USE OF DRONES (UAS) IN CIRCUMVENTION OF SECURE AREAS

Amer Smailbegovic
DTCare Sarajevo
Sarajevo, Bosnia and Hercegovina
amer@dtcare.org

Metodija Dojcinovski (Ret)
Military Academy
Skopje, North Macedonia
metodija.dojcinovski@ugd.edu.mk

Abstract: ***The recent hostilities in the East (Ukraine, Azerbaijan) are showing the capabilities and multitude of the Unmanned Aircraft Systems (UAS), colloquially known as drones, which are fielded by various security forces as well as other entities. The proliferation and ubiquity of various sizes of UAS, their low detectability profile and ability to gather various information and intelligence in real-time, makes them a formidable tool and considerable adversary when applied within the secured zones. This study shows some of the trends in use of UAS to monitor, track and interdict incursions, track and predict incursion routes in the light of recent initiatives to deploy and develop fleets of medium-endurance, all-weather drones that would effectively patrol the frontiers of EU and some neighboring nations. The increased use of drones by nation states in law enforcement creates various conundrums with regards to privacy, decision making, militarization of border and overall accountability. On the opposite side, the proliferation of drones in the illicit uses enables smuggling, counter-intelligence, counter-surveillance or even direct action by the non-state, transnational or criminal enterprises. The paper presents some of the potential scenarios in which the drones may be used on either side of the security equation to develop better understanding of the threat environment, technological means, limitations and operational use.***

Keywords: Drone, UAS, Surveillance, Security perimeter, C4ISR

1. INTRODUCTION

The merging crises of 2020-2023 (migrations, pandemic, hostilities) have fast-tracked variety of programs aimed at improving stand-off surveillance and security [1]. One element of the renewed interest in the overall surveillance architecture is the use of drones as tools for long-loitering, persistence-surveillance platforms [2]. The use of drones on on the borders of EU has been operationalized since 2009 and has expanded in its scope and capability to encompass variety of platforms, sensor systems to form its own command-communication-control-computers and intelligence-surveillance-reconnaissance (C4ISR) component [3]. These activities are also overprinted on the trends observed in the Western Balkans, primarily in the use of multi-intelligence

technical means [4] as well as increased securitization of migrants (Sabanija 2021)

2. DRONE CONUNDRUM

Unmanned Aerial Vehicles/Systems UAV/UAS, colloquially known as drones are nowadays becoming ubiquitous in all elements of life: on one end of the spectrum they are viewed as toys for entertainment and leisurely activities, whilst on the other end of the spectrum they veer into the particular niche for executing variety of specialized tasks (logistics, mapping, communications and military applications). The partial autonomy of drones provides new added value and a force multiplier in an advanced economy, digital landscape but also as evolving threats to the modern society.

Number of incidents involving the drones and general public [5] are expected to increase and escalate as they are deployed across the variety of cultural landscapes and challenge the notions of privacy and property [6]. The everyday use also challenges the notion of ethics [7], especially in police work (Heesen, Schuster and Arzt 2019), civil liberties (Reynolds 2019) and indoor use (Molina, et al. 2018). The recent use of drones to track and enforce COVID-19 pandemics spread and quarantining [8], manage borders [9] and track migrations in Southern Europe [10] have resulted in a considerable reevaluation of the drone deployment framework and practices in individual countries as well as in EU. The new rules regulate both the technical, legal and operational requirements for drone usage within the European Union and oblige operators of drones to register in the EU Member State where they have their primary place of residence or their main place of business. Beyond EU, there are also studies questioning the current U.S. doctrine and reliance on the UAS systems. The principal quandary is a moral dilemma whether the effectiveness of weaponized UAS that remove the human warfighter from the battlefield would lower not only the costs and risks associated with fighting, but the political "bar" to initiating hostilities [11] as well, in U.S. but also enable its allies as well as the adversaries [12].
The rapid development and availability of technological innovation suggests that drones will be capable of many missions currently performed by small aircraft and helicopters, but far cheaper, easier and in many cases stealthier. The proliferation of this inexpensive and readily available COTS technology will make the application for terrorist (or non-state actor) use easy to achieve and difficult to counter.

3. DETECTION AND COUNTERMEASURES

When discussing the utility of drone in the realm of border protection and wider border-related C4ISR, it is important to outline the potential observables and signatures that are sought in the way of managing migrations and countering illegal border crossings. The drone is not a replacement for the personnel deployed in the field, but it can significantly aid them in their situational awareness and patrolling efforts.

3.1 DETECTION

The principal ability to use the drone in such environment depends on the drone payload, endurance (length of airborne mission), power source (on-board or replenishable) and the desired mission profile (detecting visual data, collecting signals etc.). Majority of the uses are still in the passive information-gathering source, but there are also trends of active drone use to delivery kinetic payloads and neutralize a particular "target" [13].

The table below outlines some of the main signatures and observables that can be developed by using drones in the tasks of border security:

Table 1: Key target observables detectable via drone's on-board sensors

ENVIRONMENT	VISIBLE	INFRARED	MICROWAVE
LAND	Groups of people Tracks Debris / garbage	Heat signatures Vegetation disturbance Soil disturbance	Radio transmissions Doppler anomalies Acoustic vibrations
MARITIME	Vessels Wake and waves Flotsam	Heat signatures Top-cover detection Fuel residue	Radio transmissions Wave disturbance

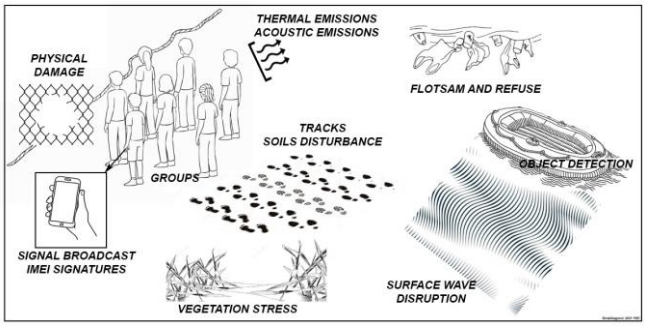

Figure 1: Key target observables detectable via drone's on-board sensors (original drawing)

It is often a combination of these observables that draws the attention of the drone's operator / analyst or an automated target-classification system highlighting a potential anomaly; recent advances in the automatic scene recognition and anomaly identification allows for a more rapid characterization of the imaged area [14]. For example, a group of would-be border crossers would generate multiple signatures that, when combined, would suggest that there is a border crossing in progress or that it has occurred (see Figure 1).

The ability of drone to cover relatively large swaths of ground or to loiter over particular areas of interest (AOI), which have been identified as problematic, is an important element of the border surveillance matrix given its inherent size and complexities. As such, an important element in narrowing down the area and detecting personnel, incursions and even hostile drones is the growing ability to monitor signals and communications via IMEI/IMSI capture method [15]. Every electronic-transmitting instrument is assigned a characteristic identifier known as International Mobile Equipment Identifier (IMEI) and the assigned number is unique to every unit. Installing a passive antenna scanning system onto a drone, it is possible to collect International Mobile Subscriber Number (IMSI) and the Electronic Serial Number (ESN) numbers of mobile phones in that area and see who is in that given area. Upon registering the presence of the receiver, it can be cross-referenced against the directory of known units.

Should an unknown transmitter appear in the area, the system can pin-point the location using the characteristic IMEI and based on the signal strength of the device it is possible to find the exact location of the mobile phone or another transmitter (radio or hostile drone telemetry).

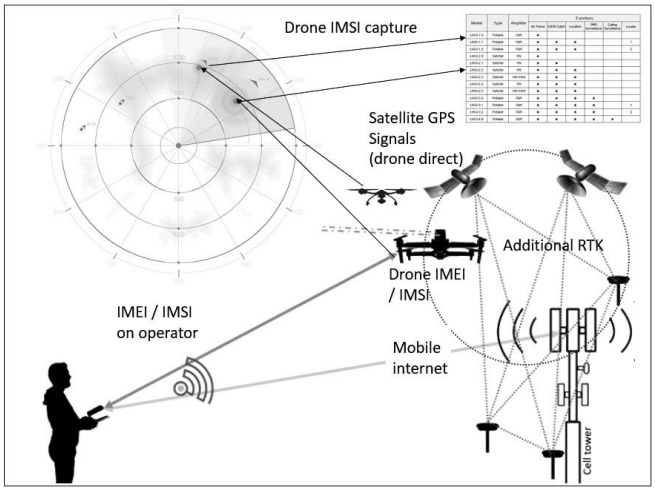

Figure 2: Elements of drone / operator IMEI-IMSI capture utilizing GPS, advanced real-time kinematic (RTK) corrections and air-to-ground communications between the drone and the operator (original drawing with adaptations from Sundance Media Group 2022).

3.2 COUNTERMEASURES

The same technology and means can be employed in reverse by the groups or an individual intent on circumventing the border crossing protocols and any associated C4ISR / ISR activity. While there is a well-established array of camouflage, concealment and deception (CCD) tactics against ISR assets [16], the challenge in countering drones is their unpredictability, relative invisibility and ability to image the target from the variety of angles. Hence any CCD tactics employed against the active ISR drone need to be adaptive and dynamic to evade the detection or proactive in the sense of eliminating the opposing ISR asset [17]. The best example of such adaptive tactics can be observed from the narco-cartels operating around the coast of Florida, USA: when the U.S. border authorities started employing high-resolution imaging assets to spot the boats, the boats started using a blue tarpaulin cover to camouflage themselves; when the border authorities started using down-looking radar to find the camouflaged boats, the cartel started using semi-submersible crafts, and when the sonar was employed, the cartel developed the land-route through Mexico]18].

The most effective method to counter the employed perimeter ISR, appears to be the combination of extensive preparation and diversion [19] using a variety of adaptive tactics and institutional learning (in the case of trans-national criminal enterprises) to successfully employ drones against the other drones. An example of such tactic is presented in the Figure 3 below using the first-hand information from the field.

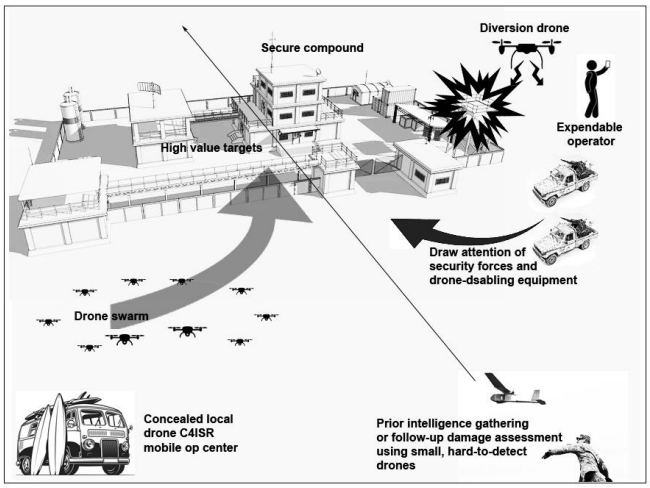

Figure 3: Potential diversion-type scenario using variety of technical means to circumvent key-point security assets and enable illegal entry (original drawing).

3.3 LIMITATIONS

Whenever discussing the utility of drones in border security or counter-border scenarios, one must take into consideration limitations related to drone use and effectiveness. The main limitations are useful payload, range/endurance, weatherproofing and hardness. Majority of the commercially available drones are relatively fragile and have limited range and staying power, however that does not preclude them from being adapted or hardened as required. The availability of better batteries and more-efficient propulsion systems has extended the drone endurance from 30 minutes to up to four hours or more, even during inclement weather. This presents a problem because the inexpensive and ubiquitous commercial drones can counter dedicated ISR drones employed at the border. It is to be expected that the new technologies are going to emerge and enhance the range and capabilities of the drones with more and more autonomy, further complicating the drone vs. drone encounters. The current air-defense and area-defense systems are still catching up in being able to offer a suitable and multi-role defense against the drones and are caught up in the infamous Arithmetic on the Frontier by Kipling [20], where the low-cost threat defeats the top-tier solution.

3.4 COUNTER-DRONE

The current research and development landscape outlines several pathways towards disruption of hostile drones through the uses of radio frequency (RF) spoofing and jamming [21], directed energy / electro-magnetic (EM) directed interference [22] and susceptibility of on-board software and electronics to such interference [23], targeting the on-board communications, as well as enabling continuity of communications if being jammed by the drone [24] IMEI firmware corruption [25] and GPS spoofing [26]. Besides EM/RF and cyber means there are also various kinetic means of drone elimination [27] or capture using a net [28] or other types of obstructions forming a layered defence system.

4. CONCLUSIONS

The current contest between the opposing drones is confined to ISR / counter-ISR and diversion in which the variable technical capacities (and costs) are facing off in an increasingly contested

airspace. Specialty multi-sensor drones will continue becoming irreplaceable and frequently employed as ISR tools by the law enforcement to monitor multiple areas and secure points of entry along the borders. However, with commercial drones becoming smaller, more adept and autonomous, it is to be expected for them to be used to track the law enforcement themselves and possibly even target them as well as their drones. There are already cases where the commercially available and specially-adapted drones are used in targeted assassinations [29].

In the current migration-related trends, it is expected that nation states or collective border security entities (i.e. FRONTEX) will continue expanding their drone fleets and integrated C4ISR methods to get the best out of tracking various observables and targeting parameters to interdict illegal border-crossings and manage migration trends. The overall trend is expected to trickle down to even non-EU member states who are likely to implement drones as a tool in border management and monitoring. Given that there are also considerable financial interests for various trans-national criminal organizations to sustain human smuggling and illegal border-crossings [30], it may be reasonable to expect expansion of drone use to provide real-time, tactical information on the deployment of security forces and ISR assets in order to effect a successful illegal border crossings [31].

REFERENCES

[1] Kaunert, C., and S. Leonard. 2013. *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe.* New York, NY, USA: Palgrave Studies in European Union Politics.

[2] Pendall, David. 2005. *The Promise of Persistent Surveillance: What are the Implications for the Common Operating Picture?* Monograph, FT. Leavenworth, KS, USA: US Army Command and General Staff College.

[3] Matthias, Monroy. 2021. "Border drones (Part 1): Unmanned surveillance of the EU's external borders by Frontex." *Security Architectures and Police Collaboration in the EU.* 07 22. Accessed 1 22, 2022. https://digit.site36.net/2021/07/22/border-drones-part-1-unmanned-surveillance-of-the-eus-external-borders-by-frontex/.

[4] Smailbegovic, A., and N. Korajlic. 2021. *Compendium on crisis management in the Western Balkans: selected articles on regional crisis management : 2019-2021.* Sarajevo: Faculty of Criminal Justice and Security Studies, University of Sarajevo, Bosnia and Herzegovina.

[5] Wild, Graham, John Murray, and Glenn Baxter. 2016. " Exploring Civil Drone Accidents and Incidents to Help Prevent Potential Air Disasters." *Aerospace. 3. 22.* 3-22.

[6] Nassi, Ben, Asaf Shabtai, Ryusuke Masuoka, and Yuval Elovici. 2019. "SoK-Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps." *arXiv:1903.05155.*

[7] Wilson, R.L. 2014. "Ethical issues with use of Drone aircraft,." *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering.* Chicago, IL, USA: IEEE. 1-4.

[8] Kitchin, Rob. 2020. "Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19." *Space and Polity* https://doi.org/10.1080/13562576.2020.1770587 .

[9] Krajickova, K. 2014. Drones´Deployment by Frontex and Fundamental Rights and Civil Liberties. . Thesis, Enschede, NL: University of Twente.

[10] Marin, L., and K. Krajčíková. 2016. "Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights." In *Drones and unmanned aerial systems: Legal and social implications for security and surveillance*, by Ales Zavrsnik, pp.101-127. Ljubljana: University of Ljubljana, Slovenia.

[11] Harris, K.E. 2016. Asymmetric Strategies and Asymmetric Threats: A Structural-realist Critique of Drone Strikes in Pakistan, 2004-2014. Thesis, Washington, D.C.: Virginia Polytechnic Institute and State University.

[12] Hamilton, Mark. 2017. *The Third Offset, Remotely Piloted Systems, and Moral Hazards.* Thesis, Carlisle, PA: U.S. Army War College.

[13] Yaacoub, J. P., H. Noura, O. Salman, and A. Chehab. 2020. "Security analysis of drones systems: Attacks, limitations, and recommendations." *Internet of Things, 11, 100218.* https://doi.org/10.1016/j.iot.2020.100218.

[14] Lokman, G., and G. Yilmaz. 2014. "A new method for anomaly detection and target recognition." *2014 International Conference on Unmanned Aircraft Systems (ICUAS).* DOI:10.1109/ICUAS.2014.6842300.

[15] Dabrowski, A, N Pianta, T Klepp, M Mulazzani, and E. Weippl. 2014. "IMSI-catch me if you can: IMSI-catcher-catchers." *ACSAC '14: Proceedings of the 30th Annual Computer Security Applications Conference* . ICPS. 246–255.

[16] Maillard, W. 2005. Investigation of CONOPS for ISR and Weapon Systems in Missions against Targets Employing Deceptive Tactics. White Paper, El Segundo, CA, USA: Aerospace Corp.

[17] Jerome, David. 2020. "Military Drones and Robots: The New Revolution in Military Affairs." In *Examining War and Conflict around the World.* , by David Jerome, 418. Santa Barbara, CA: ABC-CLIO LLC.

[18] Sullivan, J.P., and R.J. Mexican Bunker. 2017. "Mexican Cartel Strategic Note No.18: Narcodrones on the Border and Beyond. ." *Small Wars Journals.*

[19] Schmersahl, A.R. 2018. Fifty Feet Above the Wall: Cartel Drones in the U.S.-Mexico Border Zone Airspace, and What to Do About Them. Thesis, Monterey, CA: Naval Postgraduate School.

[20] Kipling, R. 2013. "Arithmetic on the Frontier." In *Poems of Rudyard Kipling*, by T. Pinney, https://www.kiplingsociety.co.uk/poem/poems_arith.htm. Cambridge, UK: Cambridge University Press.

[21] Abunada, A.H., A.Y. Osman, A. Khandakar, M.E. Chowdhury, T. Khattab, and F. Touati. 2020. "Design and Implementation of a RF Based Anti-Drone System. ." *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT),.* IEEE. 35-42.

[22] Michel, Arthur Holland. 2018. *Counter Drone Systems.* White Paper, Berlin, Germany: Bard College.

[23] Lopes-Esteves, J., E. Cottais, and C. Kasmi. 2018. "Software Instrumentation of an Unmanned Aerial Vehicle for HPEM Effects Detection." *2nd URSI Atlantic Radio Science Meeting (AT-RASC),.* Meloneras: IEEE. 1-4.

[24] Masood, Ali, Davide Scazzoli, Navuday Sharma, Yannick Le Moullec, Rizwan Ahmad, Luca Reggiani, Maurizio Magarini, and Muhammad Mahtab. Alam. 2020. "Surveying pervasive public safety communication technologies in the context of terrorist attacks." *Physical Communication 41* https://doi.org/10.1016/j.phycom.2020.101109.

[25] Esteves, J. L., E. Cottais, and C. Kasmi. 2018. "Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV." *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE).* Amsterdam, NL: IEEE. 48-52.

[26] Gaspar, J., R. Ferreira, and P. Sebastião. 2020. "Capture of UAVs Through GPS Spoofing Using Low-Cost SDR Platforms." *Wireless Pers Commun* https://doi.org/10.1007/s11277-020-07211-7.

[27] Vitalii, V., Oleksii Martyniuk, Volodymyr Mirnenko, and Pavlo. Openko. 2019. "General Approach to Counter Unmanned Aerial Vehicles." *Safety & Defense, 5* 6-12.

[28] Rothe, J., M. Strohmeier, and S. Montenegro. 2019. "A concept for catching drones with a net carried by cooperative UAVs ." *2019 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR).* Würzburg, Germany: IEEE. 126-132.

[29] Abdulla, Namo. 2021. "Drones Pose New Challenge to Iraqi Security ." *Voice of America.* 11 10. Accessed 1 21, 2022. https://www.voanews.com/a/drones-pose-new-challenge-to-iraqi-security/6307828.html.

[30] Snel, E, O Bilgel, and R. Staring. 2021. "Migration trajectories and transnational support within and beyond Europe." *Journal of Ethnic*

and Migration Studies, V.47, 11. https://doi.org/10.1080/1369183X.2020.1804189.

[31] Smailbegovic, A., Korajlic N., Ahic J., and Toth I. 2020. "Geospatial considerations within border surveillance networks and response articulation with regard to the migrant crisis in the Western Balkans." *Annals of Disaster Risk Sciences, Vol.3/1.*