United Nations General Assembly (GA)

Description of Committee

The General Assembly (GA) is the key representative body of the **United Nations**. It includes all 193 member states; each member state has one vote. It is empowered through Article 11 of the **UN Charter** to “consider the general principle of cooperation in the maintenance of international peace and **security**.”[1] The GA addresses all aspects of UN work, including humanitarian; peace and security; and human rights matters, and it can refer threats to peace to the Security Council for discussion. Although the resolutions of the GA are **non-binding**, they are important international documents because they are supported by the majority of countries in the world. The actions of the General Assembly provide a code of sorts for other UN bodies, as well as for the international community as a whole.

As a representative of your country’s government in the General Assembly of the United Nations, it is important to have a full understanding of the purpose, functions, and abilities that the General Assembly possesses.

The General Assembly has the power to 1) make recommendations on peace and security; 2) elect members to UN organizations; 3) decide admissions, suspensions, and expulsion of members; 4) consider and approve the budget; 5) discuss and make recommendations regarding changes to the UN Charter and organs of the UN; 6) initiate studies and make recommendations to promote international political cooperation.[1] You will be focusing on the first point: making recommendations on peace and security.

Every nation in the United Nations holds a seat in the General Assembly and has one vote during voting procedures. This system is used to promote equality – all votes hold the same amount of power regardless of a country’s size or population. For designated important issues, a two-thirds majority is required for a resolution to pass; all other votes are held as a simple majority.

Topic: The Prevention and Countering of Cyberterrorism

What is Cyberterrorism?

The Internet is a key resource and tool in today's world. With almost three billion users worldwide,[2] the Internet has never been more necessary to keep global society functioning. **Cyberterrorism** is the politically motivated use of computers, the Internet, and information technology in an attack designed to cause widespread disruption and fear in a society.[3]

The term *cyberterrorism* is a controversial one; mostly because there is no standard definition for the word **terrorism**. "During the 1970s and 1980s … United Nations attempts to define the term foundered mainly due to differences of opinion between various members about the use of violence in the context of conflicts over national liberation and self-determination..”[4] The difference between 'terrorists' and 'freedom fighters' is still a major issue today, and as such there is still no official UN definition of terrorism.

Narrow vs. Broad Definition

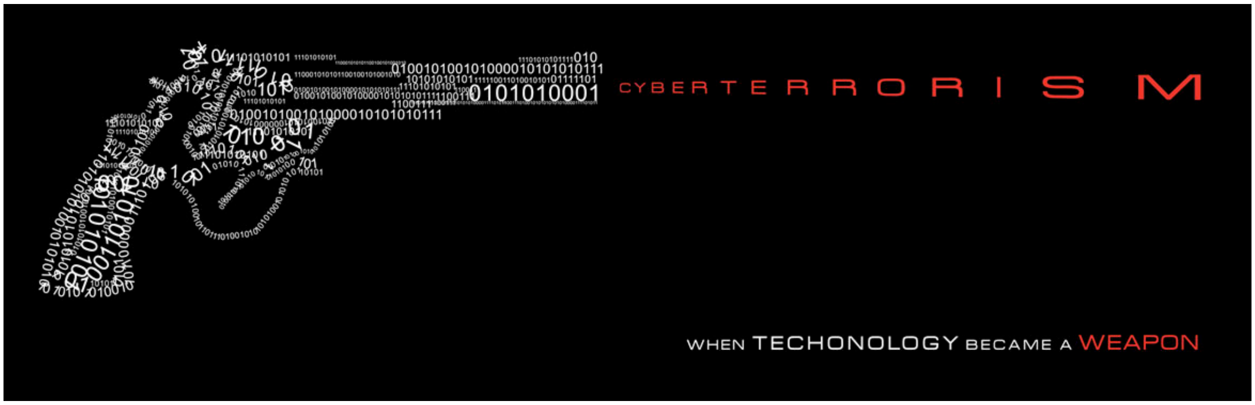
Experts usually fall into one of two camps regarding the definition of cyberterrorism. A narrow definition holds that cyberterrorism refers exclusively to attacks on information technology infrastructure by known terrorist organizations to cause widespread fear.[5] There are very few, if any, instances of this type of cyberterrorism.

A broad definition of cyberterrorism would define cyberterrorism as "the use of information technology by terrorist groups and individuals to further their agenda."[6] This would include using the Internet in what would be a legal manner if not for the fact that the people using it are terrorists. Almost all reported instances of cyberterrorism fall under this category.

> "Besides bearing little relation to any actual cyber incidents, the term [cyberterrorism] also fails to capture the bulk of what terrorists are doing in cyberspace. Terrorists are making extensive use of cyberspace to facilitate their objectives, and it is important to understand, exploit, and counter this use. Too much emphasis on cyberterror, especially if it is not a serious threat, could detract from other counter-terrorist efforts in the cyber domain."[7]
>
> - US Naval Postgraduate School
> Professor Dorothy E. Denning

What *isn't* Cyberterrorism?

It is indisputable that the term 'cyberterrorism' lies at the intersection of terrorism and the world of computers and the Internet. However, the use of these technologies by terrorists does not *necessarily* indicate cyberterrorism. To add to the confusion, the general public will often use such terms as **cybercrime**, **cyberwar**, and **hacktivism** interchangeably with cyberterrorism, when there are in fact subtle differences.[8] Experts disagree on to what extent each of these terms overlap; this is a subtopic which might be discussed at the conference.



Cybercrime is simply a crime committed through cyberspace. For example, imagine a scenario in which a criminal organization steals money from a company or an individual by breaking in to their online accounts. This is not in itself cyberterrorism because the organization's motive is purely financial. Other examples of cybercrime are the sale of illegal drugs over the Internet or Internet-based copyright infringement (piracy).

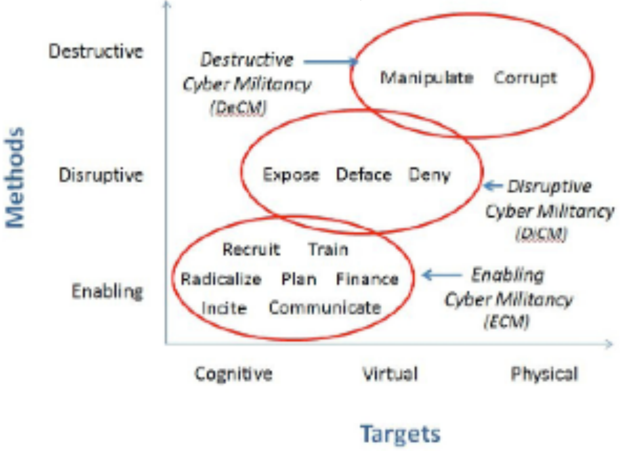
Cyberwar is the use of the Internet and information technology by one state against another state. It can be either to cause destruction through sabotage or it can be merely to gather intelligence as espionage. Some experts prefer the term 'information warfare' to 'cyberwar.'[9] Regardless of the name, cyberwar is still war, and should be treated as such in the international scene. 'Cyberterrorism' usually refers to deeds committed by **non-state actors**. The issue arises when it comes to state-sponsored cyberterrorist groups.

Hacktivism, like terrorism, is politically motivated. Seen in the most positive light, hacktivism is the electronic counterpart to conventional acts of protest such as civil disobedience.[8] However, hacktivism which causes significant harm to digital networks might be called cyberterrorism.

Clusters of Cyberterrorism

Jonalan Brickey, US Army Cyber Command Fellow at the Combating Terrorism Center at West Point, has identified three main clusters of cyberterrorism, as illustrated in the figure to the right. It is a qualitative approximation — that is, an inexact picture — of the spread of terrorist activities from research on the Internet to actual destruction of property or lives along two axes.[8] The x-axis represents the targets of cyberterrorism operations; the y-axis portrays the methods used. Thus the 'enabling' (ECM) cluster is characterized by the gathering of information and the target is 'cognitive.'

Clusters of Cyberterrorism

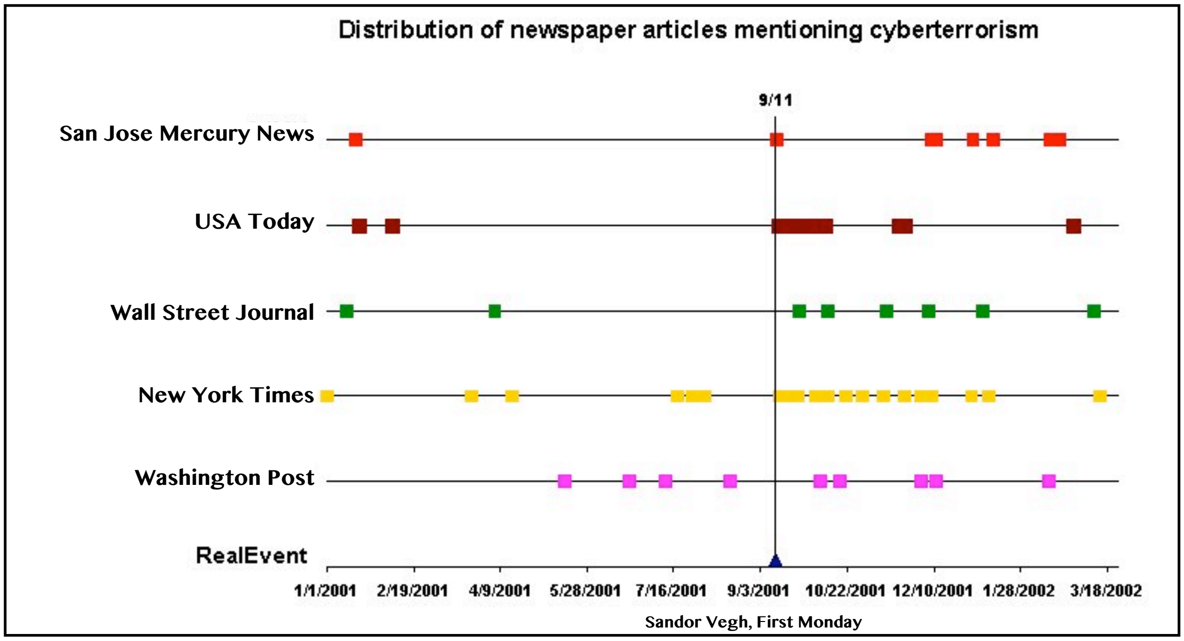


The ECM cluster is one that does not meet the narrow definition of cyberterrorism. However, because the cluster serves a supporting role to the Disruptive and Destructive clusters, it *is* cyberterrorism by the broad definition.

History

Public interest in cyberterrorism began in the 1980s, when the term was coined. The topic was not subjected to serious research until the late 1990s as fear of the coming **Y2K** problem spread. As the public was drawn in to the fear of computer failure, so were experts. Although Y2K was not at all a terrorist plot, it drew attention to cybersecurity and by extension cyberterrorism as a whole.[10]

Interest reached a maximum immediately after the September 11 attacks of 2001, a series of four coordinated terrorist attacks initiated by al-Qaeda against the United States during which terrorists hijacked civilian jetliners to fly into buildings, including the World Trade Center in New York City and the Pentagon in Arlington, Virginia. The threat of many different variants of terrorism — from chemical to biological to cyber — was thrust into the world spotlight and stuck.[11]

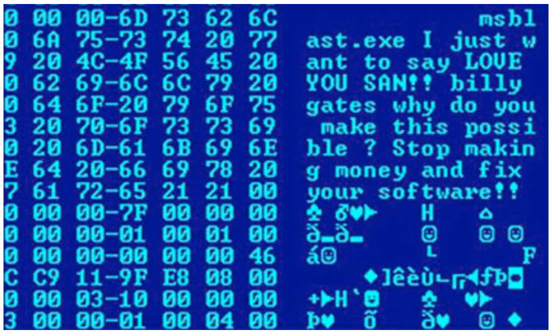


Types of Cyberattacks

Cyberterrorist groups have tried many different strategies for exerting influence across cyberspace, from various types of **malware**, including **viruses** and **worms**, to **denial of service attacks**.

A *computer virus* is a malware program which is attached to another program or file. When the program or file is executed, the virus spreads without the consent of the user, copying itself onto yet more files.[12] Viruses are most often used in cyberattacks to cause damage to systems run by computers.

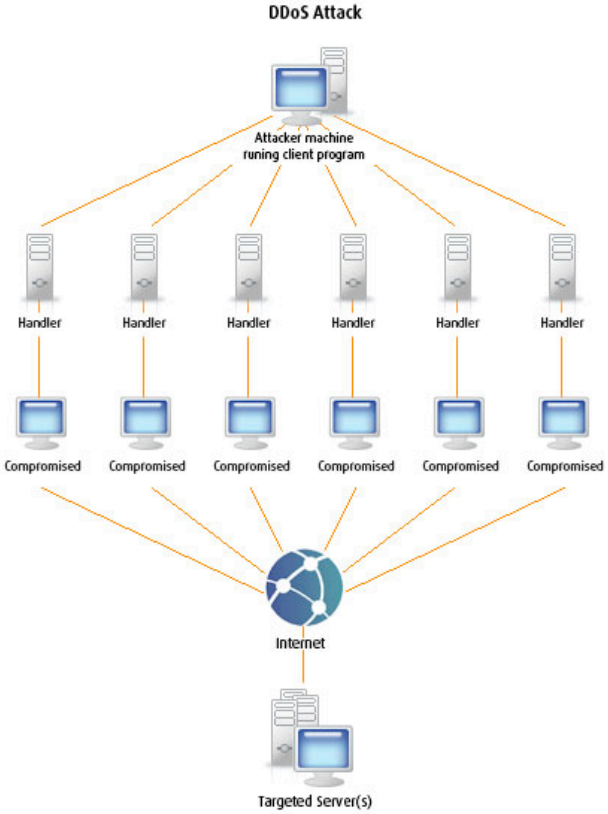
A *computer worm* is like a virus in that it replicates itself in order to spread. However, a worm does not need to attach itself to another program or file.[12] Unlike a virus, which can only spread when its host file is executed, a worm can spread without any additional input from the user.



```
0 00 00-6D 73 62 6C             msbl
0 6A 75-73 74 20 77  ast.exe I just w
9 20 4C-4F 56 45 20  ant to say LOVE
0 62 69-6C 6C 79 20  YOU SAN!! billy
0 64 6F-20 79 6F 75  gates why do you
3 20 70-6F 73 73 69   make this possi
0 20 6D-61 6B 69 6E  ble ? Stop makin
E 64 20-66 69 78 20  g money and fix
7 61 72-65 21 21 00  your software!!
0 00 00-7F 00 00 00  ♠ ỡ♥▶    H    △
0 00 00-01 00 01 00  ỡ_ỡ_     ☺    ☺ ☺
0 00 00-00 00 00 46  á☺       └      F
C C9 11-9F E8 08 00      ♦]êèù└╓◀ƒÞ■
0 00 03-10 00 00 00  +▶H`☻    ♠   ♥▶
3 00 00-01 00 04 00  Þ♥  õ    ỡ♥   ☺ ♦
```

August 2003 Blaster Worm code

A *denial of service* (DoS) attack is designed to render a computer network useless by flooding it with a large volume of traffic.[13] This is done using one or more computers to constantly request information from the target. The requests can take the form of reloading a webpage or sending thousands of emails in a short timespan. The volume of requests leave the system unable to perform its intended task. The computers used in the attack are likely personal computers infected by a virus, worm, or other type of malware.[13] When more than one computer is used, the attack is termed 'distributed denial of service' (DDoS).



Case Studies

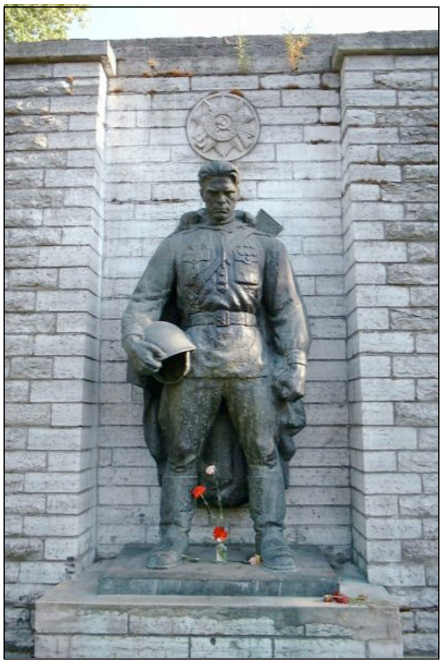
September 11 Attacks

As previously mentioned, public interest in cyberterrorism reached a new peak after 9/11.[11] Many began to wonder if the scale of the attacks could be replicated using communications technology. The 9/11 Commission Report revealed that several of the attack's conspirators used the Internet in preparation of the attacks.[14] It was used by some of the terrorists involved to find flight schools where they would learn to fly the commercial jetliners they anticipated hijacking. Some also purchased plane tickets online, and two terrorists communicated the final details of the attacks in code on an online chat room a few weeks beforehand.[14]

> "The emergence of the World Wide Web has given terrorists a much easier means of acquiring information and exercising command and control over their operations."
> - The 9/11 Commission Report

2007 Estonian Cyberattacks

Estonia, a country of 1.3 million on the Baltic Sea, was subject to a series of massive cyberattacks in April of 2007. The distributed denial of service attacks were targeted towards the websites of Estonian government as well as banks, universities, and newspapers.[15] The cyberattacks served as a protest against the relocation of a Soviet war memorial by the Estonian government, which was also being protested in the streets by many of Estonia's ethnic Russians. In a country where an estimated 60% of people relied on the Internet for 'crucial' services each day, the attack effectively brought the country to its knees.[16] Although the Russian government was accused at first, the instigators of the attack were found to be young Russians with no known ties to the Russian government.[16] Though this is the real-world event which most closely meets the narrow definition of cyberterrorism, it may still be best defined as 'hacktivism in the extreme' because the attackers were not members of a known terrorist group.



The Bronze Soldier of Tallinn, the memorial in question

2010 Stuxnet Worm

Stuxnet is a computer worm that was first discovered in June 2010. Its target was the software used to control centrifuges involved in the processing of **uranium** in Iran, and by extension, the centrifuges themselves.[17] Stuxnet was spread mostly via infected USB memory sticks. When first introduced to a new computer, it scanned for the targeted software. If it was found, the worm then issued unusual commands to the centrifuges, eventually damaging them; otherwise, the worm lay dormant. The cyberattack was responsible for damaging roughly one-fifth of Iran's centrifuges.[17] The attackers were revealed to be Israel and the United States, motivated by the fear of Iran developing nuclear weapons made with uranium processed in these centrifuges.[17] Given that the parties involved were states, this is not an example of cyberterrorism — it is closer to cyberwar.

Is the Threat Exaggerated?

Practically ever since experts have been warning the public of the coming cyberterrorist armageddon, other experts have been arguing that the threat is totally overstated. They point out that by the narrow definition of cyberterrorism, virtually no incidents have been recorded. Peter W. Singer found in November of 2012 over 31,000 magazine and journal articles about cyberterrorism, but not a single death or injury attributable to a cyberterrorist attack.[18]

By the broad definition, cyberterrorism, while not widespread, is present; though this means only that terrorists have been known to use the Internet when planning or executing attacks, it is not to be ignored. However, the most notable confrontations in cyberspace are between states or are instigated by state-sponsored groups.

Gabriel Weimann explains the popularity of cyberterrorism in the media and as a method for terrorists:

> Psychological, political, and economic forces have combined to promote the fear of cyberterrorism. From a psychological perspective, two of the greatest fears of modern time are combined in the term "cyberterrorism." The fear of random, violent victimization blends well with the distrust and outright fear of computer technology…
>
> But although the fear of cyberterrorism may be manipulated and exaggerated, we can neither deny nor ignore it. Paradoxically, success in the "war on terror" is likely to make terrorists turn increasingly to unconventional weapons, such as cyberterrorism. And as a new, more computer-savvy generation of terrorists comes of age, the danger seems set to increase.[19]

UN Actions

The United Nations has discussed the issue of cyberterrorism in the past, but mainly in the context of a method of terrorism as a whole. The foundational document of UN counterterrorism policy is Security Council Resolution 1373 (passed 28 September 2001),[20] adopted in the wake of the September 11 attacks. It laid out the United Nation's policy on terrorism and provided several binding directives on how to combat terrorism across the globe. It also established the **Counter-Terrorism Committee (CTC)** to which states were called upon to report the steps they had taken to implement the resolution.[20] Resolution 1377 (12 November 2001)[21] repeated the importance of Resolution 1373 and expanded the role of the Counter-Terrorism Committee, inviting it to "explore ways in which States can be assisted" in accordance with S/RES/1373.

In 2005, the then UN Secretary-General Kofi Annan laid out a five-pillar strategy for countering terrorism. His points were "first, to dissuade disaffected groups from choosing terrorism as a tactic to achieve their goals; second, to deny terrorists the means to carry out their attacks; third, to deter states from supporting terrorists; fourth, to develop state capacity to prevent terrorism; and fifth, to defend human rights in the struggle against terrorism."[22] A year later, the General Assembly adopted Resolution 60/288 (2006),[23] formally announcing the United Nations Global Counter-Terrorism Strategy. Section II, paragraph 12 of this document established the Working Group on Countering the Use of the Internet for Terrorist Purposes.

The Security Council hears a briefing from its subsidiary Counter-Terrorism Committee, May 2010

This working group is the only UN body dedicated exclusively to cyberterrorism issues and is under the umbrella of the **UN Counter-Terrorism Implementation Task Force (CTITF)**.[24] In 2010 the Working Group concentrated on the legal and technical issues surrounding terrorist use of the Internet; in 2011, it "started focusing its activities on using the Internet to counter the appeal of terrorism, specifically by analyzing the role of counter-narratives and effective messengers who can deliver these narratives."[25]

A CITIF workshop on the implementation of the United Nations Global Counter-Terrorism Strategy

Prevention

Cybersecurity measures have increased worldwide after the entrance of cyberattacks to the international stage. The most obvious way to defend against cyberterrorism is by increasing cyberdefenses. For example, worms and viruses can be protected against by installing regular security updates and patches to limit vulnerabilities in software.[26] Additional antivirus software can be installed on machines for extra security. Regular backups of data can help recover information lost if a virus or worm erases it. DDoS attacks can be defended against with security systems such as **firewalls**, which can selectively limit traffic coming in from certain sources.[27] However, there is a limit to how much firewalls can do when the resources of a terrorist group are used against them.

The United Nations has taken the position that cyberterrorism is best treated as traditional terrorism excepting its nontraditional realm of attack. Thus, traditional methods for countering cyberterrorism, such as Kofi Annan's five pillars (dissuade, deny, deter, develop, and defend), quoted on the preceding page, still apply. Yet there is still room for improvement in how to best adapt these methods to counter cyberterrorism; it is the role of delegates to find this improvements.

International cooperation regarding cyberterrorism is difficult to pull together as states become increasingly defensive in cyberspace. States often do not share intelligence regarding cyberterrorism and are already developing military-affiliated groups to maintain control in cyberspace.[28] Organizations such as the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence[29] are steps in the right direction, combining the resources of several states to better counter cyberterrorism and other cyber threats.

Conclusion

Cyberterrorism remains a threat to nations everywhere. At the conference, delegates must share ideas, methods, best practices, and tested solutions on how to best address the issue of cyberterrorism. None of the many facets of cyberterrorism may be neglected, but delegations must take care to work within the constraints of national sovereignty. Knowledge of past actions by one's own country, the United Nations, and cyberterrorist themselves will be vital in forming a solution.

Questions to Consider

1. Why is it important to address the issue of cyberterrorism?
2. What is a definition for cyberterrorism that can be agreed upon by the member states? (Your country's definitions of terrorism and cyberterrorism would be beneficial to include in your position paper.)
3. How does cyberterrorism differ from cybercrime, cyberwar, and hacktivism — or does it? How should these issues be dealt with on an international level?
4. If a terrorist group uses the Internet to illegally obtain funds, is this cyberterrorism? What if the group is using the Internet legally to plan or manage an illegal action?
5. What are the forms a cyberterroist attack is most likely to take, and how can these attacks be countered? What preventive measures can be taking to prevent and counter instances of cyberterrorism on both the national and international level?
6. How can member states prevent and counter cyberattacks on the following infrastructures?
    a. Critical computer systems; including civilian, corporate, and military networks
    b. Vital public works such as electric grids, power plants, waterworks, air traffic control, dams, etc.
    c. Financial records and databases
7. How can former Secretary-General Kofi Annan's five-pillar approach for countering terrorism and the subsequent UN Global Counter-Terrorism Strategy be adapted and improved to address cyberterrorism?
8. How can current UN bodies, such as the Counter-Terrorism Committee (CTC), the Counter-Terrorism Implementation Task Force (CTITF), and the Working Group on Countering the Use of the Internet for Terrorist Purposes, be fully leveraged?
9. What are the roles of non-governmental organizations (NGOs) in the context of cyberterrorism? How can the resources and abilities of NGOs be maximized to counter cyberterrorist threats?
10. Should member states be obligated to actively search for signs of future terrorist incidents? What means may states use to search their own citizens?
11. How can member states best work together and collaborate with each other on countering cyberterrorism?

Terms and Concepts (in order of appearance)

United Nations: an international organization that promotes international law, security, economic development, social progress, human rights, civil rights, civil liberties, political freedoms, democracy, and world peace

UN Charter: the foundational treaty of the United Nations

Security: the state of being free from danger or threat

Non-binding resolution: written agreement unable to develop into a law; used to make recommendations or to convey approval or disapproval

Terrorism: the politically motivated use violence or the threat of violence designed to cause widespread disruption and fear in a society

Cyberterrorism: the politically motivated use of computers and information technology in an attack or threat of attack designed to cause widespread disruption and fear in a society

Non-state actor: an entity which has significant international political influence but does not 'belong' to any particular country

Cybercrime: crime committed by individuals or organizations using cyber tools

Cyberwar: warfare conducted in the cyberspace domain between nation-states

Hacktivism: use of the digital world by activists to voice dissent or support for a cause

Y2K: the year 2000; experts feared worldwide computer turmoil because computers abbreviated the year to two digits, making the year 2000 indistinguishable from 1900: it turned out to be much less of a problem than anticipated, having little overall effect

Malware: short for 'malicious software;' includes viruses and worms

Virus: a malware program that installs itself without the user's consent, then attempts to replicate and install itself on other devices by attaching itself to another program or file

Worm: a malware program similar to a virus but distinguished by its capability to spread without needing to attach itself to another program or file

[D]DoS: [distributed] denial of service attack — one [or more, if it is a 'distributed' DoS] computers is/are used to request so much information from the target computer that the target is unable to fulfill requests from legitimate users

Uranium: an element that can be used to power nuclear plants but also to make nuclear weapons

CTC: the UN Security Council Counter-Terrorism Committee, established by S/RES/1373, which oversees UN Security Council agenda items on terrorism

CTITF: The UN Counter-Terrorism Implementation Task Force, a body formed by GA Resolution 60/288 (2006) to coordinate UN efforts on terrorism

Firewall: a software or hardware computer element designed to block incoming traffic from selected sources while still catering to requests from authorized users and allowing outward communication

Further Reading

Each of the following documents in both *Further Reading* and *References* are valuable in the perspective they give in the prevention and countering of cyberterrorism; they serve as excellent resources for beginning research. *Further Reading* sources are simply recommended sources not cited in the main text of the background guide; cited sources are just as useful. All web sources in both *Further Reading* and in *References* were accessed August 2014.

Ahmad Kamal, "The Law of Cyber-Space: An Invitation to the Table of Negotiations," *United Nations Institute of Training and Research*, 2005. un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf

Alex P. Schmid, *The Routledge Handbook of Terrorism Research* (New York: Routledge, 2011). books.google.com/books?id=MLY5MwXhtDsC

Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton University Press, 2011). press.princeton.edu/titles/9012.html

United Nations Counter-Terrorism Implementation Task Force, *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes,* February 2009. un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf

United Nations General Assembly, *Uniting against terrorism: recommendations for a global counter-terrorism strategy,* 27 April 2006. undocs.org/A/60/825

United Nations Office on Drugs and Crime, "The use of the Internet for terrorist purposes," *United Nations Counter-Terrorism Implementation Task Force*, 2012. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

United Nations Security Council, "Counter-Terrorism Committee," *Counter-Terrorism Committee Executive Directorate*, 2013. un.org/en/sc/ctc/

References

1. United Nations, *Charter of the United Nations*, 24 October 1945. un.org/en/documents/charter/

2. "Internet Live Stats," *Real Time Statistics Project*, 2014. internetlivestats.com/internet-users/

3. Angus Martin, "The Right of Self-Defence Under International Law: The Response to the Terrorist Attacks of 11 September," *Current Issues Brief* 8 (2002). http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/CIB/cib0102/02CIB08#international

4. Dorothy E. Denning, "Cyberterrorism: The Logic Bomb versus the Truck Bomb," *Global Dialogue* 2, no. 4 (2000). worlddialogue.org/content.php?id=111

5. Sarah Gordon and Richard Ford, "Cyberterrorism?" *Symantec Security Response*, 2003. symantec.com/avcenter/reference/cyberterrorism.pdf

6. "Cyberterrorism," *National Council of State Legislatures*. www.ncsl.org/programs/lis/cip/cyberterrorism.htm

7. Dorothy E. Denning, "A View of Cyberterrorism Five Years Later," *Naval Postgraduate School Center on Terrorism and Irregular Warfare* (2006). calhoun.nps.edu/bitstream/handle/10945/37160/Cyberterror_2006.pdf

8. Jonalan Brickey, "Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace," *CTC Sentinel* 5, no. 8 (2012). ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace

9. William L. Tafoya, "Cyber Terror," *FBI Law Enforcement Bulletin* (November 2011). fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

10. John D. Hwang, "Help for cyberterrorism: Y2K's silver lining?" *IT Professional* 1, no. 1 (1999). doi.org/10.1109/6294.774797

11. Sandor Vegh, "The media's portrayal of hacking, hackers, and hacktivism before and after September 11," *First Monday* 10, no. 2 (2005). firstmonday.org/ojs/index.php/fm/article/view/1206/1126

12. "What Is the Difference: Viruses, Worms, Trojans, and Bots?" *Cisco Systems*, 2014. cisco.com/web/about/security/intelligence/virus-worm-diffs.html

13. "What is a DDoS Attack?" *Arbor Networks*, 2014. digitalattackmap.com/understanding-ddos/

14. 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: U.S. Government Printing Office, 2004), 157-164. 9-11commission.gov/report/911Report.pdf

15. Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9, no. 1 (2008). europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html

16. Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review* 18, no. 2 (2009). iar-gwu.org/node/65

17. Michael B. Kelley, “The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought,” *Business Insider* (New York), 20 November 2013. businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

18. Peter W. Singer, “The Cyber Terror Bogeyman,” *Armed Forces Journal* (Springfield, VA), 1 November 2012. armedforcesjournal.com/the-cyber-terror-bogeyman/

19. Gabriel Weimann, “Cyberterrorism: How Real Is the Threat?” *United States Institute of Peace Special Report* 119 (2004). permanent.access.gpo.gov/lps51621/sr119.pdf

20. United Nations Security Council, *Resolution 1373,* 28 September 2001. undocs.org/s/res/1373(2001)

21. United Nations Security Council, *Resolution 1377,* 12 November 2001. undocs.org/s/res/1377(2001)

22. Kofi Annan, “A Global Strategy for Fighting Terrorism,” (Speech to the Closing Plenary of the International Summit on Democracy, Terrorism and Security, Madrid, 10 March 2005). http://www.un.org/News/Press/docs/2005/sgsm9757.doc.htm

23. United Nations General Assembly, *Resolution 60/288*, 20 September 2006. undocs.org/a/res/60/288

24. United Nations, “Counter-Terrorism Implementation Task Force,” *Department of Political Affairs of the United Nations*, 2014. http://www.un.org/en/terrorism/ctitf/index.shtml

25. United Nations, “Working Group on Countering the Use of the Internet for Terrorist Purposes,” *United Nations Counter-Terrorism Implementation Task Force*, 2014. http://www.un.org/en/terrorism/ctitf/wg_counteringinternet.shtml

26. Michael Kassner, “How antivirus software works: Is it worth it?” *TechRepublic,* January 2010. techrepublic.com/blog/it-security/how-antivirus-software-works-is-it-worth-it/

27. “Defeating DDoS Attacks,” *Cisco Systems,* 2004. cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.pdf

28. Nick Hopkins, “Militarisation of cyberspace: how the global power struggle moved online,” *The Guardian* (London), 16 April 2012. theguardian.com/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle

29. “NATO Cooperative Cyber Defence Centre of Excellence,” *North Atlantic Treaty Organization,* 2014. https://www.ccdcoe.org/about-us.html

Produced by Seth Colbert-Pollack for the United Nations Association of Minnesota