Study Guide

Committee: Disarmament and International Security Council (DISEC)

Topic: The Question of Cyber Terrorism

Introduction:

Cyber terrorism is the use of internet based terror attacks, done deliberately in order to create disturbances or havoc in the usual workings of the internet. Attacks through cyber terrorism can be found in various forms of illegal activities whose number is on a constant increase.

There are various ways to gain access to information in cyberspace: attackers can exploit vulnerabilities in software and hardware, or by tricking people into opening infected emails or websites. Upon doing so, attackers can infect the host's computer with malicious software. They can also take advantage of people who fail to follow basic cyber security practices - such as changing their passwords frequently or updating their antivirus protection on a regular basis. Once these hackers have access to a computer, they can steal or distort the information stored on it, corrupt its operations and program it to attack other computers. In many cases, victims suffer a theft of their identity and/or their personal assets

As the number of connected devices increase, the likelihood of a singularly more destructive cyber incident becomes increasingly possible. This is why countermeasures must be made to minimise the dangers of cyber terrorism.

Definition of Key Terms:

Antivirus - Software which attempts to identify and delete or isolate malware.

Black Hat - A hacker who works to harm others .

Blacklist - A list of computers, IP addresses, usernames or other identifiers to block from access to a computing resource.

Civilian Participation - The involvement of non-military persons in welfare. they are able to remotely participate in direct attacks against opponents.

Communications Privacy Law - Laws which regulate access to electronic computer communications.

Computer Network Attack - Actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.

COTS Software - Commercial Off The Shelf Software. These are software that is prepackaged and sold as a commodity rather than custom written for a specific user/organisation or purpose.

Crimeware - Software tools designed to aid criminals in perpetrating online crime. It refers onto to programs not generally considered desirable or usable for ordinary tasks.

Cybercrime - In the broadest definition, cybercrime includes all crime perpetrated with or involving a computer. It is a crime that is committed using a computer or network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. the crime may take place on the computer alone or in addition to other locations.

Cyber Terrorism - A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Cyber Warfare - Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.

Data Mining - The process of extracting hidden information and correlations from one or more databases or collections of data that would not normally be revealed by a simple database query.

Hacker - Advanced computer users who spend a lot of time on or with computers and work hard to find vulnerabilities in IT systems.

Internet Service Providers - A company that offers access to the internet. Internet service providers may also provide add-on services such as web hosting, electronic mail, virus scanning, SPAM filtering, etc.

PII - Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Malware - Software which is designed to infiltrate a user's computer specifically for malicious purposes.

White Hat - A computer hacker who works to find and fix computer security risks. White hat consultants are often hired to attempt to break into their client's network to see if all security holes have been addressed.

Contextual Information:

In today's society, Cyber Terrorism is becoming an increasing threat towards all aspects of life. This includes governments, firms, and individuals on a worldwide scale. Cyber terrorirism is deemed as such a significant threat, that from 2013-2015, the *US Director of National Intelligence* named Cyber as the number one strategic threat to the United States, placing it *ahead* of terrorism, for the first time since the 9/11 attacks. The availability and ubuiquity of mobile devices and social media, is one of the most significant causes for this, in addition to the world's increasing reliance upon technology to store data and carry out essential services. Due to the abundance of technology in MEDC countries - such as the US, UK, China, Japan and Canada, it is likely that they will be particularly affected by the increasing use of Cyber methods for terrorist organisations to achieve their goals.

Shockingly, a recent UN survey, carried out in July 2017, revealed that only about half of all countries have a cyber security strategy, or are in the process of developing one. These countries are, in order: Singapore, United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France and Canada. With Russia ranked 11th.

In recent years, **the UK** has concentrated its efforts towards improving its cyber security - anticipating a cyber attack by the radical Islamic-State group. This was achieved, firstly, through the introduction of the *National Cyber Security Strategy,* from 2011-2016 - a government funded strategy of £860m ($603m), carried out by the *National Cyber Security Programme* - a separate, state-run organisation. However, this approach failed to achieve the necessary scale of change required. Therefore, the UK government's new 2017-2021 strategy, will work under three main objectives: 1. TO DEFEND against evolving cyber threats, to respond effectively to incidents, and to educate the UK popualtion with the knowledge, and ability to defend themselves. 2. TO DETER & DISRUPT hostile action taken against the UK, whilst pursuing and prosecuting offenders. 3. TO DEVELOP and innovative the cyber security industry, utilising world-leading scientific research to meet, and overcome future threats and challenges.

In **the US**, the recently-appointed Trump Administration is planning to write a new cyber security strategy, in replacement to the one developed by the Obama Administration. White House representatives have argued that the policy documents developed under Obama, including the *2011 International Strategy for Cyberspace* and the *2016 Cybersecurity National Action Plan*, have become outdated, and fail to consider the threat of recent technological developments, and the more advanced

methods of cyber warfare. Like the UK, the Trump Administration plan to base the new 2017 cyber strategy around 3 main components: 1. IMPROVING the security of federal government computer networks. 2. LEVERAGING government resources to better secure critical infrastructure, such as hospitals, banks, airports and financial firms. 3. ESTABLISHING norms of good behavior in cyberspace and punishing bad behavior. In 2017, the Administration invested over $19 billion for cybersecurity, as part of the President's 2017 Fiscal Year Budget.

Australia is increasingly a target for cybercrime and espionage, and has dedicated huge amounts of resources to develop its new cyber security strategy. Australia's strategy is more complex than those of the UK and the US. It consists of 5 objectives, each of which thr strategy hopes to achieve before 2020. Each objective also has priority actions:



A NATIONAL CYBER PARTNERSHIP

Governments, businesses and the research community together advance Australia's cyber security

Priority actions

Co-leadership: The Government and business leaders take the lead on co-designed, national cyber security initiatives, including through the Prime Minister holding annual cyber security meetings with business leaders.

Build stronger partnerships: The Government clearly identifies lead responsibilities and relocates the Australian Cyber Security Centre to engage with business more effectively.

Understand costs to the economy: The Government sponsors research to better understand the cost of malicious cyber activities to the economy.



STRONG CYBER DEFENCES

Australia's networks and systems are hard to compromise and resilient to cyber attacks.

Priority actions

Detect, deter and respond: Open jointly operated cyber threat sharing centres and an online cyber threat sharing portal. Tackle cyber threats with improved intelligence, analytic and response capability.

Raise the bar: Co-design voluntary cyber security governance 'health checks', national good practice guidelines, conduct joint exercising and develop and leverage advanced technology to make Australia a harder target against cyber threats. Conduct cyber security assessments of Government agencies.



GLOBAL RESPONSIBILITY AND INFLUENCE

Australia actively promotes an open, free and secure cyberspace.

Priority actions

Champion an open, free and secure internet: Advocate to retain an open, free and secure internet, in the Indo-Pacific region and globally.

Shut down safe havens: Partner internationally to shut down safe havens and prevent cybercrime and other malicious cyber activity.

Build capacity: Help build capacity in our region and globally against malicious cyber activities.



GROWTH AND INNOVATION

Australian businesses grow and prosper through cyber security innovation

Priority actions

Enable cyber security innovation: Drive investment in cyber security innovation through the Cyber Security Growth Centre and innovation network to strengthen cyber defences, grow our economy and create jobs.

Enable cyber security businesses to develop and expand: Support new businesses and promote the export of Australian cyber security products and services.

Enable cyber security research and development: Ensure our cyber security R&D is responsive to the challenges.



A CYBER SMART NATION

Australians have the cyber security skills and knowledge to thrive in the digital age.

Priority actions

Develop the right skills and expertise:
Address cyber security skills shortages to develop a highly-skilled cyber security workforce, starting with academic centres of cyber security excellence and increasing diversity.

Raise national cyber security awareness:
Lift all Australians' awareness of cyber risks and benefits through sustained joint public-private national awareness raising initiatives.

The annual cost of online identity theft in **Canada** has been estimated at nearly $1.9 billion. Consequently, at the beginning of 2017, the Canadian Government instigated a similar cyber security strategy to that of US and UK, consisting of 3 main aims: 1. SECURING Government systems. Canadians trust the Government with their personal and corporate information, and to deliver services to them. They also trust that the Government will act to defend Canada's cyber sovereignty, protecting and advancing Canada's national security and economic interests. 2. PARTNERING, to secure other cyber systems outside Canada's federal Government. Canada's economic prosperity security depends on the smooth functioning of systems outside the Government. In cooperation with territorial governments, and the private sector, the Government will take steps to strengthen Canada's cyber resiliency, and that of its critical infrastructure sectors. 3. HELPING Canadians to be secure online. The Government will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime

In October 2015, **France** also introduced a new strategy to combat cyber security. Similar to Australia, the strategy consists of 5 main objectives: 1. DEFENCE & SECURITY of State information systems and infrastructures. By developing autonomous strategic thinking, supported by world-class research, France will ensure the ongoing defence of its fundamental interests in cyberspace. France will also continue to reinforce the resilience and security of its networks, in case of a major cyberattack. 2. DIGITAL TRUST & PRIVACY. Increased public protection will be based on heightened vigilance regarding the use of personal data. 3. RAISING AWARENESS. Steps will be taken to raise the awareness of schoolchildren and students, in tackling online attacks and potential dangers. The French government will also train an increased number of Cyberspace experts. 4. A DIGITAL ENVIRONMENT will be created, which is favourable towards French companies in the digital sector, who provide technological products and services. 5. EUROPEAN CYBERSPACE STABILITY. The regulation of international relations in cyberspace has become a major issue. France will promote a road map for European digital strategic autonomy, and fortify its nuence in international bodies - providing support to the least-protected countries to build their cybersecurity capabilities.

Major Countries and Organizations Involved:

North Atlantic Treaty Organisation (NATO) - Their main focus in cyber defence is to protect its own networks and enhance resilience across the Alliance

G7 - The G7 (or G-7 or Group of Seven) is a group consisting of Canada, France, Germany, Italy, Japan, the United Kingdom and the United States. It was reformatted from the G8 in 2014, due to

Russia's suspension from the group. The G8 was established in 1997, and was an inter-governmental political forum, with the participation of the major industrialized countries in the world, that viewed themselves as democracies. The G7 serves the same purpose.

G20 - The G20 (or G-20 or Group of Twenty) is an international forum for the governments and central bank governors from Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, the Russian Federation, Saudi Arabia, South Africa, South Korea, Turkey, the United Kingdom, the United States, and the European Union. Founded in 1999, the G20 aims to discuss policy pertaining to the promotion of international financial stability. It seeks to address issues that go beyond the responsibilities of any one organization.

OECD - The Organisation for Economic Co-operation and Development is an intergovernmental economic organisation with 35 member countries, founded in 1961 to stimulate economic progress and world trade.

APEC - Asia-Pacific Economic Cooperation (APEC) is a forum for 21 Pacific Rim member economies that promotes free trade throughout the Asia-Pacific region.

OAS - The Organisation armée secrète or OAS (meaning Secret Army Organisation) was a short-lived right-wing French paramilitary organisation during the Algerian War (1954–62). The OAS carried out terrorist attacks, including bombings and assassinations, in an attempt to prevent Algeria's independence from French colonial rule.

CTITF - The Counter-Terrorism Implementation Task Force (CTITF) was established by the Secretary-General in 2005 and endorsed by the General Assembly through the United Nations Global Counter-Terrorism Strategy, which was adopted by consensus in 2006. The mandate of the CTITF is to strengthen coordination and coherence of counter-terrorism efforts of the United Nations system.

IMPACT - IMPACT is a NGO founded in the late 1980s by Sir John Wilson. It was instigated with a means of empowering local communities and finding simple, low-cost ways of preventing disabilities.

Timeline of Events:

Date:	**Event:**
1982	CIA found a way to disrupt the operation of a Siberian gas pipeline of Russia without using traditional explosive devices such as missiles or bombs. They caused Siberian gas pipeline to explode using a portion of a

code in the computer system that controls its operation in what they tagged as ‘logic bomb’. The resulting fire could be seen from space.

2003 General Assembly adopted A/RES/57/239 without voting as it was noted that the need for the international community to address and reassess their government to prepare for the new globalized world bridged through cyberspace.

2004 A series of coordinated ‘cyber raids’ was discovered in what the FBI believed to originate from government-supported cells in China. The raids were dubbed as ‘Titan Raid,’ and the hackers were able to infiltrate several computer networks including those at NASA and the Lockheed Martin, Redstone Arsenal, and Sandia National Laboratories. The acts posed dangers of not only making off with military intelligence and classified data, but also paved the way for other hackers and espionage entities to infiltrate these systems as they leave backdoors.

2005 The government of Estonia was subjected to cyber terrorism by the Nashi, a pro-Kremlin group from Transnistria. They used ping floods and botnets to penetrate and take down key government websites rendering them useless.p

2006 In the Global Counter-Terrorism Strategy adopted by the General Assembly, Members States pledge to “coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet”.

2006 The Secretary of the US Air Force announced the creation of the Air Force’s newest MAJCOM, the Air Force Cyber Command, which would be tasked with monitoring and defending American interests in

cyberspace.

2009 A series of coordinated attacks against major government, financial websites and news agencies of both the United States and South Korea involving the activation of botnet. Servers were overloaded by a DDoS attack and the number of hijacked computers included 50,000 from the Symantec's Security Technology Response Group, 20,000 from the National Intelligence Service of South Korea, and more than 166,000 from Vietnamese computer security researchers.

2011 Foreign hackers with IP addresses from China infiltrated three departments within the Canadian government and transmitted classified information back to themselves.

2011 A data breach in Epsilon, one of the world's largest provider of marketing and handling services to industry giants such as JP Morgan Chase, Best Buy, and many other major financial services, retailers and other major companies. The estimated damage cost ranged from $224 million to $4 billion.

2011 Israel announced the formation of its cyber security body, "National Internet Defence Task Force", making it responsible for developing tools to secure vital Israeli online infrastructure. The main responsibility of the task force will be to expand the state's ability to defend vital infrastructure networks against cybernetic terrorist attacks

2012 A modular computer malware called Flame, also known as Skywiper, was used to attack computer systems in Middle Eastern countries that run Microsoft Windows onas their operating system. It infected over 1000 machines from private institutions, educational institutions, and

government organisations.

Relevant UN Treaties and Events:

- Partnered with the International Multilateral Partnership Against Cyber Threats (2011)

Possible Solutions:

A potential issue that may face governments and NGOs working to fight against cyber terrorism and cyber attacks, is the issue of personal privacy (or PII). The question posed is how will governments ensure that the integrity and privacy of its citizens remains intact, in the persuit of neutralising a cyber threat? How will goverments establish a boundary between the prevention of cyber terrorism, yet still ensuring that citizen PII remains largely untouched. It will be useful to consider the importance which each member state places upon its citizens' privacy and anonymity. For example, a state with a long history of cyber restriction and surveillance - such as China or the DRNK - will likely be less concerned with upholding the interests of its citiziens in cyberspace. This will undoubtably cause contention between member states - as members such as France and Canada place a lot of emphasis upon citizen security within their cyber strategies.

Another issue that may result in digagreement between members is the issue of international cyber responsibility - should member governments still be responsible for their citizen's cybersecurity and anonymity when they're in another country? For example, should a Canadian citizen still be protected by the Canadian government and terms of the Canadian cyber strategy, if they're visiting the USA (and vice versa)? If this isn't the case, foreign citizens will subject to the cyber surveillance of the host state. This could increase international transparency and trust, however, it could also result in member-member tensions.

Bibliography:

INTRODUCTION TO CYBER TERRORISM

https://en.m.wikipedia.org/wiki/Cyberterroris

http://www.itpro.co.uk/security/29726/what-is-cyber-terroris

https://www.nato.int/docu/review/2013/Cyber/Cyber-attack-hurt/EN/index.ht

GLOSSARY OF CYBER TERMINOLOGY - Simple, and Complex Versions

https://motherboard.vice.com/en_us/article/mg79v4/hacking-glossar

https://niccs.us-cert.gov/glossar

UN STRATEGY REPORT

http://www.un.org/apps/news/story.asp?NewsID=57119#.Wm4uuHqnyh

UK STRATEGY

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

US STRATEGY

http://www.defenseone.com/technology/2017/10/trump-administration-plans-new-cybersecurity-strategy/142042

AUSTRALIAN STRATEGY

https://cybersecuritystrategy.pmc.gov.au/executive-summary/index.html

CANADIAN STRATEGY

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pd

FRENCH STRATEGY

http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

APEC

https://en.m.wikipedia.org/wiki/Asia-Pacific_Economic_Cooperation

G20

https://en.m.wikipedia.org/wiki/G20

G7

https://en.m.wikipedia.org/wiki/Group_of_Seven

CTITF

https://www.un.org/counterterrorism/ctitf/en/about-task-force

IMPACT

http://www.impact.org.uk/#&panel1-

OAS

https://en.m.wikipedia.org/wiki/Organisation_armée_secrèt

TIMELINE OF CYBER ATTACKS (NOT NECESSARY TERROR-RELATED) - really useful

https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.ht

https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Timeline.pd

ISSUES WITH PRIVACY & CYBER TERRORISM

http://www.bbc.com/future/story/20170808-tracking-terrorists-online-might-invade-your-privac