Regulating Anti-Drone Systems in times of extensive use of military Drones

Keywords: Anti-drone systems/ defense/security/C-UAS

Sofia Stellatou, sofia_stellatou@yahoo.gr, has a Master of Laws degree in Air and Space Law from McGill University.

Abstract

The increased use of unmanned aircraft systems (UAS) as “weapons” has created the need for anti-drone systems or protective “domes” development and deployment by all governments. From surveillance to military attack, States choose the air space more and more to showcase their powers and undertake several kinds of operations. As expected, this brings to the surface legal gaps and challenges in the regulatory infrastructure of States separately and collectively.

This paper examines the emerging governance challenges surrounding anti-drone technologies. The study adopts a comparative legal methodology among Israel, USA, China, the UK, Ukraine and Türkiye analyzing their C-UAS and the legal bases. It also incorporates case studies of operational anti-drone systems deployed, especially by states that have suffered military attacks in the past years, e.g. Ukraine and Middle-Eastern states. The central research question asks how legal and regulatory frameworks can effectively accommodate counter-UAS systems while preserving aviation safety, fundamental rights, and the lawful use of drones.

This article joins the discussion on how laws about air travel and security rules should change to deal with the increasing use of technologies that counter drones. It tries to prove that we need simple, consistent rules to protect ourselves from bad and military drone use. We have to make sure we are safe from drones that might be used to harm us. The article wants to help figure out how to make these rules work better.

Introduction

The anti-UAS technologies have evolved and multiplied throughout the years and their uses are numerous and timely. Governments increasingly deploy counter-UAS technologies to detect, track, and neutralize dangerous and unauthorized drones. These integrated systems combine radar, radio-frequency sensors, electro-optical surveillance, and mitigation tools such as signal disruption, interception, or directed-energy measures. Despite their growing operational use, the legal framework governing their deployment remains fragmented and underdeveloped, particularly in civil airspace.

The report starts by looking at the technology behind systems that counter drones and the idea of a "defensive dome" that governments use. Then it checks the current laws that indirectly deal with stopping drones - like rules for safe flying, telecom laws, and security laws - and shows where they fall short when it comes to using technology to stop drones.

The analysis argues that effective counter-UAS governance requires a multidisciplinary regulatory approach that addresses several key parameters: operational authority and accountability of public actors, proportionality and necessity in mitigation and defense measures, interoperability with existing air traffic management systems, protection of communications infrastructure, and compliance with data protection and privacy standards.

Section A: Counter- UAS Technology at a glance

Counter-drone technology encompasses a wide range of solutions that allow you to detect, classify, and mitigate drones and unmanned aerial vehicles. This is also known as counter-UAS technology because drones are a type of unmanned aerial system.

“Drone monitoring equipment” can operate passively or actively. It can perform several functions, roughly categorized in (a) detection, (b) classification or identification, (c) locating and tracking and (d) alerting. Classification and identification capabilities are particularly important; there is equipment classifying objects detected, recognizing animals from humans, objects from people but also some equipment can identify a particular model of drone, or the drone’s or controller’s digital fingerprint. Some counter-UAS technology even allows you to track the drone's location in real-time. The four main types of drone monitoring equipment are;

i. Radio frequency (RF) analysers

They're used to figure out what's going on with the radio signals between a drone and the person controlling it. These special tools, called RF Analysers, have one or more antennas that pick up the radio waves and a processor that looks at the RF spectrum. This helps identify the controller, which is really useful when it comes to prosecuting someone - it can prove that a specific drone and controller were being used at a certain time and place. This can be a powerful tool in investigations.

ii. Acoustic sensors (Microphones)

This kind of counter-drone technology works in a passive way, using a microphone or a group of microphones to pick up the sounds made by drones and figure out where they're coming from. It only works over very short distances, up to 300-500 meters, and is often used to keep an eye on areas that other sensors can't see.

iii. Optical sensors (Cameras)

Optical sensors can pick up light in various wavelengths, such as visible and infrared, and even thermal radiation, which helps them spot drones whether it's daytime or nighttime. With the latest advancements in optical sensor technology, the resolution has gotten better, and when you add AI-powered detection, tracking, and classification, it becomes even more effective. This means that optical sensors can now provide more accurate and detailed information about detected drones, making them a valuable tool for drone detection and tracking systems.

iv. Radar

Drone detection radar or counter-UAS radar sends out radio signals. The reflection of that signal as it bounces off an object serves to measure its direction and distance. The majority of those are designed for large object tracking, e.g. civil aircraft. However, there are specialist counter-UAS technology which include radar that tracks smaller objects. This type of equipment, requires a transmission license and frequency checks to prevent radio interference.

As we go beyond just monitoring and move towards more proactive methods, there are technologies out there that can help us take "Drone Countermeasures" to the next level. This can involve actually destroying the drone, neutralizing it, or even taking control of it. But here's the thing: in most countries, the current rules and regulations are pretty strict

about using these kinds of countermeasures. There are some exceptions, though - like for military or law enforcement agencies, they're allowed to use them.

When it comes to dealing with unmanned aircraft, authorities are using a mix of different methods to counter the threats they pose. These methods include electronic, cyber, and physical measures, which allow for a proportionate response to different types of threats. In many cases, the goal is to disrupt or redirect a drone without actually destroying it. To achieve this, non-kinetic measures like radio-frequency interference and satellite navigation manipulation are often used. These methods can help reduce the risk of damage and debris, but they also raise some important concerns. For example, they can interfere with civilian communications and navigation services, as well as other legitimate uses of the radio spectrum. As a result, there are some key legal questions that need to be addressed, including how to manage the radio spectrum, ensure aviation safety, and determine when it is acceptable for states to intentionally interfere with wireless communications. The use of these countermeasures is complex and requires careful consideration of the potential risks and benefits. By understanding the different methods available and the challenges they pose, authorities can develop effective strategies for responding to unmanned aerial threats. This is an important issue, as the use of drones is becoming increasingly common, and the need for effective countermeasures is growing.

When other methods don't work, authorities might use physical ways to stop a threat, like high-energy laser systems or drones that catch other drones with nets. Laser systems are a cheaper way to deal with many aerial threats without using traditional ammo, and net-based systems try to disable and catch a drone instead of destroying it, so it can be examined later. However, both methods have operational and legal problems. Laser systems need strict safety rules to avoid hurting people or planes by mistake, and net-based systems are limited by how far they can reach and what kind of drone they're trying to catch. For example, the net might not work well if the drone is too fast or too small. Additionally, there are concerns about where and when these systems can be used, and who is allowed to use them. Overall, while these physical methods can be useful, they need to be carefully controlled and regulated to ensure they are used safely and effectively.

Recent developments have also seen the emergence of cyber-based countermeasures capable of identifying, monitoring, and, in certain cases, assuming control of hostile drones. Unlike traditional interception methods, these technologies seek to neutralise the threat by exploiting vulnerabilities in a drone's communication or software systems, while preserving the aircraft and any associated evidence. Their use, however, raises complex legal issues concerning cybersecurity, data protection, attribution, and the limits of lawful State intervention in digital systems. More broadly, the increasing integration of electronic, cyber, and physical countermeasures within a single defensive framework illustrates that the principal legal challenge is no longer the availability of effective technologies, but the establishment of suitable, applicable regulatory frameworks.

Many tech companies around the world offer a wide range of unmanned aerial systems, or UAS, at different price points and with various features. Sometimes, governments work together to create custom systems that meet their specific needs, taking into account the actions of rival countries, and focusing on keeping the details secret, designing them strategically, and making sure they work effectively. This collaboration allows governments to get exactly what they need from their UAS, whether it's for surveillance, research, or other purposes.

Section B: Leading countries and their anti-drone systems

When you look at how different countries use systems to counter drones, it's clear that some nations are more advanced and experienced than others. Countries like Israel, the United States, Ukraine, China, the UK, and Türkiye are leading the way. If you study their approaches to dealing with unmanned aerial systems, you'll notice some common traits. One key thing they have in common is a comprehensive strategy that combines various technologies to defend against drone attacks. This approach targets all possible threats and weapons, showing a holistic understanding of the issue. By using multiple technologies together, these countries can better protect themselves from the different types of drone attacks that might occur.

i. Israel

Israel has created a very advanced system to defend against unmanned aerial systems, combining multiple layers of protection. This includes using missiles, electronic warfare, artificial intelligence, and special energy weapons. The country's air defense system now includes ways to counter drones, with some Iron Dome batteries able to intercept certain types of UAVs, as well as rockets. Meanwhile, David's Sling and Arrow systems provide protection against more significant aerial threats, working together to create a strong defense network.

To protect against drones, special systems are used. These systems have different ways to detect drones, like using radio waves, radar, and special cameras that can see in the dark or feel heat. They can also mess with the drone's communications and GPS. By combining all the information from these detectors, the system can accurately find and track the drone. Then, a computer system helps decide what to do with the drone, using artificial intelligence to figure out what the drone is, where it's going, and what to do to stop it. This makes it easier to deal with the threat and send something to intercept the drone if needed.

A big step forward in technology is the Iron Beam, a powerful laser weapon that can stop drones, rockets, and mortar rounds by focusing heat on key parts. Compared to using missiles to intercept them, laser systems are much cheaper to use each time and have unlimited "bullets", but they can be less effective in bad weather like fog, rain, dust, or smoke. Israel's approach of combining different methods makes it harder for drones to attack in groups, while also saving money by choosing when to use physical or non-physical attacks. This means they can handle attacks more efficiently and at a lower cost.

ii. USA

The United States uses a system to stop enemy drones that has many layers. This system combines different ways to attack, like using electronics to disrupt the drone, shooting it down with a laser or missile, and using computers to make decisions. Instead of just relying on shooting down the drone with a missile, the US military chooses the best way to stop the drone based on what it's like and how it's behaving. This approach helps the military be more effective and flexible when dealing with different types of drone threats.

Electronic warfare is still a key way to defend against attacks. By using radio-frequency jamming, we can disrupt the communication between drones and their operators, making it hard for them to work together. At the same time, GNSS jamming and GPS spoofing can interfere with the navigation systems of drones, causing them to lose control or fly off

course. This can be really useful for mobile forces, as they can use portable electronic countermeasure devices to stop small drones without having to use expensive missile interceptors. These devices give them a way to fight back without using traditional weapons, which can be really costly.

The US has made directed-energy weapons a top priority, including powerful lasers and microwave systems. These lasers can actually damage drones by overheating important parts, like the structure or electronics. On the other hand, microwave systems send out strong pulses that can disable the electronics on multiple drones at the same time, which makes them really useful for dealing with large groups of drones.

In situations where electronic attacks don't work, precision-guided missiles and rockets can still be used to intercept targets. These systems are controlled by advanced command centers that use artificial intelligence to combine data from various sensors, such as radar, cameras, and heat detectors. The AI helps identify targets, prioritize threats, predict their paths, and choose the best interceptors, which reduces the workload for operators and speeds up response times. This multi-layered defense system greatly improves operational effectiveness, but it's still a challenge to defend against large-scale attacks by many cheap drones in a cost-efficient way. For instance, when faced with a swarm of drones, the system must be able to quickly identify and prioritize targets, and then use the most effective interceptors to take them down. For example, the command center might use radar to detect incoming drones, and then use electro-optical sensors to identify and track them. The AI would then predict the drones' trajectories and select the best interceptors to take them out. Despite these capabilities, defending against large-scale drone attacks remains a complex problem that requires continued innovation and investment.

iii. Ukraine

When Russia launched its full-scale invasion in 2022, Ukraine quickly changed its approach to dealing with enemy drones. Instead of just using traditional air defense systems, Ukraine created a flexible system that combines different technologies. This system uses digital tools to get a clear picture of what's happening, electronic warfare to disrupt enemy communications, mobile units that can fire at drones, and special drones that can intercept enemy drones. By combining military technology with civilian digital infrastructure, Ukraine has been able to adapt quickly to the changing situation and improve its defenses against unmanned aircraft. This approach has allowed Ukraine to stay one step ahead of its enemies and protect its airspace more effectively.

One of the most innovative parts of this system is something called Sky Map. It's a way for people to work together to keep an eye on things, using information from regular people, local authorities, and military sensors all in one place. By taking all these different reports and matching them up with radar data, the system can find small drones that might be flying too low to be seen by regular radar. This helps get defenses ready quickly. The system uses special tools to figure out exactly where these drones are, which makes it easier to track them and respond fast. This is really important because it can help keep people safe from drones that might be trying to sneak in undetected.

Electronic warfare constitutes another key layer of Ukraine's defence. Radio-frequency jamming, GNSS (GPS) jamming, and spoofing techniques disrupt drone communications and navigation, often forcing UAVs to deviate from their intended routes or lose operational

capability without kinetic engagement. As Russian drones have increasingly adopted autonomous navigation and anti-jamming features, Ukraine has continuously adapted its EW systems, resulting in an ongoing technological competition.

Ukraine has set up special teams that can move around and shoot down drones using big machine guns, guns that can shoot at airplanes, devices that can see heat, strong lights, and small radar systems. Now, they have a new way to stop enemy drones that is not too expensive: using drones that can see what's in front of them to catch and destroy other drones that are spying or waiting to attack. This way of using one drone to fight another makes Ukraine less dependent on costly missiles and gives them more options to deal with new threats from the air.

iv. China

China has made a lot of progress in creating a system to counter unmanned aircraft, which is one of the most advanced in the world. This system focuses on using directed-energy weapons, electronic warfare, and a layered air defense approach. One of the most well-known systems is the Silent Hunter, a high-energy laser that can destroy or disable small and medium-sized drones by targeting their critical components with thermal energy. Another system, the LW-30 laser, is designed to counter drones and other low-altitude threats. These systems work together with various sensors, including radar, electro-optical, infrared, and radio-frequency sensors, to provide continuous surveillance and track targets. This integrated approach allows for effective detection and response to aerial threats. The use of directed-energy weapons, in particular, offers a promising solution for countering unmanned aircraft, and China's advancements in this area are notable. By combining these technologies, China has developed a robust counter-unmanned aircraft system capability.

China uses special techniques to stop drones from working properly, like blocking their radio signals and interfering with their navigation systems. This way, they can disrupt the drones before they need to use force to take them down. They're also using artificial intelligence to help their command centers automatically identify targets, figure out which threats are the most important, and decide which weapons to use. Laser systems are a good way to counter drones, especially when they're coming in large groups, because they're relatively cheap to use. However, their effectiveness can be reduced by bad weather like heavy rain, fog, or lots of particles in the air.

v. United Kingdom

The UK is working on a special system to stop unwanted drones, called C-UAS. They're focusing on using powerful lasers and creating a command center to control everything. The main project is called DragonFire, which is a strong laser that can hit drones with great precision. This laser can damage important parts of the drone, making it unable to fly. Compared to traditional missiles, DragonFire is much cheaper to use and can fire many times without running out of ammo, making it great for defending against lots of drones at once.

The UK is combining radar, electro-optical sensors, and other systems to create a unified framework for managing battlespace. This framework can identify, track, and classify many aerial targets at the same time. It uses AI to help make decisions quickly, choosing the best countermeasure based on the type of target and the environment. However, like other laser-based technologies, the effectiveness of this system can be limited by environmental factors. For example, weather conditions can affect how well the system works. The UK's

approach to integrating these different systems and using AI for decision support is a key part of its efforts to improve its defense capabilities. By bringing together different types of sensors and systems, the UK can get a more complete picture of the battlespace and respond more effectively to threats.

vi. Türkiye

Türkiye has rapidly expanded its indigenous C-UAS capabilities through the development of electronic warfare systems, directed-energy weapons, and mobile kinetic platforms. The Kangal electronic warfare system detects and jams RF communication links and satellite navigation signals, disrupting hostile UAV operations without kinetic engagement. Complementing this capability is the ŞAHİN laser weapon, designed to disable drones through concentrated thermal energy, offering a cost-effective solution against small aerial threats.

For defence against moving targets, Turkey uses systems like the KORKUT, a self-propelled anti-aircraft gun. This gun uses special ammunition that can be programmed to explode in the air, which helps it hit drones and other low-flying targets. These systems are all connected through a network that uses radar and other sensors to track targets and make sure they are hit. Turkey has used these systems in places like Syria, Libya, and the South Caucasus, and they have worked well. But, like other systems that try to stop drones, Turkey's systems still have trouble with drones that can work on their own and avoid being jammed, as well as with big groups of drones attacking at the same time.

Section C: Respective current legal and regulatory frameworks

In the US and the UK, there are laws that specifically deal with Counter-Unmanned Aircraft Systems (C-UAS). However, in most other countries, there aren't any special laws just for C-UAS. Instead, the rules are based on broader laws related to defense, national security, the military, aviation, telecommunications, and emergency responses. These laws are often supplemented by secret military rules, orders from ministers, or operational guidelines that aren't available to the public. This means that the legal basis for C-UAS in these countries is not always clear or transparent. As a result, it can be difficult to understand how C-UAS is regulated in many parts of the world. The lack of specific laws and publicly available information can make it challenging to develop effective strategies for dealing with the threats posed by unmanned aircraft systems.

i. Israel

Israel's counter-drone operations are principally regulated through its Defence Service Law,[1] national security legislation, and military regulations administered by the Israel Defense Forces (IDF) and the Ministry of Defense. Airspace management is coordinated with the Civil Aviation Authority of Israel (CAAI), while spectrum use is regulated by the Ministry of Communications.

Israeli systems for stopping enemy drones work closely with the military to quickly respond to threats in the air while also keeping in touch with civilian air traffic controllers. The use of electronic warfare, such as jamming radio frequencies and GPS signals, is carefully controlled

[1] *Defence Service Law (Consolidated Version), 5746–1986* (Israel).

because it can affect how civilians communicate and navigate. For example, laser systems like Iron Beam need very specific rules for identifying targets, deciding how to engage them, and avoiding other aircraft and populated areas to minimize risks to friendly planes and people on the ground. This is important to prevent accidents and ensure safe operations. By following these procedures, the Israeli military can effectively use these systems to protect against aerial threats while also protecting civilians and their own forces.

ii. USA

The US has a really detailed set of laws that control how the country deals with unauthorized drone operations. Most of the power to detect, track, and stop drones comes from the Preventing Emerging Threats Act of 2018.[2] This law gives certain government agencies, like the Department of Homeland Security, the authority to take action against drones that pose a threat to important facilities, assets, or operations. These agencies can use various methods to detect and track drones, and they can even disrupt or destroy the drones if necessary. What's important to note is that this law allows these agencies to do things that would normally be against the rules, like interfering with telecommunications or computer systems, as long as they consider people's privacy and civil liberties. The law is designed to help keep people and places safe from drones that could be used to cause harm. For example, if a drone is flying near a major airport or a government building, the authorities can take action to stop it. The goal is to balance safety and security with the need to protect people's rights and freedoms.

A complementary legal basis exists under 10 U.S.C. §130i, which provides the Department of Defense with authority to protect military installations and other designated defence assets from unmanned aircraft threats. The provision enables the armed forces to employ a broad range of countermeasures, including detection, tracking, warning, disruption, seizure, and, where necessary, destruction of threatening unmanned aircraft. This framework reflects the specific security requirements of military environments, where rapid neutralisation of hostile drones may be necessary to protect personnel, infrastructure, and sensitive operations. Nevertheless, the exercise of these powers remains subject to internal procedures, coordination requirements, and restrictions designed to minimise risks to civilian aviation, communications networks, and surrounding communities.

The Federal Aviation Administration (FAA) continues to regulate national airspace under 14 CFR and generally prohibits interference with civil aircraft, including drones, unless a specific statutory exemption applies.

Other important groups that play a role in this area are the Department of Justice, the Federal Bureau of Investigation, and the Federal Communications Commission. The Federal Communications Commission is in charge of managing the use of radio frequencies, which means that interrupting radio signals, known as RF jamming, is not allowed for private companies or most government agencies unless they have special permission. As a result, the military and federal agencies that work on countering unmanned aircraft systems must follow very strict rules and regulations, including those related to the use of radio frequencies, aviation safety, and protecting people's privacy and rights.

[2] *Preventing Emerging Threats Act of 2018*, Pub L No 115-254, div H, 132 Stat 3186, 3522 (2018)

iii. Ukraine

Ukraine has made big changes to its laws and rules for dealing with drone threats since Russia's full-scale invasion started in 2022. The country's efforts to counter drones, known as C-UAS activities, are mainly guided by martial law, emergency defense laws, and military rules set by the Ministry of Defence of Ukraine. Several groups share the responsibility of carrying out these operations, including the Armed Forces of Ukraine, the Air Force, the Security Service of Ukraine, and the State Special Communications Service. These groups work together to protect Ukraine's airspace and respond to drone threats under the current laws and regulations.

The use of digital tools like Sky Map is changing how military air defense works, and it's also creating new legal problems. For example, there are concerns about protecting people's data, keeping information safe from cyber attacks, and making sure the information being used is reliable. Additionally, when civilians get involved in military operations, it raises questions about their role and how they fit into the bigger picture. We've seen that electronic warfare and GPS interference can be used as defensive tactics, but sometimes they can also affect things like civilian navigation systems and commercial drones. The conflict has also shown how complicated the law can be when it comes to using autonomous drones that can intercept other objects. There are questions about who is in charge, how to assign responsibility, and how to make sure these drones are used in a way that follows the rules of war, including being able to distinguish between different targets and not causing too much harm.

iv. China

China has rules to control drone operations, using a mix of laws like the Civil Aviation Law,[3] the National Defense Law,[4] the National Security Law,[5] along with military rules managed by the People's Liberation Army. The Civil Aviation Administration of China oversees civilian drone rules, while the Ministry of Industry and Information Technology handles spectrum management. These laws include the Civil Aviation Law of 2021, the National Defense Law of 2020, and the National Security Law of 2015, which all work together to regulate drone operations in China. By having these laws in place, China aims to ensure safe and secure use of drones, balancing the needs of different users and minimizing potential risks. This regulatory framework is important for the country's aviation and national security, and it helps to promote the responsible use of drones.

China has a system in place to control its airspace, which gives the government a lot of power to find, stop, and get rid of drones that aren't allowed to be there. To follow the rules, people who own drones have to register them, put special electronic IDs on them, and stay out of certain areas. They also need to get permission to fly in areas that are restricted. China's laws make it easy to quickly use new technologies like electronic warfare and lasers, but some people are worried that this might not be fair, that it could invade people's privacy, and that there isn't enough independent oversight to make sure everything is being

[3] *Civil Aviation Law of the People's Republic of China* (People's Republic of China), 2021.
[4] *Law of the People's Republic of China on National Defense* (People's Republic of China), 2020.
[5] *National Security Law of the People's Republic of China* (People's Republic of China), 2015.

done correctly. The government has a lot of control over what happens in the air, and this can be a problem if it's not balanced with protections for people's rights.

v. United Kingdom

The UK doesn't have one law that covers everything related to counter-drone activities. Instead, it uses a mix of laws from different areas like aviation, policing, telecommunications, and national security. For example, the Air Navigation Order 2016 and the Civil Aviation Act 1982[6] are used to regulate activities related to drones. The Civil Aviation Authority is in charge of making sure civil drones are used safely, while the Ministry of Defence handles military drone activities. Police forces are responsible for enforcing the law when it comes to drones, using the Air Traffic Management and Unmanned Aircraft Act 2021.[7] This law helps police keep an eye on drones and make sure they're not used in a way that could harm people or cause problems. The UK's approach to regulating drones is complex, but it's designed to balance the need to allow drones to be used safely with the need to prevent them from being used in a way that could cause harm. By using a combination of different laws and regulations, the UK is able to keep track of drone activities and make sure they're not a threat to national security.

The Air Traffic Management and Unmanned Aircraft Act 2021 introduced enhanced enforcement powers relating to unlawful drone operations, including measures enabling authorities to investigate offences, require information, and seize unmanned aircraft connected with prohibited activities. These provisions primarily support law enforcement responses rather than providing a comprehensive framework for military counter-UAS capabilities.

The rules for flying in the UK are also affected by the Air Navigation Order 2016, which sets out rules and limits for drones, such as not flying near airports. These rules don't directly allow for technology to stop drones, but they do create boundaries that these technologies try to enforce. Another important law is the Wireless Telegraphy Act 2006, which controls the use of radio waves and generally doesn't allow interfering with communications without permission. This means that using technology to disrupt drone signals needs special permission and coordination with the people in charge of radio frequencies, showing the difficulty of balancing security needs with protecting regular communications and navigation services. For example, if someone wants to use a technology that jams drone signals, they need to get permission first and make sure it doesn't interfere with other important communications. This is a challenge because it's hard to stop drones without affecting other things that use radio waves. The UK government has to balance the need to stop drones with the need to protect other important communications, like those used by airplanes and emergency services. Overall, the rules in the UK for flying drones and stopping them are complex and need to be carefully managed to ensure safety and security. The government has to consider many different factors and balance competing needs to create effective regulations.

[6] *Civil Aviation Act 1982* (UK), 1982, c 16.
[7] *Air Traffic Management and Unmanned Aircraft Act 2021* (UK), 2021, c 12.

Counter-drone technologies deployed by military or police authorities must comply with aviation safety requirements, data protection legislation, the Human Rights Act 1998, and spectrum regulation administered by Ofcom.

vi. Türkiye

In Turkey, the government has rules to control the use of drones. These rules are part of the country's defense laws, as well as the Turkish Civil Aviation Law.[8] The Directorate General of Civil Aviation is in charge of making sure these rules are followed. The military is responsible for deploying drones, and the Information and Communication Technologies Authority manages the radio frequencies used by drones. For example, the Turkish Civil Aviation Law, which was passed in 1983, is an important part of these regulations.

Section D: Common Compliance Requirements and Conclusions

When it comes to laws about stopping unmanned aircraft, or drones, from causing trouble, countries have different rules. But most of these laws have some things in common. They usually say that people in charge of stopping drones need to work with the national aviation authorities to keep the airspace safe. They also need to get permission to use certain radio frequencies, following the country's telecommunications laws and international rules. Additionally, they have to make sure their systems are secure from cyber threats and protect the data they collect. This is especially important for systems that use artificial intelligence to make decisions. For example, when stopping drones, the systems used to control them need to be able to communicate safely and securely. This means using the right radio frequencies and protecting against cyber attacks. It's like having a special set of rules to make sure everything runs smoothly and safely. Overall, the goal is to keep people and things safe from drones that might be used for bad purposes. By having these rules and safeguards in place, countries can help prevent problems and make sure their airspace is secure.

When it comes to dealing with drones, most systems need a way to accurately identify and verify whether a drone is friendly or not, before taking any action against it. This is crucial in military operations, where the rules of engagement are based on principles like necessity, proportionality, distinction, and precaution. For instance, you need to make sure you're targeting the right drone, and that your response is proportionate to the threat. In order to deploy countermeasures like kinetic, electronic, or directed-energy systems, you need personnel who are properly trained and authorized to operate these systems. They must work within established frameworks to ensure that they are complying with both domestic and international laws. This is important to prevent any unintended consequences or violations of legal obligations. The key is to have a robust system in place that can distinguish between hostile and friendly drones, and to have clear guidelines and protocols for responding to different types of threats. By doing so, you can minimize the risks associated with drone threats, while also ensuring that you are operating within the bounds of the law.

Airspace Authorisation and Civil Aviation Coordination

[8] *Turkish Civil Aviation Law* (Türkiye), Law No 2920 (1983).

Managing airspace is a big deal when it comes to following the rules. When drones are used for counter-drone operations, they can pose a risk to regular air traffic, especially near airports, important infrastructure, or crowded cities. So, the military and police need to work closely with the people in charge of civil aviation to make sure they don't create problems for manned planes or approved drone flights. This is important to avoid accidents and ensure safe skies for everyone. By coordinating with each other, they can prevent hazards and keep the airspace safe.

The idea that countries have total control over the air above their land comes from a basic principle. This principle is stated in Article 1 of the Chicago Convention on International Civil Aviation.[9] While countries have the right to protect their air from hostile drones, they must do so without putting civilian air travel at risk. As military systems to counter drones are used more in civilian air traffic control, it's crucial to have good procedures in place to avoid conflicts, share information in real-time, and have compatible command systems. This is important because countries need to balance their right to defend themselves with the need to keep air travel safe and efficient. The Chicago Convention, which was agreed upon on December 7, 1944, and went into effect on April 4, 1947, sets out this principle in its first article.

Spectrum Management and Electronic Warfare

Using special devices to block or confuse drone signals is a really effective way to stop them without actually shooting them down. This can be done by jamming radio frequencies, messing with GPS signals, or even tricking the drone into thinking it's somewhere else. But here's the thing: these methods can also cause problems because they can interfere with other electronic signals that aren't supposed to be targeted, and that can be a big issue when it comes to following the rules.

National telecommunications authorities and the ITU strictly control how the radio spectrum is used. This means that any electronic warfare activities need to be approved, limited to specific areas when possible, and coordinated to avoid interfering with important things like civilian communications, satellite navigation, emergency services, and critical infrastructure. We've seen this become a problem recently, with GPS jamming during conflicts causing problems for commercial aviation, maritime navigation, telecommunications, and precision timing systems - the effects of electromagnetic interference often go beyond the intended target. As a result, countries are facing a challenge: they need to balance the need for military operations with their responsibility to prevent unnecessary interference with civilian use of the radio spectrum. For example, this can be seen in the ITU's Radio Regulations,[10] which outline the rules for using the radio spectrum to minimize harmful interference.

Identification, Target Verification and Rules of Engagement

To take any action, it's crucial that operators first confirm the aircraft is a real threat. This means they need to be able to identify, classify, and verify the target accurately. It's not as

---

[9] *Convention on International Civil Aviation*, 7 December 1944, 15 UNTS 295 (entered into force 4 April 1947), art 1.

[10] *Radio Regulations* (Geneva: International Telecommunication Union, 2024).

simple as it used to be, because these days, airspace is filled with all sorts of things like commercial drones, UAVs used by public authorities, and autonomous aircraft, all flying around at the same time. So, operators have to be careful to make sure they're dealing with a legitimate threat, and not something harmless. This is important because the consequences of making a mistake could be serious.

To ensure compliance, it's crucial to have strong sensor fusion, dependable AI algorithms, and clear rules of engagement that reduce the risk of misidentifying drones. If we can't tell the difference between hostile drones and civilian aircraft, it could lead to interfering with legitimate aviation activities or causing unintended harm to innocent people. In military operations, these requirements are based on the principles of distinction and precaution under international humanitarian law. This means defenders must verify their targets are military objectives before using force. It's all about being careful and precise to avoid mistakes. By having robust systems in place, we can minimize the risks and ensure that our actions are lawful and proportionate. This is especially important in complex environments where civilian aircraft and drones may be present, and the consequences of misidentification could be severe.

Necessity and Proportionality

The principles of necessity and proportionality underpin virtually every legal framework governing counter-drone operations. Defensive measures should be limited to those reasonably required to neutralise the threat while minimising collateral effects.

This principle also influences the selection of countermeasures. Electronic disruption may be preferable where a drone can be safely disabled without physical destruction, whereas kinetic interception may be justified only when non-kinetic alternatives are ineffective or where the threat poses an imminent risk to life or critical infrastructure. Similarly, directed-energy weapons such as high-energy lasers offer greater precision and reduced collateral damage than explosive interceptors but remain subject to operational limitations and aviation safety considerations.

Data Protection, Privacy and Artificial Intelligence

Today's systems for detecting and stopping unauthorized drones, known as C-UAS, are using more and more advanced technology to keep watch all the time. This includes using radar, special cameras that can see in different light, heat-sensing cameras, arrays of microphones, and systems that can detect and analyze radio signals, all backed up by artificial intelligence. These tools help us get a better picture of what's going on, but they also create a huge amount of data about regular airplanes, buildings, and people.

To follow the rules and regulations, we need to stick to the laws that protect people's personal information, keep computers and networks safe, and respect people's privacy. In the European Union, for instance, watching people or activities might mean we have to follow the General Data Protection Regulation (GDPR)[11] and the Law Enforcement

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation*), [2016] OJ L 119/1.

Directive,[12] depending on who is in charge. Using artificial intelligence adds more rules to think about, like being transparent about how algorithms work, having humans oversee things, and being accountable, especially when automated systems help make decisions about who to watch. For example, the General Data Protection Regulation is a law that was passed in 2016 to protect people's personal information and make sure it can be moved freely. There's also the Law Enforcement Directive, which is another law that was passed in 2016 to protect people's personal information when it's used by the authorities to prevent or investigate crimes. We need to think about how these laws affect the way we use artificial intelligence to watch people or activities. We have to be transparent about how our algorithms work and make sure humans are involved in the decision-making process. This is especially important when automated systems are used to help make decisions about who to watch or what activities to monitor. By following these rules and regulations, we can make sure that we're protecting people's personal information and respecting their privacy, while also keeping our computers and networks safe. This is an important part of being responsible and making sure our actions are fair and just. It's also worth noting that these laws and regulations are in place to help prevent the misuse of personal information and to protect people's rights. By following them, we can help build trust and make sure that our actions are transparent and accountable. This is an ongoing process that requires careful consideration and attention to detail, but it's an important part of being a responsible and respectful member of society.

Cybersecurity and System Integrity

As counter-drone systems become increasingly networked, cybersecurity has emerged as a critical compliance requirement. Integrated command-and-control platforms depend on continuous data exchange between sensors, communication networks, and interception systems, creating potential vulnerabilities to cyber intrusion, spoofing, data manipulation, or denial-of-service attacks.

The suitable cybersecurity practices will protect from a cyberattack against a C-UAS network which could compromise threat detection, generate false targets, or disrupt defensive responses.

Accountability and Human Control

An emerging compliance issue concerns the degree of human involvement in increasingly autonomous counter-drone systems. Current international practice continues to emphasise meaningful human control over decisions involving the use of force. Human operators remain legally responsible for authorising engagements, ensuring compliance with applicable rules of engagement, and preventing unlawful targeting. As autonomous technologies continue to evolve, maintaining effective human oversight will remain central to both domestic regulation and the broader international debate on autonomous weapons systems.

[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (*Law Enforcement Directive*), [2016] OJ L 119/89.

Conclusion

After delving into the counter-drones technologies, their applications and the choices made by engaged States, we moved on to the correlation of such operations with their legislative backbone. It is evident that technologies and innovation emerge and evolve faster that regulations can be developed. States cannot predict future issues and create variable provisions in advance. Existing laws were drafted when C-UAS were simpler and their capabilities far less. What is more, many legal frameworks regulate the effects of these technologies (e.g., interference with spectrum, airspace disruption, use of force, surveillance) rather than the technologies themselves. This suggests that future regulation may need to focus on operational effects rather than specific systems.

Furthermore, as the deployment of such systems combines different authorities' work and expertise -defence, aviation, telecommunications, data protection, national security- questions are raised on whether it would be useful to establish either a separate authority or a board consisting of representatives of each authority studying relevant matters and drafting regulations, taking into account all compliance requirements and conflicting interests and circumstances. With the exception of the United States, there is lack of harmonization among the multiple disciplines involved at a C-UAS mission in active countries' legislations.

Another interesting point of discussion is the distinction between military and civilian C-UAS. Many legal systems provide relatively broad authority for military use during armed conflict or protection of defence assets, but impose much stricter limitations on civilian authorities protecting airports, prisons, critical infrastructure, or public events. This difference is becoming increasingly significant as drone threats expand beyond traditional military contexts.