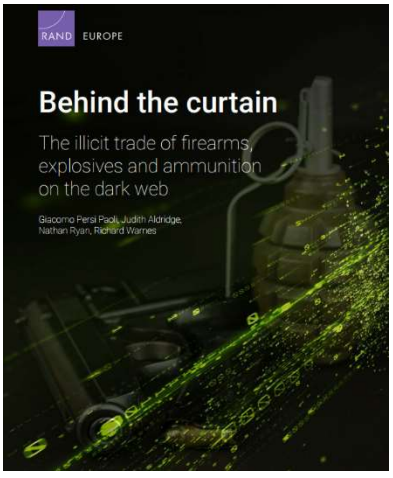
DISEC

# Disarmament & Security Committee



## AtidMUN VII



# Table of Contents

# Chair letters

## Ofek Magrafta

Dear delegates,

It is my absolute pleasure to welcome you to the Disarmament and International Security Committee.

My name is Ofek, and I've been doing MUN for over 4 years. My first experience in the Environment Committee at TIMEMUN Conference was awarded "the best delegate"- it was wonderful for a 6th-grade novice. Nowadays, I especially like the Security Council and European Council Committees, having under my belt a few TIMEMUN and AtidMUN and many other national conferences. I have been both mentoring and participating in many MUN conferences, which develops my research, teamwork, presentation, and persuasion skills, which are super important for young people.

In this conference, we will be talking about Fourth and Fifth-generation warfare as well as targeting the illicit arms trade on the Dark Web- unresolved crises in our stormy world.

I look forward to seeing you talk and pass creative resolutions on these pressing issues.

If you have any questions, please don't hesitate to contact and spam Ronald on: ronaldrakov@gmail.com

Sincerely,

Ofek Magrafta

## Ronald Rakov

Honorable delegates,

Welcome to the DISEC committee of AtidMUN VII. My name is Ronald Rakov and I will be your chair along with Ofek.

I'm a junior studying at Hakfar Hayarok High school, and I live in Petah Tiqva. Apart from doing Model UN, I also participate in debate activities, which are super fun. Additionally, I mentor and participate in both Model UN and in debate.

In the committee, we will discuss two interesting and important topics. We encourage you to speak up, cooperate with other delegates, and together write the greatest resolutions ever.

I am available for any questions that you may text me on WhatsApp: (0503408080) or fill in Ofek's inbox: ofek.magrafta@gmail.com

Sincerely,

Ronald Rakov

# Introduction to the Committee

The Disarmament and International Security Committee (DISEC) is the First Committee of the United Nations General Assembly. The committee concerns itself with questions of international importance regarding the security and demilitarization throughout all countries and regions, along with ensuring that citizens across the globe remain protected.

The General Assembly First Committee: Disarmament and International Security (DISEC) deals with issues relating to disarmament, global challenges, and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime. It considers all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments. The Committee comprises all member nations of the United Nations, and even though its mandate is limited to recommendations, it has proven to be one of the most influential bodies in the United Nations, as its resolutions deal with some of the most complex topics in the international community. The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament.

For more information: https://www.un.org/en/ga/first/

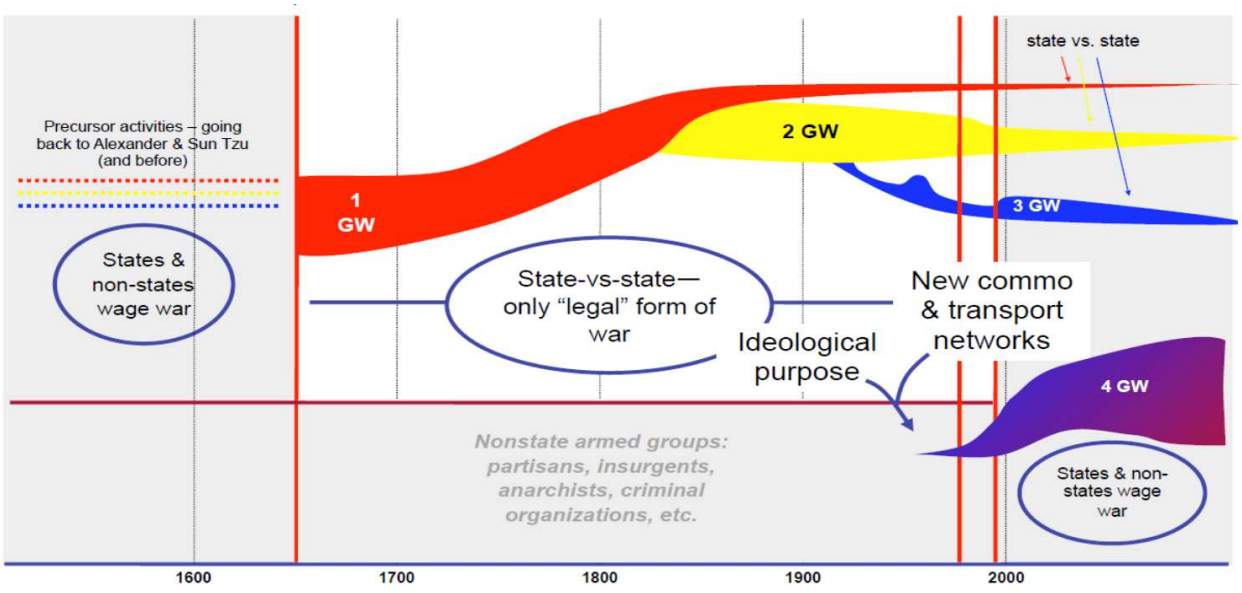
# Topic A: Fourth and Fifth Generation Warfare

## Background to the Issue

Throughout world history, different concepts of categorizing warfare have been created.

One of these concepts is the concept of warfare generations, first coined by author William S. Lind.

The concept of warfare generations divides modern warfare into five generations, each having a unique time period and features.




## The Five Warfare Generations

- **First-generation warfare** refers to the Ancient and Post-classical battles fought with massed manpower, using phalanx, line and column tactics with uniformed soldiers governed by the state.
- **Second-generation warfare** is the early modern tactics used after the invention of the rifled musket and breech-loading weapons and continuing through the development of the machine gun and indirect fire. The term *second generation warfare* was created by the U.S. military in 1989.

- **Third-generation warfare** focuses on using Late modern technology-derived tactics of leveraging speed, stealth and surprise to bypass the enemy's lines and collapse their forces from the rear. Essentially, this was the end of linear warfare on a tactical level, with units seeking not simply to meet each other face to face but to outmaneuver each other to gain the greatest advantage.
- **Fourth-generation warfare** as presented by Lind et al. is characterized by a "post-modern" return to decentralized forms of warfare, blurring of the lines between war and politics, combatants and civilians due to nation states' loss of their near-monopoly on combat forces, returning to modes of conflict common in pre-modern times.
- **Fifth-generation warfare** is conducted primarily through non-kinetic military action, such as social engineering, misinformation, cyberattacks, along with emerging technologies such as artificial intelligence and fully autonomous systems. Fifth generation warfare has been described by Daniel Abbot as a war of "information and perception".

Fourth and fifth generation warfare is defined as a decentralized and non-organized warfare, appearing in the form of violence, terror and attacks by non-state actors.

Another characterization of this type of warfare is a combined use of kinetic force (active lethal force) and non-kinetic force (indirect force); for example, the use of cyber-attacks and political violence.

This committee's topic is particularly related to the fourth and fifth warfare generations, which are considered to be the warfare used since the 60s decade of the 20th century.

As such, in the committee, we will discuss different types of warfare, will debate the consequences and outcomes of this type of warfare and write a resolution on the topic.


## History

- 1980 - Author William S. Lind first uses the term 'fourth generation warfare' in a Marine Corps article: "The Changing Face of War: Into the Fourth Generation".
- March 12th, 1947-December 26th, 1991- The first war classified as a fourth generation warfare war, the Cold war commences between the United states, Russia and their respective allies. During this war, many fourth generation tactics were used such as economic violence, political violence and decentralized battles of small unorganized groups against state actors such as militaries.
- February 16th, 1992- Hassan Nassralah takes the role of Hezbollah's Secretary General. Hezbollah, a Shia islamist group classified by most european and arab countries as a terrorist organization, is a modern example of 4GW.

  Its acts of sporadic terrorism, propaganda and mental fight are all features of 4GW.

Figure 1: Hamas Soldiers.

- 2006- Marine Corps Colonel Thomas X. Hammes expands the concept of 4GW in his book "The sling and the stone".
- March 20th, 2003-2011- A war between American and Iraqi forces commences in Iraq. Started as a result of US forces invading Iraq, 5GW had a big presence in the war.
- 2016 - Russian president, Vladimir Putin attempts to interfere with the elections in the United States. In the 2016 elections, the 2 main candidates, Donald Trump and Hilary Clinton ran for office. Putin, who favored the republican candidate, orders a plan to boost Trump's campaign and cause enticement in the US.

## Fourth Generation Warfare (4GW)

### What is 4GW?

Fourth generation warfare is a type of warfare that emerged in the Cold War era, and is defined as warfare combining economic, political and social war.

Typically, it is an asymmetrical battle- one party is a violent non-state actor (VNSA), while the other party is a state. The VNSA might use military tactics against the state to achieve their goals; however, 4GW is specifically characterized as a warfare employing moral and mental means to reach the goal.

Another feature of 4GW is decentralized warfare, as opposed to organized groups, in previous warfare generations. Often, the VNSA is unorganized, and multiple small groups engage in combat, something that poses a challenge on one hand, and a disadvantage on the other hand.As these groups are not unified, and lack great power, strong leaderships might be able to neutralize their threats, and cause them to turn against each other. With that being said, a lack of a clear vulnerability impedes on the ability to fight against a specific target.

In the 21st century, warfare categorized as 4GW has been utilized in many conflicts, uprisings and events involving both states and non-state actors.

There are three main aspects to 4GW:

1. Political aspect - One 4GW strategy is the use of political warfare in order to weaken a government, push it to the side and force it to comply with demands, or rather acquire influence and political power. One prime example of such actions can be found in Lebanon. The structure of the Lebanese Parliament was formed after the Civil War in order to ensure that all ethnic minorities in Lebanon are proportionately represented in the Parliament. Nonetheless, Hezbollah, a Shiite group backed by Iran has gradually succeeded to penetrate into Lebanese politics, and is now an inseparable and highly influential part of the country's leadership. Hassan Nasrallah, Hezbollah's Secretary General is a more powerful and influential figure than the president of Lebanon.
2. Economic aspect - parties may choose to act against each other by attempts to weaken the other side economically. The most famous attack is the 9/11 attack against the world trade center, which directly targeted a major financial hub. Another form of inflicting economical damage is through cyber-attacks that target economic bottlenecks, such as the cyber-attack committed against the Shahid Rajaee port, one of Iran's biggest seaports in May 2020.

3. Social aspect - In addition to military force and economic and political war, non-state actors also act in the social arena. This can be done through social media, or protesting. This type of warfare aims to cause backlash and criticism against the enemy state. In addition, the non-state actor may cause a controversy which can split a nation into multiple positions, which will force the state to deal with at least two fronts, the security front and the social one. One example of such tactics is the leaking of videos portraying the abuse of prisoners inside Iran's Evin prison and their dire living conditions, in August 2021 by an Iranian opposition group called "Ali's Justice".

## Fifth Generation Warfare (5GW)

5GW is as of yet unequivocal in nature. Right now, there is no generally settled upon definition for 5GW. It is likewise signified as Unrestricted, or Open Source Warfare. Despite that, this structure is quickly making more and more appearances in today's world. When and how did 5GW begin? According to the meaning of Non-Contact Warfare, it would make sense that annihilating a particular objective without a human seeing it is the best definition. In the event that this supposition that is right, 5GW procedures began with long-range

gunnery and maritime gunfire utilizing rifled-barrel weapons.

But actually 5GW became a well-known phenomenon only after the 9/11tragedy. It is characterized as the utilization of "all means at all" does in fact mean what it says which means using measures that do and don't involve military force, or arm power or even loss of lives at all - to compel the foe to serve one's own advantage. Its first recognizable appearance happened in the United States during the events of 2001.

September 11th attacks on the world trade center, 11/9/2011

Lately, military masterminds have been centered around "fourth-age" fighting – that is, clashes over thoughts. Contrast that with industrialized "third-age" war battled by customary armed forces over land and assets. The U.S. and what's more, US Allies are as of now proficient at 3GW and have developing capacities in 4GW. 5GW is new but is now in full power after Russia is credited with the primary coordinated execution for an enormous scope.

What is 5GW? As per Marine Lt. Col. Stanton Coerr, "The battlefield will be something strange – cyberspace, or the Cleveland water supply, or Wall Street's banking systems, or YouTube. The mission will be instilling fear, and it will succeed". Fifth era fighting is an endeavor to achieve vital goals using publicity and data assault vectors. It's completed by obscure entertainers for obscure reasons. Regardless of whether the center adversary is recognized, the casualty country cannot comprehend the reason or ultimate objective. The space in which 5GW is done is as of yet advancing and because of the casualty association or country being ignorant of the where, why, and how; it's impractical to counter until hurt has effectively been caused.

## Fighting 5GW

Battling 5GW can be described as counterinsurgency. Counterinsurgency exchanges the philosophical and ethnic insights made by 4GW, breaking the social connection between non-state entertainers/agitators and the overall population. The counterinsurgent should drive cultural change, focus on the social upsides of

extremists and everybody, battle on a scholarly level, and deny agitators a foe to battle against delivering it unimaginable for the general population and radicals to recognize the counterinsurgents' goals. These strategies structure a non- hostile connection among counterinsurgents and individuals; therefore, it ensures regular folks' prosperity and endurance.

Counterinsurgency makes a place of refuge, well known security and agreeable characters. Be that as it may, strangely this counterinsurgent association adds to the reliance of the populace on counterinsurgents. Accordingly, states must rather oppose this neo-colonial government of forced viewpoints in forming belief systems with expectations of settling every political matter.

## Current Situation

In the 21st century, 4GW has evolved into what is called the fifth generation warfare (5GW), and many ongoing conflicts fall under this type of warfare because the 5GW only added additional methods (such as cybercrimes)

### Iraq Conflict (2003)

President George W. Bush declared the end of serious combat in Iraq on May 1, 2003.

While most Americans were overjoyed by the news, historians recognized that it just meant the easy part was finished.

Peace did not break out in the months that followed, and the troops did not return home.

Iraqi rebels have retaliated forcefully.

Every day, instead of tranquillity, Americans read of the death of another soldier, car explosions and civilian deaths.

A sequence of explosives struck a police academy graduation ceremony, the Jordanian Embassy, and the United Nations (UN) headquarters in Baghdad just

three months later, in August. Mohammed Bakr al-Hakim, leader of Iraq's supreme council for Islamist revolution was assassinated, and the Baghdad chief of police was targeted. The anti-coalition campaign began with these attacks.

Another fourth-generation conflict has broken out in Iraq.

At the same time as the situation in Iraq was deteriorating, the situation in Afghanistan was deteriorating into a fourth-generation conflict.

While al Qaeda and the Taliban did not openly assault US forces, they were working hard to destabilize the US-backed Hamid Kharzai administration.

Attacks on and threats against oil pipelines in Iraq are both economic and political in nature. By boosting the price of oil, the rebels imposed a tax on the whole global economy. They expected that such attacks would destabilize the Iraqi government while also putting economic and political pressure on the US.

This reflects the essence of 4GW- largely a political, social and economic war rather than a military based one.

Fourth-generation warriors exploit international, transnational, national, and subnational networks politically for their own purposes. A growing variety of international platforms are available: The United Nations, the North Atlantic Treaty Organization (NATO), the World Bank, the Organization of Petroleum Exporting Countries, and dozens of others. Each organization has a different function in international affairs, but each has its own vulnerabilities and can be used to convey a political message to its leadership and then to target capital cities.

While these international organizations may not be able to directly influence national leaders' decisions, they can be utilized to slow down or halt international action.

The primary goal of 4GW is to cause political damage and paralysis in a target state.

## The Challenges and Difficulties of 4GW and 5GW

One of the biggest worries of both DISEC command and the fruitful activities of outfitted NSAs is the progression of deadly implements. Since the parties fighting are not states and don't act appropriately, their acquisitions of arms are typically attached to illegal channels making their control and guidelines progressively troublesome.

Hoping to address demobilization, the United Nations supported the Arms Trade Treaty in 2013 to assist with setting up a more widespread guideline of lawful arms exchanges, known as the white market. Notwithstanding, the arrangement needs global cooperation, and because it is non-existent, many arms exchanges are left unregulated. While NSAs regularly can't finish exchanges on the white market, they can in a roundabout way supply themselves through assaulting reserves and state ordinances that rely upon it. In Sierra Leone, an awry assault brought about the mass striking of an UN Peacekeeper store in light of the fact that the UN powers were told not to draw in with NSAs. This brought about the Revolutionary United Front procuring AK-47s and projectile launchers from arms bought legitimately by UN related operations.

While worldwide guidelines have been slow, there has been more accomplishment with local activities like ECOWAS, the Economic Community of West African States, which has set up drives on arms libraries and ordered shows on little arms and light weapons use. Neither of these arrangements have ensured a good outcome with numerous unlawful exchanges till staying undocumented; nonetheless, it mirrors the effective endeavors that can result through joint effort with other states.

As it stands, recorded arms exchanges with NSAs are low, mirroring that a greater part of their armaments are the result of unlawful exchanges, the bootleg market, or through legitimate state arms purchases that are then illegally offered to assailant gatherings, the dark market.

Furthermore, internal state disturbance can frequently dominate the capacity of the public authority to address NSA dangers inside their state. This strife can regularly be attached to focused on social or ethnic ties like in Kenya, a state with partitioned ethnic gatherings, where recently, President Mwai Kibaki has felt free to choose whatever number of officials from his ethnic gathering he could, isolating the state services and diminishing their capacity to focus on human security endeavors.

The decentralized and portable nature of NSAs further confuses hilter kilter clashes. The gatherings control huge areas of land that frequently get over boundaries and range locales that would be hard for numerous countries to get.

Alluding back to the Boko Haram case, the complete space of the three states with Boko Haram's essence is multiple times the size of Switzerland with the timberland where the student prisoners were taken to being double the size of Belgium. Besides, the lines of these states, in the same way as many others, are inconceivably permeable with the Nigerian Immigration Service recording upwards of "1,487 unlawful courses into Nigeria and 84 ordinary courses."

Lastly, the capacity of NSAs to participate in the struggle in one state and afterward retreat into another adjoining state makes an extra obstruction. These gatherings are consequently ready for additional perseverance because of their capacity to take advantage of the standard of worldwide sway which keeps a state from following these gatherings across borders without endorsement from the adjoining state.

A last snag to think about while countering hilter kilter clashes is NSAs that might seem disordered however really have solid frameworks of administration. These organizations regularly address regulated contentions and produce "complex informal communities, preparing projects, and supply lines or material sources." When combatting NSAs, nations frequently disregard the spot in the public arena that the gathering fills and the requirements it meets.

To address this new period of battle and contain continuous dangers, governments need to address the fundamental worries that are sustaining support inside the general population. While factors eventually differ on a situational premise, the proceeding with truth is that except if these obstacles are tended to, the unbalanced struggle will continue. For a state to really comprehend their enemy, they need to allude back to the verifiable setting and comprehend the manner in which it impacts current plans.

## Questions to Consider:

- How does 4GW and 5GW look in your country?
- What is your country's position concerning the use of the 4th and the 5th Warfare in your country/region/ globally?
- Were there any conflicts related to these that involved your country?
- Do the consequences and flaws of 4GW and 5GW outweigh the benefits and innovation?
- Do the consequences and flaws of 4GW and 5GW outweigh the benefits and innovation?
- Why was 4GW and 5GW invented in the first place?
- Which examples of these can the world see nowadays?
- How would the world look without cyber, economic, social and political war?
- How will warfare look in the future? Why can your country predict this development?

## Bibliography

1. Aaron Karp, Regina Karp. "Global Insurgency and the Future of Armed Conflict: Debating Fourth-g." *Taylor & Francis*, Taylor & Francis, 4 Sept. 2007, www.taylorfrancis.com/books/edit/10.4324/9780203089279/global-

insurgency-future-armed-conflict-aaron-karp-regina-karp-terry-terriff?refId=e091fad0-925e-41a0-bd56-0076ca163296.

2. Arentsen, Jonathan. "Asymmetrical Warfare- Background Guide." *Squarespace*, static1.squarespace.com/static/5705469907eaa06209c4dab3/t/5e0abf1f9df9c819e0d3a44c/1577762594330/DISEC-editable.pdf.
3. "Fourth- and FIFTH-GENERATION Warfare: Technology and Perceptions." *Fourth- and Fifth-Generation Warfare: Technology and Perceptions - San Diego International Law Journal - School of Law - University of San Diego*, www.sandiego.edu/law/academics/journals/ilj/?_focus=3225.
4. "Fourth-Generation Warfare." *Wikipedia*, Wikimedia Foundation, 24 July 2021, en.wikipedia.org/wiki/Fourth-generation_warfare.
5. "Generations of Warfare." *Wikipedia*, Wikimedia Foundation, 17 July 2021, en.wikipedia.org/wiki/Generations_of_warfare#First_generation.
6. Qureshi, Waseem Ahmad. "Fourth- and Fifth-Generation Warfare: Technology and Perceptions ." *Digital.sandiego.edu*, digital.sandiego.edu/cgi/viewcontent.cgi?article=1293&context=ilj.
7. Staff, Superesse. "Fifth Generation Warfare - How We Have Already Entered an Ambiguous Wwiii." *Superesse*, 15 Apr. 2021, www.superessestraps.com/blogs/news/fifth-generation-warfare-how-we-have-already-entered-an-ambiguous-wwiii.
8. Yumpu.com. "E-Book Download the Sling and the Stone: On War in the 21st Century Full Description." *Yumpu.com*, www.yumpu.com/en/document/read/63744001/e-book-download-the-sling-and-the-stone-on-war-in-the-21st-century-full-description.

# Topic B: Targeting the Illicit Arms Trade on the Dark Web

## Important Terms

- World Wide Web - an information system where documents and other web resources are identified by Uniform Resource Locators, which may be interlinked by hyperlinks, and are accessible over the Internet.
- Surface web - The Surface Web is the portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines (Google Chrome, Firefox, Edge, etc). It is the opposite of the deep web, the part of the web not indexed (searchable) by a web search engine
- Deep web - The deep web, invisible web, or hidden web are parts of the World Wide Web whose contents are not indexed (searchable) by standard Web search engines. This is in contrast to the "surface web", which is accessible to anyone using the Internet
- Dark web - The dark web forms a small part of the deep web, but requires custom software in order to access its content such as TOR (Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication - it enables its users to surf the Internet, chat and send instant messages anonymously and is used by a wide variety of people for both licit and illicit purposes). Identities and locations of dark net users stay anonymous and cannot be tracked due to the layered encryption system. The dark net encryption technology routes users' data through a large number of intermediate servers, which protects the users' identity and guarantees anonymity.
- Cryptomarket - Online marketplace on the hidden part of the web that has been intentionally hidden and is inaccessible through standard web browsers. It sells illegal drugs and other goods (such as firearms) and

services and customers can search and compare products and prices across multiple vendors.

- Silk road - The first large anonymous online cryptomarket located on the dark net. It was founded in 2011 and was shut down by the FBI in 2013. Several weeks after the taking down of Silk Road, Silk Road 2.0 was launched, which is why the former is also referred to as Silk Road 1.0 or SR1.
- Administrator - The administrator sits 'at the top of the crypto market hierarchy 'and within this role has 'full access to the cryptomarket'. The administrator has an executive and managing role on the marketplace, is responsible for the policies on the marketplace, and fulfils the role of treasurer with regard to cryptocurrency

## Background to the Topic

The average person using the internet uses the surface web, which accounts for about only 4% of what the World Wide Web holds. The rest of the World Wide Web is the Deep Web, which covers anything that regular search engines cannot detect (regular search engines like Google Chrome or Firefox). However, within the Deep Web lies the Dark Web, an intentionally hidden portion of the Internet plagued by criminal activity. The Dark Web itself is not inherently illegal; in fact, the platform has multiple benevolent purposes. Journalists in hostile territories utilize the Dark Web to report on politics, and it acts as a safe haven for many whistle-blowers and political dissidents. In fact, almost 2 out of 3 reported Dark Web users are there for casual and legal use. However, the same anonymity that aids these parties for good purposes has also made the Dark Web useful for illegal activity.

In this committee, we will be focusing on one illicit activity on the Dark Web - the arms trade in the dark web. Governments around the world are already combating illicit marketplaces that sell these arms. However, for each site taken down, a new one emerges, making it extremely difficult for law enforcement to fight this issue.

While it should be noted that the sale of arms on the Dark Web makes up a small percentage of global illegal arms sales as a whole, its convenience and anonymity have sparked exponential growth in recent years and threaten to only multiply in the near future. Arms trade enables armed violence which leads to many human rights violations. In order to protect citizens in all countries in the world, delegates must find a way to combat this market.

## History

July 2001 — The 2001 UN Programme of Action to Prevent, Combat, and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (PoA) is adopted by UN member states. The PoA contains regional, national, and global commitments to combat the illicit trade in small arms and light weapons.

November 23, 2001 — The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is adopted. It is the first international treaty focusing on crimes committed via the Internet and other computer networks.

September 20, 2002 — The Onion Router (Tor), a private Internet browsing network, is created by computer scientists Roger Dingledine and Nick Mathewson. The project is primarily funded by the U.S. Naval Research Laboratory, which hopes to facilitate safer communication with intelligence sources across the globe.

July 3, 2005 — The Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts, and Components, and Ammunition (Firearms Protocol) officially enter into force. It is the only legally binding instrument to counter the illicit trafficking of firearms at an international level.

2006 — The Tor network is re-launched as a non-profit organization titled "The TOR Project" in order to help manage the platform as its popularity rises.17 Tor is a software that relays users' and websites' traffic through thousands of servers,

thus making Tor users essentially untraceable and anonymous; Tor has been widely used to access dark websites.

2009 — Satoshi Nakamoto founds Bitcoin, a form of cryptocurrency that will soon become the primary source of digital currency utilized on Dark Web markets.

February 2011 — Silk Road is founded and launched by an individual under the alias of "Dread Pirate Roberts;" (DPR) it is the first modern dark net marketplace to be brought into existence and dominate the competition for the widespread sale of illicit items and services on the Dark Web.

October 2013 — The FBI seizes and takes down the Silk Road.

December 24, 2014 — The Arms Trade Treaty (ATT) officially enters into force. The UN treaty aims to regulate international trade in conventional arms, including small arms, battle tanks, combat aircraft, and warships. The ATT does not impact a state's domestic gun control laws or other firearm ownership policies.

July 20, 2017 — Two major law enforcement operations, led by the FBI, the U.S. Drug Enforcement Agency (DEA), the Dutch National Police, and the European Union Agency for Law Enforcement Cooperation (Europol), successfully seize and shut down Dark Web marketplaces Alphabay and Hansa (Operation Bayonet).

## Current situation

The rise of scamming, heightened policing, and low volume of weapons sales on the dark web has spread caution in the dark web community, if not widespread doubt, about the viability of using dark web marketplaces to buy weapons on the dark web. Yet, recent cases documented by governmental agencies or reported by the media suggest that dark web arms trafficking is a real phenomenon.

Today, weapons are still offered on a number of cryptomarkets and purchased by individuals.

There are three different high-level contexts relevant to dark web-enabled arms trafficking: terrorism, organised crime and vulnerable or 'fixated people'. All these cases contain instances of individuals or groups, albeit with differing intentions, that have purchased or sold firearms on the dark web or attempted to do so.

It is important to note another product on the darknet that relates to this topic, guides and tutorials that teach the customer how to turn replica/alarm guns into real weapons, or even 3D print a working weapon.

## So How do Darknet Markets Work?

### Cryptomarkets

Cryptomarkets are a part of the dark web. They can be compared to Ebay or Amazon for illegal goods. They bring together sellers that are called vendors, and create a market. That market is managed by the administrators of the cryptomarket and in return the administrators take commissions on sales. Cryptomarkets also provide third-party services that afford a degree of payment protection to customers, (using a system in which the vendors only get paid after the customer gets the product, by having the cryptomarket as a middleman holding the money until the customer confirms they received the product) and a third party dispute adjudication. Cryptomarkets use cryptocurrency (such as Bitcoin, Ether, Litecoin) for payment and let the customers rate the vendors with scores which are displayed on the marketplace to help customers select reliable vendors and avoid scams.

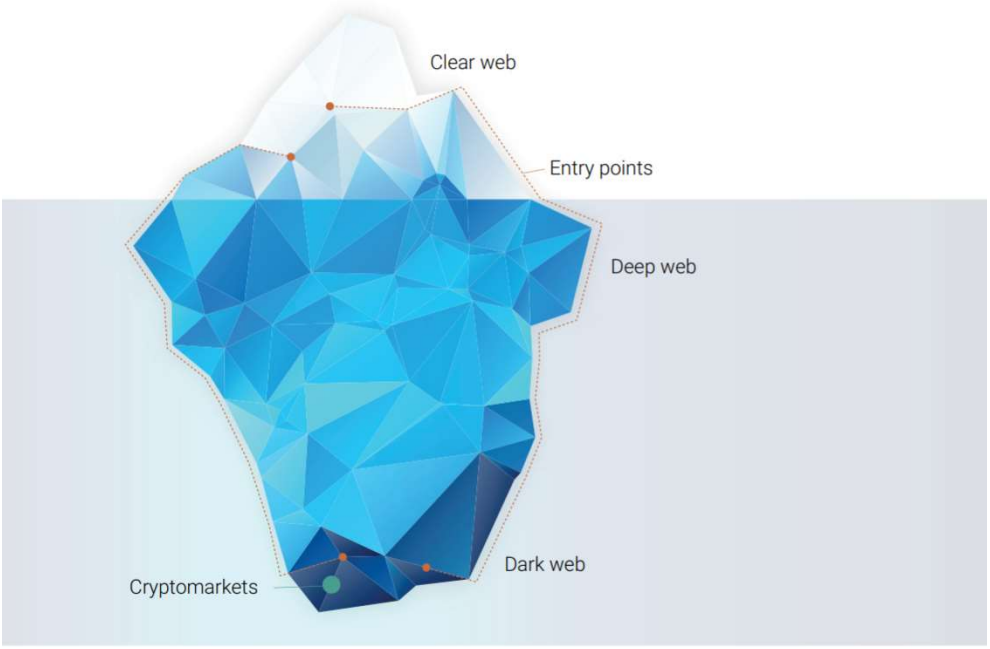



Figure 1: The location of clear, deep and dark webs, and cryptomarkets.

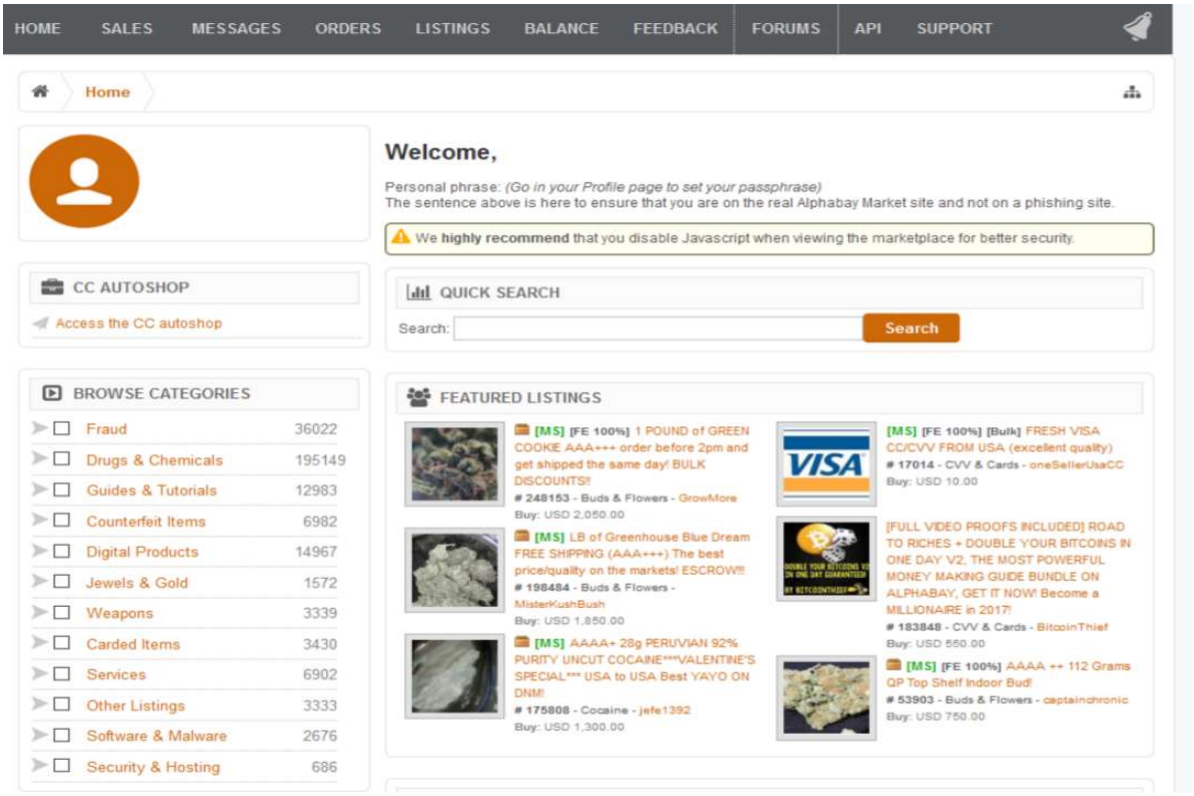



Figure 2: Homepage of a cryptomarket.

## Vendors

Vendor shops are set up by a vendor to host sales for that vendor alone. These vendors sell directly to customers willing to make purchases without the third-party services provided on cryptomarkets. This way they don't need to pay commissions on their sales to cryptomarkets. Vendor shops specialise in particular products or services, and often trade on reputation track records earned via cryptomarket selling to generate customer trust. Many vendor shop owners trade simultaneously on cryptomarkets.


Figure 3: Home page of a Vendor shop.

## Trust Between Vendors and Customers

When you buy things on EBay, you always have the risk of being scammed, getting a bad product, or paying without getting the product. Customers on the Darknet carry a lot more of such risk in every transaction. For that reason, cryptomarkets created a scoring system for the vendors on the cryptomarket - previous buyers can rate and give feedback to the vendor. The score and feedback are presented to other potential buyers, just like legitimate business. With that being said, customer feedback isn't a perfect guide for potential buyers. Vendors can manipulate their feedback by creating fake customer accounts through which

to make purchases from themselves, thereby generating false feedback. Marketplace administrators generally have rules that prohibit scams (if scams on the cryptomarket become common, it harms the cryptomarket's reputation, which leads to fewer customers, which results in less profit for the administrators); but it is impossible to eliminate them completely. Buyers can also consult the 'scam reports' sections of marketplace discussion forums, which alert them to vendors with unresolved or confirmed accusations of scamming. In the context of firearms vendors operating on cryptomarkets, the low volume of sales – compared to the high volume of sales by drug vendors – yields a reduced opportunity to get feedback from buyers.

Surprising as it may be, vendors have concerns about scams from their customers as well. A buyer having received an order may claim otherwise. Vendors' stated refund and reship policies illustrate the risk to profit entailed by parcel loss must be accepted to keep customers happy and continue to generate positive feedback. To prevent this, vendors have a number of strategies at their disposal. First is to choose their buyers - just like buyers can access the vendor's reputation metrics, the vendor can access the potential buyer's purchase history and choose to avoid customers new to the marketplace, or refuse to sell to those with disputes associated with their transactions. A second way is to ask buyers to pay without escrow protection; thus, the vendor can be paid up front. Third, a vendor can specify a refund and reship policy according to the buyer's purchase history. For example:

- ``We have good stealth, and have not had any orders not received. We know it is unlikely but if it happens, we will check your past stats and if they're good, you can choose 100% reship or refund.:
- 'Refunds: 50% of the price, but 75% refund for regular buyers. Customers with < 10 successful buys will get NO refund.'

- 'Reshipping only to folks with five or more previous buys and no returns. I will never ask you to finalise early, but please release the coins to me as soon as you receive the shipment. Fair's fair.'

To conclude, the main pillar holding together these vendors is trust between the vendors and the buyers.

## The Subject of Payment

While there are similarities between purchasing things on the clear web and the darknet, like choosing a product they wish to purchase, and clicking the familiar 'Buy now' button on the product listing page. Similarly to purchases on legal clear web shops, buyers must register with the marketplace and have sufficient funds to complete the purchase. One difference between clear and dark web markets is the form of payment. On dark web markets, payments are made with cryptocurrencies (Bitcoin, Ethereum, etc.). Transactions made using cryptocurrencies are not necessarily linked to the real-world identities of buyers and sellers, and this makes it difficult for law enforcement to trace illegal transactions. Obtaining cryptocurrency is the trickiest part of dark web purchasing. In addition, buying cryptocurrencies to make illicit purchases, or selling them to 'cash out' into local currencies, creates additional security risks for users. Having obtained sufficient funds in a cryptocurrency accepted on a cryptomarket, the buyer initiates a transaction by clicking 'Buy now'. However, payment is not immediately received by the vendor, but instead held in deposit by the marketplace, known as payment escrow. The vendor then packages the product and ships the parcel via postal services or private courier company. Once the order is received and the buyer is satisfied, the buyer returns to the marketplace to 'finalise' the order, at which point payment is released by the marketplace from escrow and transferred to the vendor's account. In this way, escrow provides protection for the buyer: if an order is not received or the product is not as advertised, the buyer declines to finalise the purchase, and the

vendor is not paid. Some cryptomarkets now support multi-signature escrow transactions that require sign-off from two out of three parties – the buyer, the seller, and the marketplace itself – to release funds. Unlike the traditional, centralised escrow, it is impossible for one party alone to retrieve payment.


Figure 4: Overview How the escrow service provided by the cryptomarkets operates from left to right.

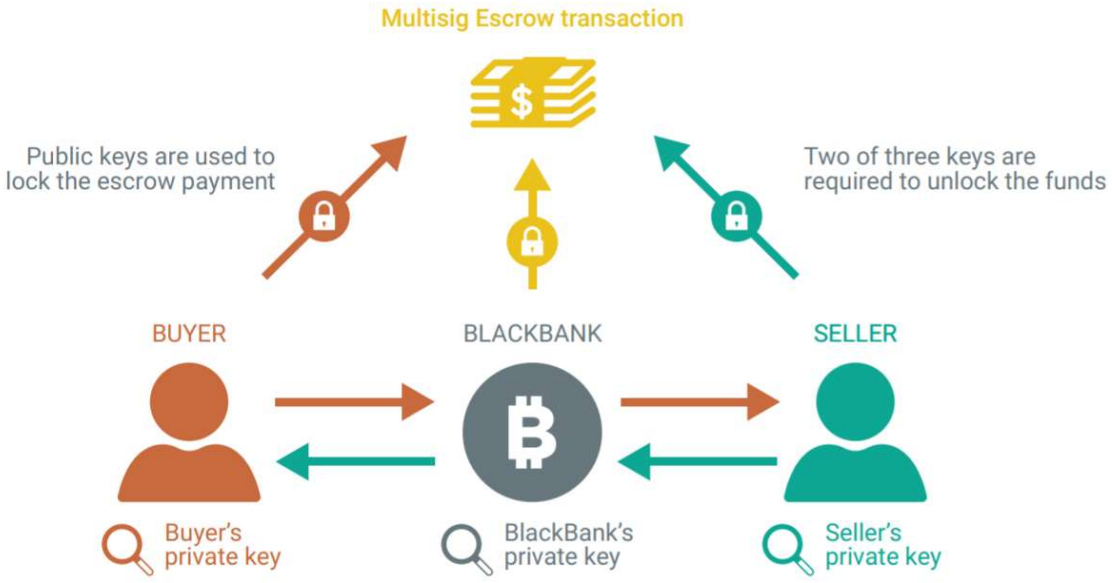



Figure 5: Overview of how the multi signature escrow service provided by the cryptomarkets operates

## The Physical Transaction

For physical products (ammunition and weapons), vendors must rely on postal services to ship orders to customers. Dark web markets provide vendors with an

opportunity to transact with customers across a wider geographical reach than is possible with conventional illegal markets, and the postal system is an enabler in this process. Recent research suggests that cryptomarket users identify these 'offline' activities of dark web transactions as the primary source of risk of detection and apprehension by law enforcement. For vendors, these activities include sourcing packaging materials and making drop-offs into postal systems. For buyers, receiving deliveries is identified as a risky aspect of cryptomarket purchasing

## Possible Solutions

It is important to understand that the dark web does not produce new weapons; it merely acts as an enabler of trafficking, with weapons and ammunition having to be shipped and delivered in the 'real world'. Therefore, good traditional policing and investigative techniques will remain vital in responding to this threat. In addition, traditional firearms control measures designed to tackle illicit trafficking remain of the utmost importance to reduce the availability of illegal firearms. These include efficient marking and record keeping practices, international cooperation for tracing, and good stockpile management.

Seeing as trust between buyers and vendors is crucial for a successful deal, breaking that trust between buyers and vendors can frighten potential customers from getting scammed thereby reducing the size of the market.

Arresting the administrators of the cryptomarket will help close the cryptomarkets, and since new cryptomarkets are less trusted by customers it will reduce the scope of the market.

As chairs we ask you, please try to bring your own ideas about how to target the illicit arms trade on the Dark Web, and think of the specifics. It is highly recommended both for your enjoyment and winning in the MUN.

**And remember, you speak, propose and act from your country's position.**

## Questions to Consider

- What is the legislation in your country regarding the dark web, cryptomarkets and arms trade both from the dark web and in general?
- To what extent does cryptocurrency play a role in the Dark Web?
- How can legislation against the illicit arms trade on the dark web benefit your country?
- What are the positive effects of the dark web?
- How common is illicit arms trade on the dark web in your country?
- What are the global effects of illicit arms trade on the dark web?
- What are the effects in your country that are caused by illicit arms trade on the dark web?
- What is the exact international legislation against illicit arms trade on the dark web?
- How can the illicit arms trade on the dark web be stopped or at least reduced to a minimum?

## Bibliography

https://medium.com/@SmallArmsSurvey/beyond-the-dark-web-arms-trafficking-in-thedigital-age-56ddd806587a.

"Dark Web Becomes Huge Market for Weapons Trade | Business Standard News."

Business-Standard, April 21, 2019,

*"Dark Web Plays Growing Role in Illegal Arms - Economic and Social Research Council."

Economic and Social Research Council,

https://esrc.ukri.org/news-events-and-publications/news/news-items/dark-web-playsgrowing-role-in-illegal-arms/.

*"Darknet Market Definition." Investopedia,

https://www.investopedia.com/terms/d/darknet-market-cryptomarket.asp.

*Davis, Clayton. "Addressing the Challenges of Enforcing the Law on the Dark Web | S.J.

Quinney College of Law." S.J. Quinney College of Law, December 11, 2017,

https://law.utah.edu/addressing-the-challenges-of-enforcing-the-law-on-the-dark-web/.

*Kumar, Aditi, and Rosenbach, Eric. "The Truth about the Dark Web." IMF,

https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-

https://www.rsa.com/en-us/blog/2016-02/role-tor-cybercrime.

*"Understanding the Trade in Small Arms and Light Weapons on the Dark Web – UNODA."

United Nations,

https://www.un.org/disarmament/update/understanding-the-trade-in-small-arms-and-lightweapons-on-the-dark-web/.

"UNODC Study on Firearms 2015." United Nations Office on Drugs and Crime, 2015,

www.unodc.org/documents/firearms-protocol/UNODC_Study_on_Firearms_WEB.pdf.