COMMITTEE GUIDE

DISEC

DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE

Benjamín Quintero Llano and Mariana Valencia

2023

Contents

Presidents' Letter

Dear Delegates,

Welcome to CCBMUN XXI! Before we start, we would like to express our gratitude to all of you for participating in the twenty-first edition of the CCBMUN, a massive undertaking. We are Mariana Valencia and Benjamin Quintero, and we are proud and thrilled to be your presidents during this model. During the next few days, you and your fellow delegates will share in debate, discussion, dialogue, resolution writing, and a LOT of partisan bickering. Remember to maintain your delegation's interests; however, also keep in mind the committee's objective of global disarmament and ensuring international security. Get to know your country, the topics and your fellow delegates. Don't forget to speak with confidence and security, and be willing to cooperate.

For our part, we plan on using everything we have learned from our past MUNs to offer an enriching model with new learning opportunities, and to make sure this committee is always active, engaging, and home to thoughtful discourse. Both topics were designed to stimulate debate and diplomatic thinking.

From our time as delegates we know first-hand the anticipation and stress that one can face on the eve of the model, and hope that this guide, among other resources, will be able to ease this anxiety and to help you both to be and to feel prepared. While preparation for this model can be gruelling and often time consuming, we also know that once the day of the model arrives, all your hard work will pay off. Being able to participate in a replica of a world changing organisation with a global influence not only allows for an exhilarating and exciting experience, but also gives you a glimpse of real life politics and diplomacy.

We hope to be able to help you make the most of this model. This will be our first model as presidents; we are really excited to meet you all! Please feel free to contact us if you have any questions, difficulties or are simply curious about some aspect of the topics or model. :)

Good luck at the model!

Benjamin and Mariana (DISEC Chair)
disec@cali.edu.co

Topic 1: *Repercussions And Consequences Of Cyber Warfare And Terrorism*

I. History/Context

Up until the use of cyber technology to bring about malicious acts both against civilian and non civilian targets, offences had much more direct and physical involvement, and were generally much easier to detect and prosecute. Warfare, terrorism, and crime were consequently also much easier to differentiate. But the seemingly endless possibilities and opportunities, and the degree of availability that exists in the online world, have made such distinct lines between state, state-sponsored, non-state, belligerent and non-belligerent groups much less clear. Oftentimes it can be very difficult to find and detect the perpetrators or to classify cyberattacks, because hackers are adept at maintaining anonymity. Additionally, operations are often not connected to geographical or political boundaries.

Cyberwarfare is often defined as interstate conflict in cyber space, while cyberterrorism involves religious, political, ideologically or similarly motivated cyberattacks that result in significant harm. Some experts, however, choose to define these terms in narrower or broader contexts. Cyberterrorism can, under some definitions, refer to cyberattacks in general, but under other definitions they refer only to cyberattacks which are carried out specifically by insurgent groups against information networks. Cyberwarfare can, similarly, sometimes also include state-sponsored groups as well as the primary state.

To provide some general outlines, cyberwarfare differs from cyberterrorism in that the main targets are non-civilian, those directly involved in the conflict, which contrast with cyberterrorism where targets are often civilian and not necessarily directly involved in hostilities. Neither should be confused with cybercrime, which deals with judicially prosecuted, internal, and/or personally motivated cyberattacks. However, these three terms, as previously mentioned, vary a lot depending on who is defining them; this has caused a lot of difficulty when addressing these cyber problems.

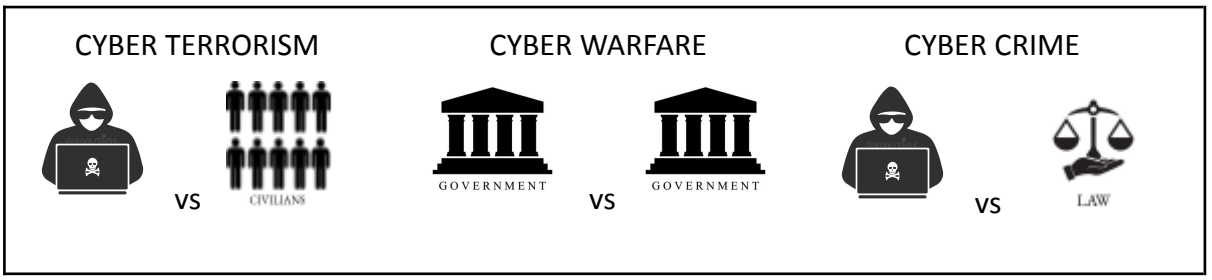

Figure 1: *This figure shows a simple infographic evidencing the key differences between cyber terrorism, cyber warfare, and cyber crime.*

Behind both cyberwarfare and cyberterrorism there are cyberattacks. While the first recorded cyberattack of any kind was back in 1834 in France, when the telegram system relaying financial information was compromised by two bond traders and their accomplices, cyberattacks as we know them came after the development of the first digital computer in 1943. The first two decades after the development of the first digital computer saw an overall absence of cyber offences. This can be attributed to various reasons: the very limited access to the technology; its novelty; and the fact that devices weren't networked and wouldn't be until 1969. Despite this, certain incidents involving break-ins to computer labs, just for the sake of altering networks rather than for any possible gain, did transcur.

The first network that emerged, before the existence of the internet, was ARPANET, (Advanced Research Projects Agency Network). ARPANET, which was part of the US defence department, was created in order to help Pentagon-funded research institutions share information with each other. And it was here that the first computer virus, known as the Creeper, was developed. While it was not malicious, the self replicating programme revealed a weakness in the system.

And so, parallel to the development of new methods of cyberattacks, was the development of cyber defence and security. One of the first instances of an antivirus programme was the Reaper, which was created in order to eliminate the Creeper. In 1988, the Morris Worm, which according to its creator was initially intended to assess the size of the ARPANET, struck about 6000 computers causing hundreds of thousands of dollars in damages. The Morris

Worm worked by reinstalling itself on computers, until they eventually crashed, making it the first 'Denial of Service' (DoS) attack. As cyberattacks became more and more dangerous, antiviral software was forced to become more effective and prevalent.

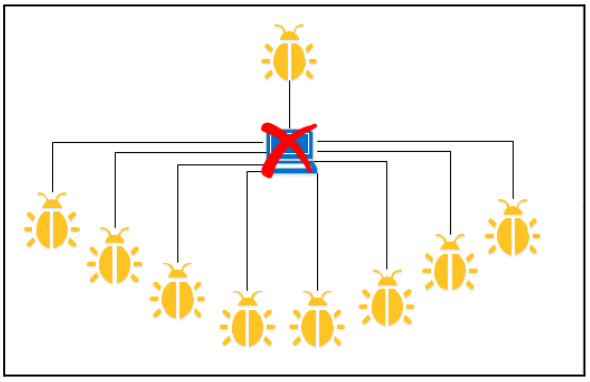

Figure 2: *This figure shows how the morris worm was able to damage computers by continuously redownloading itself on it, before passing on to another computer.*

In 1989, the World Wide Web allowed the internet to become public domain and globalised. More malware, viruses, and other cybertech were used to commit offences with individual damages running into the millions. The theorised threat of cyber warfare had become all the more real. Cyberwarfare quickly went from the possibility of cyber espionage on enemy systems, to cyberattacks on military networks, then to cyberattacks on the part of an enemy state's critical infrastructure that's connected to online networks.

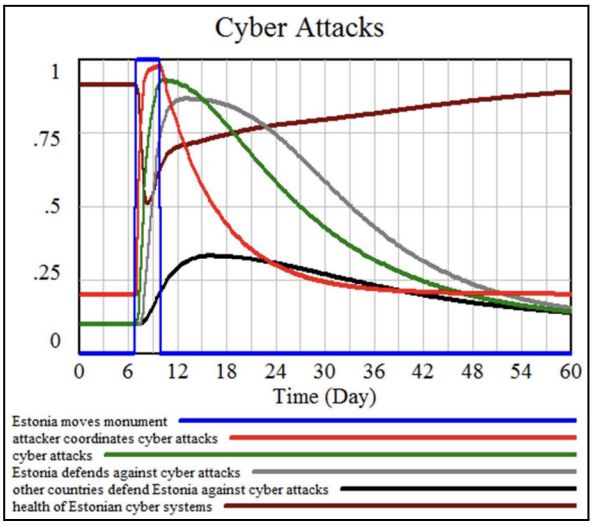

Figure 3: *This figure shows correlation between the movement of the Estonian monument and the 2007 Estonian cyber attacks, among other things.*

In 2007, the world saw cyberwarfare carried out for the first time in Estonia in a series of Distributed Denial of Service (DDoS) attacks. The attacks lasted for 22 days and came after a decision by the country's government to relocate a soviet-era monument. The relocation of the statue, which had for many Estonians remained a symbol of soviet oppression, led many ethnic Russian-Estonians to riot and perpetrate cybercrimes. However, according to Estonian authorities, many of these cyberattacks actually originated from Russia or Russian state institutions. The fact that Estonia is a NATO country also goes to show how cyber warfare allows nation states to bypass military treaties, while still causing significant harm. Although this was the first time that a nation was a target of cyberattacks by another nation, it wouldn't be the last.

II. Current Situation

Cyberattacks have been on an incessant rise, not only in terms of frequency, but also in terms of the extent of their damage. With cybercrime damages expected to cost the global economy more than 10 trillion USD a year by 2025, cyber warfare and cyberterrorism present an unprecedented threat to global security. In particular, they bring the potential for the exploitation of communication networks and digital information by hostile groups.

In the year following the attack on Estonia, Georgia was also faced with cyberwarfare attacks. These cyberattacks were accompanied with an actual invasion. Georgia saw various government sites hacked while tanks rolled in, occupying the regions of Abkhazia and South Ossetia.

While Russia was responsible for many of the earliest cyberwarfare attacks, it wasn't the only nation involved. Things got serious in 2010, when a virus known as Stuxnet was discovered and revealed to be targeting Iran's nuclear enrichment centrifuges. It was the first virus designed to attack an industrial control centre. It would download itself on microsoft computers via a USB flash drive, before spreading across the network and reaching the control centre. It is speculated that the virus was partially successful given that the eventuating of the virus also coincided with various major technical problems at the Natanz nuclear facilities, the reported shutdown of Iranian centrifuges in 2009, and the resignation

of president of the Atomic Energy Organization of Iran, Gholam Reza Aghazadeh. The cyberweapon is highly suspected to have been developed by the United States and Israel, in an attempt to restrict Iran from having nuclear capacities.

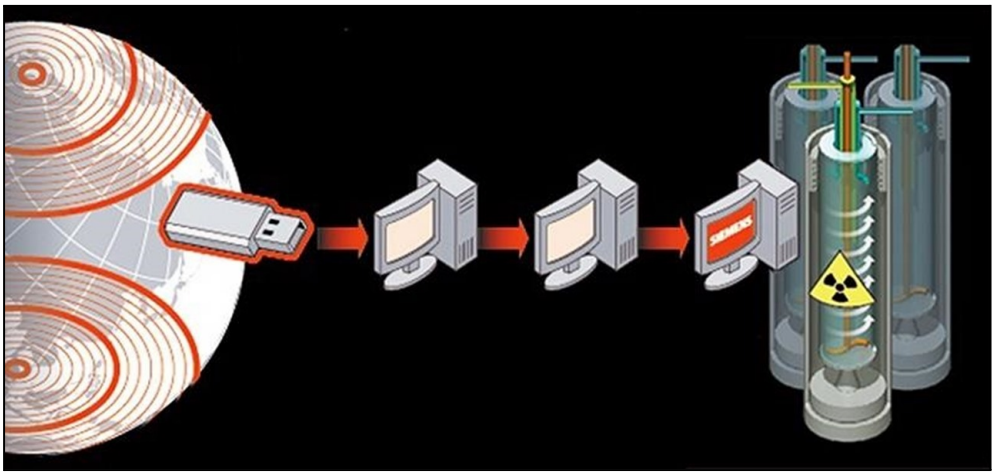

Figure 4: *This figure shows the process behind the Stuxnet viral infection and how it was able to infect Iranian centrifuges.*

Since then, Iran has retaliated several times, with targets including a Saudi oil firm and US banks, among others. Another key actor is North Korea which has conducted continuous DoS and ransomware attacks against both South Korea and the United States. With the ransomware attacks, the nation has been able to continue to fund further cyberattacks. A recent example was the attack on Sony Pictures after their release of "The Interview" which was estimated to have cost the company over 30 million dollars in damages.

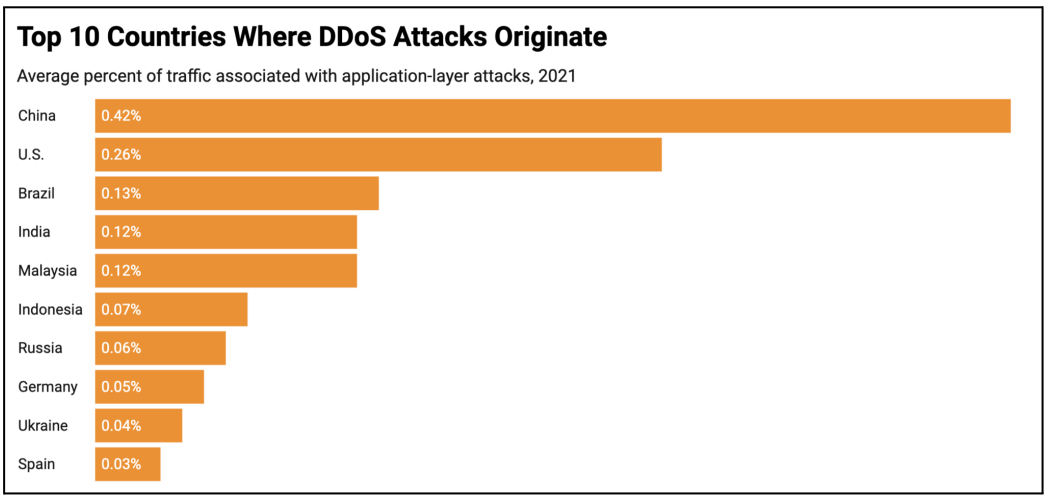

Figure 5: *This figure shows the main countries were DDoS attacks originated in the last quarter of 2021*

The most notable actor in cyberwarfare, reportedly making up more than 40% of all DDoS attacks in the last quarter of 2021, is China. It provides another prime example, Operation Aurora from 2010. Operation Aurora was a multifaceted cyberattack on US companies. The victims included Google, Adobe, Yahoo, Morgan Stanley, Symantec, among many others. Beyond stolen commercial intellectual property, Google reported that the accounts of various Chinese activists had been hacked. The attack was allegedly perpetrated by the Elderwood Group, a Beijing-based cyberespionage group with ties to China's principal military force.

One of the most recent cases of cyberwarfare, where an actual cyber war was witnessed, involving cyberattacks from both sides, has been in the conflict between Russia and Ukraine. One of the earliest attacks was a cyberespionage campaign against Ukraine that began in 2013 and which is known as Operation Armageddon. Cyberwarfare attacks between these two states have persisted to the present day.

In 2015, the world saw the capabilities of cyberattacks and cyberterrorism to fullfill military and political agendas. Russia unleashed an attack against Ukraine's power grid, affecting close to a quarter of a million people. It was accomplished by a Russian advanced persistent threat (ATP) group, which refers to when hackers infiltrate a system and remain undetected in it for long periods of time. It was done through an initial wave of spear-phishing emails, (counterfeit messages intended to extract sensitive information) followed by malware, DoS attacks, and disruptive internal operations. Its civilian-focused nature makes this, under some definitions, an example of cyberterrorism. Russian cyberwarfare attacks against Ukraine have affected various national sectors and industries. Ukraine has also responded, with groups like the IT army of Ukraine, which has participated both defensively and offensively. Ukraine has additionally gotten vast amounts of support from Western powers, who have helped the nation develop further cyber defences. Despite the very traceless essence of cyberattacks, data has shown that up to 35% of politically motivated attacks in cyberspace have had connections with either China or Russia.

As cyberweapons become more advanced, and cyberattacks more potent, national cyber campaigns and cyberwarfare become a highly attractive option for nation states. Not only do they have a high benefit to cost ratio, but they can be executed both in times of peace as well as in times of war. Operation Aurora and the 2007 attack on Estonia are examples of this. They can also weaken and harm another country without the requirement of physical force, while also strengthening the perpetrator, as is the case when trade secrets are stolen, or of ransomware attacks. Yet another incentive is anonymity. And while the mentioned examples have appeared to have somewhat clear targets and sources, in cyberspace, it is almost impossible to find out where the attack is coming from. This incredible versatility means that no country can ever be safe from cyberattacks, and the need for cyber defences to make attackers desist is astronomical. All these factors have made cyberwarfare a very real threat that, if not addressed by the international community, will see no decline.

The motives for participating in malign cyber activity are endless. In the wrong hands, destruction and harm can be the consequence. This is where another fear stems in. What should happen if insurgent groups with cyber capabilities carry out attacks via cyberspace? With the internet intertwined in almost every aspect of human life, it is also a powerful weapon, available not only to state actors. The internet is already used for planning, organising, and recruitment. So how real is this threat?

To see how much damage could be inflicted solely with cyberweapons, one has to review the vulnerabilities that exist. It is true that human society, including critical infrastructure, is greatly dependent on online networks. Nonetheless, experts have often minimised this threat due to other factors. While insurgent groups could potentially attack critical infrastructure, affecting a lot of civilians, it will not have the terrorising nature that more direct insurgent attacks have because it is, firstly, less evident, more controlled, and more temporary. To terrorise, it would have to be a multi-targeted attack against more than one piece of infrastructure. Attacking, for example, a single dam, would more likely to be mildly irritating for the region than nationally demoralising, because of the existence of alternatives and the unlikelihood of sole reliance on just one piece of infrastructure. Disruptions happen all the time, so to truly have an impact, there would have to be a series of attacks. The

problem is that systems are often separate and different, making this process highly complicated. Not even considering cybersecurity, even if this is accomplished, networks can often be fixed and restored within a short period of time. This is partly the reason why many experts have criticised the over-dramatization of cyberterrorism and mass cyber-destruction.

Currently, these are the main types of attacks that are perpetrated both by state and non-state actors:

Denial of Service (DoS) attack: Is a type of cyberattack where the assailant attempts to bring down a network and exhaust a site's resources by flooding it with fake demands, requests, and online traffic. When there are multiple assailants and systems attacking the same site it is considered a Distributed DoS attack (DDoS).

Malware attack: Is a type of cyberattack in which a harmful software infiltrates a network or computer. Malware attacks serve a wide variety of purposes including disruption, information theft, and extortion. The three main vectors for malicious software attacks include: the Trojan Horse, in which the malware is disguised as another software programme which is downloaded; a virus - a malware that is triggered by the user; and a worm - a self replicating malware that doesn't require user activation.

Ransomware attack: Is a type of malware attack that forces the victim to pay a ransom in order to regain access to its own digital information that had been "held ransom" by the malware. Over 200 million ransomware attacks took place worldwide in just the first half of 2021.

Spyware attack: Is a type of malware attack that secretly gathers critical information from the victim before then passing the data to a third party.

Phishing attack: Is a type of cyberattack that involves fraudulent emails or messages that tricks people into giving away sensitive information or downloading malware. Oftentimes, phishing attacks are used to open the way for other cyberattacks.

Supply Chain attack: Is a type of attack that targets the vulnerable links that an organisation or company may possess

Disinformation/ Propaganda: The cyberspace can also be used to spread false information purposely, in what are often politically motivated campaigns. This type of attack should not be undermined as it can be harmful to a nation's electoral system as was seen in Russia's meddling in the 2016 US election.

As aforementioned, the very often borderless essence of cybercrime and cyberattacks, have made transborder and international solutions necessary. This is also why the fact that there is no consensus on even the basic terms for these international security threats, is highly problematic.

Given its relative novelty, there is a general lack of international regulations and legislation regarding cyber warfare and terrorism. Nonetheless, this does not mean that there are no available tools. A very significant report, utilised in tackling cyber warfare and related problems, have been the Tallinn Manuals. The Tallinn Manuals include two reports that were devised by legal scholars and experts in cyber affairs, in Tallinn, Estonia following the 2007 cyberattacks; this was done at the request of NATO, and they address how international law is applicable to cyber warfare. The first Tallinn Manual addressed the more threatening cyber issues and those related to military conflict, while the second addressed issues both in and out of conflict.

Cybersecurity developments vary widely across the globe, instead of cohesive unanimous actions, most governments have tried to independently deal with this issue. Some examples of national measures that can be taken, and in certain cases have been taken include: the establishment of a cybersecurity task force; the establishment of a protection centre for

critical information infrastructure; the development cybersecurity training courses for government officials; the development and re-evaluation of cyber laws and regulations to address the gap between information and communication technologies (ICT); and legal frameworks, establishment of national coordinating measures and guidelines, cyberattack advisories, among others.

Some important entities that have been involved in combating this issue include the Council of Europe, International Telecommunication Union (ITU) and, of course, the United Nations first committee.

III. Key points of the debate

- Defining what constitutes cyberwarfare and cyberterrorism
- Addressing unsanctioned and unpenalized cyberattacks by hostile nations
- Guaranteeing cybersecurity and defences for defenceless states
- Preventive measures that could ensure safety from cyber terrorism
- Establishment of punishments and regulations for cyberwarfare and cyberterrorism
- The possible consequences and repercussions of cyberterrorism
- The possible consequences and repercussions of cyberwarfare

IV. Guiding questions

1. What cyber offences and attacks has your nation been involved in or perpetrated?
2. Has your nation experienced any kind of cyberattacks ranging from sabotage, espionage, DoS, or propaganda campaigns?
3. What institutions does your nation have built in place for ensuring cybersecurity and protecting vital infrastructure?
4. Does your nation have any digital task force? Does it operate both defensively and offensively?
5. Are there any cybercrime groups that operate from your nation? Do they have ties with your own government?
6. What are your nation's cyber capabilities? How does it rank with others?
7. Has your nation been making any recent advancements in cyberspace?

8. How safe is your nation's cyberspace and online security?
9. What solutions has your delegation proposed to this problem? What domestic regulations does it have in place; additionally, what international regulations does it advocate for?

V. Bibliography

A brief history of hacking. Kaspersky IT Encyclopedia. (n.d.). https://encyclopedia.kaspersky.com/knowledge/a-brief-history-of-hacking/

Arctic Wolf. (2022, November 16). A Brief History of Cybercrime. Arctic Wolf. https://arcticwolf.com/resources/blog/decade-of-cybercrime/

Bhadwal, A. (2023, July 13). The history of cyber security: A detailed guide [infographic]. KnowledgeHut. https://www.knowledgehut.com/blog/security/history-of-cyber-security

Board of Regents of the University System of Georgia. (n.d.). A brief history of the internet. Online Library Learning Center. https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml

Chadd, K. (2020, November 30). The history of cybercrime and cybersecurity, 1940-2020. Cybercrime Magazine. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

Climer, S. (2019, July 3). History of cyberattacks from the Morris Worm to exactis. Mindsight. https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/

Council on Foreign Relations. (2010, January). Connect the dots on state-sponsored cyber incidents - operation aurora. Council on Foreign Relations. https://www.cfr.org/cyber-operations/operation-aurora

Elderwood. Elderwood, Elderwood Gang, Beijing Group, Sneaky Panda, Group G0066 | MITRE ATT&CK®. (2021). https://attack.mitre.org/groups/G0066/

Greenberg, A. (2019, August 23). Cyberwar: The complete guide. Wired. https://www.wired.com/story/cyberwar-guide/

Grimes, R. (2012, January 10). Why internet crime goes unpunished. CSO Online. https://www.csoonline.com/article/548638/cyber-crime-why-internet-crime-goes-unpunished.html

Kamen, D. (2023, July 5). What is a Cyber War. NEIT. https://www.neit.edu/blog/what-is-a-cyber-war-explained#:~:text=The%20history%20of%2

0cyber%20warfare%20goes%20back%20to%20the%201980s,digital%20warfare%20and%20espionage%20increased

Knell, N. (2022, April 13). Top 10 countries where cyberattacks originate. GovTech. https://www.govtech.com/security/hacking-top-ten.html

Lewis, J. A. (2002, December). Assessing the risks of cyber terrorism, cyber war and other cyber ... Center for Strategic and International Studies. https://www.researchgate.net/profile/James-Lewis-9/publication/245508226_Assessing_the_Risks_of_Cyber_Terrorism_Cyber_War_and_Other_Cyber_Threats/links/5e25be2192851c89c9b49515/Assessing-the-Risks-of-Cyber-Terrorism-Cyber-War-and-Other-Cyber-Threats.pdf?origin=publication_detail

M, S. (2023, July 21). 21 top cyberattacks you should know in 2023. Simplilearn.com. https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

PC Docs. (2021). The history of cybercrime and why cyber security is so important today. PC Docs. https://www.pc-docs.co.uk/the-history-of-cybercrime-and-why-cyber-security-is-so-important-today/

Standage, T. (2018, May 31). 1834: The First Cyberattack. Schneier on security. https://www.schneier.com/blog/archives/2018/05/1834_the_first_.html

Wright, G. (2021, November). What is ARPANET and what's its significance? Networking. https://www.techtarget.com/searchnetworking/definition/ARPANET#:~:text=The%20U.S.%20Advanced%20Research%20Projects,for%20academic%20and%20research%20purposes.

Talihärm, A. M. (2013, August). Towards Cyberpeace: Managing cyberwar through international cooperation. United Nations. https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

Top 5 most notorious attacks in the history of Cyber Warfare. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare

What is a denial of service attack (dos) ?. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

What is cyber warfare: Types, examples & mitigation: Imperva. Learning Center. (2021, November 9). https://www.imperva.com/learn/application-security/cyber-warfare/

Wolf, M. (2014). Stuxnet. Stuxnet - an overview | ScienceDirect Topics. https://www.sciencedirect.com/topics/computer-science/stuxnet#:~:text=Stuxnet%20is%20a%20worm%20that,than%20a%20year%20before%20that

Figure 1: Katrink 2003. (2018, September 19). Icon of a hacker with a laptop. stock vector - illustration of Hack, person: 126441531. Dreamstime. https://www.dreamstime.com/icon-hacker-laptop-icon-hacker-laptop-silhouette-vector-illustration-image126441531

Mark1987. (n.d.). *Government PNG transparent images free download: Vector files*. Pngtree. https://pngtree.com/freepng/government-icon_4769155.html

Figure 2: GoMindsight. (2019, March 21). History of cyberattacks from the Morris Worm to exactis. Mindsight. https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/

Figure 3: Naugle, A. B., Bernard, M. L., & Lochard, I. (2016, April 1). Simulating political and attack dynamics of the 2007 Estonian cyberattacks. simulating political and attack dynamics of the 2007 estonian cyberattacks. (Conference) | OSTI.GOV. https://www.osti.gov/servlets/purl/1364997

Figure 4: Occupytheweb. (2015, May 19). What the heck was stuxnet!?. WonderHowTo. https://null-byte.wonderhowto.com/news/what-heck-was-stuxnet-0160816/

Figure 5: Yoachimik, O. (2022, April 12). DDoS attack trends for Q4 2021. The Cloudflare Blog. https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/

Topic 2: *Post-War Military Proliferation And Instability In Iraq*

I. History/Context

From 1980 to 1988, the nations of Iraq and Iran were involved in a war for the possession of the Shatt Al Arab, that took thousands of lives, and saw the use of chemical weapons (CW) and military artefacts such as missiles, rifles and air defences systems by both sides. These armaments continue to remain prevalent, mainly in Iraq.

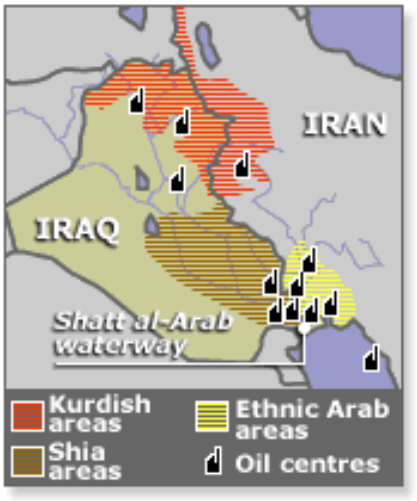

Figure 1: *Iran Iraq conflict 1980-1988 (BBC)*

The war started when the Iraqi army, under the leadership of the dictator Saddam Hussein, invaded Iran, led by Ayatollah Khomeini, in an attempt to gain complete control of the Shatt al-Arab River, in order to annex the oil-rich Iranian province. The Iraqi army, however, mis-estimated Iran's military strength and fighting capabilities, and was met with unexpected resistance from Iran, which had the intention of safeguarding the Islamic Revolution from international threats.

In order to successfully deter the Iraqi invasion, the Iranian leadership was convinced it had to increase its forces, army and development, which caused the conflict to escalate. The counter-attack ultimately resulted in a setback for the Iraqis across the Karun River and a bloody stalemate that would continue with no side ensuring victory. As both sides sought greater military might, they began to rely more and more on external support.

Weapon suppliers of Iran included the US, USSR, France, Italy, Great Britain, East Germany, Switzerland, Israel, Syria, North Korea, South Korea, Algeria, Libya, Argentina and Brazil before the war and China, France, Italy, Syria, South Yemen, North Korea, South Korea, Taiwan, Vietnam, Algeria, Libya and Argentina during the war.

For Iraq, suppliers included the USSR, France, Brazil, West Germany, Italy, Spain, Czechoslovakia, East Germany, Hungary, Poland, Yugoslavia, Austria, Switzerland, Egypt, Jordan, North Korea, Brazil, Chile, Morocco, Ethiopia, Sudan, and Brazil before the war and the USSR, China, West Germany, Italy, Portugal, Spain, Great Britain, Czechoslovakia, East Germany, Poland, Egypt, Jordan, Kuwait, Saudi Arabia, UAE, Pakistan, North Korea, and the Philippines during the war.

Much of what the US traded was through its private sector and often came indirectly through allies like Israel, Egypt, Jordan, and Saudi Arabia, given that it was not truly sanctioned by the government. These weapons brought in by foreign allies were involved in the violation of international humanitarian law with 500,000 lives being lost on each side, almost 1,000,000 lives in total. This raises the question of whether the nations sending in these arms should also be held responsible.

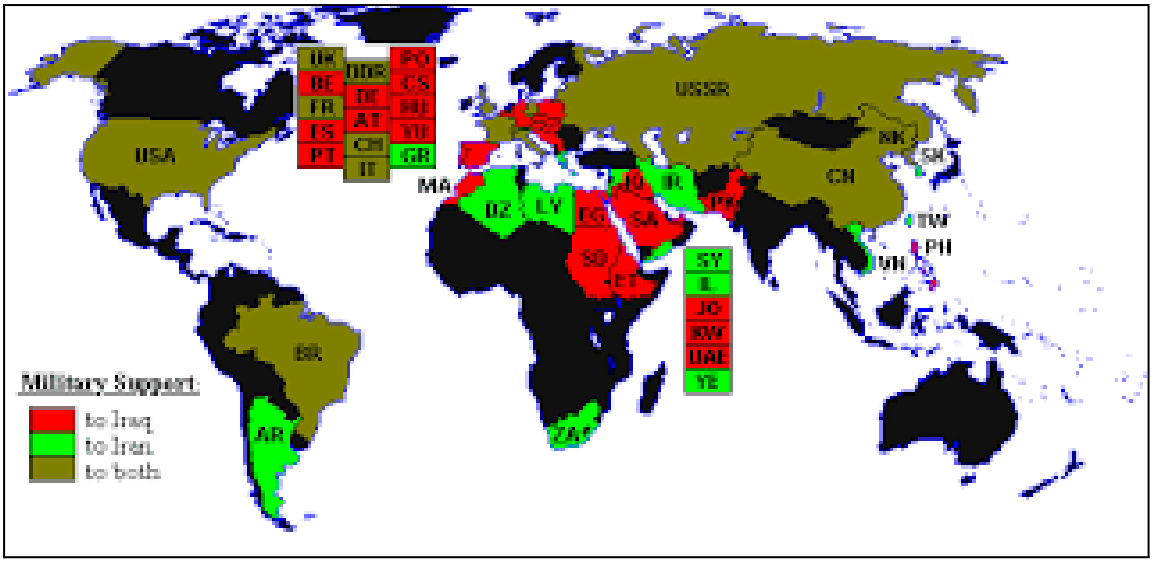

Figure 2: *The map below is a graphical representation that shows which countries were involved in the war and whether they were supporting Iraq, Iran or both.*

As we can observe, many countries such as the United States, along with China, the Soviet Union, Brazil, and North Korea were involved in supplying both sides of the conflict. This is important, and also controversial, because it demonstrates how many foreign weapon suppliers did not, in fact, care about the impact of their products on the war or have any ties with Iran or Iraq; instead they were motivated by greed and profit-oriented policies. It can be understood that the justification for fueling these conflicts was the accumulation of wealth.

In the United States, this became a political scandal of Ronald Reagan's administration. Reagan had allowed and facilitated arms sale during this war, despite an arms embargo on Iran. Moreover, earnings from these weapon exports were then used to fund a marxist-oposition rebel group in Nicaragua known as the Contras. The scandal is often referred to as the Iran-Contra affair.

During the Iran-Iraq war, the two countries were involved in the use of chemical weapons (CW). Their use demonstrated immense military effectiveness and destructive proliferation and so were employed by both sides in military tactics and varying strategies.

After that, the United States, Russia and China, designed and manufactured an arsenal to keep the weapons and artillery safe from citizens and illegal groups. This was done taking into account that the number of Iraqi weapons had been on the rise during the late 1970s at the beginning of the modern global arms market, and only ended up worsening with the war with more than 34 countries supplying armaments.

The arsenal functioned for some time, until it began to be looted. The lack of leadership on the ground on the government's part, along with the inaction when it came to the unregulated flow of these weapons, allowed outlawed groups such as the Islamic State, among others, to take advantage of this access to arms power and maintain control.
Just two years following the ceasefire of the Iran-Iraq war in 1988, Saddam Hussein gave the order to invade Kuwait, using the armaments that had been provided by international arms dealers during the war against Iran. This was done to gain regional influence, nullify its debt

with Kuwait, punish Kuwait for not abiding by the Organization of the Petroleum Exporting Countries (OPEC) regulation's and, of course, to get access to Kuwait´s vast oil reserves. The invasion force greatly outnumbered Kuwait's forces, and Iraq's mechanised and motorised infantry, helicopters, and squadron bombers steamrolled through. Iraq then proceeded to militarily occupy the country.

The international community was quick to condemn these actions. After issuing a deadline to leave Kuwait that was not kept, the United Nations encouraged states to use all necessary means to expel Iraq from Kuwait. This was the first Gulf War. A US-led coalition of 39 nations was able to successfully liberate Kuwait and then invade Iraq.

Once the coalition had occupied Iraq, the United Nations quickly located Iraqi chemical weapons and related equipment and destroyed them, thus ensuring that Iraq would discontinue nuclear, chemical, and biological weapons programmes. Iraq's chemical weapons stockpile, which it had utilised in the Iran-Iraq war, and its nuclear and biological weapons programmes had become a threat to international security. However, despite these actions by the UN, the US government was not convinced that this was the end of the problem. It used the alleged development of weapons of mass destruction (WMD) in Iraq to justify an invasion in 2003. The 2003-2011 war in Iraq would not only see the deployment of more arms but would lead to the discovery of old ones.

II. Current Situation

During the US military intervention in Iraq, American and American-backed Iraqi troops discovered the existence of dangerous armaments. These were armaments that were not connected to the active development of WMD, which the US had cited as the primary reason for the invasion. In fact, the US Senate later released reports that much of the Bush administration's statements had been misleading. Further reviews found that Iraq had actually already ceased the development of WMD before the invasion. According to sources from the New York Times, close to 5,000 chemical warheads and weaponry were found, but no WMD. While the war had initially been undertaken to bring about an end to the supposed active development of weapons of mass destruction, what was instead uncovered

was military remnants from a Saddam Hussein era that had been provided by foreign exporters, including western powers themselves.

Uncontrolled and mass weaponry influx are not the only legacy of military interventions in Iraq.

The second US led intervention, which had far less support, was not only poorly justified, but brought about great destruction and loss. From 2003 to 2007, the number of internally displaced people went from non-registered to over 2.5 million. Furthermore, by 2007, the number of refugees also peaked at over 2 million. Many of the people leaving the country were skilled professionals, such as doctors. In fact, according to the Iraq medical association, approximately half of Iraq's doctors left following the US invasion with many more internally displaced, helping aggravate an already worrisome health crisis. This loss of human capital also had a particularly detrimental effect on Iraq's developing economy.

Another byproduct was the further exacerbation of the nation's systematic corruption. Following the invasion, the US established poorly developed institutions in Iraq that, as The World Politics Review puts it, "built on sectarian allocation, entrenched political divisions." The government became unable to provide basic essential services, something it struggles with to this day.

It can be said that Saddam's 30 year autocratic regime resulted in state-enforced violence, intimidation, fear, human rights violations and a very oppressive government. However, by toppling Saddam's government, the coalition forces created a power vacuum, which would be filled by armed groups such as ISIS, groups that were further supported by the influx of weapons and armaments.

The transition from Saddam's autocratic rule to a struggling democracy has posed a great challenge to the nation's stability, security, and general prosperity. It resulted in the political, social and sectarian fragmentation of Iraq, resulting in a weak state with domestic actors, implying an internal factionalism and worrying decentralisation. Although the country has

seen certain advances in specific areas, its security sector is in a very poor state. Due to it being highly entangled with outside forces and politics, and having a very low degree of self-sufficiency and autonomy, Iraq's security sector is simply not capable of guaranteeing nationwide safety and internal security. Again, institutions developed by the US failed to provide strong foundations, and while Saddam was tyrannical, his government did provide centralization and strong administrative control.

Figure 3: *A photograph depicting the war between Iran and Iraq and heavy armaments utilised.*

These incessant weapons circulations have allowed the Islamic State and other outlawed groups to obtain military might which they use irresponsibly. Some of the criminal actions that have been committed with this weaponry include abuses, killings and torture. It has also forced thousands of families to leave their homes, because if they stay they are risking their lives.

In short, the Islamic State of Iraq and the Levant is a Salafi (a radical totalitarian Islamist movement) jihadist (the conduct that every Muslim should lead on a path away from all kinds of faults, deviations or temptations) militant organisation which seeks to establish a caliphate in Iraq and Syria.

After a UN investigation, it was found that the Islamic State extremists had committed several crimes against humanity as well as war crimes against the Christian community,

including: persecution; sexual violence; enslavement; and the destruction of religious spaces. For years the outlaw group took over Iraqi cities, fomenting chaos throughout the country and in parts of Syria. In 2017, after three years of battle, the Islamic state was finally dismantled, but it continued to exist in silence, organising attacks in different parts of Iraq.

The UN has written various reports that describe the crimes committed by the Islamic group in the region; the group has also been commonly referred to as the IS, DAESH, and ISIL. What makes this problem worrisome for the international community is that, despite being located mainly in Iraq and Syria, ISIS has been known to operate globally by working with local affiliates across the world; according to some reports, terrorist attacks actually saw a rise from 2019 to 2020. In fact, in 2020, ISIS was responsible for over 5000 casualties in just West Africa.

Although present-day Iraq does not pose the same military threat as 20 years ago, instability still abounds, mostly due to the presence of external powers. Although largely subdued, according to retired Marine Corps Gen. Frank McKenzie, who led US Central Command, “Iraq is still under pressure from ISIS” In fact, there are currently over 2500 U.S troops based in Iraq, despite efforts to withdraw troops. The consequences of the past continue to haunt its present.

Along with its history of military conflict, the nation is also plagued by its geographical location. Located between Saudi Arabia, Iran, Jordan, and Syria, weaponry that was not even destined for Iraq and regional conflict can further affect the country in a negative way. One example of this is the transport of weapons to assist the Lebanese Hezbollah, an Iran backed Shiite Muslim political party and militant group which, according to the Council on Foreign Relations, is a group that “is driven by its opposition to Israel and its resistance to Western influence in the Middle East.” Weapons for this cause often pass through Iraq.

The weak federal military control, combined with successive years of political dishonesty by the Iraqi government, have made this a complex problem, affecting in turn public security and international humanitarian law.

III. Key points of the debate

- The irresponsible way in which weapons were delivered to Iraq by different countries of the world
- Iraqi political dishonesty and its repercussions
- How humanitarian international law has been fractured in Iraq, and what are the possible solutions
- How can the weapons trade be regulated in order to prevent insurgent groups.
- The impact of Iraqi based armed groups on international security and citizens.

IV. Guiding questions

1. Does your nation assist the Iraqi army in any way? If so, how?
2. How has your nation contributed to military proliferation in Iraq?
3. Has your nation instigated conflict in Iraq? If so, how is your nation involved?
4. Does your nation believe the Iraqi army and security forces are sufficient for the control of arsenals or does it advocate for foreign involvement?
5. Does your nation contribute to guaranteeing the fulfilment of human rights and international humanitarian law? Why or why not?
6. Would your nation be against the establishment of a committee to evaluate the risk conditions of the nations receiving the arms forces to guarantee international humanitarian law?
7. What regulations or penalties does your nation have in place regarding arms distribution, exportation, and/or acquisition?
8. Does your nation host any organised armed groups?
9. Has your nation proposed any solutions to the problem?

V. Bibliography

Ali, Javed. “Chemical Weapons and the Iran-Iraq War: A Case Study in Noncompliance.” The Nonproliferation Review, vol. 8, no. 1, Mar. 2001, pp. 43–58, Iran-Iraq War | Causes,

Iran Deal. (2016). Retrieved July 18, 2023, from The White House website: https://obamawhitehouse.archives.gov/issues/foreign-policy/iran-deal

How Islamic State got its weapons. (2015). Retrieved July 18, 2023, from @AmnestyUK website: https://www.amnesty.org.uk/how-isis-islamic-state-isil-got-its-weapons-iraq-syria

Lederer, E. M. (2022, December 2). UN: Iraq Christians were victims of Islamic State war crimes. Retrieved July 18, 2023, from AP News website: https://apnews.com/article/islamic-state-group-religion-crime-middle-east-war-crimes-fbd3629899879210ea4adf14f7a6fdf6#:~:text=The%20report%20to%20the%20U.N.,of%20cultural%20and%20religious%20sites

Lewis, D. (2021, May 9). Challenges of the Security Sector in Iraq after Saddam. Retrieved July 18, 2023, from Vision of Humanity website: https://www.visionofhumanity.org/iraqs-security-sector-faces-serious-challenges/

MMP: Islamic State. (2021). Retrieved July 18, 2023, from Stanford.edu website: https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state

Schumann, A. (2023, June 23). Melding U.S. Non-Proliferation Strategy with Middle East De-Escalation Dynamics - Center for Arms Control and Non-Proliferation. Retrieved July 18, 2023, from Center for Arms Control and Non-Proliferation website: https://armscontrolcenter.org/melding-u-s-non-proliferation-strategy-with-middle-east-de-escalation-dynamics/

Summary, Casualties, & Facts | Britannica. (2023). In Encyclopædia Britannica. Retrieved from https://www.britannica.com/event/Iran-Iraq-War#ref344820

War, I.-I. (2022). Iran-Iraq War Causes, Overview & Timeline | Who Won the Iran-Iraq War? - Video & Lesson Transcript | Study.com. Retrieved July 18, 2023, from study.com website: https://study.com/learn/lesson/iran-iraq-war-causes-overview-timeline.html#:~:text=The%20war%20ended%20in%20a,similar%20numbers%20for%20both%20sides

www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf, https://doi.org/10.1080/10736700108436837. https://www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf

Figure 1: Sadam´s Iraq - Key Events. (2023). Gstatic.com. https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQAv8XLSZmcfxnvC90vDz9p4Bp_Hne3IN9s0wIjgyrYwRYQKWMMyCbJiP73EJuYJdHgoFk&usqp=CAU

Figure 2: GUERRA IRÁN-IRAk ( ). (2019). Slideplayer.es. https://slideplayer.es/slide/146436/#google_vignette

Figure 3: Mahmoud, S. S. (2020, September 22). Legacy of Iran-Iraq War still reverberates 40 years later. Conflict News | Al Jazeera. https://www.aljazeera.com/news/2020/9/22/legacy-of-iran-iraq-war-still-reverberates-40-years-later