CALTRAIN'25

GENERAL ASSEMBLY

FIRST COMMITTEE

DISEC GUIDE

Agenda Item: Regulating the use of emerging military technologies in modern warfare

Academic Assistant: İbrahim Ege Ekiz

Table of Contents

1. Letter from the Secretary Generals:

Esteemed Participants,

As the Co-Secretary-Generals of Cağaloğlu Model United Nations, it is our distinct honor to welcome you all to the 2nd edition of CALTRAIN, which will take place on December 6th and 7th, 2025. It is with great pleasure that we present the study guide for DISEC, which aims to equip you with the essential knowledge and context for the upcoming two days. After months of preparation and dedicated effort, we are proud to say that we are now just one step away from CALTRAIN 2025. We hope that, by reading this guide, you will feel as ready and enthusiastic as we are. Without a doubt, this conference would not be possible without the contributions of our remarkable academic team. We are extending our gratitude to our Head of Academy, Azra Kayar; our Heads of Crisis, Ahmet Taha Özkul and his deputy Elif Köse; our devoted and hardworking team members; and our motivated trainees. Their commitment and passion have brought this vision to life and elevated CALMUN's academic quality to its peak. Furthermore, I would also like to extend my best wishes to all delegates participating in CALTRAIN 2025. Whether this is your first conference or not, we thank each of you for taking a step forward and joining us. We truly hope that CALTRAIN will be a special experience that you will remember warmly in the future. From our perspective, MUN is about motivation, enjoyment, meaningful discussion, and connection. We wish each delegate an inspiring, engaging, and memorable experience.

Warm regards,

Meryem Sultan Çok, Akay Engin

Co-Secretary-Generals of CALTRAIN'25

2. Glossary:

Artificial Intelligence(AI): Artificial thinking models consisting of a set of logic networks that replicate human thinking and learning patterns and mimic the functioning of neurons. This technology is frequently used to solve problems created by multivariate problems, particularly those requiring strategies based on variable circumstances. The throughput of an artificial thinking model depends on the processing power available to it and the quality of the training strategy. If you improve these two parameters positively, you will create a machine that can solve problems only humans can solve at speeds impossible for humans.

Bot: Software robots that work according to the logic chains of the codes written within their structure. Because software is a virtual product, bots are much easier to copy and mass-produce than other products. Bots can also be used as cyberwarfare tools through methods such as overloading servers.

Cyber: Umbrella term for concepts related to computers and the virtual world. One of the most critical characteristics of cyberspace is that everything it contains is actually a combination of many datasets. Because datasets can be manipulated, they are vulnerable to any cyberattack.

Cryptography: The branch of science that combines the fields of mathematics and computers, including methods of encrypting something and decrypting it. A significant portion of encryption methods today are based on prime numbers and the prime factorization of very large numbers. This method, called RSA, traces its origins back to the British during World War II.

Drone: Aircraft that do not have a crew or pilot, are remotely controlled or operate in automated mode, and are generally cheaper and smaller than airplanes. Drones are emerging as an alternative to expensive and, in some cases, overly destructive fighter jets. Drones are capable of shooting down aircraft on their own, as well as drones that are very small but still possess high destructive power relative to their size.

3. Introduction:

As technology advances, warfare naturally undergoes change. Unfortunately, the uncertain nature of change can sometimes lead to disasters caused by uncontrolled technologies. Managing and regulating such unstable technologies and ensuring their use under conditions that do not endanger civilian life or human rights is one of the DISEC committee's most important missions.

Technologies used on the battlefield today continue to repeat history with creating security challenges. However, these security challenges have characteristics that impact areas not previously seen. This has led to the need to impose specific restrictions on these technologies. Therefore, uncontrolled battlefields require DISEC oversight.

4. Overview:

It must be said that this decade has been an unfortunate one for peace. Humanity is witnessing many fronts around the world. Naturally, this state of low stability has resulted in a global desire for armaments. This desire, in turn, has led to the enrichment of sectors involving weapons and warfare technologies and the development of new technologies or the improvement of existing ones. As humanity, we are quite accustomed to this pattern, and to avoid military crises like those of World War II, we must prevent potential unfortunate futures by managing new technologies under international laws and restrictions.

To briefly list the highlights of these emerging technologies: drone technology, which makes air warfare cheap and difficult to detect; cyberattack technologies targeting the computational data models adopted by all current systems; and finally, psychological warfare methods resulting from the accessibility of media technologies to the world and nations.

Drone technologies emerged on the global agenda after 2015 and have become an indispensable weapon of air warfare since 2020. Drones are a cheap and effective combat force used by both terrorist organizations and the world's largest military forces. One of their most important characteristics is that they are completely unmanned aerial vehicles, making them the first choice for air units in high-risk operations. Another advantage is their

extremely low cost of production (compared to aircraft). Losing a drone may be a minor loss for a state, but losing an F-35 is a major setback. Their most notable features are their high portability and stealth. For example, with a simple intelligence operation, you can insert dozens of drones into your opponent's environment, giving you a massive advantage in the event of a war.

Cyber attacks are a military strategy that has been on the agenda for many years, but as time progresses, this method is becoming increasingly powerful in our increasingly virtual world. The best part of this attack method is that it almost never results in the loss of any soldiers or personnel. While it is a highly secure strategy, it is also highly damaging. One of the most popular features of cyberattacks is their anonymity. When a cyberattack is launched between states, it is often difficult to find evidence that would legally convict the attacking state, giving states the incentive to bend the boundaries of international law.

Psychological warfare is quite archaic compared to other methods of warfare. With a history of nearly 2,500 years, psychological warfare was once based on giving false signals to an opponent to gain a war advantage, but today, this ancient tradition has become virtually obsolete. Psychological warfare is now used to manipulate public opinion within states. For example, by publishing a news report exposing corruption in your opponent's country, you can create a crisis in the enemy country and gain a war advantage. However, we encounter far more radical examples in real life. Today, countries can go so far as to undermine democratic elections by manipulating the media, distributing fake news, and discrediting other countries' politicians. Psychological warfare methods, intensified by the globalized and virtual world, have reached a point where they undermine the democratic rights of citizens and clearly require regulation.

5. Major Operations and Leading Technologies:

When examining warfare technologies, there is a need to follow a different approach than the usual procedure. While examining the history of technology and the engineering path of its development will inform us about its potential, this approach is ineffective if we want to examine its impact on the world and its practical applications. Therefore, rather than focusing entirely on the technologies themselves, directing our primary focus to the history of operations will be more beneficial. While this approach is much more effective, there is a point worth mentioning: Since most of them are not open to the public, it is extremely

difficult to find documented sources examining operations involving modern technologies . Therefore, particularly in the areas of cyberwarfare and psychological warfare (due to the high levels of anonymity), the commonalities of operations will be examined rather than specific operations.

a. Major Drone Operations:

The United States is one of the pioneers of major drone operations in history. The United States frequently uses drones to eliminate targets in the Disposition Matrix, kill list for anti US parties. However, non-secession operations have also been conducted. Between 2004 and 2018, drone bombings by militants in Pakistan killed over 3,000 militants and nearly 1,000 civilians. The US particularly utilizes drones in intercontinental air operations. Another example of these operations is the shooting down of senior Al-Qaeda members by American drones while they were traveling to Yemen. Despite some success, these operations frequently end in tragedy. In August 2021, a drone strike in Kabul, Afghanistan, killed 10 civilians, seven of whom were children. Thanks to drones, the destruction of specific targets in countries separated by oceans has now become possible, and the number of civilian casualties associated with this purpose has also increased.

By the 2020s, drones had entered their golden age. With this rise, many scandals and problems began to emerge. The first of these scandals was when a Turkish drone equipped with artificial intelligence and carrying explosives accidentally struck the Libyan army. The incident was brought to the United Nations Security Council in 2021 and resolved. However, the ability of a drone to fire without command was a concerning technology. While these incidents were taking place, a curious trend began among drug cartels in Mexico. Cartels have now begun using drones in their execution operations. Another alarming development was the active use of this technology by even major criminal organizations. In 2020, Azerbaijan used drones as a highly effective war strategy against Armenia. Türkiye also used drones for border clearance during the Syrian war. Drones' ability to track the number of people killed played a crucial role in both propaganda and data analysis.

However, the 2022 Russia-Ukraine war took drone warfare techniques to a whole new level. As the war began, Ukrainian factories were put into a state of emergency. All production facilities in the country were used for drone production. Later in the war, information began to leak that Ukraine had purchased 200,000 drones. Using these drones, Ukraine neutralized a

large portion of Russia's air infrastructure. This operation initiated a competition between aircraft and drones for efficiency.

The most effective use of drone technology was observed during the Iran-Israel war. While drones are inferior to aircraft in terms of destructive power, they are considerably superior in terms of stealth. Israel's "Rising Lion" operation was essentially based on this principle. Once the necessary intelligence was provided, the Israeli air force was able to precisely destroy the most critical links in the chain of command. While the primary focus of this operation was, of course, gathering intelligence, operating beyond air defense systems is not feasible with massive aircraft, although some drones may present an exception.

b. Cutting Edge Drone Technologies:

To determine the regulations that will maintain drone validity and relevance over time, it is first necessary to understand the current state of drone technology. This requires examining some cutting-edge technologies that have not yet emerged but are still undergoing development and are quite promising. The most promising drone models in this area today are the Boeing MQ-28 Ghost Bat, the ShieldAI MQ-35A V-BAT, and the AM-FPV.

i. Boeing MQ-28 Ghost Bat:

The MQ-28 is a brand new model that made its first flight in March 2025. The MQ-28 presents a unique approach to drone technology that has not been seen before. We typically view drones as alternative flight forces deployed in risky operations due to its cheap production procedure. However, the MQ-28 shines with its defensive capabilities rather than its offensive prowess. It is a fully automated air support unit whose purpose is to strengthen the defensive capabilities of its partner aircraft. To put it more concretely, MQ-28s operate under a "mother aircraft," much like worker bees protecting the queen bee. The MQ-28 is equipped with advanced radar and enemy detection systems, transmitting the information gathered from these systems to the mother aircraft to which it is attached, allowing the pilot to be alerted to potential threats much earlier than they would otherwise be. While we have not seen the MQ-28 during test flights, many technicians indicate that this aircraft will be modeled to neutralize threats

targeting the mother aircraft. The MQ-28 is currently used as an active defense mechanism by passive aircraft like the E-7 (the E-7 is more of an intelligence aircraft than a fighter jet; it can be considered a flying radar), but the US and Austrians appear to have different plans for this technology. The ultimate goal is to make the F-35, which stands at the pinnacle of aircraft technology, invulnerable in the airspace by being supported by the MQ-28s. It is expected the MQ-28 technology to be put into active use towards the last quarter of 2026.

ii. ShieldAI MQ-35A V-BAT

There is a drone that takes the exact opposite approach to the MQ-28 drone that has been examined above: the V-bat, a tiny airborne giant. The V-bat is revolutionizing the drone industry not with its innovative ideas, but with its innovative design and the immense danger inherent in its small body. When it is examined the V-bat's most striking feature, it is obviously its unusual airframe. As shown in the photo, the V-bat is an upright drone and lacks any wheel mechanism. This feature eliminates the need for the aerial infrastructure required by conventional drones (which require a long, flat, and smooth path for takeoff and landing). By uprighting its body during landing, the V-bat can land and take off even in rural and mountainous areas. Another feature of the V-bat is its relatively small size. Drones are divided into five groups based on their size and power capacity. While the V-bat falls into groups 2 and 3 in terms of size, it falls into groups 4 and 5 (drone models nearly as large as aircraft) in terms of destructiveness and power. One of the reasons it can be so destructive despite its small size lies in the Hivemind technology developed by Shield-AI. This technology allows multiple V-bats to work together fully automated and operate as a unified entity. The V-bat's current use is as an aircraft to assist naval forces with attacks and information. While similar to the MQ-28 in this respect, the V-bat generally operates from a ship and specializes in information gathering and attack rather than defense.

iii. AM-FPV

The last two drones that have been reviewed were truly breathtaking machines of engineering and highly innovative ideas, but the AM-FPV is simply terrifying technology. When it comes to war, sometimes modern technology is irrelevant, because fast technology can provide absolute advantage. The AM-FPV is not a massive vehicle, but it is a very simple one. It lacks some of the features of the drones we mentioned above: no flight automation, no advanced radars, and no massive body (models larger than 30 cm are extremely rare). Its ability to fly for more than 30 minutes is nothing short of miraculous. But the AM-FPV is undoubtedly the pinnacle of drone warfare. This lies in its simplicity; producing an AM-FPV takes 11 minutes and is absurdly cheap. Despite this simplicity, it boasts a system capable of successfully performing bombing and reconnaissance missions. At the peak of mass production, this product surpasses all other technologies in the industry in a real-world war. This technology is the answer to how Ukraine destroyed Russia's air infrastructure in a single operation and accounts for 20% of Ukraine's military's offensive power. Let us consider a hypothetical scenario to add some meaning to the numbers and assume your enemy destroys one of your drones, typically in Group 4 or 5. Replacing this drone would take you a month, even in the fastest and most focused way possible. However, your enemy has invested in mass-producing AM-FPV drones and produces one every 11 minutes. By the time you replace your drone, your opponent will have 3,927 AM-FPV drones in their arsenal. There is one last technological obstacle to this drone technology becoming a definitive air force. If engineers can apply V-Bat's hivemind technology to these drones and minimize production time, we have an air force that no air defense system can compete with. This is truly alarming technology.

c. Major Cyberwarfare Operations:

Because cyberwarfare has a much longer history than drone technologies, there are numerous operations and experiences. However, if cyberattacks were the sole focus, these three countries would need to be examined:

The first of these countries is China. China leads the world in cyberwarfare. The continued existence of China-based private companies, in collaboration with the state, provides China with a stable and dense data flow. However, it would be completely wrong to say that China is content with this massive data flow. Since China's cybersecurity systems became established, it has invested in establishing units that exploit vulnerabilities in these systems to conduct intelligence operations. Nowadays, cyberattacks are a common occurrence for countries not part of China's bloc. Unfortunately, due to the anonymous nature of cyberattacks, proving the responsibility of a cyberattack in international courts is nearly impossible. This has transformed cyberattacks from an act of aggression into a weapon that allows states to terrorize each other. China, of course, is not the only country benefiting from this disarray.

Russia is one of the leading countries when it comes to cyber war. Most of Russia's major cyberattacks have targeted the Caucasus and Ukraine. Two historical operations have specifically targeted Ukraine. One involved locking down all government units and destroying data using an Excel-like application required by Ukrainian government departments. This operation was a resounding success and resulted in a serious crisis in Ukraine. Another targeted Ukraine's electrical system, causing chaos and power outages across much of the country. Russia's operations are among the best examples of how devastating a major cyberattack can be. A well-executed cyberattack is powerful enough to cripple a nation.

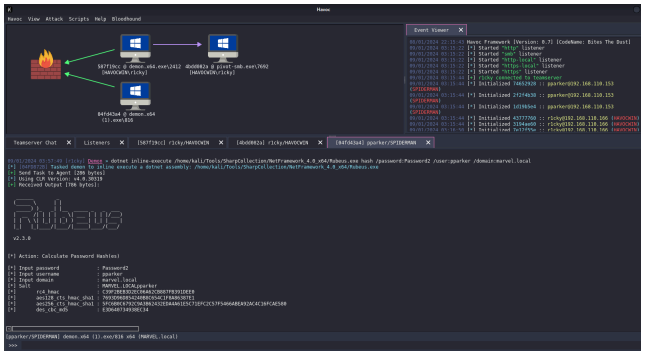
The United States also has a long list of entrenched operations throughout its history, but just two of these are more than enough to demonstrate how powerful cyberattacks can be. The first of these operations is quite primitive, dating back to the Cold War. It involved the Trojan horse, one of the most famous and classic viruses ever created. Thanks to this virus, the Americans gained access to Soviet chemical factories, causing a series of massive explosions. Despite all this chaos and damage, Soviet Russia never blamed the United States. Another major American cyberattack was directed at Iran. The US was able to destroy Iran's nuclear facilities on the ground with air units, but as a precaution, the Iranians constructed some underground nuclear facilities. This time, the Americans infiltrated these systems using

virtual means and sabotaged the facilities. This operation is a very clear example of cyberattacks. It is even possible to infiltrate and sabotage the underground facilities of countries separated by continents.

d. Cutting Edge Cyberwarfare Technologies

Human-powered cyberattacks were already a formidable revolution in warfare. However, cyberwarfare continues to develop and evolve at a much faster pace than any other warfare method. Especially with the use of AI in cyberattacks, vulnerabilities that would take days for the human eye to detect can be found and exploited in seconds. Three technologies pose serious threats to the cyber world today: AI-Powered Offensive Cyber Platforms (e.g., DarkRiver, HavocNet), Post-Quantum Cryptography (PQC), and Cognitive Electronic Warfare (CEW).

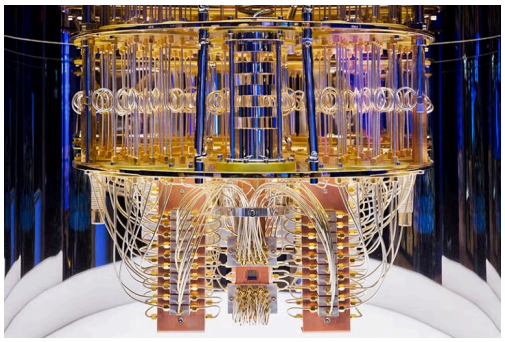
i. AI-Powered Offensive Cyber Platforms



When it comes to cybersecurity and attacks, the most vulnerabilities arise when a product is first released to service. These types of vulnerabilities are called “zero-day” vulnerabilities. Therefore, when a product under cyber threat is released to market, a race begins. Developers must develop a fix for potential vulnerabilities before hackers can detect them. Because there are generally many more feedback opportunities, the developer can perfect the system before the attacker. Even after this stage, there are many ways to enter the system, but all of these ways require a mistake from one of the developer's employees. Otherwise, once zero-day vulnerabilities are fixed, direct infiltration into the system will be impossible again. As you can see, this is essentially a race for speed. And history shows us that robots generally win the race for speed by overwhelming advantage. Therefore, hackers can infiltrate the system from day zero by training a specialized AI model to detect vulnerabilities. The problematic part is, once the system is infiltrated, it is almost impossible to detect it. Furthermore, even if a developer were to respond by training an AI model to detect vulnerabilities, it would fail because that model would also need to close the

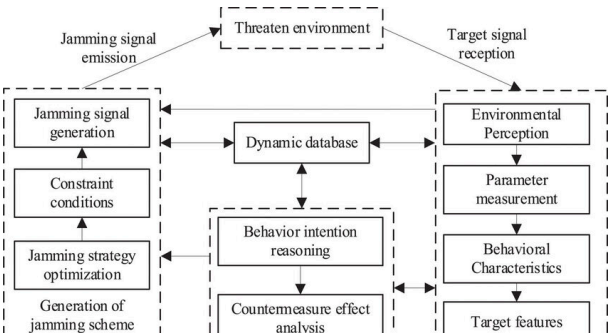
vulnerabilities in a way that would not harm the system. Naturally, the hackers' AIs often win this race. That is the nature of this technology.

ii. Post-Quantum Cryptography (PQC)



There could be some questions about the relationship between quantum computing and cyberwarfare. To understand this, understanding a bit of cryptography history is needed. Cracking passwords and stealing your opponent's information has been a critical aspect of warfare throughout history. However, when computers entered the stage of history, classical encryption methods became ineffective because passwords written using human calculations and codes can be broken in any way when the correct algorithms are used. There was a need for a secure system instead of a method that carries the risk of being broken. This requires a process that computers find very difficult: prime factorization of numbers. While this process is not a particularly challenging task for computers, its most critical feature is that the difficulty of this task increases dramatically as the numbers get larger. So, nowadays encryption is made using numbers that computers could not factor even for hundreds of years. The principle of this system will not nowbe explained since it is out of this guide’s scope, but anyone who wants to can explore the RSA method. Simply put, if you can quickly factor a number into its prime factors, you can break any password you want. There is no clever or alternative solution to this problem; the only solution is to build very, very powerful computers. When people think of powerful computers, they think of quantum computers, the pinnacle of this field. While they still cannot work properly, quantum computers are predicted to be able to factor even very large numbers very quickly. A country's ability to develop this technology to this point would give it an invincible and formidable advantage in cyberspace.

iii. Cognitive Electronic Warfare (CEW)



The cyber technologies that have been discussed so far have only covered

interactions within cyberspace, because interfering with physical/electronic assets from within cyberspace is a much more complex problem than it seems. Every device receives commands using an encrypted signal and then operates accordingly. Analyzing these signals, identifying which devices they belong to, and then attempting to control that device (which also requires analyzing the source code's interaction with the machine to be able to use it) is simply not something anyone could do on an active battlefield, even if they had an army of experts. Of course, this applies to humans, because it is essentially a speed problem, and as mentioned before, machines have a superiority over humans in speed. Therefore, if someone could develop an AI model supported by extremely high processing power and trained on very large databases over a very long period of time, this model could theoretically neutralize any remotely controlled, signal-activated electronic weapon. What has been described here is merely the basic idea of the CEW models currently under development. This technology is still fresh and new, having flourished as the AI sector has become a $100 billion industry, but it does not promise anything theoretically impossible. The biggest problem with this technology is that training such an AI requires performance beyond conventional methods. This is because there are no models developed on this subject in the past. However, successfully implementing this technology could be enough to disrupt the entire drone industry.

e. Modern Psychological Warfare Methods

This topic will be examined under the title of method because psychological warfare has become an extremely abstract concept these days. To identify the psychological warfare methods employed by one country against another, there would be a need to sit down for years and analyze bots, posts, the direction of mass opinion shifts, and which countries might benefit from these changes—they are endless. Therefore, except for very rare university studies, countries no longer directly aim to identify the sources of psychological changes in their public opinion. Instead, they focus on managing the consequences.

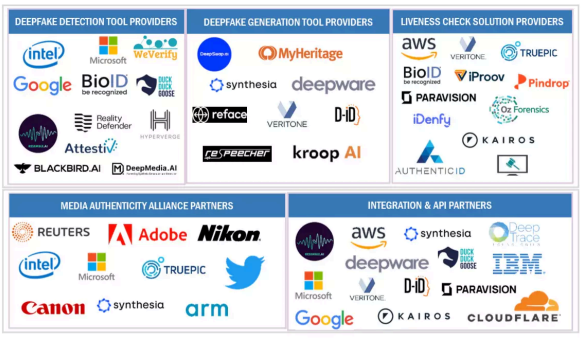
Let us give an example to make it clearer: Türkiye has a largely Muslim demographic, but upon closer examination, a much smaller portion of this Muslim segment is seen as radical . The conclusion this demographic analysis yields is that if a war broke out in the Middle East between two countries of different religions such as the Israel Palestine war, Türkiye would adopt a pragmatic stance. However, if you are an anti-Israeli Middle Eastern country, and you want a militarily powerful ally like Türkiye to support your cause against Israel, Türkiye

lacks the demographics to support this. Then you will need to implement certain methods to radicalize Turkish society. The easiest way is to use government-affiliated social media bots to promote anti-Israeli rhetoric in Türkiye and make them stand out. Going a step further, you can fund groups whose political views align with yours on social media to boost their prominence. Going a step further, you can fund and incite organizations with links to radical groups in Türkiye to organize demonstrations within the country. If your plan has worked so far, you have now exerted radical-motivated pressure on the Turkish government. Naturally, since Türkiye is a democracy, public unrest will begin to be reflected in the rhetoric of political figures. You can expect a domino effect, influencing government decisions. However, you are not the only force regulating public opinion in Türkiye. After all, bureaucratic figures in Türkiye can take control of politics and return the state to its original, natural paradigmatic position. Of course, the example I gave above is entirely hypothetical and has no connection to reality, but it clearly illustrates the methods and steps of modern psychological warfare. These methods proceed in the form of prominence, funding, organization, radicalization, and exertion of pressure. Modern states employ such policies even in simple diplomacy. However, sometimes they cross borders and attempt to control the democratic system in a country, which clearly means attacking the democratic rights of citizens.

f. Cutting Edge Psychological Warfare Technologies:

There might be an idea about technological advancements' importances in a subject as abstract as psychological warfare, but this statement would be quite inaccurate. Because psychological warfare is directly linked to the media, any change made to media technologies and how they are manipulated significantly alters the nature of psychological warfare. Let us consider three methods that demonstrate the limitations of this technology: AI-Generated Deepfake Ecosystems, AI-Controlled Propaganda Bots, and Cognitive Terrain Mapping (CTM).

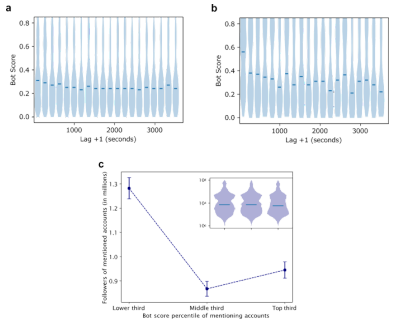
i. AI-Generated Deepfake Ecosystems



To grasp this technology, we first need to understand what deepfake technology is. Deepfake technology is essentially a productive application of computer vision

analysis, which allows computers to perceive the world through vision. In computer vision, computers interpret people's existence by analyzing the angles of their joints and the connections between them. For example, a diagram of the movement of a person's facial muscles can be generated, and a person's emotional state can be analyzed by a computer. This also means that if your muscle movement patterns are analyzed accurately enough and combined with visual data of a person's face, we have a digital model of a person's face. As you can imagine, we can superimpose this model on other people's faces, and if their bodies are close enough to real person's body (which is quite easy, as long as they are not naked), we can edit a video of another person's action and present it as if that person did it himself. If we do this to someone who has committed a crime or someone engaging in socially acceptable behavior, this person's personal reputation can be severely damaged. Even if the changes made to the video are detectable with proper technical analysis, this person's public image will not be easily altered. Having facial models of multiple prominent figures at disposal also provides a perfect propaganda tool. This way, can weaken a politician who espouses an ideological viewpoint your government disapproves of, thus dealing a blow to numerous political movements.

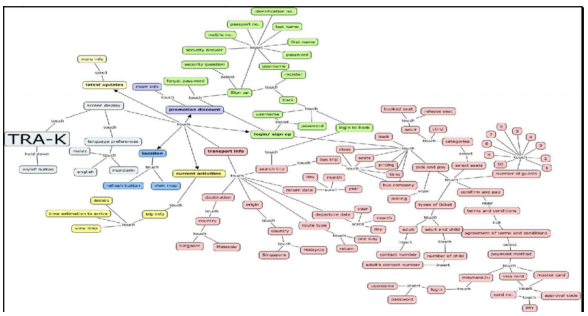
ii. AI-Controlled Propaganda Bots



Let us begin this discussion of technology with some alarming data. The fact is that 51% of internet users are now bots. This data alone proves that most of what internet users' see is not human-made. Furthermore, studies on Reddit show that AI-powered versions of these bots can exert influence indistinguishable from real people in political arenas. In other words, even someone that discusses online may no longer be human. This means, from a propaganda perspective, that a vast number of accounts can now be checked cheaply and without being caught by social media platforms' anti-bot practices, and these accounts will exhibit such behavior that it is impossible for another human to determine whether they are truly human. When the early stages of artificial intelligence technology is examined, we see that technicians working on the subject are trying to design models that think like humans. However, because models that think like humans lack superiority over humans, this goal quickly shifted. However, AIs that think like humans may have an interesting characteristic:

for example, they can change a person's mind because they react like a real person. This means machines that can manipulate public opinion. While their success rates are debatable, it is clear they can influence certain segments of the population. They can be particularly effective in older populations.

iii. Cognitive Terrain Mapping (CTM)



In fact, this technology is not directly developed for psychological warfare; it is a feature inherent in artificial intelligence models. It could be thought of these features as if a human were trying to break down an event into its parameters and predict its likely outcome, but humans' perception of a topic is very limited, and their update rate is exceedingly slow. These limitations could be addressed by replacing humans with an AI. This ability of AI to continuously analyze and reconstruct these groups and their ideological relationships is called CTM. Essentially, AI does nothing more than create a mental map of the ideological interactions of the masses. This provides an objective way to monitor the methods applied to the masses we intend to manipulate. If the observed trend goes toward the desired changes in this mapping method, it indicates that the psychological warfare methods employed are working. Furthermore, this mapping method can help to observe which ideologies are dominant and the trends in change. Using this data, it can be observed which psychological methods and approaches the masses are dealing with are receptive to. This technology, which plays a crucial role in both analyzing and developing methods, has reduced the engineering of societies from a verbal matter to manipulable values in the abstract. In this respect, it can be said to be the heart of psychological warfare.

6. Timeline of Important Events:

- In 2003, the United States launched an unprecedented, intercontinental operation to hunt Islamist militants in Pakistan. It was one of the world's first full-scale drone operations. The operation resulted in the neutralization of numerous militants and the deaths of civilians.

- In 2016, Russia was accused of interfering in the American elections. It allegedly conducted numerous cyberattacks to damage the campaigns of Democratic politicians. Some of the attacks included leaking emails and manipulating social media.

- In 2018, the United States, using information received from Saudi Arabian intelligence, neutralized 50 al-Qaeda members traveling to Yemen by car using drone bombings. At the time, such a consistent assassination across continents was a world first.

- In 2020, the war between Azerbaijan and Armenia drew attention with Azerbaijan's use of drone technology, setting an example for the world. Furthermore, thanks to the drones' ability to keep track of the number of people killed, Azerbaijan conducted a successful propaganda campaign throughout the war.

- In 2020, a Turkish drone accidentally bombed the Libyan army. This drone was piloted by an AI model and launched the attack without any human intervention. The incident sparked an international crisis and was escalated to the United Nations Security Council in 2021. After lengthy discussions, this incident became the first AI-driven drone attack in history.

- The Ukraine-Russia war, which began in 2022, was one of the most glaring examples of the active use of drones. Russia actively used drones alongside its air operations, while Ukraine countered Russia with its mass-produced drones.

- In 2024, some pirate terrorist groups terrorizing the Red Sea began using military drones. These terrorist organizations were believed to be supported by Iran and to have acquired their technology from there. The fact that the pirates specifically targeted Israel and its allies reinforced this claim.

- One of the most significant examples of drone use in the field in 2025 was the Israel-Iran war. Israel actively used drone technology to disrupt chains of command, while Iran carried out the world's largest drone attack.

7. Major Stakeholders and Their Positions:

Method of Deciding Policies of Nation: In this section, a topic that has not yet gained much traction on the global agenda will be examined, and since some countries' policies on the subject are unclear, their technological policies will be outlined based on their investments in these technologies and their superiority in that area. To this end, a general overview and list their current state of modern warfare under three headings will be provided. I will divide these countries' technologies into four groups; S, A, B, and C represent their levels, from best to worst, relative to the global average.

United States

The US has made significant progress compared to the rest of the world in all three technologies used in modern warfare. In addition to the US's frequent use of drones in its operations in the Middle East, its efforts to control media worldwide are a matter of global awareness. However, when examined specifically in the cyber warfare arena, the US lags behind its number one rival, China. Internationally, imposing restrictions in this area would place the US in a more secure cybersecurity position. However, it would be remiss for the US, which has invested billions of dollars in the other two warfare domains, to see these sectors restricted. Nevertheless, moderate measures could create a platform for the US to leverage.

Drone Warfare: (S) Because the US is one of the first countries in the world to invest in drone technology and is the country where the companies responsible for innovative

technologies in the sector are located. In addition, it is one of the most experienced countries in drone operations.

Cyberwarfare: (A) Because the US maintains a cyber army, whether to counter cyber threats from China or to conduct operations against points it cannot reach in the Middle East. The US employs cybersecurity experts in its intelligence units and develops technologies under NATO.

Psychological Warfare: (A) Because the United States owns a large portion of the world's media and leads the world in content consumption. It also funds groups aligned with its views around the world and orchestrates propaganda campaigns on social media using bots.

Russia

Russia uses all these warfare techniques on the battlefield, but their successes are debatable. Russia is almost as successful as China in cyberattacks. While not as aggressive as China, Russia has a highly effective strategy of attracting its country's skilled experts to the cyberwarfare arena. Meanwhile, Russia lags significantly behind its rival Ukraine in drone warfare. While it was one of the earliest countries to invest in drone warfare, it could compensate for this weakness in warfare by imposing potential restrictions on the technology. This approach would also disrupt Ukraine's massive investment in drones. Russia does not have a good history of psychological warfare; it has violated other countries' freedoms in numerous ways, whether through propaganda inherited from the Soviet era or through regime change efforts in the Middle East.

Drone Warfare: (A) Because Russia made active investments in drone technology, and besides, it can successfully mobilize drones in combat operations.

Cyberwarfare: (A) Because Russia has conducted the largest cyberwarfare operations in its history. It provides scholarships and financial support programs to domestically trained experts, and it is attempting to mobilize its own population in this area.

Psychological Warfare: (A) Russia is one of the largest bot-owning countries in the world, so much so that there are articles written about the propaganda it used during the invasion of Ukraine.

China

China is currently pulling the world's hair out with these modern warfare methods. It also possesses a frighteningly large operational capacity. It terrorizes its enemies around the world through cyberattacks. It supports private companies with its global commercial power and collects data from around the world through technological products produced by these companies. With its state-backed hacker units, China is currently at the forefront of this field. When it comes to drone technology, we see that China interprets this technology as an intelligence tool used to gather information rather than a warfare technology. Chinese drones can be found all over the world. When it comes to psychological warfare, China already has a massive propaganda tool: TikTok, with billions of users.

Drone Warfare: (B) China uses its drones for intelligence purposes rather than on the battlefield. There is no evidence to suggest they possess advanced technology. Assuming they do not, restricting the technology would be in China's best interest.

Cyberwarfare: (S) China's cyber operations, particularly against the United States, are countless. It is believed to have a cyber army of 3,000 to 5,000 specialists. For China, cyberattacks are a way to terrorize its enemies.

Psychological Warfare: (S) China controls much of the world's media. Many private companies tend to produce products that celebrate Chinese culture because of the large number of Chinese customers. Furthermore, China has a bot army similar to Russia's.

United Kingdom

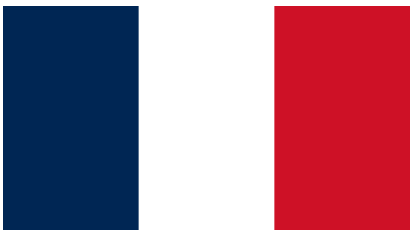
While the United Kingdom has not gradually begun to weaken among the world's major powers due to the Middle East's fall under American influence, it still wields a formidable military force. In cyberwarfare, the United Kingdom's operations are conducted by its intelligence unit, MI6. The United Kingdom demonstrates moderate effectiveness in cyberwarfare. This mediocrity also applies to drone technology. Despite possessing powerful drone technologies, the United Kingdom does not actively use them in operations. When it comes to psychological warfare, they lack the propaganda power they once possessed during World War II. This is a natural consequence of the recent political and economic crises within the United Kingdom. As a result, the United Kingdom has moderate investment in these technologies.

Drone Warfare: (B) They have no documented operations in drone warfare, but they do have powerful drones in their arsenal, but they are not groundbreaking technologies, and restricting the technology would be in the UK's interest.

Cyberwarfare: (B) Even if the UK intelligence agencies actively used cyberspace, they would not have any major documented operations. Controlling technology would be in the UK's best interest.

Psychological Warfare: (B) They're following a moderate course in psychological warfare, and even though they have intelligence operations, they do not have any special investments. Restrictions would be in their favor.

France



Despite not having participated in active warfare for a long time, France is meticulous about keeping its military modern. France has established and developed an army dedicated to cybersecurity and warfare since 2016. While it has not yet seen a single dedicated operation, it is one of the few countries with an army solely dedicated to cyberwarfare. In terms of drone technology, it is at a similar level to the United Kingdom. While it has combat-capable drones, we have not

seen them in use. France has a special unit of 300 soldiers for psychological warfare. This unit is responsible for the execution and success of all French psychological operations.

Drone Warfare: (B) Despite having powerful drones in their arsenal, no use has been observed. Their situation is similar to the UK; restricting the technology would be beneficial.

Cyberwarfare: (A) It has a dedicated cyber army of 1,000 technicians. Even without documented operations, it is a highly invested area.

Psychological Warfare: (B) In fact, France maintains a 600-person department for psychological warfare, but we have no direct data on its activities.

Iran

As one of the biggest opponents of the American population in the Middle East, Iran is frequently subjected to attacks and military harassment. Iran's military ranks among the top countries in the Middle East in terms of technological advancement. It is also a country striving to invest in modern warfare technologies. They have considerable advancement in drone technology. In fact, the largest drone attack in the world was a swarm of attacks carried out by Iran during the Iran-Israel war. Iran is a country that lags somewhat behind in cyberspace. When it comes to psychological warfare, Iran is known for its influence on the Arab Peninsula.

Drone Warfare: (B) They have used drones in combat but have not had much success in existing operations. They're considered average in terms of drone technology. Restricting technology serves their interests.

Cyberwarfare: (C) They have no known success in cyberwarfare. Restrictions would be in their best interest.

Psychological Warfare: (B) There are various propaganda campaigns that have been launched to persuade groups in the Middle East to join the cause against Israel, and they are considered partially successful.

India

India is a rising power among the world's armies. In one area, particularly cybersecurity, India stands at the top of the world. India has built a highly sensitive data protection system and certainly boasts a high profile in computer science. It also has no hesitation in using cyber technologies against its longtime enemy, Pakistan. They also possess a powerful arsenal of drone technology. While they may have an advantage in psychological warfare thanks to their virtual visibility, it is not as if they use them very actively.

Drone Warfare: (B) Although they are in their arsenal, they are not actively used. Restricting them would be beneficial.

Cyberwarfare: (S) It is by far the world's leading country in cybersecurity. It has numerous units divided into cybersecurity groups. It houses some of the world's most elite experts.

Psychological Warfare: (B) They have no documented success or investment in psychological warfare, but they have a lot of bots.

Türkiye

Turkey is a prominent military power in the Middle East and Europe. Its investments in modern technologies are also extremely high. It is among the world's leading countries, particularly in terms of both research and development on drone technologies and the production and use of its own drones. Furthermore, Turkey does not hesitate to use the technologies it develops in drones as a political tool within its own country. While it is prominent among Middle Eastern countries in psychological warfare, it lags behind first-world countries. It has no known army or official operations in cyberwarfare.

Drone Warfare: (S) It is among the world's largest manufacturers. Its most prominent field of expertise is in the military sector. It has also conducted numerous successful operations. It is among the world's leading technological leaders when the matter is drones.

Cyberwarfare: (C) No documented operations or housing investments

Psychological Warfare: (C) Very little documented operations or housing investments

8. Points to Cover:

1. Which regulations should be applied to Drone tech?

2. How to solve the anonymity issue of cyber attacks and terrors?

3. How to regulate psychological warfare to protect the rights of civilians?

4. What kind of regulations should be made regarding the use of Artificial Intelligence in the battlefield, or should there be any regulations at all?

5. How can the auditing of the decided regulations be ensured?

9. Possible Solutions

- The most frightening aspect of cyberattacks is their anonymity. Solving this problem can be quite difficult without technical knowledge. One approach could be to establish an international organization that gathers the necessary technicians. This would allow countries claiming to have been subjected to cyberattacks to seek compensation under international law, thus solving the problem of anonymity. However, establishing an organization is a complex solution. Issues such as how technicians will be recruited from each country, how the organization will be funded, and how the organization operates need to be explained and detailed.

- The main problem with drone technologies is their accessibility and the lack of legal restrictions. The most direct solution to this problem is to establish certain restrictions that restrict drone technologies. For example, first, we could determine how this technology should fall into the hands of criminal organizations and terrorist organizations, and then we could implement restrictions that address more abstract and less urgent problems, such as limiting the use of artificial intelligence on drones.

- Psychological warfare methods are the most difficult to control because they utilize much more abstract and anonymous methods than others. One of the first solutions that could be proposed is the design of an artificial intelligence model that identifies a general source by classifying the number of bots and types of propaganda on social media to document these acts of psychological warfare. Furthermore, such a solution would be the first artificial intelligence experiment in UN history. If a more standardized solution is desired, a sub-organization could be established as a branch of the cybersecurity organization to identify the countries of origin of psychological attacks. The two problems could be solved under one roof.

10. Resources and Links for Future Research:

SOF Week 2025: PDW unveils attritable FPV drone for SOF operations at scale | Shephard

DefenseTech Brief – May 12, 2025 - Defense Update:

Futuristic war drone: a deadly update in 2025 - The EYE

MQ-28 Ghost Bats Controlled From E-7 Wedgetail In Loyal Wingman Test

Cognitive EW - EMSOPEDIA

RSA Algorithm in Cryptography - GeeksforGeeks

MQ-28

Post-Quantum Cryptography | CSRC

Cognitive Terrain Mapping - Information Professionals Association