LEGAL STATUS OF ANTI-DRONE SYSTEMS UNDER INTERNATIONAL LAW

Andrei-Alexandru STOICA*

Abstract

The idea behind countering drone systems has been an ongoing issue for both states and the international community as it became clear that unmanned vehicles are going to become an integral part of any state's arsenal and infrastructure.

As drone technology developed so did the necessity to protect communities, borders and even rights from prying eyes and possible incursions. Furthermore, the requirement to protect communities and high value objectives has been detrimental after drone technology became accessible to a larger demographic, but while a large spectrum of drones can be bought by almost anyone, the same can't be said about counter-drone technology, which is currently sparse or exclusively in governmental control. Most anti-drone systems on the market are variants of existing anti-weaponry devices that were given another capability, but sometimes without meeting the requirements for certification or receiving a proper updated mechanical or software part.

This paper will focus on outlining a series of anti-drone systems that are available and how they are being currently used by states inside and outside their borders, but also to show who is allowed to use them and under what circumstances. Furthermore, the paper will showcase why international law is important in governing how counter-drone systems are deployed and used by states and why international law will be a frontrunner in the legalization process of said systems.

As a conclusion, the paper will mediate between current legal systems from states that have adopted anti-drone systems and how the international community must ensure the safety of other states and their citizens from the growing threat of unlawful drone deployment

Keywords: *drones, international law, counter-drone, human rights, terrorism*

1. The legality of drone systems under current international law.

In aviation, space, or ever roads, drones have achieved a level of implication that robotics and automation failed to gather and as such a drone is considered an unpiloted craft that can be used in such a way that the safety of the pilot is put firsthand, while ensuring less mechanical difficulties.

As such, drones have been around for a long time, some of the earliest recorded usages were from the time period of 1848-1849 when the Austrian Empire attacked Venice with a revolutionary tactic for that time period, an air raid. The air raid was conducted with balloons strapped with explosives while a copper wire acted as a trigger mechanism for dropping the bombs[1]. The bombs did not cause major damage but the psychological impact was devastating to the inhabitants.

Once technology evolved, drones were supposed to help the Allies in World War 2 to carry out bombing runs without the need to put lives in danger[2]. As such, B-24 bombers were supposed to be remote controlled so that they can destroy German bunkers in occupied France, but unfortunately the program ended in a disaster.

Later on, development went from controlled aircraft to controlled missiles, which offered the real proto-drone by today's standards. This marked the usage of surveillance drones in conflicts such as Vietnam, where over 550 drones had been lost and over 3000 intelligence missions were conducted[3].

While these drones had the capability to use weapons during combat situations throughout the Vietnam, Bosnia, Kosovo, Yemen conflicts and culminating with the Taliban insurgency, the first proper drone strike featuring the signature targeted killing nomenclature was in 2001 when the United States of America used a Predator drone to strike Mullah Omar, a Taliban leader, but failed to strike the target and instead caused other insignificant damage to the Taliban cause. This strike alone almost caused the operation to come to a halt[4] and caused a rupture in the chain of command.

The need to equip drones with lethal and non-lethal equipment came after CIA failed to take out Osama bin Laden in 2000, when after flying a drone over bin Laden's compound US forces figured that by the time the Tomahawk missiles would hit the area, bin Laden would have gotten away and would go into hiding. This moment sparked the need to equip drones with equipment needed for different outcomes.

* Phd. Candidate, Faculty of Law, Doctoral School, International Public Law, University Nicolae Titulescu (stoica.andrei.alexandru@gmail.com)

[1] Ron Bartsch, James Coyne, Drones in society. Exploring the strange new world of unmanned aircraft, Routledge, 2017, ISBN 978-131-5409-65-8.

[2] John Sifton, A brief history of drones, The Nation, 07.02.2012.

[3] Sam Biddle, America's killer drones of the Vietnam War, gizmodo.com, 14.03.2012.

[4] Chris Woods, The story of American's very first drone strike, The Atlantic, 30.05.2015.

Seeing the growing spectrum of activities where drones are active it's only safe to assume that a need to counteract these devices and vehicles from illicit activities is a must in a democratic society that acknowledges the rule of law.

While drone usage has skyrocketed signaling a global market value of over 127 billion dollars[5] , so must the legal framework ensure that only legal drone systems are permitted to operate inside a state's border and outside of it. Drones operate in helping with traffic solutions, energy transportation and production, but also in city and rural infrastructure development and as such the possibility of an illicit action must be countered.

The issue with drone defense mechanism is that the legality mechanism described by Article 36 of the Additional Protocol I to the Geneva Conventions (1949) has to be met before the mechanism is deployed[6]. As such, a minimum legal standard has to be achieved before drones and anti-drone systems are deployed in both conflict and peace activities.

But seeing as how drones have been around for hundreds of years and only after two world wars where they acknowledged through the Paris Convention of 1919 and Chicago Convention of 1944 when unmanned aircrafts (balloons, unmanned planes and guided aircraft) had to be integrated in the airspace of a state and ensure that state actors and citizens respect territorial limitations and also obtain the proper documents to legally own and fly said devices[7]. No aircraft capable of being flown without a pilot shall be flown without an onboard pilot over the territory of another State without special authorization by that State and in accordance with the terms of such authorization. Each State undertakes to insure that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft.

However, state practice has downplayed the efficiency of these norms, meaning that both public and private entities have to find other, more long-term solutions that also fall into these legal limitations outlined by current treaties.

2. Means and methods of countering the unmanned vehicle threat.

The growing drone technology implementation in agriculture, tourism, law enforcement and transport also brought new threats to these fields, while also endangering data protection legislation.

For example, U.S. forces captured drones belonging to the Islamic State which were supposed to be used as improvised bombers. The sound of the drone rotors gave them away and as such the ground forces managed to take out the drones using standard ammunition[8]. A similar scenario played out in Venezuela in 2018, when two drones had been spotted near President Nicolas Maduro who at that time was giving a speech. One drone exploded near the venue and another missed the mark and crashed, but while the attack did not injure anyone, the psychological impact of the explosion dispersed the crowd.

Another important event in which a drone was countered is marked by the downing of the RQ-170 Sentinel drone that was spying Iranian facilities in 2011[9]. The drone was taken out not with conventional anti-air methods, but instead had its software hacked and flown down without causing real physical damage. Fast forwarding to 2018, Israel confirmed shooting down a drone that was similar to the old RQ-170 Sentinel model that was captured by Iranian forces in 2011[10].

The year 2018 also marked a growing trend of drones being captured or destroyed in armed conflicts as Russian forces captured drones armed with explosives near its army bases near Lattakia (Syria). Of the 13 drones that were identified, 7 where taken out with conventional anti-air methods and 6 had been hacked by electronic warfare units[11]. Albeit primitive looking by todays standards, the makeshift design choice was intended as it helped the craft avoid jammers and radars while also lowering production costs, but still relied on satellite navigation.

Other counter-drone incidents involved the usage of Patriot Missile Defense Systems deployed in Israel, in 2017 and 2018, as a means to enforce the 1974 Agreement on Separation of Forces and as such to enforce the demilitarized zone between Syria and Israel[12]. This sparked a lot of criticism from western states since a standard Patriot missile costs somewhere in between 1 to 6 million USD dollars, while the drones involved in these skirmishes were very cheap.

All these incidents show how easy drone can be used to create cheap and efficient chaos on the battlefield and can spark a new trend in terrorism threats and conducts on civilian targets far away from any battlefields.

An Israel Intelligence Heritage and Commemoration Center report from 2018 on the global

[5] PWC, Clarity from above, PwC global report on the commercial applications of drone technology, May 2016.
[6] Steven J. Barela, Legitimacy and drones: Investigating the legality, morality and efficacy of UCAVs, Routledge, 2016, ISBN 9781315592152.
[7] Martha Magdalena Bradley, Drones and the Chicago Convention, University of Pretoria, 2014, pg. 10-13.
[8] Michael Hamann, Can you legally counter a drone?, Policemag, 16.11.2018.
[9] Alex Spilius, Iran shows off captured US drone, The Telegraph, 08.12.2011.
[10] Jamie Tarabay, Israel: Iranian drone was shot down was based on captured US drone, CNN, 12.02.2018.
[11] Vladimir Isachenkov, Whose drone did the Russian military capture in Syria?, Military Times, 11.01.2018.
[12] Associated Press, Israel again fires Patriot missile at drone from Syria, 13.07.2018.

jihadi phenomenon[13] highlighted that ISIS used drones for terrorism acts and intelligence gathering activities since 2014. A lot of these drones had been acquisitioned from Europe and delivered to Syria and Iraq to be used against the national and foreign forces deployed there.

After the downfall of the Islamic State, terrorists' part of the movement issued threats that retaliatory terrorist acts would be taken against western cities via drones. Propaganda videos developed in Syria and Iraq showed how drones released bombs on unsuspecting targets in cities and caused collateral damage as result.

Further analysis of this type of new-age terrorism revealed that operatives had to fill-out feedback forms on the results they achieved or did not achieve[14]. In the early years of the conflict, the Islamic State tried to use drones as efficient spy planes, but later on changed their tactics to better reflect those of the United States or United Kingdom, both of them using armed drones to strike targets with signature strikes. About one-third of the aircraft, some as small as model airplanes, dropped bombs or were rigged with explosives to detonate on the ground, while Iraqi officials said bombs dropped by the drones, which were primarily quad copters, had killed dozens of governmental soldiers, caused a lot of injuries and it had a particular value as a propaganda tool.

The document also points out that most of these drones had been commercial drones that anyone can buy from a store and had been retrofitted with explosives with ease, making them lethal, but not really a game-changer in the conflict.

The RAND Corporation and World Economic Forum also published a report[15] that explains how there is basically no barrier in acquiring and arming a store-bought drone and how the proliferation of certain emerging technologies has effectively diffused power and made it available at the lowest levels.

This potential to take down airliners, governmental buildings, landmarks or to conduct assassinations has no limit and current means and methods of defense cannot stop this growing phenomenon.

The report also claims that Hezbollah and Houthi rebels have managed to learn, without external aid, how to operate small drones in order to take down air defenses, while also concluding that the worst nightmare for any security service or law enforcement agency is that anyone can drop chemical, biological or nuclear poisoned materials from drones, more so as 2020 will spark a boom in drone transport technology.

One of the most acknowledged events in which drones caused serious discontent was marked by the 2018 Gatwick airport chaos[16] that was caused by individuals who operated personal drones very close to the airport and by doing so almost caused an aviation incident that could cost human lives. The incident led to a 36 hour lockdown and at least 6 arrests, while also causing western based governments to admit that a nationwide counter-drone strategy is required in order to prevent unlawful drone usage.

The problem with the Gatwick incident is that most drone using states had been warned in advance regarding such vulnerabilities. The FBI told the U.S. Senate that drone threats are escalading and that security agencies require new tools in order to protect civilian lives and property[17] and so President Donald Trump gave new powers to federal authorities in order to develop programs, deploy tools and tackle emerging drone threats by removing them, however it would be deemed necessary, from the sky. Since 2017, the Federal Aviation Agency has banned drones over military bases, national landmarks, nuclear sites, airports and other sensitive areas, ever since the 1 million drones' registration mark had been hit.

Others claim that Gatwick was just the tip of the iceberg as terrorists would much rather hit objectives where mass gatherings happen, such as stadiums. These gatherings can average around 40 000 people at a time and as such a terrorist attack would much rather take place there than at an airport[18].

To counter such a threat, the U.S.A. devised a radar that can identify targets based on their physical characteristics, meaning that the radar can identify birds, balloons and drones, while also communicating the flight path to the radar operator. Afterwards, the drone can be intercepted with electronic jammers or lasers. This radar was tested and certified by the Federal Communications Commission in 2019 as the radar was used to protect the Super Bowl LIII event[19].

This radar came as a legal response to a loophole that forbid local law enforcements to tackle drones as these unmanned vehicles could only be targeted and handled by federal agencies. To help local authorities, the Trump administration opened up projects that will help both public and private sectors to control ongoing drone traffic around sensitive areas and as such to deter potential unlawful activities.

The United Kingdom used the Drone Dome[20] to counter drones by soft-killing and ceding control in order to safely land the threat. The Drone Dome was first used in the conflict against ISIS and helped coalition forces to liberate Mosul. The system itself is

[13] Meir Amit Intelligence and Terrorism Information Center, ISIS's use of drones in Syria and Iraq and the threat of using them overseas to carry out terrorist attacks, 29.10.2018.
[14] Eric Schmitt, Papers offer a peek at ISIS drones, lethal and largely off-the-shelf, New York Times, 31.01.2017.
[15] WEForum and RAND Corporation, Drone terrorism is now a reality and we need a plan to counter that, Geostrategy Platform, 20.08.2018.
[16] Gareth Davies, Gatwick chaos: Arrests made over drones after fresh scare, The Telegraph, 22.12.2018.
[17] David Shepardson, FBI chief says threats from drones to US steadily escalating, Reuters, 10.10.2018.
[18] Zak Doffman, Forget Gatwick, why the deadliest terrorist threat from drones is not in our airports, Forbes, 27.12.2018.
[19] Haye Kesteloo, Super Bowl drone drama to be prevented with 3D radar system, Dronedj.com, 29.01.2019
[20] iHLS, Israeli technology defeated Gatwick Airport drones, 23.12.2018.

mounted on a moving platform and can jam controls in a 360 degrees arc. The manufacturer also sells a laser mounted system that can hard-kill targets. The radar itself can identify different kinds of targets from up to 5 kilometers away[21].

While technology against technology might seem the proper answer, other states tried to find a cheaper alternative to combat drones. The Netherlands[22] and Russian Federation[23] tried using hawks to hunt drones, but later found out that these birds of prey are not capable in tackling heavier drones and instead tried using falcons to capture drones, both states having success on a small scale and will require a lot of time before it can be implemented in every large city.

Japan saw a need to counter drones after the 2015 Tokyo incident, when a drone carrying a poisonous substance was found on the roof of the Prime-Minister's house. This sparked the Japanese police to train a special taskforce capable of preventing and capturing drones that fly to close to sensitive locations by flying a drone armed with a large net[24].

The Russian Federation on the other hand developed the Stupor gun, an electromagnetic pulse gun that can take out drones and even small aircraft or helicopters by knocking out the link between the operator and his craft. Support documentation explains that the device is capable of suppressing navigation and transmission channels used by unmanned aerial vehicles, as well as their photo and video cameras within the electro-optical range of frequencies[25].

While most the aforementioned equipment is found mostly in the hand of specialized operators that are part of state public authorities, a lot of accessible anti-drone equipment can be bought by individuals who want to protect their property from unlawful operations.

For example, SkyWall100[26] is a shoulder mounted gun that fires a homing projectile, which opens up and captures the drone with a net, then pulls the drone down to the ground with a parachute, making it a non-lethal approach to drones. On the other hand, the DroneShield[27] is a gun that fires electromagnetic pulses towards the drone, terminating the connection with its operator and so allows the gun owner to control the drone and land it without destroying it.

Both these options are based on already tested equipment that is found in the arsenal of army and law enforcement agencies. Also, it's important to note that a lot of other similar equipment have been showcased, most of these means and methods of countering drones having spawned a plethora of similar competition.

However, the most efficient anti-drone system was the software-lock that drone manufacturers integrated from the start, at least in advanced drones that offer their own operating system. For example, the Chinese drone manufacturer, DJI, developed a software based mechanism that prevents the drone from flying in an unlawful manner or close to protected areas, while also making the drone to refuse commands if the operator does not update the drone to meet legislative criteria[28]. The software-lock also offers a kill-switch meant to allow authorities to neutralize a threat preemptively, but unfortunately the locking software was later hacked by different hacker groups and was easily bypassed by anyone interested.

This prompted DJI to integrate a new mechanism instead of the lock, a mechanism that requires the user to pass a flight knowledge quiz that also involves understanding legal aspects of lawful flight[29]. The software was tested in the United Kingdom, Australia and China and could be implemented by other drone manufacturers at a later stage.

One of the shortcomings of inefficient drone traffic control and improper registration in a national registrar is that crimes get more efficient due to new technologies being introduced into the fray. For example, the United Kingdom face a growing number of drone operators that act as drug dealers and use their drones to smuggle drugs inside prisons[30]. A similar practice was also spotted in Canada, Australia and the United States of America.

To counter the drug carrying drones, prisons started using more barb-wire as an efficient low tech solution, but are also testing anti-drone electronic jammers and guns.

Still these solutions are in a testing phase and current legislation found in almost all drone operating states does not offer enough of a guarantee that operators will have a lawful conduct nor does it offer enough protection for potential victims of unlawful conduct.

Without a proper certified anti-drone mechanism, states have to resort to improvised solutions while testing methods of countering drones and certifying these methods to ensure a legal and fair use. For example, Germany and the United Kingdom have been testing an automated response system that connects to different and existing gathering tools (satellite, radar, cctv) and afterwards deploys a counter drone that after

[21] Times of Israel, UK army said to use Israeli-made system to end drone chaos at London airport, 21.12.2018.
[22] Thuy Ong, Dutch police will stop using drone-hunting eagles since they weren't doing what they're told, The Verge, 12.12.2017.
[23] Moscow Times, Kremlin trained falcons capable of taking down drones, 29.01.2018.
[24] Rhiannon Williams, Tokyo police are using drones with nets to catch other drones, The Telegraph, 21.01.2016.
[25] Tass, Russian Defense Ministry develops electromagnetic gun to counter drones, 22.08.2017.
[26] OpenWorks youtube channel, video presentation of said equipment can be accessible at this link: https://www.youtube.com/watch?v=M6tT1GapCe4.
[27] DroneShield gun promotional video can be found at this link: https://www.youtube.com/watch?v=fpmVTbBB0Qc.
[28] Mike Murphy, DJI is letting people override its software that prevents its drones flying in restricted areas, Qz.com, 06.07.2016.
[29] DJI, DJI introduces knowledge quiz for drone pilots in the UK, 21.12.2017.
[30] BBC, Well-organized gang flew drones carrying drugs into prisons, 30.08.2018.

it acquires its target it captures it with a net-gun[31]. However, the manufacturer has yet to certify the mechanism and also claimed that such technology is still in early stages, meanwhile other incidents such as Gatwick can happen anytime.

Meanwhile, drone incidents continue to rise and the potential of these types of conducts to cause a tragic event will continue uncontested. In China a person was detained for flying up-close to a commercial airliner that was doing a landing maneuver near an airport[32], while in Canada a drone hit a plane, causing light damage, with the owner remaining unidentifiable and forcing the government to start a real legal reform[33].

3. The legal standpoint regarding anti-drone systems.

Drone legislation has been passed in a number of states, in thanks to the International Civil Aviation Organization and European Union paving the way and thus ensuring that states have a similar legislation in regards to operators and their obligations to fly or operate under strict guidelines, anti-drone technology is relatively new and has yet to fully comply with article 36 of the Additional Protocol I to the Geneva Conventions (1949) or other international covenants.

The problem with legislation is that major players in the drone industry, such as the United States of America, forbid usage of counter-drone technology to the general populace and only certify state actors to handle with such technology. Counter-drone mechanisms have been tested during armed conflicts, but in an internal state affair, it could cause collateral damage and could be considered disproportionate[34]. For example, by using a drone jammer it would affect not only the targeted drone but also other gadgets, radio-communication devices and even the health of living beings.

Authorities could end up violating national statues regarding wiretapping, sabotage and computer fraud laws if the countermeasures are deployed without a clear understanding of the rules and regulations that apply. The common denominators in counter-drone technology are detectors and defenders. These terms are being advertised as counter drone technology are not really counter technology but are just drone detectors, the systems can't really do anything to stop drones, rather they identify the drone and its operator and also alert police forces in order to locate the drone operator on the ground and force the drone to the ground.

In the European Union detectors (radars) that have the possibility to detect drones have been tested and will be fully integrated in the European Aviation Safety Agency and EUROCONTROL air traffic and navigation system once the unified airspace regulation will be adopted.

Although many radars exist, they do not all comply with the laws, because they either use the right frequencies but are not yet certified or they do not use the appropriate frequency for a given state. Frequencies allocation is not the same for every state and all of these allocations must be done by a certified authority[35]. Also, most radars are placed near seaports or airports and have a technical radius of detection so a lot of space inside a state remains uncovered.

Other methods of detection include acoustic, optical and infrared detection, but all of these have shortcomings when dealing with homemade drones or drones that are not equipped with telecommunication capabilities. For example, unmanned underwater vehicles have low acoustic and electromagnetic signature, making them difficult to locate by these means, thus making them ideal for underwater intelligence gathering, mine detection and neutralization and can also traverse the polar ice cap[36].

While almost all radar systems are certified and article 36 (Additional Protocol I, Geneva Conventions of 1949), some are currently being developed to be integrated inside a drones, meaning that drones can identify drones in their respective field of activity. For example, the JY-300 is a Chinese drone, equipped with an autonomous module that can perform take-offs and landings, also the drone can be mounted with sea-target detection radar, synthetic aperture radar and optical and electronic surveillance apparatus[37].

As noted, the identifying a target does not equate to neutralizing the threat and so it must be used in conjunction with other methods.

The most common target-neutralizing methods described are the classic radar and conventional lethal or non-lethal ammunition. This means that the Convention on Certain Conventional Weapons[38] (1980) and its 5 protocols has to have its criteria met beforehand in armed conflicts. Out of the protocols, Protocol IV[39] has an interesting prohibition regarding the usage of lasers seeing as how lasers are not expressly prohibited unless they were designed to inflict blindness.

[31] iHLS, Drone traffic prompts anti-drone security experimentation, 21.02.2019.
[32] Euan McKirdy, Drone's operator detained for flying near Chinese airplane, CNN, 17.01.2017.
[33] Sherisse Pham, Drone hits passenger plane in Canada, CNN, 16.10.2017.
[34] Jonathan Rupprecht, Ability to stop drone attacks in U.S. is lacking, Forbes, 21.12.2018.
[35] GovernmentEuropa, The legal and technical requierments for countering drone technology, 08.06.2018.
[36] Michael Schmitt, International law and the military use of unmanned maritime systems, International Review of the Red Cross (2016), 98 (2), 567–592. doi:10.1017/S1816383117000339.
[37] Zhao Lei, Flying radar is first early-warning drone, ChinaDaily, 10.11.2018.
[38] Entered into force in December 1983.
[39] Came into force in July 1998.

However, drones and their operators cannot be blinded since the Protocol does not prohibit attacks against binoculars, periscopes, telescopes, and other optical equipment because the attack does not affect the operator who in most cases watching from very far away or is behind a screen and allows for attacks on electronic optical equipment, because damaging it would not cause human injury, as such drones only get their internals destroyed and not the human operator.

Legally countering drones can also be done with firearms and depending on who the shooter is (private person, police force, and army), weapons can be used from small scale and small stopping power, such as pistols, to heavier ordinance such as missiles or shells.

Jamming and hacking seem like the more elegant solution since a drone requires telecommunication channels to function, and in most cases the link between operator and drone is not encrypted.

Both jamming and hacking represent a kind of approach that has side-effects, meaning that it is indiscriminate and disproportionate if used without proper planning. For example, the United States of America through the Federal Aviation Agency in 2018[40] explained in a circular letter sent to airports that jamming technology can create a host of problems, such as electromagnetic and radio interference affecting safety of flight and air traffic management issues.

The object of jamming is to render radio transmissions unintelligible by causing interference, as such, but by using said jamming devices civilians and law enforcement agencies could very well fall short on the standards developed by the International Telecommunication Union in 2016 regarding Radio Regulations[41] and also the Union`s Constitution[42]. The risks associated with counter-drone methods involve the usage of blocking transmissions that are reserved for special situations (police, medical or firefighters) and can even block air traffic control radar beacons.

Jamming in armed conflicts can however be permitted as long as it does not violate article 8 of the Hague Convention for the Protection of Cultural Property[43] and the attack complies with Rule 8 of the Customary International Humanitarian Law adopted by the International Committee of the Red Cross[44]. As such, civilian communication lines have to be protected from jamming as they are not military objectives per-se, yet numerous military manuals and official statements consider that an area of land can constitute a military objective if it fulfils the conditions contained in the definition and in turn a jammer can hit that entire area, drones included, without it being considered a violation of international humanitarian law.

Drone jamming, done in either civilian or armed conflict situation, has to also comply with article 36 of the Additional Protocol I, as the device must be certified by a state authority and has to have a legal basis to operate. Most states have criminalized the interference with lines of communication and as such only state actors could legally take down a drone with jamming devices, this means that the law prohibits willful or malicious interference to government communications; subjects the operator to possible fines, imprisonment, or both.

Hacking (or spoofing) on the other hand is subject to a series of conventions and guidelines that are not legally binding, except for customary law that is common in all situations of armed conflict and international human rights law. For example, the Tallinn Manual 2.0[45] applies the doctrine of state responsibility, codified mainly in the International Law Commission's Articles on State Responsibility (2001) and so any kind of cyber operation targeted towards any specific terminal (including drones) translates to international responsibility for a cyber-related act that is attributable to the state and that constitutes a breach of an international legal obligation, neither physical damage nor injury is required for a cyber-act to be an internationally wrongful act and geography is not determinative in determining state responsibility.

While traditional counter-drone methods such as lasers or bullets can offer a near irrefutable indication of attribution of an activity to a state's actors, jamming and hacking cannot be so easily be traced. However, all state actors implicated in the usage of hacking and jamming technology must respect human rights law regardless.

As an example of how the legal system could react to counter-drone mechanisms, a U.S.A. national court had analyzed a case regarding the shooting down of a drone that was hovering near private property. The local judge in Kentucky that judged the criminal charges that were brought against the drone slayer stated that he had the right to shoot the drone since it was an invasion of privacy. Later, the decision was appealed to a District Court, the appeal was dismissed as lacking of subject matter jurisdiction and thus the protection of private property against drones saw a surge in the need of proper anti-drone devices[46]. It's important to point out that the drone slayer case happened in a state (from the United States of America) that allows citizens to fire weapons more freely, other states from the U.S.A., Europe or other places will not

[40] Office of Airports Safety and Standards, U.S. Department of Transportation Federal Aviation Administration, 19.07.2018, accessible at https://www.faa.gov/airports/airport_safety/media/Counter-UAS-Airport-Sponsor-Letter-July-2018.pdf.
[41] Radio Regulations Articles, 2016, ITU.
[42] ITU, Geneva, adopted in 1992.
[43] Entered into force on 7.08.1956.
[44] Jean-Marie Henckaerts , Louise Doswald-Beck, Customary International Humanitarian Law, Vol. I, 2009, ISBN 978-0-521-00528-9, pg. 29-32.
[45] Eric Talbot Jensen, The Tallinn Manual 2.0: Highlights And Insights, Georgetown Journal Of International Law, Vol. 48, 2017, pg. 735-778.
[46] Dusty Wooddell, The 'Drone Slayer' Has Case Dismissed By Federal Judge After Shooting Down Neighbor's Drone, Fstoppers, 27.03.2017.

tolerate illegal weapon discharges and will require interested parties that suffered from unlawful drone usage to seek protection from state authorities.

Currently the Federal Aviation Agency and the European Union Aviation Safety Agency both have similar classification for types of drones, some being in the same category as aircraft and so using counter-drone mechanism could be a criminal act since some drones fall under a special category that has a very special legal protection.

In 2018, a man in Texas was arrested for criminal mischief after he shot a drone that was operated by his neighbor. The drone was not on his private property but on the neighbor's side but the attacker claimed that it caused some light damage to the trees near his house and as such protected his property. Since the drone was not violating his property, the attack was deemed as a criminal offense[47].

As counter-drone systems allows the possibility to take-over the drone and its controls, state legislation requires that operators (in certain categories) be certified and/or own a pilot license for that type of vehicle. This means that if a person counters a drone by taking over the drone, which said person should own a certification to also operate it as operating without proper papers could also lead to administrative measures and even criminal offenses.

In a Congress Report compiled by the United States Government Accountability Office[48] found that over 6000 drone sightings near sensitive objectives had been reported in the U.S.A. since 2014, but only 49 of these were followed by a legal action. In most cases, the operator could not be identified and the drones rarely show up on current radar technology. Until a unified space for both traditional aircraft and drones is set up, small flying drones will continue to cause problems for authorities.

As it stands I.C.A.O.'s Manual on Remotely Piloted Aircraft Systems[49] and JARUS's recommendations[50] are the only generally civilian and commercial norms that are accepted on an international scale, and as such offer the best perspectives for states to adopt a stance on countering drone threats. What the Congress Report compiled by G.A.O. did outline was that only a handful of states (members of the international community) adopted national legislation that requires drone operators to obtain operational certificates and to register with a national registrar, thus allowing an uncontrolled proliferation of unmanned vehicles.

Currently, the United States of America has started a legislative reform to allow governmental agencies to mitigate drone threats that come close to sensitive areas, while also exempting counter-drone activities from federal criminal laws[51], while the European Union adopted the Drones Amsterdam Declaration[52] in order to implement the U-space Demonstrator Network, a system that will allow better security and privacy legislation and enforcement mechanisms in order to prevent unlawful usage of drones.

As drones become smaller and faster so must the response to unlawfulness be on par with the development of said drones. In the future, soldiers will have to carry anti-drone equipment when going on the battlefield and so military squads will compromise of drone and anti-drone users, with their respective gear[53].

4. Conclusions

To summarize, counter-drone legislation is an integral part of drone legislation, one cannot function without the other, but technology has evolved in a rapid burst and so states must identify the best solution to counter not only legally manufactured drones but also homemade drones that function on other frequencies and with different load-outs than the commercially available ones.

As more states open registrars for different kinds of drones and adopt better detection capabilities, so will homemade drones have to comply to universally accepted standards or face legal action from state authorities in order to comply. There are enough counter-drone devices, both work-in-progress and traditional to ensure that private property and privacy are protected from unlawful conduct and also to protect military objectives. The only downside is that everyone is going for the cheaper alternative instead of trying to identify solutions that do not require the usage of force or tampering.

Such solutions are already offered by international organizations in the form of registrars, universal design standards and the possibility to impose fines and even jail time to those who do not comply to socities rules. Unfortunetly, society had to endure the growing fear of ISIS terror threats of improvised drone bombs to grasp the problem while other incidents where human lives where put in harms way, such as the 2017 Seatle incident where a person got 30 days of jail time and a fine for crashing a drone in a person and causing said person to be knocked unconsciously[54].

The year 2017 also saw the incident between a civilian drone and an army helicopter, back when the United Nations General Assembly was in session. The army helicopter was doing a patrol mission, while the

[47] Haye Kesteloo, Man shoots gun at neighbor's drone, Dronedj, 19.11.2018.
[48] GAO, Small Unmanned Aircraft Systems FAA Should Improve Its Management Of Safety Risks, GAO-18-110, May 2018.
[49] DOC 10019, ICAO, 2015.
[50] Accessible on https://rpas-regulations.com/community-info/jarus/.
[51] DHS Science and Technology Directorate, Countering Unmanned Aircraft Systems – Fact Sheet 2018, DHS.gov.
[52] Amsterdam 28 November 2018, accessible at https://ec.europa.eu/transport/sites/transport/files/2018-drones-amsterdam-declaration.pdf.
[53] Maj. Hassan Kamara, Rethinking the U.S. Army infantry rifle squad, Military Review, Army University Press, March-April 2018.
[54] Ben Popper, Man gets 30 days in jail for drone crash that knocked woman unconscious, The Verge, 27.02.2017.

drone was in a no-fly zone, and so the operator was found guilty of flying the drone in the no-fly zone.

Unless states move to adopt a common position on how to treat unlawful conduct, then drone countering devices will remain needed and must be certified in order to be used by law enforcement agencies and private contractors or civilians.

The lack of express legislative actions in counter-drone devices should be seen as an inaction of state actors, but rather it should be seen as a continuation of adapting current legislation to current issues.

However, unless a unified space for drones to be accepted in is not developed, then the proliferation of drones will remain a problem that will have to tackle and so even a soft-ban of drone could happen, a move that may seem counter-productive to the current economy where aautomation represents a key development in combating lack of human resources. Current estmations point out that 2030[55][56] will be the year of autonomy in jobs, where drones and robots in general will overtake the number of people and so being able to counter rouge or hijacked robots will be deemed mandatory.

References

- Ron Bartsch, James Coyne, Drones in society. Exploring the strange new world of unmanned aircraft, 2017;
- John Sifton, A brief history of drones, The Nation, 07.02.2012;
- Sam Biddle, America's killer drones of the Vietnam War, Gizmodo, 14.03.2012;
- Chris Woods, The story of American's very first drone strike, The Atlantic, 30.05.2015;
- PWC, Clarity from above, PwC global report on the commercial applications of drone technology, May 2016;
- Steven J. Barela, Legitimacy and drones: Investigating the legality, morality and efficacy of UCAVs, 2016;
- Martha Magdalena Bradley, Drones and the Chicago Convention, 2014;
- Michael Hamann, Can you legally counter a drone?, Policemag, 16.11.2018;
- Alex Spilius, Iran shows off captured US drone, The Telegraph, 08.12.2011;
- Jamie Tarabay, Israel: Iranian drone was shot down was based on captured US drone, CNN, 12.02.2018;
- Vladimir Isachenkov, Whose drone did the Russian military capture in Syria?, Military Times, 11.01.2018;
- Associated Press, Israel again fires Patriot missile at drone from Syria, 13.07.2018;
- Meir Amit Intelligence and Terrorism Information Center, ISIS's use of drones in Syria and Iraq and the threat of using them overseas to carry out terrorist attacks, 29.10.2018;
- Eric Schmitt, Papers offer a peek at ISIS drones, lethal and largely off-the-shelf, New York Times, 31.01.2017;
- WEForum and RAND Corporation, Drone terrorism is now a reality and we need a plan to counter that, Geostrategy Platform, 20.08.2018;
- Gareth Davies, Gatwick chaos: Arrests made over drones after fresh scare, The Telegraph, 22.12.2018;
- David Shepardson, FBI chief says threats from drones to US steadily escalating, Reuters, 10.10.2018;
- Zak Doffman, Forget Gatwick, why the deadliest terrorist threat from drones is not in our airports, Forbes, 27.12.2018;
- Haye Kesteloo, Super Bowl drone drama to be prevented with 3D radar system, Dronedj, 29.01.2019;
- iHLS, Israeli technology defeated Gatwick Airport drones, iHLS, 23.12.2018;
- Times of Israel, UK army said to use Israeli-made system to end drone chaos at London airport, Times of Israel, 21.12.2018;
- Thuy Ong, Dutch police will stop using drone-hunting eagles since they weren't doing what they're told, The Verge, 12.12.2017;
- Moscow Times, Kremlin trained falcons capable of taking down drones, Moscow Times, 29.01.2018;
- Rhiannon Williams, Tokyo police are using drones with nets to catch other drones, The Telegraph, 21.01.2016;
- Tass, Russian Defense Ministry develops electromagnetic gun to counter drones, 22.08.2017;
- Mike Murphy, DJI is letting people override its software that prevents its drones flying in restricted areas, Qz.com, 06.07.2016;
- DJI, DJI introduces knowledge quiz for drone pilots in the UK, 21.12.2017;
- BBC, Well-organized gang flew drones carrying drugs into prisons, 30.08.2018;
- iHLS, Drone traffic prompts anti-drone security experimentation, 21.02.2019;
- Euan McKirdy, Drone's operator detained for flying near Chinese airplane, CNN, 17.01.2017;
- Sherisse Pham, Drone hits passenger plane in Canada, CNN, 16.10.2017;
- Jonathan Rupprecht, Ability to stop drone attacks in U.S. is lacking, Forbes, 21.12.2018;
- Michael Schmitt, International law and the military use of unmanned maritime systems, International Review of the Red Cross (2016);
- Zhao Lei, Flying radar is first early-warning drone, ChinaDaily, 10.11.2018;
- Geneva Conventions 1949 and Additional Protocol I from 1977;

[55] PwC report that can be accesibile from this website: https://www.pwc.co.uk/services/economics-policy/insights/the-impact-of-automation-on-jobs.html.

[56] Mark Muro, Automation and artificial intelligence, Brookings Metropolitan Policy Program, January 2019.

- Paris Convention of 1919;
- Chicago Convention of 1944;
- 1974 Agreement on Separation of Forces;
- I.C.A.O.'s Manual on Remotely Piloted Aircraft Systems, 2015;
- Office of Airports Safety and Standards, U.S. Department of Transportation Federal Aviation Administration, 19.07.2018;
- Radio Regulations Articles, 2016, ITU;
- ITU Constitution and Convention, 1992;
- Hague Convention for the Protection of Cultural Property, 1956;
- Jean-Marie Henckaerts , Louise Doswald-Beck, Customary International Humanitarian Law, Vol. I, 2009;
- Eric Talbot Jensen, The Tallinn Manual 2.0: Highlights And Insights, 2017;
- Dusty Wooddell, The 'Drone Slayer' Has Case Dismissed By Federal Judge After Shooting Down Neighbor's Drone, Fstoppers, 27.03.2017;
- Haye Kesteloo, Man shoots gun at neighbor's drone, Dronedj, 19.11.2018;
- GAO, Small Unmanned Aircraft Systems FAA Should Improve Its Management Of Safety Risks, 2018;
- Amsterdam Declaration, 2018;
- Maj. Hassan Kamara, Rethinking the U.S. Army infantry rifle squad, Military Review, March-April 2018;
- Ben Popper, Man gets 30 days in jail for drone crash that knocked woman unconscious, The Verge, 27.02.2017;
- Mark Muro, Automation and artificial intelligence, Brookings Metropolitan Policy Program, January 2019.