**Introduction**

On the 27th of April 2007, Estonia experienced the first of a series of cyber attacks which would go on to shape laws, policies, and attitudes within and outside its borders. The country was bombarded by thousands of independent actors, resulting in the complete loss of most internet services for three weeks. The Estonian parliament, banks and media were all targeted in the midst of political disagreements with Russia. Although not the first incident of cyber terrorism, this was definitely one of the most destructive, managing to make an entire country go offline. In response, the world’s first ever regulations concerning actions in cyberspace were drafted, hoping to prevent such incidents from occurring in the future.

However, incidents of cyber terrorism and espionage continued and remain a major threat to international security. Not only can they create mistrust and paranoia between nations, but also paralyse the organizations and resources core to their economic, social and political stability. This is especially true when such acts are initiated by countries and their related bodies, placing the world’s most sophisticated technology in the wrong hands. As members of the United Nations, it is the responsibility of countries to use their resources, voices and cooperation to strengthen international cyber security and work towards a world where state-sponsored cyber terrorism and espionage are void. Organizations such as the Kaspersky Lab and the Cooperative Cyber Defence Center of Excellence have made strides toward combating the issue, although they are restricted by an acute lack of relevant treaties and laws.

The year is 2019 and most of the world is now well aware of the implications of cyber terrorism and espionage but little has been done to address this critical issue. Malicious technologies continue to develop at an exponential pace, becoming increasingly complex and destructive by the day. These can be used to gain a competitive advantage or to inhibit a country’s ability to fight back in political situations. In order to catch up to and quell this development, nations will need to develop and implement astute solutions which ensure international peace and security in the decades to come.
Definition of Key Terms

State-sponsored

A state-sponsored action is one which is directly or indirectly carried out by a government body. Direct state-sponsored incidents involve the use of government technology, military forces, and networks. Indirect state-sponsored incidents involve ideological or financial support of Non-State Actors (NSAs) which are not directly tied to any particular government entity. For example, a country using its own troops to initiate an attack on another would be direct, while the financing of a rebel group engaged in warfare would be indirect.

Cyber terrorism

NATO’s Cooperative Cyber Defence Center of Excellence (CCDCOE) defines cyber terrorism as “premeditated, politically motivated attacks by sub-national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against noncombatant targets.” In this context, ‘violence’ can extend itself to include non-physical forms of harm such as exposing sensitive information, threatening individual safety and economic degradation. Specific incidents of cyber terrorism are referred to as ‘cyber attacks’.

Espionage

Espionage is the act of obtaining confidential information, usually military or political resources, without the permission and/or knowledge of the holder of such information. The act of carrying out espionage is commonly referred to as “spying” with those involved being “spies”.

Advanced Persistent Threat

An Advanced Persistent Threat (APT) is a form of cyber attack in which the perpetrators gain access to and remain in a computer system for extended periods of time. Due to their sophisticated nature, APTs are often state-sponsored as only the most advanced governments and NSAs would have access to such technology.

Malware

Malware is a software specifically designed to disrupt, damage or gain unauthorized access to a computer system. Advanced forms of malware, known as ‘computer worms’, are able to replicate themselves in order to spread to other targets. This is a very common tactic used in APTs so that the source of malware can be destroyed while its traces remain on other devices. Another class of malware,
known as a ‘wiper’, aims to wipe (completely eradicate) the computer it infects, erasing all important information.

**Distributed Denial-of-Service**

A Distributed Denial-of-Service (DDoS) attack is a form of cyber attack in which a targeted server or network is disrupted by overwhelming it with internet traffic. For example, a website may stop working after being flooded by hundreds of thousands of visits. DDoS attacks generally use a ‘botnet’ - a network of interconnected devices each serving as a ‘bot’. For example, the perpetrator of a DDoS attack may compromise thousands of computers and use them to direct traffic toward a specific target. Each computer would be a bot intertwined into a larger botnet.

**Hacktivism**

Hacktivism is the use of technology to promote a political and/or social agenda. Although this is generally carried out by NSAs working alone, there have been incidents of state-sponsored cyber attacks motivated by political/social change. Individuals involved in such attacks are known as ‘hacktivists’.

**Background Information**

**Corporate cyber attacks**

In modern history, several cyber attacks have targeted specific firms in order to gain a competitive advantage or obtain sensitive information.

**Operation Aurora**

The first major incident of this kind was dubbed ‘Operation Aurora’ and consisted of a series of cyber attacks from June to December of 2009. The attacks are considered an Advanced Persistent Threat (APT) and targeted several US firms including Google, Yahoo, Adobe and Dow Chemical. Cyber espionage group Elderwood is said to be responsible for the attacks and has been linked to the People’s Liberation Army (PLA) - China’s armed forces - specifically Unit 61398. One of the tactics used was to embed malware on company websites frequently visited by employees which would download itself onto their computers. Once downloaded, the malware would have access to devices and documents within the employee’s network, such as business emails, trademarked designs and company plans. As a result of the attacks, Google ceased their operations in mainland China and instead redirected all their servers to Hong Kong, which is subject to more lenient censorship laws. This not only led to a major decline in
Google China’s market share but, more importantly, negatively affected US-China relations in cyberspace.

**Operation Socialist**

Operation Socialist, which also began in 2009, differed greatly from this incident in that it was directly state-sponsored and targeted a corporation with immediate ties to a government. The operation was carried out by the UK’s Government Communications Headquarters (GCHQ) in collaboration with the rest of the “Five Eyes” - Australia, Canada, New Zealand and the United States. The alliance hoped to develop technologies capable of scanning and infiltrating global networks in order to spy on individuals and obtain their mobile data. Specifically, they intended to monitor select European surveillance targets and monitor communications between Europe and the rest of the world. GCHQ decided to target Belgacom, Belgium’s government telecommunications network, due to its connections across several continents and weaknesses discovered through initial reconnaissance. Belgacom’s extensive reach can be seen in a map created by GCHQ (right) when planning for the operation.

GCHQ’s plan was to penetrate Belgacom’s security mechanisms through key employees such as system administrators and engineers who had access to confidential data. Once identified, the engineers were redirected to a website that looked like LinkedIn, through which their computers were infected with malware at an accelerated rate (similar attacks are referred to as ‘Quantum Insert’ attacks). GCHQ considered the attacks a success and even managed to intercept other telecommunication networks related to Belgacom by the end of 2011. The attacks were only discovered due to a malfunction in Belgacom’s email servers in 2012, which it investigated with assistance from Dutch cybersecurity company Fox-IT. The firm described the identified malware as the most sophisticated APT it had ever seen, and continued to investigate and restore compromised assets (private computers, computer systems, routers, etc.) until late 2013. The UK has publicly denied its involvement in the incident, which continues to be investigated by Belgian military intelligence, and remains infamous for being the first occurrence of an EU member state conducting a cyber attack on another. Operation Socialist is also infamous for the lack of retribution administered to those involved despite substantial evidence provided. Although Belgium attempted to prosecute the UK through Europol, the agency claimed that it only deals with criminal matters with perpetrators outside of the European Union. It is estimated that Belgium spent
over $55 million improving its cybersecurity systems following the incident, which remains its only line of
defence until legislation is created to address this crucial issue.

**Shamoon**

Despite Operation Aurora and Operation Socialist’s undeniable harm to firms and individuals alike, both of these were operations concerning espionage more so than cyber terrorism. However, there have also been cases of cyber attacks targeting corporations which, due to their highly destructive nature, are considered to be acts of cyber terrorism or even cyber warfare. One such incident concerns Shamoon, an infamous piece of malware, which targeted state-owned Saudi Arabian petroleum and natural gas company Aramco in 2012. The attackers gained access to the company’s networks through a malicious link emailed to an Aramco employee, masquerading as legitimate. The attack itself took place on the 15th of August, taking advantage of the fact that most employees were on holiday celebrating Ramadan. Shamoon, being classified as a wiper, completely erased data from and permanently disabled over 30,000 computer systems, forcing Aramco to go offline in fear of the worm spreading further across the internet.

Although Aramco claimed that the company swiftly recovered from the incident, business was severely affected for over five months due to contracts, communications, reports and other corporate documents having to be done by hand, through fax or using typewriters. The company managed to replace the targeted assets, purchasing so many hard drives (over 50,000) that the prices of computers increased worldwide until January of the following year. The economic toll on the company was further widened by their need to invest in enhanced computer networks and an extended cybersecurity team in order to go back online. Responsibility for the incident has been claimed by the “Cutting Sword of Justice”, who were motivated by Aramco’s support of the authoritarian Al Saud regime. In later investigations into the incident, the United States allegedly discovered connections between Shamoon and the Iranian government.

**Cyber warfare**

Although all cases of cyber warfare are harmful in their own right, particular incidents have sparked important questions regarding cybersecurity or had crucial historical or political significance.

**2007 cyber attacks on Estonia**

The first of these took place in 2007, emerging from Estonia’s decision to relocate a WWII memorial known as the ‘Bronze Soldier of Tallinn’ together with the graves of several WWII soldiers. The soldier had cultural value to Russia, who was vocal about its disapproval of the relocation. This set off a series of cyber attacks on Estonia, beginning on the 27th of April and lasting three weeks. The attacks
were largely comprised of Distributed Denial-of-Service (DDoS) attacks on government websites, banks and news portals, rendering them completely inaccessible. There were also repeated attempts to edit the Bronze Soldier of Tallin’s wikipedia page, highlighting the motivation behind the incident. The attacks were important in emphasizing the ways in which political disputes can bleed into cyberspace and raised questions as to the accountability of countries in regards to their citizens’ actions. In response to the incident, NATO established the Cooperative Cyber Defence Center of Excellence (CCDCOE) in May of 2008, which aims to ensure the cybersecurity of its member states through expert education, training, research and policies regarding cyber terrorism and espionage. The CCDCOE has been operating out of Tallinn ever since.

**Cyber attacks during the Russo-Georgian conflict**

Another notable incident of cyber warfare involving Russia took place during the nation’s war against Georgia in August of 2008. Even before the war began, on the 20th of July, the Georgian president’s official government website was disabled through a DDoS attack. On the 5th of August, Russian news portals OSInform and OSRadio were hacked and had their websites’ content replaced with that of Alania TV, a Georgian television service. That same day, the Baku–Tbilisi–Ceyhan (BTC) pipeline exploded through a cyber attack on its control systems which caused the line to build up with pressure. Investigators suspect Russia might have been to blame due to their strategic interests in the war. As seen in the image below, the BTC traverses Turkey, Georgia and Azerbaijan while completely circumventing Russian territory. This threatens Russia’s control over the region and gives power to Georgia.

On the 9th of August, large portions of Georgia’s internet traffic was hijacked and redirected to servers in Russia and Turkey, allegedly controlled by Russian hackers.

On the 10th, Russian news agency RIA Novosti’s website was disabled. On the 11th, Georgia’s government websites faced a series of severe and targeted cyber attacks. Websites belonging to the Georgian president, the National Bank of Georgia and the Georgian Parliament had their contents replaced with images comparing the Georgian president to Adolf Hitler among other 20th-century dictators. Azerbaijani news agency Day.Az also had its servers targeted due to them reporting the war in favor of Georgia. As a result, the Georgian president's website was moved to US servers and Estonia offered to host other targeted websites which were temporarily operating on the Google-owned website Blogger. Georgia continued to suffer from continuous DDoS attacks, originating largely from pro-Russian
websites such as StopGeorgia, which offered the software and instructions necessary to conduct such an attack. Any individual could simply download the software, select a targeted address and contribute to the cyber war with the click of a button. The conflict officially ended through a ceasefire on the 14th of August and remains the first incident of a cyber war coinciding with a traditional one.

**July 2009 cyber attacks**

In July of 2009, South Korea and the United States experienced a series of cyber attacks targeting important government, financial and news websites. The first set of attacks took place on the 4th of July (US independence day) and targeted key American websites such as Amazon, the White House and the New York Stock Exchange. The second set of attacks took place on the 7th and targeted South Korean government websites including the Ministry of Defence, the National Intelligence Service and the National Assembly. The final set of attacks began on the 9th and targeted both websites in South Korea, comprising of the National Intelligence Service together with a major bank and major news agency, and the United States Department website. Although the attacks were solely disruptive in nature and did not obtain or wipe any sensitive information, they presented a major economic cost in that individuals were prevented from conducting financial transactions, making online purchases or engaging in business. This incident is unique in that it involved several international victims who were targeted simultaneously. Furthermore, it highlights the ease with which the perpetrators of cyber warfare are able to mask their identities through the anonymity of cyberspace. Although the culprit of these attacks was never confirmed, North Korea is highly suspected as they conducted a missile test on the same day as the first set of attacks which also took place shortly after the passage of UN Security Council Resolution 1874, which imposed tighter economic sanctions on the state. As perpetrators of cyber terrorism and espionage continue to develop ways of remaining undetected, countries will need to decide what level of doubt is acceptable when persecuting the states involved.

**Operation olympic games**

The United States was also involved in another notable instance of cyber warfare known as ‘Operation Olympic Games’. This was a collaboration between the governments of Israel and the United States and sought to slow the development of nuclear weapons in Iran. The Operation consisted of a ‘beacon program’ which was introduced into a major uranium plant in Natanz through an infected USB stick. The program was used to gather information about the configuration of the plant's technologies, namely its computers, and pass it on to each country’s respective intelligence agencies. Using this information, a highly sophisticated computer worm was then created and reintroduced into the plant which was capable of reprogramming the centrifuges used to process uranium. Beginning in 2008, several centrifuges at the plant began to malfunction and even explode as the worm caused them to spin at speeds they were not designed to. This culminated in the attacks of 2010 where the worm managed to
Government Espionage

Unlike corporate espionage, government espionage explicitly targets a government and its related bodies and is often so sophisticated that it is carried out by governments themselves.

Titan Rain

The first significant case of government espionage was a series of cyber attacks beginning in 2003. The attacks were discovered and coined 'Titan Rain' in 2004 by an analyst in the US government who also labeled them an APT. He managed to trace the origins of the attacks to China, which has led many to believe that the perpetrators were linked to PLA Unit 61398 due to their access to sophisticated technology and involvement in other incidents of cyber espionage. The cyber attacks themselves consisted of the theft of classified military and government information through institutions such as NASA as well as military networks across the country. The attacks eventually died down after targeting other countries such as the United Kingdom. Although the specific pieces of information stolen may have not been of great importance, Titan Rain was infamous for conveying the ease at which government information could be compromised. Furthermore, it worsened relations between China and other powerful nations such as the US and the UK who feared that this was only the beginning of China’s delve into cyber terrorism and espionage.

GhostNet

Unfortunately, the fear surrounding Titan Rain was not unfounded as China continued to conduct cyber espionage operations, the next of which being GhostNet. GhostNet infected over 1,000 computers belonging to individuals, corporations and governments in over 103 countries, making it one of the most international incidences of cyber espionage. Starting in 2008, computers belonging to embassies and government officials were specifically targeted in order to obtain sensitive information. The malware used was also capable of surveillance through the hijacking of the compromised computers’ microphone and camera systems. Most of the details regarding the attacks were obtained by the Information Warfare Monitor (IWM) who also traced the attacks back to China, possibly being the work of the PLA. The IWM later investigated other cyber espionage incidents similar to GhostNet, namely, the Shadow Network.
Flame

Despite GhostNet’s significant spread and sophistication, it pales in comparison to another infamous piece of malware known as Flame. Flame is considered by some experts to be the most elaborate APT ever created, capable of executing dozens of unique functions and taking up 20 times as much storage space as Stuxnet. It is estimated that Flame was first released into cyberspace in 2010, although this cannot be confirmed as its creators manipulated its properties to make it appear as if it was created in the 90s. Notable for its reach, the malware spreads indiscriminately and has infected thousands of targets ranging from individuals to corporations and government entities. Among the extensive list of functions at its disposal, Flame is capable of recording audio, monitoring keyboard activity and taking screenshots, especially of private conversations between users. These sensitive pieces of information are then covertly sent back to those in control of the malware, allowing its presence within a computer system to easily go unrecognized.

![Map of Flame victims](image)

Flame’s initial victims were overwhelmingly based in the Middle East, as seen in the image above, although it has continued to spread and develop in its capabilities since its inception. The majority of the attacks in the region consisted of Flame’s aforementioned surveillance components, while many others involved a wiper component which destroyed large amounts of sensitive information. This sparked the attention of the UN’s International Telecommunication Union (ITU), who requested the help of cybersecurity experts in analyzing the malware, which led to its initial discovery. Flame continues to reside in cyberspace, taking on many forms, and highlights the heinous extent to which modern cyber espionage can obtain information as intimate as our private conversations.
Cyber attacks on the DNC

One of the most recent cases of cyber espionage were the 2016 cyber attacks on the United States Democratic National Committee (DNC). The attacks were intended to disrupt the US presidential election by revealing compromising information about candidate Hillary Clinton. This began with a malicious email sent to Clinton’s campaign chairman on the 19th of March, masquerading as an email from Google requesting he update his password. After consulting a member of staff, he was told, through a typographical error, “This is a legitimate email” rather than the intended “This is an illegitimate email.” Following this advice, the chairman provided his password, giving the hackers access to his account. The following month, they continued to send similar emails to other Clinton staffers, allowing them to steal confidential data and access 33 computers at the DNC. On the 22nd of July, amidst investigations by the CIA and the FBI, over 20,000 of the compromised emails were released on WikiLeaks - a hacktivist website aimed at bringing confidential information to the public eye.

By the end of the year, additional information such as phone numbers and private messages were released and the CIA and Department of Homeland Security concluded the attacks were state-sponsored by Russia in an attempt to improve Trump’s chances of winning the election. Russia completely denied these accusations which culminated in the US sanctioning Russia and asking 35 Russian diplomats in the country to leave. Later investigations, some of which are still ongoing, uncovered further evidence linking the attacks to the Russian government. Additionally, the investigations found that over 3,000 Facebook advertisements leading up to the election had connections to Russia and geographically targeted states which Trump won by a slight majority. On the 16th of February, 2018, 13 Russian nationals as well as three Russian entities were charged with conspiracy to defraud the United States by allegedly meddling in the elections, primarily through the aforementioned targeted advertisements. This incident is important in that it greatly shaped contemporary relations between Russia and the United States and conveys the ways in which cyber espionage can be used to manipulate political and social beliefs.

Major Countries and Organizations Involved

China

China plays an infamously major role in this issue due to them conducting several aforementioned cyber attacks. These include Operation Aurora, GhostNet and Titan Rain, which are all predominantly cases of cyber espionage. This is consistent with China’s foreign policy as the country houses strict censorship laws and is vocal about spying on its citizens, which it justifies as a means to detect covert criminal activity. Despite this, however, China has repeatedly denied their involvement in
international cyber espionage incidents and claims that this is restricted to within its borders. Historically, the incidents China is suspected to have been involved in specifically concern PLA Unit 61398, which many member states and cybersecurity firms suspect is behind the aforementioned cyber operations.

USA

The United States is involved in practically all aspects of this issue to some extent. Firstly, the country has fallen victim to several incidents of cyber terrorism and espionage including Operation Aurora, GhostNet, Titan Rain, and the July 2009 cyber attacks. The country’s financial, political and military influence have formerly been the major reasons for it to be targeted. Conversely, however, the United States has also been behind several notable cases of cyber terrorism and espionage such as Operation Socialist and Operation Olympic Games. This places it in a unique situation as the country is also known for its sophisticated cybersecurity and military intelligence networks which have even been used to incriminate it in relation to these aforementioned operations. For example, the United States National Security Agency (NSA) is notable for its former agent Edward Snowden who was exiled to Russia after releasing a plethora of sensitive government documents online. Several of these were related to cyber terrorism and espionage, such as extensive details concerning Operation Socialist and its link to the United States.

Russia

Russia is infamous for participating in cyber terrorism and espionage as a means to further its political agenda. This can be seen in the 2007 cyber attacks on Estonia, where Russia disagreed with the country’s decision to relocate a WWII memorial, and the August 2008 cyber attacks during the Russo-Georgian war. Although neither has been proven to be directly state-sponsored, this can be inferred in various ways. Firstly, in regards to Estonia, the argument can be made that Russia’s vocal disagreement with and lack of assistance toward Estonia comprised political support for the individuals conducting the attacks, making the events state-sponsored. Similarly, during the Russo-Georgian wars, Russia’s reluctance to disable websites actively promoting and providing resources to aid in cyber warfare against Georgia may signify their compliance with the attacks. Additionally, the fact that the initial cyber attacks took place before the war had even begun and later attacks coincided with martial efforts signify that the perpetrators were at the very least aware of the government’s military operations.

Ukraine

Ukraine has experienced multiple cyber attacks following the annexation of Crimea and its deteriorating relations with Russia. In the final months of 2016, Ukrainian institutions were targeted by 6,500 attacks that focussed on the defence and finance ministries, as well as causing a blackout in the
capital of Kiev. Official investigations indicated that the attacks had been perpetrated by Russian military hacking group “Sandworms”. On the 30th of June 2017, the Ukranian Security Service (SBU) also labelled them as responsible for a series of cyberattacks through the Petya malware. The attack was a ransomware which threatened to overwrite and encrypt important computer files unless their demands in Bitcoin currency were met. Rather than for financial gain, it is evident that the purpose of the attacks were to affect the state owned businesses, ministries and banks as the ransomware was operated to wipe out data instead of encrypting them. The total damage was estimated to about US$10 billion. The Petya malware was sourced from the compromised system update of a tax accounting software MeDoc. Ukranian officials have stated that the company will face “criminal responsibility” as further investigations showed that there were backdoors installed in the MeDoc system from May of 2017. The relaxed security of large domestic firms can jeopardize the state of an entire nation.

Kaspersky Lab

The Kaspersky Lab is a cybersecurity organization based in Moscow which develops antivirus and online encryption software as well as other cybersecurity products and services. The group is best known for having discovered Stuxnet and Flame and helping lay the foundations of the understanding of these infamous pieces of malware among others. The organization’s website contains detailed analysis of these aforementioned pieces of malware which anyone can access to become more educated on the topic of cyber terrorism and espionage. The Kaspersky Lab protects over 400 million users through its various services and continues to be at the forefront of research into and the fight against cyber warfare.

Timeline of Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>Titan Rain cyber attacks begin obtaining classified information from the US</td>
</tr>
<tr>
<td>2004</td>
<td>Titan Rain is discovered by a government analyst</td>
</tr>
<tr>
<td>27th of April, 2007</td>
<td>Estonia experiences a cyber attack at the hands of Russian hacktivists</td>
</tr>
<tr>
<td>2008</td>
<td>Stuxnet compromises a major uranium plant in Natanz, leading to malfunction</td>
</tr>
<tr>
<td>2008</td>
<td>GhostNet is initiated, targeting embassies and individuals in over 100 countries</td>
</tr>
</tbody>
</table>
May 2008  NATO’s CCDCOE is formed in Tallinn

5th of August 2008  The BTC pipeline is remotely detonated through a cyber attack

11th of August 2008  Major Georgian government websites are compromised and defaced

14th of August 2008  The Russo-Georgian war officially ends in a ceasefire

2009  Operation Socialist is first devised by the Five Eyes alliance

June - December 2009  Operation Aurora takes place, affecting dozens of US firms

July 2009  Three sets of cyber attacks are initiated on key American and Korean websites

2010  Flame is estimated to have first been used as a weapon of cyber espionage

2010  1,000 centrifuges in Natanz are destroyed by the Stuxnet worm

2010  Google ceases operations in China

2011  Operation Socialist is successfully executed

2012  Operation Socialist is discovered by Belgacom employees

15th of August 2012  Aramco faces a cyber attack at the hands of Shamoon malware

15th of March 2013  The Tallinn Manual is released by the CCDCOE

March - April 2016  33 DNC emails and computer systems are compromised

22nd of July 2016  DNC phone numbers, emails and private messages are released on WikiLeaks

August - December 2016  US blames and sanctions Russia for cyber attacks, diplomats of both exiled

February 2017  The Tallinn Manual 2.0 is released by the CCDCOE

16th of February 2018  13 Russian nationals and three Russian entities charged for the 2016 attacks
**Relevant UN Treaties and Events**

- Combating the Criminal Misuse of Information Technologies, 22 January 2001 (A/RES/55/63)

**Previous Attempts to solve the Issue**

The Cooperative Cyber Defence Center of Excellence (CCDCOE) describes itself as a “cyber defence hub” which supports its member states through cybersecurity expertise. The organization has four ‘focus areas’ through which this is done: Technology, Operations, Strategy and Law. The CCDCOE takes pride in this, saying it “embodies and fosters cooperation of like-minded nations”, and incorporates all four areas in each of its major services. For example, the CCDCOE website contains a library of regularly-updated and well-researched articles and analyses of major events concerning cyber terrorism and espionage, each of which has its relevant focus areas labelled. In addition to this, a group of experts in each of the four areas offer sophisticated training courses and consultation for business owners and government officials seeking to reduce their risk of becoming victim to a cyber attack.

The CCDCOE is essential to this issue as it remains the only organization which has drafted transnational treaties and other documents aimed specifically at cyber terrorism and espionage. This was first done through the Tallinn Manual on the International Law Applicable to Cyber Warfare, commonly referred to as simply the Tallinn Manual, released on the 15th of March, 2013. The manual consists of a set of detailed ‘black letter rules’ which apply international law to cyberspace, such as specifying all nations’ right to sovereignty of their own cyberspace just as they have sovereignty to the territory within their borders. The manual was later updated in February of 2017 with the release of the Tallinn Manual 2.0, which expanded on the original manual by including cyber operations of a less destructive and more day-to-day nature in addition to cyber warfare. Although the manuals are not legally binding and have therefore never been used to prosecute nations engaged in cyber terrorism and espionage, they serve as the first step in reaching a solution through international cooperation.
Possible Solutions

When considering solutions to the issue of state-sponsored cyber terrorism and espionage, there are several problems which must be addressed. Firstly, one of the major reasons behind the increasing prevalence of state-sponsored cyber attacks is a lack of criminal accountability. This can be observed even in incidences where the perpetrators of the attacks were confirmed, such as Operation Socialist and Operation Olympic Games, but faced no legal repercussions for their actions. Without a rigid legal framework, cyber terrorism and espionage will continue to take place as countries will be able to gain political and military advantages at no cost. The development of laws similar to those seen in the Tallinn Manual 2.0 could help address this, although they would need to be formed into ratifiable treaties, so that they are effective, and provide incentives to signatories (e.g. cybersecurity services), so that they are beneficial to member states.

Furthermore, such laws may benefit from applying cyber warfare to current international law rather than solely vice versa. For example, applying the concept of sovereignty to cyberspace may be difficult to objectively measure and define. However, applying acts of cyber terrorism on physical infrastructure, such as the explosion of the BTC pipeline and Stuxnet’s destruction of centrifuges, to already established international laws concerning the destruction of property and physical harm to people, would be much easier to understand and not require any new laws to be created.

Additionally, the uncertainty present when investigating cases of cyber terrorism and espionage must be considered. This arises from the fact that it is exceedingly easy to remain anonymous online and even mislead investigators through false information, such as Flame appearing to have been created in the 1990s. Operations in which the perpetrators cannot be confirmed but can instead be highly suspected, such as North Korea’s involvement in the July 2009 cyber attacks, would never be resolved without considering this issue, even with a comprehensive legal framework. One possible solution would be to develop a universal definition of ‘state-sponsored’ including cases of inaction, such as a country failing to address cyber attacks committed by its citizens (e.g hacktivists) despite being able to. Not only would this lead to global efforts to reduce cyber terrorism and espionage within member states’ borders, but it would also remove the uncertainty present when prosecuting the culprit of a cyber attack. For example, if an APT is traced back to China, the country would receive legal repercussions for failing to identify or combat the group responsible in the case that this was not state-sponsored.

Moreover, transnational cybersecurity initiatives such as NATO’s CCDCOE could serve as preventative measures for future cases of cyber terrorism and espionage. These are important as countries overwhelmed by cyber attacks may require the support of other nations in order to remain online. This can be seen through the 2007 cyber attacks on Estonia, which resulted in a complete shutdown of its banking and government services for three weeks. By contrast, through the support of
Estonia and the United States, Georgia managed to maintain its digital presence throughout the Russo-Georgian conflict, when it would have likely faced a similar fate to Estonia otherwise.

**Guiding Questions**

- To what extent are countries responsible for cyber attacks carried out by their citizens?
- What level of uncertainty should be allowed when prosecuting a nation of a cyber attack?
- What distinguishes cyber terrorism targeting physical infrastructure from traditional terrorism?
- Is cyber espionage ever justified? If so, when?

**Appendices**

I.  [https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf](https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf) (Tallinn Manual 2.0)

   Consists of the beginning of the Tallinn Manual 2.0, which remains the most comprehensive document addressing legislation surrounding cyber terrorism and espionage. This can be used to understand the purpose of the manual as well as an overview of its contents before commencing further investigation.

II.  [https://ccdcoe.org/](https://ccdcoe.org/) (CCDCOE Site)

   Contains resources such as recent news concerning cyber warfare (‘Library’) as well as cybersecurity documents (‘Research’) that may be useful to better understand and remain updated on the issue.

III.  [https://www.cfr.org/interactive/cyber-operations](https://www.cfr.org/interactive/cyber-operations) (Cyber Operations Tracker)

   Includes a brief overview of all major cyber operations since 2005, including summaries of each incident and a timeline of when they took place. This can be used to investigate additional incidents of cyber terrorism and espionage which may be relevant to a specific country or simply be of interest.

**Bibliography**


