DEFINING AND MITIGATING CYBER TERRORISM AND CYBER WARFARE

CHAIR	VICE-CHAIR	MODERATORS
ANANTHAKRISHNAN N	BRINDA GRAMA	DHRUV AANAND, LAKSHYA A

Table of Contents

Address from Chair

Dear delegate,

We, the Executive Board, cordially welcome you to our first ever R-NPSMUN. Congratulations on being allotted in the United Nations General Assembly – Disarmament and International Security Committee (UNGA-DISEC). The UNGA-DISEC, also known as the First Committee, is a vital part of the United Nations. It was created after the second world war, when weapons of all sorts ravaged the world. Disarmament is seen as one of the most necessary steps to peace, and we urge you to keep this basic tenet in mind throughout your time in committee.

This simulation of the First Committee will focus on the keen analysis of critical affairs facing the world at large; keeping that in mind, our target is to come out with politically correct arguments so as to reach short- and long-term solutions to the predicaments presented. While representing a country on an international platform, researching your foreign policy in as much detail as possible is as crucial as exploring and associating with the agenda. The contents of the background guide are known to the entire committee and the Executive Board; therefore, we recommend strongly that you increase your radius of research. Nothing is off limits, and you will be surprised how information you would believe irrelevant will suddenly come in handy during the discussion. There is no such thing as too much research!

We have seen good, bad and ugly forms of policy-making all around the world; we hope to see the best form of it here. A favourable mix of creativity and logic is all you need to formulate policies; the only reason research is not included in that list is because it is a prerequisite to your presence in the committee itself. We are simply here to steer you towards creating a better world, but the actual process is in your hands. Strive to benefit as much of the world as possible, and bear no biases towards or against anyone; you will definitely come out on top.

The agenda that we will be discussing at the UNGA-DISEC, R-NPSMUN 18 is **Defining and Mitigating Cyber-terrorism and Cyber Warfare**. Once again, it would indeed be an honour to receive each and every one of you; we hope your time here is not only fulfilling and educational, but also enjoyable and rewarding. If you need any assistance from us, please do not hesitate to contact us.

Warmest regards,
DISEC Executive Board

Introduction to the Committee

The Disarmament and International Security Committee was established in 1993. It is the First Committee of the United Nations General Assembly. DISEC deals with issues regarding the promotion, establishment, and subsequent maintenance of global peace while simultaneously working to prevent weapons proliferation. Under Article 11 of Chapter IV of the UN Charter, "The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armament."

DISEC is one of the larger committees of the United Nations and has been pivotal in the discourse of problem solving in multidimensional topics. In hopes of achieving this, DISEC formulates further ideas and actions for other UN committees.

Introduction to the Agenda

Cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

Cyber warfare is defined as politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare.

The authors define cyber war as an extension of policy by actions taken in cyberspace by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security.

Delegates have to come up with a viable definition in order to define the topic the agenda mentions, and also come up with feasible ways to mitigate cyber terrorism and cyber warfare using examples from the past.

History related to the Agenda

Cyber terrorism and cyber warfare originated during World War II itself, when a Logic Bomb was used on the Siberian Gas Pipeline. What began there is, today, seen most often in the form of WannaCry, Stuxnet, NotPetya, BadRabbit, etc. A brief narration of some prominent events follows.

Logic Bomb

The CIA allegedly found a way to disrupt the operation of a Siberian gas pipeline to Russia without using traditional explosive devices such as missiles or bombs. Instead, they caused the 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." It is extremely difficult to come to an absolute understanding of what actually caused the Siberian pipeline explosion. There have been numerous claims suggesting that the CIA were involved in the explosion. However, much like any other government classified cases the public have been shadowed. Then again there have been a widespread of rumours targeting the CIA, even considering them to be the developer of the AIDS virus intending it to be a biological weapon. Inevitably, the real cause of the Siberian gas pipeline explosion may never be revealed to the public, only the government agencies involved or the technical engineers involved will ever know.

Moonlight Maze

In September 1999 Newsweek broke the story that the United States was under a sustained cyber attack. They claimed that thousands of sensitive but unclassified documents relating to technologies with military applications had been stolen. Further reports at the time pointed the finger at the Russian government as a possible source of the attack, but details were limited. The investigation widened as the attackers compromised important research institutions such as the Army, Los Alamos and Sandia national laboratories. The victims covered the United States, United Kingdom, Canada, Brazil and Germany.

In a summary of the case during the investigation, the author of a document records one "non-US person" had been identified, as had one "piece of malicious code". The documents don't go into detail of what these are. Moonlight Maze marked the beginning of a new era of constant cyber-espionage. They were quickly followed by the Titan Rain attacks — allegedly this time of Chinese, not Russian, origins.

Titan Rain

Chinese hackers, some believed to be from the People's Liberation Army, have been attacking the computer networks of British government departments according to The Guardian. The attackers hit the network at the Foreign Office as well as those in other key departments. The disclosures came after reports that the Chinese military had hacked into a Pentagon military computer network in

June. The Financial Times said American officials called it the most successful cyber attack on the US defence department.

Defence department officials confirmed that there had been a "detected penetration" of elements of the email system used by the network serving the office of Robert Gates, the US defence secretary. US officials were reported to have said that an investigation had discovered that the People's Liberation Army (PLA) was responsible. The US gave the codename "Titan Rain" to the growing number of Chinese attacks, notably directed at the Pentagon but also hitting other US government departments. The latest attack caused some minor administrative disruptions, but there had been no adverse impact on operations, an official said. The attack has caused quite some friction between the US and Chinese governments.

Estonian Cyberwar

On 27 April 2007, Estonia was also hit by major cyber-attacks which in some cases lasted weeks. Online services of Estonian banks, media outlets and government bodies were taken down by unprecedented levels of internet traffic. Massive waves of spam were sent by botnets and huge amounts of automated online requests swamped servers. The result for Estonians citizens was that cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news.

The country's leading IT experts are also trained by the Ministry of Defence. But in addition they are security vetted and remain anonymous. But there is no concrete evidence that these attacks were actually carried out by the Russian government. On condition of anonymity, an Estonian government official told the BBC that evidence suggested the attack "was orchestrated by the Kremlin, and malicious gangs then seized the opportunity to join in and do their own bit to attack Estonia". Hostile states often count on copycat hackers, criminal groups and freelance political actors jumping on the bandwagon.

The attacks have stuck in the national consciousness by proving to Estonians the importance of cyber security.

Flame

Research into Flame was carried out in conjunction with the UN's International Telecommunication Union. They had been investigating another malware threat, known as Wiper, which was reportedly deleting data on machines in western Asia. In the past, targeted malware - such as Stuxnet - has targeted nuclear infrastructure in Iran. Others like Duqu have sought to infiltrate networks in order to steal data. This new threat appears not to cause physical damage, but to collect huge amounts of sensitive information, said Kaspersky's chief malware expert Vitaly Kamluk. "Once a system is infected, Flame begins a complex set of operations, including sniffing the network traffic, taking screenshots, recording audio conversations, intercepting the keyboard, and so on," he said.

More than 600 specific targets were hit, Mr Kamluk said, ranging from individuals, businesses, academic institutions and government systems. Iran's National Computer Emergency Response Team posted a security alert stating that it believed Flame was responsible for "recent incidents of mass data loss" in the country. The malware code itself is 20MB in size - making it some 20 times larger than the Stuxnet virus. The researchers said it could take several years to analyse.

Among the countries affected by the attack are Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt. "The geography of the targets and also the complexity of the threat leaves no doubt about it being a nation-state that sponsored the research that went into it," Mr Kamluk said. The malware is capable of recording audio via a microphone, before compressing it and sending it back to the attacker. It is also able to take screenshots of on-screen activity, automatically detecting when "interesting" programs - such as email or instant messaging - were open.

WannaCry, NotPetya, BadRabbit

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue, an exploit in older Windows systems released by The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems. The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country. In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack.

On June 27, 2017, a digital attack campaign struck banks, airports and power companies in Ukraine, Russia and parts of Europe. Security experts who analyzed the attack determined its behavior was consistent with a form of ransomware called Petya. They also observed the campaign was using a familiar exploit to spread to vulnerable machines. Threat intelligence provider Symantec Security Response confirms that Petya ransomware is responsible for the digital attacks. In a tweet, it reveals the threat is using EternalBlue. Kaspersky Lab tweets out a statement clarifying that the ransomworm is not a variant of Petya but is actually a new ransomware they named “NotPetya.” They also reveal the threat has affected approximately 2,000 organizations at the time of their posting. “The superficial resemblance to Petya is only skin deep. Although there is significant code sharing, the real Petya was a criminal enterprise for making money. This is definitely not designed

to make money. This is designed to spread fast and cause damage, with a plausibly deniable cover of 'ransomware.'"

Reports appeared in October 2017 that a new ransomware outbreak was hitting organisations in Russia and Ukraine. Victims included the Russian newswire Interfax, Ukraine's Odessa airport, and the Kiev subway system. Media outlets like Fontanka.ru found their website's disrupted by the attack, and urged readers to follow them on social media for updates while systems were restored. The ransomware, which was dubbed "BadRabbit", showed a number of similarities to the hard-hitting NotPetya attack which successfully attacked organisations in Russia, Ukraine and elsewhere earlier in the year. Researchers at Group-IB, however, identified that BadRabbit had been distributed in a different fashion – using a number of compromised news websites as a means of infecting computers. Visitors to the compromised sites found themselves greeted by a pop-up urging them to install a Adobe Flash update onto their Windows PCs. Of course, the downloaded file did not originate from Adobe, and was a disguise for the ransomware. The use of phoney security updates to infect innocent users' computers with malware is nothing new, of course. Once again this is evidence that an attack does not have to be highly sophisticated to succeed. In addition, the ransomware contains an SMB component that allows the attack to spread laterally through an organisation, exploiting poorly-chosen passwords to find other computers to infect. Once a PC was infected, BadRabbit could begin to do its main dirty work – encrypting files, and displaying a ransom message on the victim's screen. Precisely who is responsible for the NotPetya and BadRabbit ransomware attacks isn't yet known. But we be making a big mistake to underestimate their determination. As researchers at Kaspersky explained, it was clear that the attackers had been busy for months, setting up their network of hacked sites in preparation for the BadRabbit assault. The good news is that BadRabbit has not hit companies as hard as its predecessors like WannaCry and NotPetya.

As recent global cyber security attacks have illustrated, the failure to secure the alleged NSA cyber exploits and trojans lead to outbreaks like Wannacry, NotPetya, and the BadRabbit attacks. The responsibility for these malware attacks, according to the consensus view of the IT security community, falls on North Korean for WannaCry and Russian actors for NotPetya and BadRabbit. These are examples of mass, self-replicating and indiscriminate cyber weapon usage. Had these attacks inflicted physical damage on infrastructure resulting in a loss of life as opposed to just financial damages, the consequences could have been significant. Urgent work is required by international organizations such as the International Committee of the Red Cross, NATO, and the UN to ensure the development and use of a destructive cyber weapon is done in accordance with the same legal and security rigor applied to nuclear, biological, and chemical weapons.

Tallinn Manual

The Tallinn Manual 2.0 is the most comprehensive analysis of how existing international law applies to cyberspace. Authored by nineteen international law experts, the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", the updated and considerably expanded

second edition of the 2013 "Tallinn Manual on the International Law Applicable to Cyber Warfare", is an influential resource for legal advisers dealing with cyber issues. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence.

"This is a practical handbook for state legal advisers. The Tallinn Manual 2.0 examines what the rules for state behavior in the new domain of cyberspace are. The analysis includes both the perspective of a state that wishes to engage in cyber operations as well as that of a state that has become the victim of hostile cyber operations," says Tallinn Manual 2.0 director professor Michael Schmitt of the US Naval War College. "The 19 expert authors of the Manual identified a number of situations in which states' cyber operations might violate international law. It is not legal, for instance, for a state to hack into cyber infrastructure in another state and cause it to permanently seize operating," explains Tallinn Manual 2.0 managing editor Liis Vihul from the NATO Cooperative Cyber Defence Centre of Excellence, a knowledge hub, research centre and training facility in Tallinn. "By contrast, because international law is silent on the issue of espionage, we concluded that cyber espionage, as a general matter, does not violate international law. However, how espionage is carried out might be unlawful," Vihul elaborates. "Fundamentally, the Tallinn Manual 2.0 analysis looks into the future. So long as there is no codified international law for cyberspace, the Manual helps to clarify the application of existing law to events in the digital arena as outlines some grey areas," emphasizes Lauri Mälksoo, international law professor from the University of Tartu and member of the Estonian Academy of Sciences. "The Tallinn Manual, the most important international law initiative from 21st century Estonia, is well-known in the international legal community. I would not underestimate the importance of the handbook having been developed in and named after the capital of Estonia," Professor Mälksoo adds.

Definition of Key Terms

1. CYBERSECURITY - Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks.It refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

2. CYBER CRIME - Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage.

Malware, hacking, ransomware, virus, spyware, hijackware, backdoor, worms, Trojan horse, phishing, spoofing, pharming, phreaking, rogue security software, adware, hoax are types of cyber-crimes.

a) **Hacking -** Hacking generally refers to unauthorized intrusion into a computer or a network. It includes the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's objectives.
b) **Internet Fraud** - Encompasses a wide range of online criminal activities that deliver harm to the targets. Online frauds can include:

- Account takeover
- Click fraud
- Health scams
- Identity fraud
- Money muling
- Government agency scams
- Jobs and investment scams
- Threats and extortion scams

3. CYBER TERRORISM - Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

4. CYBER WARFARE - Cyber warfare may be defined as any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system. It includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid.

Legal Frameworks

The 1899 and 1907 Hague Conventions created the primary body of work (with significant contributions and foundational work from the Oxford 1880 "Manual of Laws and Customs of War") known as the Law of War. From this genesis, we have the first Principle of the Law of War, the Principle of Distinction.

The Principle of Distinction is the governing principle when it comes to the legal targeting and use of weapons, including cyber weapons. Under international humanitarian, law it is required that

belligerents distinguish between combatants and civilians. Implicit in this principle is the extension – which could be contentious – of the principle to infrastructure in the combat zone.

A Principle of Proportionality in the use of force is also applicable to the legal targeting and use of weapon systems, including cyber weapons. The legal targeting and use of weapons must consider the damage to civilians and their property. The damage cannot be excessive in relation to the military advantage gained. This principle requires the combatant to consider the ramifications of weapon release in terms of the potential damage to civilian (and civilian infrastructure) vs combatant (and military infrastructure).

The Principle of Military Necessity is another consideration when assessing the legality of targeting and use of weapon systems. This principle prohibits wounding or permanently injuring an opponent except during the fight. It also prohibits torture to exact confessions and other activities simply used to inflict additional damage on the enemy that does not further the military objective. Although perhaps it is far-fetched to consider cyber weapons in the above context, The Principle of Military Necessity is augmented by The Liber Code. The Liber Code further defines prohibited activity under this Principle as "in general, … any act of hostility that make the return to peace unnecessarily difficult."

Finally, governing the targeting and use of weapons including cyber weapons is the Principle of Unnecessary Suffering. Article 35.2 of the Additional Protocol I declares it is prohibited to employ weapons, projectiles and materials ,and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."

Thus, when reviewing these four principles of The Law of War, a weapon or cyber weapon released by a belligerent party which is indiscriminate, disproportionate (more damage to civilian than combatant lives and infrastructure), makes a return to peace more difficult, and inflicts unnecessary suffering is in contravention of the Law of War.

Many efforts have already been made on creating substantive and enduring documents to promote the partnership and cooperation among states upon the matter of ensuring cybersecurity for all. Regional organizations as well as international ones have drafted and signed documents, but due to a plethora of circumstantial challenges (e.g. the technological divide), their implementation is far from achievable.

Briefly, the main goals (that also reflect the implementation challenges) that the resolution endeavor tries to achieve are the following ones:
i. Reduction of frictions among national legislations
ii. The introduction of new investigative powers
iii.The facilitation of international cooperation

States are plagued by constant security dilemmas that used to refer to military insecurity, but have since developed to include from information safeguarding to environmental security issues. Despite their cooperation in many fields, states may perceive another nation's action as a threat direct or indirect to their position.

Here are some cyber weapon technical control requirements that during time of conflict and post-conflict should be aligned to The Principles:

- Exploits used in a cyber-attack need to be disclosed after the cessation of hostilities to aid in clean up
- Diligent record keeping of any targeted and infected combatant and civilian assets must be maintained
- Positive Identification of Target (PID) is required for cyber weapon destructive payloads to be activated
- Additional non-cyber intelligence and legal authority must support and confirm the activation of a destructive payload is in accordance with The Principles
- Destructive payloads cannot be activated indiscriminately
- The Trojan rootkits should be designed to uninstall themselves after a pre-determined amount of time
- Self-replication technologies (worms) are only deployed when there is an extremely low probability of moving into non-targeted infrastructure
- The targeted infrastructure is primarily military in nature
- Use of exploit, worms, and trojan rootkits on Industrial Control Systems and SCADA is done with the utmost targeting rigor

Cyber weapons are extremely difficult to discern; until a destructive payload is activated, they are generally deployed in an espionage capacity which is not in contravention to The Principles and according to The Tallinn Manual from Rule 30: Sections 2-3 do not constitute an attack.

The notion of an 'attack' is a concept that serves as the basis for a number of specific limitations and prohibitions in the law of armed conflict. For instance, civilians and civilian objects may not be 'attacked' (Rule 32). This rule sets forth a definition that draws on that found in Article 49(1) of Additional Protocol 1: 'attacks means acts of violence against the adversary, whether in [offense or defense].

By this widely accepted definition, it is the use of violence against a target that distinguishes attacks from other military operations. Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks.

The Tallinn Manual (detailed above) tells us how existing international law applies to cyberspace. The Cooperative Cyber Defence Wing of Excellence, a wing of the NATO, led a team of 19 international law experts to writing and constantly updating the Tallinn Manual.

Current Overview

The Internet has fundamentally altered the world we live in and interact and transformed the global economy. For all the vast opportunities the Internet provides, it exposes potential vulnerabilities that can be exploited by adversaries.

Cyber terrorism has become one of the most significant threats to the national and international security of the modern state, and cyberattacks are occurring with increased frequency.

Also cyber terrorism has become and is becoming more and more prominent on social media today.

The objectives of such terrorists may be political or ideological since this can be considered a form of terror. Cyber terrorism will continue to threaten national and international security. It is clear that the international community may only ignore cyber terrorism at its peril. There is more than enough reason to believe and fear that cyber terrorism could potentially cause another great depression.

Relevant Conferences

1. **International Conference on Cyber Warfare and Security (held annually since 2005)**

   Over the years, ICCWS has developed into an important conference in the cyber-security field, attracting academics, military professionals and practitioners from around the world to present their research findings in the form of empirical studies, case histories and other theoretical and practical contributions. The conference presents the viewpoint that protection against cyber threats requires a holistic approach that should cover technology, business and human aspects of the problem domain. Impact assessment, which highly involves the harmonization of technological findings with the business requirements, is a critical analysis task that commonly exists in risk, incident, event, or vulnerability management activities. Some solutions proposed include Support for Secure Code Execution in Server Operating Systems, Developing Low-Cost and Effective ICS Cyber Training Environments, Integrating Cyberspace Power into Military Power in Joint Operations Context, Effectively Exercising Deterrence in the Cyber Domain, and Cyber Resilience: An Essential new Paradigm for Ensuring National Survival.

2. **The United Nations and Cyber Warfare (September, 2016 | New York City)**

   The UN General Assembly gathered in New York City for its 71st meeting. The meeting coincided with news of 500 million compromised Yahoo user accounts, a reminder that all is not well in the world. Several countries comprise the Security Council, but of particular interest are the five permanent members: China, France, the Russian Federation, the United Kingdom, and the United States. Although France and the United Kingdom are formidable powers, the United States, China, and Russia are the most active in cyber warfare and cyber espionage. As it turns out, the UN has no set definition of what constitutes cyber warfare—even most experts outside the UN can't agree. Indeed, there are no cyber Geneva Conventions to govern cyber warfare. As of 2012, at least 11 nations have offensive cyber warfare capabilities, while at least 33 more have defensive capabilities. Among the nations

with offensive capabilities, the United States, China, and Russia have publicly announced the existence of cyber warfare units within their militaries.

3. **The International Conference on the Criminalization of Cyber Terrorism (May 15 - 16, 2017 | Abu Dhabi, United Arab Emirates)**

   This conference aims at finding common ground for the implementation of a system of international laws and legislations that addresses the roots and extensions of the terrorist phenomenon in the digital space. One of the main objectives of the conference is to launch innovative ideas in order to further international cooperation and develop a deeper understanding of the new challenges confronting legislators, government entities and international organizations facing the increasing exploitation of cyberspace by terrorist groups.

4. **European Conference on Cyber Warfare and Security (ECCWS) (28 – 29 June 2018 | Oslo, Norway)**
5. **International Cyber Security & Intelligence Conference (November 14 – 15, 2018 | Toronto, Canada)**

   The ICSIC Canada is proud to host the 2018 International Cyber Security and Intelligence Conference on November 14 – 15, 2018 in Toronto Canada. ICSIC provides a rare opportunity for global experts in Cyber security, Intelligence, Counter-Terrorism, National Infrastructure, Industry, Cyber Operations research, Law enforcement, and Legal Practitioners to proffer unified ideas and best practices on cyber safety, attacks prevention and secured cyber world. ICSIC, is a unique cyber security and intelligence conference that features high profile speakers from cyber security, privacy, intelligence, national critical infrastructure and counter-terrorism.

6. **Security & Counter Terror Expo (5th-6th March 2019 | Olympia, London)**

   As risk from lone-wolf attacks and sophisticated ransom ware increases, security professionals are faced with a growing challenge to evolve and stay one step ahead by investing in new technologies and intelligence solutions that will protect critical assets and people from today's threats. Aligned with the Home Office's CONTEST counterterrorism strategy and the Department for International Trade's export strategy, Security & Counter Terror Expo 2018 (SCTX) will address the most pertinent issues security professionals face from around the world, providing them with access to the expertise, technologies and solutions required to prevent, pursue, protect and prepare for potential attacks.

Questions to be Addressed

1. What does ‘cyber-terrorism’ involve? What is ‘cyber warfare’?
2. How might the rapid development of IT and our increasing dependence cause potential damage and malicious acts (in the case of cyber terrorism)?
3. How can DISEC mitigate the effects and repercussions of cyber-terrorism and cyber warfare?
4. How can there be unifying cyber laws? Is this a prime solution?
5. How does a law enforcement body identify and prosecute individuals or organizations that perpetrate acts of ‘cyber-terrorism’?
6. What should be the international measures to help smaller or developing countries defend themselves against the acts of ‘cyber-terrorism’?
7. Should the international community be engaged in protecting the computer networks of private companies against cyber attacks? How so?
8. How can the DISEC ensure that the international fight against cyber-terrorism does not infringe on the rights of citizens?
9. What are the methods of *preventing* cyber warfare?

Bibliography

https://static1.squarespace.com/static/533e6b7de4b0d84a3bd7c4be/t/54b3f123e4b03957d1606d08/1421078819908/DISEC.pdf

http://renaissance-mun.weebly.com/uploads/1/8/8/6/18860224/renaissance_research_report_-_ga1_cyber_warfare.pdf

https://www.lths.net/site/handlers/filedownload.ashx?moduleinstanceid=37444&dataid=35688&FileName=Background%20Guide%20DISEC.pdf

https://ccdcoe.org/tallinn-manual-20-cyber-espionage-generally-not-unlawful.html

https://www.tripwire.com/state-of-security/featured/badrabbit-runs-steam-prepared-next-ransomware-attack/

https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/

https://www.tripwire.com/state-of-security/featured/cyber-law-war/

https://www.tandfonline.com/doi/abs/10.1080/20531702.2017.1331411?journalCode=rjuf20

https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4