrorism threat facing society has changed considerably in the last 20 years. Previously, governments and (re)insurers structured their mitigation strategies and responses to deal with attacks that were large in scale.”

https://items.ssrc.org/after-september-11/is-cyber-terror-next/
An article that provides an in-depth history of cyber security and terror in the 20th century. It provides many attacks and detailed descriptions of the events.

https://www.forbes.com/sites/zakdoffman/2019/09/13/cyber-dirty-bomb-terrorist-threat-is-real-warns-us-cyber-general/#4fba69ef679f
Same as article provided above^

https://www.un.org/press/en/2014/gadis3512.doc.htm

Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at the Conclusion of Thematic Debate Segment

https://www.reuters.com/article/us-china-usa-cybersecurity-idUSKBN0TL0F120151202