HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 2. szám 107–121.
DOI: 10.32567/hm.2024.2.9

Gábor Horváth[1]

No Drone's Sky: Full Spectrum Drone Surveillance and Neutralisation Concept for Enhanced Counter-UAS Framework

(Part 2, Neutralisation)

Abstract

We are living in an era that is marked by the exponential growth of small Unmanned Aircraft Systems (sUAS), therefore the imperative for effective countermeasures against potential threats to public safety, national security, and individual privacy inherent in these airborne apparatuses has become increasingly pronounced. Following the foundational exploration of UAS surveillance in the first segment of the Counter-UAS (C-UAS) series, this second instalment shifts its gaze to the pivotal domain of drone neutralisation techniques. Investigating both soft and hard neutralisation methodologies, this study aims to unravel the intricate landscape of strategies devised to legally and securely incapacitate, disrupt, or assume control over sUAS threats. Drawing from a rich tapestry of existing literature and recent research endeavours, this paper embarks on an expedition through a spectrum of neutralisation approaches subjecting the aforementioned methodologies to rigorous scrutiny regarding their efficacy and other implications, in order to contribute substantively to the development of a resilient C-UAS framework. Moreover, this study lays the groundwork for the third part of this C-UAS series, where the author shall unfurl a vision of operation. Besides elucidating the challenges and opportunities inherent in the neutralisation of small drone threats, this study also aims to catalyse collaboration within the research community, dedicated to ensuring the secure coexistence within the airspace system.

Keywords: anti-drone, counter-UAS, drone sensing, drone neutralisation, drone surveillance

[1] Senior ATM Officer, Ministry of Defence, State Aviation Department, e-mail: horvath.gabor@uni-nke.hu

Introduction

The utilisation of small Unmanned Aircraft Systems (sUAS) is increasingly prevalent across a spectrum of malicious applications.[2] The escalating proliferation of these systems demands a re-evaluation of security measures for facilities in the foreseeable future. Traditional security protocols are anticipated to be inadequate due to the distinctive attributes of this emerging technology, facilitating swift circumvention of existing widespread systems and procedures.[3]

Consequently, numerous private, corporate and public entities find themselves inadequately equipped to mitigate threats posed by sUAS.[4] This paper categorises these threats as either *adversarial* or *unauthorised* based upon the operator's intentions, level of expertise, and the drone's operability. Both categories fall under the set of potentially harmful drone operations (Figure 1), which are defined below:

- *Adversarial sUAS (asUAS) threat* refers to the intentional and hostile use of small drones by individuals, groups, or entities with malicious intent. These threats may encompass activities such as surveillance, reconnaissance, sabotage, or direct attacks against targets of interest. Adversarial sUAS operators possess the necessary knowledge and expertise to deploy sUAS in a manner that poses risks to safety, security, and/or privacy, thereby constituting a deliberate threat to individuals, organisations, and/or critical infrastructure.
- *Unauthorised sUAS (usUAS) threat* involves the unlawful, malfunctioning, or illegal operation of small drones in violation of regulatory requirements, airspace restrictions, or established laws. These threats can arise from individuals or entities operating sUAS without proper certification, permits, or permissions, thereby posing risks to aviation safety, public security, or privacy. These activities include unauthorised, but not necessarily intended, flights in restricted airspace, interference with manned aircraft operations, and/or violations of privacy rights through unauthorised surveillance and/or data collection.

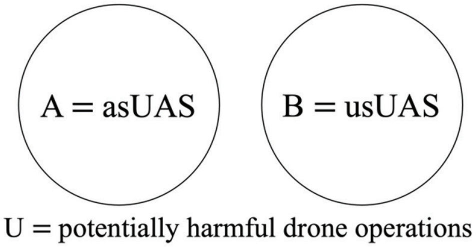

Figure 1: Presentation of potentially harmful drone operation sets
Source: compiled by the author

[2] Krajnc 2018.
[3] Jahangir–White 2021.
[4] Cline 2020.

The definitions given above play a crucial role within the confines of this study, as determining the appropriate intervention level of Counter-Unmanned Aircraft System (C-UAS) necessitates precise assessment of the extent of the small drone-induced threat. Therefore, the following sections introduce soft and hard mitigation techniques deemed most promising, then subsequently a mathematical formalisation of threat level determination is outlined, and finally conclusions are drawn to encapsulate the key findings.

Neutralisation methods

Neutralisation methods (NM) are triggered in order to counteract the threat posed by potentially harmful drone operations.[5] It is possible to activate multiple NMs simultaneously to enhance the efficiency of mitigation tactics. Additionally, these NMs may be situated on one or more distinct platforms, depending on the physical architecture of the Counter-Unmanned Aircraft System. During neutralisation C-UAS can execute the following actions:[6]

- controlling
- interrupting
- disabling
- destructing

These actions are facilitated through NMs, herein referred to as neutralisers, which have been categorised differently in different literatures,[7] but considering the aspects of set theory, the most scientifically founded solution might be the distinction between soft and hard neutralisation methods.

Soft neutralisation

Soft neutralisation (SN), within the context of C-UAS, denotes a particular approach wherein the neutralisation of a potentially harmful drone operation is achieved through methods that do not involve critical physical impact or destruction upon the targeted drone.[8] Instead, SN techniques focus on the disruption, interruption, or complete takeover of the drone's operation, effectively rendering it incapable of fulfilling its intended or unintended harmful mission. Soft neutralisation tactics are characterised by their emphasis on achieving operational success through subtle, non-destructive interventions, thereby minimising collateral damage, and preserving the integrity of the airspace environment. This multifaceted approach requires a comprehensive understanding of the target drone's capabilities, vulnerabilities, and operational context, as well as the development and deployment of sophisticated

[5] Csengeri 2019.

[6] Castrillo et al. 2022.

[7] Sander et al. 2018; Martins et al. 2020.

[8] Da Silva et al. 2023.

countermeasures tailored to neutralise its functionality while minimising the risk of unintended consequences. SNs encompass a diverse array of primarily non-kinetic means, including but not limited to electronic warfare techniques and cyber operations such as signal jamming, spoofing, hacking, while deploying countermeasures aimed at exploiting vulnerabilities in the drone's communication, navigation, or control systems.[9] Table 1 presents a comparative analysis of the key differences between various SN methods.

Table 1: Pros-cons comparison of UAS soft neutralisation methods

Method		**Principle**	**Enabler**	**Pros**	**Cons**
Jamming		Interfere with the communication system, prompting their evacuation or landing protocols.	Utilize an RF power amplifier and RF spectrum recognition technology.	Characterised by affordability, lightweight design, and compact dimensions, ensuring non-destructive interference. Suitable for concurrent application on multiple drones.	Effective solely against drones operating within the ISM[10] band, with potential interference to other ISM band devices.
Spoofing		Employ counterfeit positioning signals or simulated control commands to re-route drones.	Utilise signal analysis, data packet analysis, and decoding techniques.	Possess guidance and eviction capabilities without causing damage.	May disrupt other electronic devices. Limited effectiveness against encrypted communication channels.
Hacking		Acquire root privileges of drones' operating systems and execute requisite operations.	Engage in system penetration and analyse system vulnerabilities.	Characterised by cost-effectiveness and non-destructive capabilities.	Primarily compatible with specific operating systems and network-based protocols. May cause interference with other ISM band devices.

Source: compiled by the author

[9] Wentzel et al. 2024.

[10] ISM bands (industrial, scientific, and medical) are parts of the RF (radio-frequency) spectrum reserved for general use by, as the name suggests, scientific, medical, and industrial devices.

Jamming

A prevalent interrupting or disabling method for neutralising sUAS involves disrupting its sensors or systems using noise signals. In this paper, jamming is categorised into three main types: direct track deception, fusion, and protocol-aware, each targeting drone sensors and systems.[11] Researchers proposed a UAS team forming an air defence radar network to jam sensors, effectively tracking and jamming the targeted drones.[12] Another study utilised direct track deception and fusion to manipulate navigation and trajectory control systems, causing UAS to drift from the restricted areas.[13] Additionally, a software-defined radio (SDR)-based protocol-aware jamming system was introduced, outperforming tone and sweep methods.[14]

Researchers focused on long term evolution (LTE)-based UAS neutralisation, determining a jamming range of approximately 60 metres.[15] Furthermore, a system was developed to remotely neutralise explosive UAS in combat zones,[16] while a game theoretic approach was proposed for optimising jamming methods against UAS attackers.[17] Jamming offers non-damaging solutions to neutralise drones in restricted areas, functioning at various levels from hardware to software. However, its omni-directional effects and energy consumption pose challenges. Synthesising the studies referred above, the author suggest that jamming methods should be directional, controllable, and responsive.

Spoofing

Spoofing, as a controlling or interrupting neutraliser, involves generating fake signals to deceive the receiver of a potentially harmful drone, mimicking legitimate signals. The signals targeted for spoofing include those related to remote control, payload data, the Global Navigation Satellite System (GNSS), and sensors.[18] In order to execute spoofing, knowledge of communication protocol stacks is crucial. A study demonstrated a man-in-the-middle attack on UAS control systems, injecting control commands to interact with the UAS.[19] Another research utilized cracking software development kits (SDKs), reverse engineering, and GNSS spoofing to hijack UAS, comparing security performances of DJI and Parrot drones under exploitation attacks.[20]

Analyses were conducted on accessing internal sensors to neutralise sUAS in restricted areas that were largely successful.[21] A method to hijack the MAVLink

[11] Sliti et al. 2018.
[12] Zhao et al. 2009.
[13] Li et al. 2018.
[14] Pärlin et al. 2018.
[15] Curpen et al. 2018.
[16] Willner 2009.
[17] Bhattacharya–Başar 2010.
[18] Pistoia 2021.
[19] Rodday et al. 2016.
[20] Dey et al. 2018.
[21] Esteves et al. 2018.

protocol on ArduPilot Mega 2.5 autopilot was presented, and a probabilistic attack model against UAS using denial of service attacks was proposed.[22] A physical-layer spoofing attack based on angle of arrival and path loss factors to recognise and locate UAS was suggested.[23]

Hacking

Drone hacking, as primarily a controlling or interrupting neutraliser, has been a subject of research for many years, focusing primarily on external interference, and networking methods referring to the exploitation of vulnerabilities in sUAS control systems or communication networks to disrupt or neutralise potentially harmful drone operations.[24] Outer interference methods require close proximity of interference devices to sUAS sensors such as inertial measurement units (IMUs) and GNSS, ensuring accurate data retrieval.[25] It is worth highlighting that sUAS rely primarily on Wi-Fi and cellular networks for communication, presenting vulnerabilities that malicious actors exploit to seize control of the drone. By infiltrating these networks, attackers can manipulate the autopilot, issuing directives for secure take-off or redirection.

A C-UAS may exploit network vulnerabilities to intercept communication packets, modify commands, or enforce authentication checks randomly. The sensory arsenal of a drone offers additional hacking opportunities for counteractivity.

Hard neutralisation

Hard neutralisation (HN), within the realm of C-UAS, delineates a methodology characterised by the direct physical incapacitation or destruction of a potentially harmful drone. In contrast to SN techniques, which focus mainly on non-kinetic means of neutralisation, HN methods entail the use of kinetic or electromagnetic force to eliminate the threat posed by the target drone.[26] The implementation of HN measures necessitates precision targeting, modern weapon systems, and effective command and control mechanisms to ensure accurate engagement and minimise collateral damage. Furthermore, the decision to employ HN techniques often requires careful consideration of the operational environment, potential legal implications, and the risk of unintended consequences.

Despite their effectiveness in neutralising immediate threats, HN methods may entail significant logistical, ethical, and diplomatic considerations, making them a subject of rigorous analysis and debate outside the broader framework of C-UAS operations.[27] HN measures include the utilisation of kinetic or direct energy weapons

[22] Ficco et al. 2022.
[23] Huang 2018.
[24] Rodday 2016.
[25] Balestrieri et al. 2021.
[26] Pistoia 2021.
[27] Arteche et al. 2017.

to interrupt, disable, or destroy the potentially harmful drone. Additionally, hard neutralisation tactics may involve the deployment of physical barriers, such as nets, or drones equipped with capture devices, to physically detain or capture the target sUAS.[28] Table 2 presents a comparative analysis of the various drone HN methods.

Table 2: Pros-cons comparison of UAS hard neutralisation methods

Method	Principle	Enabler	Pros	Cons
Kinetic Energy Weapons	Utilise physical impact to disable or destroy drones.	Projectile launcher platforms.	Highly effective HN method, relatively low cost per kill ratio.	High probability of collateral damage, limited range.
Direct Energy Weapons	Employ directed energy (e.g. lasers, microwaves) to disrupt or destroy drones.	Laser systems, microwave emitters, etc.	Precise targeting, rapid response, SN capability.	Limited range, high cost per kill ratio.
Physical Barriers	Utilise physical obstacles to prevent drone intrusion.	Fencing, nets, walls, barricades, drones, etc.	Minimal risk of collateral damage, relatively cheap, deterrent, SN capability.	Limited use due to deployment-specific, space consuming nature.

Source: compiled by the author

Kinetic energy weapons

Kinetic energy weapons (KEW) are designed to physically impede potentially harmful drones, necessitating precise targeting and tracking.[29] KEW must closely engage with the drone under attack to effectively neutralise it. There is a broad spectrum of KEW HN methods, involving even trained birds, through weaponised drones and relatively simple projectile launcher platforms.[30]

Kinetic based neutralisers, such as machine guns, guided missiles, and artillery, rely on physical munitions to incapacitate drones with certain guided missiles necessitating tracking systems while others utilise optical sensors for detection. These solutions are costly, primarily used in military settings, and can cause collateral damage upon impact, therefore not optimal against sUAS.[31] Collision drones represent another kind of KEW approach, where dedicated agile and highly manoeuvrable drones equipped with detection and tracking capabilities pursue and collide with the target sUAS. They utilise computer vision techniques for detection and may carry explosives to

[28] Rudys et al. 2022.

[29] Pistoia 2021.

[30] Chamola et al. 2020.

[31] Kang et al. 2020.

maximise impact. However, like projectile-based neutralisers, they can cause collateral damage and have longer neutralisation delays. Ultimately, collision drones are disposable systems, acting as a hybrid between drones and missiles.[32]

Direct energy weapons

Direct energy weapons (DEW) possess the capability to emit electromagnetic energy across a broad spectrum, affecting targeted drones' electronics either temporarily or permanently. These electromagnetic waves are classified into two categories: narrowband (or high-power microwaves) and wideband. Each category exhibits distinct characteristics. Narrowband electromagnetics operate on a single-tone frequency, demanding high power levels, while wideband electromagnetics distribute energy over a wider band with short pulses. Precise targeting of DEW is imperative for their effectiveness, as improper directionality can diminish lethality. Moreover, accurate assessment of neutralisation effectiveness post-usage is crucial.[33]

Laser-based neutralisers, on the other hand, can incapacitate or destroy sUAS by ionising their path and emitting an electric current. Lasers are categorised as low-power or high-power variants, and as such, require precise aiming and tracking. High-power lasers are capable of inflicting destructive damage.[34] However, challenges such as technological complexity, weather sensitivity, and accurate targeting persist. While effective in military settings, the deployment of DEWs in civilian environments is fraught with risks, including potential collateral damage and interference with general aviation operations. Additionally, their large size, weight, and power requirements limit their integration primarily to terrestrial platforms, rendering them unsuitable for deployment on low-altitude platforms like mini drones.

Physical barriers

Net capture, a physical approach, entails deploying nets to hinder sUAS mobility. C-UAS employ guns or specialised weapons to activate the net, immobilising the drone upon contact. A deployable net capture system was developed for installation on aircraft or authorised UAS, capable of apprehending unauthorised or unsafe drones.[35] Another novel idea presents a spin-launched UAS projectile engineered to deploy a capturing net, seamlessly integrated within the projectile's warhead and activated through conventional firearms.[36] Physical capture strategies prioritise the immobilisation of drones and their control systems, offering advantages such as ease of use, lightweight construction, and rapid assembly. Although physical capture approaches are efficient and cost-effective, they may pose risks to pilots as captured

[32] Brust et al. 2021.

[33] Borja 2023.

[34] Taillandier et al. 2023.

[35] Pistoia 2021.

[36] Blyskal 2019.

drones could sustain damage at varying levels. A drone interceptor, equipped with nets launched from firearms, adeptly detect and swiftly intercept moving targets, leveraging multispectral on-board sensing for remote or autonomous precision capture of potentially harmful sUAS.[37]

Threat level determination

A properly automated, optimally functioning C-UAS system can select the most practical NM with the best efficiency in any given situation as quickly as possible. The primary prerequisite for this is the precise determination of the threat level (TL). Taking this idea into account, the author presents a theory of logical connectivity based on binary mathematical foundations that, using the concepts discussed above, facilitates achieving the appropriate level of automation for C-UAS while simultaneously selecting the most effective NM. In formulating the theory, the methodological foundations were provided by the philosophical principle known as *Occam's razor,* resulting in an abductive heuristic model[38] that herein applied deriving from the smallest possible set of elements based on the binary values: *0* and *1.* When determining the threat level, three parameters, *intention, risk,* and *operability,* have been identified, each of which can assume values between 0 and 1 (Table 3), therefore a TL contains a 3-digit binary code.

Table 3: Threat parameters' binary values

Value	**0**	**1**
Intention	asUAS	usUAS
Risk	high	moderate (or lower)
Operability	high	moderate (or lower)

Source: compiled by the author

Intention

Intention embodies the purpose or objective behind the actions of sUAS. It encompasses the goals, motives, and planned behaviours of the drone operator or controlling entity. Understanding the intention behind drone activities is crucial for gauging the level of threat posed by the drone and devising an appropriate response strategy, where a value of *0* signifies an asUAS and *1* signifies usUAS intent.

Analysing the intention of a drone operation aids in assessing the severity of the threat it poses. Intention can reveal whether the drone's activities are benign (usUAS), such as aerial photography or surveying, or malevolent (asUAS), such as surveillance,

[37] Kang et al. 2020.

[38] McFadden 2021.

intrusion, or potential attacks. The evaluation combines factors like the drone's flight pattern, payload, and proximity to sensitive areas.[39]

Furthermore, comprehending the intention behind drone operations assists in selecting the most effective NM. For instance, if the operator's intention suggests hostile actions or potential harm, a HN method, like KEW or DEW, may be warranted to promptly eliminate the threat. Vice versa, if the intention seems non-threatening or the risk level is low, a softer approach, such as signal jamming or communication disruption, may be more suitable to neutralise the drone without causing undue damage or escalation. Thus, intention plays a pivotal role in guiding the decision-making process for choosing between hard or soft neutralisation methods in C-UAS operations.

Risk

Risk refers to the likelihood and potential consequences of harm or damage resulting from the presence or actions of potentially harmful drones. It entails assessing various factors, including the capabilities of the drone, its proximity to critical infrastructure or sensitive areas, and the intentions of the operator, to determine the level of threat posed by the drone.[40]

In the process of TL determination, risk analysis plays a crucial role in evaluating the severity of the threat posed by a drone and guiding the selection of an appropriate neutralisation method. Risk assessment involves considering the probability of a drone causing harm or disruption, as well as the potential impact of such events on security, safety, and operations. Factors such as the drone's flight path, altitude, speed, payload capability, and communication protocols are taken into account when determining the risk level associated with a drone. Additionally, the vulnerability of critical assets or personnel to drone-related threats is assessed to gauge the potential consequences of an incident.[41]

Based on the assessed risk level, decisions can be made regarding the deployment of HN or SN methods. If the risk is considered high (*0* value), indicating a significant threat to security or safety, hard neutralisation methods such as KEW or DEW may be necessary to swiftly eliminate the threat. Conversely, if the risk is moderate (*1* value) or the threat is less severe, softer approaches such as signal jamming or communication disruption may be sufficient to neutralise the drone without causing undue harm or escalation.

Operability

Operability refers to the operational capability and effectiveness of both the sUAS and its operators in responding to and neutralising drone threats. Within the confines

[39] Palik 2013.
[40] Sander et al. 2018.
[41] Jahangir–White 2021.

of this study it encompasses not only the technical capabilities of the drone but also the presumed knowledge, skills, and decision-making abilities of the operators responsible for its deployment.

The operability of a sUAS and its operators plays a critical role in assessing the appropriate response to a perceived threat posed by potentially harmful drones.[42] Determining operability involves the investigation of the drone's flight path, altitude, speed, payload capability, and communication protocols. In this context, operability is classified into two distinct levels: *0* representing high operability, and *1* indicating moderate or lower operability.

In short, operability, encompassing both technical capabilities and operator proficiency, is a fundamental aspect of TL determination of a sUAS operation, guiding the selection of appropriate neutralisation strategies to address varying threat scenarios.

Decision making

Based on the binary determination of the three threat parameters, a total of eight different scenarios (Table 4) can be envisioned, providing the simplest theoretical description using all accessible data and thus satisfying the criterion outlined above by *Occam's razor.*

Table 4: Recommended NM for each threat level

	Hard neutralisation			**Soft neutralisation**		
Parameter	**Intention**	**Risk**	**Operability**	**Intention**	**Risk**	**Operability**
Threat level	0	0	0	0	1	1
	0	0	1	1	0	0
	0	1	0	1	1	0
	1	0	1	1	1	1

Source: compiled by the author

As illustrated in Table 4, the highest conceivable threat arises when facing asUAS (intention = *0*) paired with high level of risk (risk = *0*) and operability (operability = *0*). Vice versa, the inverse scenario occurs when a usUAS (intention = *1*) is assigned alongside moderate risk (risk = *1*) and operability (operability = *1*) values within the system. While the choice of NM may seem obvious for options at the extremes of the spectrum, deliberation over whether to opt for hard or soft neutralisation becomes more contentious, particularly around the median values. It is essential to emphasise that while the recommendations outlined in Table 4 can be considered as general guidelines, they may vary for a specific system (e.g. '*0 1 1*' could be addressed with HN since it has malevolent intention, if the environment otherwise allows this method).

[42] Arteche et al. 2017.

Conclusion

The examination of neutralisation methods for countering drone threats underscores the critical need for effective strategies to safeguard public safety, national security, and individual privacy. This study has explored a spectrum of soft and hard neutralisation methodologies, shedding light on their efficacy and other implications within the broader framework of C-UAS operations. By delving into soft neutralisation techniques such as jamming, spoofing, and hacking, as well as hard neutralisation methods including kinetic energy weapons, direct energy weapons, and physical barriers, this paper has provided a comprehensive analysis of the diverse approaches available for mitigating sUAS threats.

The genuine theory unfolded of this research, guided by the principle of Occam's razor, emphasises the importance of a minimalist, logical yet easily streamlined approach to threat level determination in C-UAS operations. By distilling complex threat scenarios into binary parameters of intention, risk, and operability, this study has facilitated the development of an abductive heuristic model for selecting the most appropriate neutralisation method. Through the application of this model, decision-makers can efficiently assess threat levels and deploy the optimal neutralisation method, whether soft or hard, to address the specific context of each situation.

Addressing possible opposing viewpoints, it is acknowledged that the choice between soft and hard neutralisation methods may be subject to debate, particularly in scenarios where threat parameters fall within intermediate values. However, by prioritising simplicity and efficiency in threat level determination, the proposed model offers a pragmatic framework for navigating such complexities and making informed decisions in C-UAS operations.

Furthermore, it is imperative to recognise that this study represents Part 2 in a series of papers on C-UAS, laying the groundwork for the final paper currently in progress. As such, the findings and methodologies presented herein pave the way for Part 3, which will focus on the vision of operation for comprehensive UAS surveillance and neutralisation frameworks. By building upon the insights gained from this study, the forthcoming paper will further elucidate the challenges and opportunities in the evolving landscape of C-UAS technologies and strategies.

In summary, the investigation conducted in this paper underscores the multifaceted nature of UAS threats and the importance of adopting innovative and adaptive approaches to counter them effectively. By embracing the principles of Occam's razor and logical connectivity, decision-makers can navigate the complexities of C-UAS operations with clarity and precision, ultimately enhancing the resilience and security of our airspace systems.

Acknowledgement

This paper was prepared with the professional support of the Doctoral Student Scholarship Program of the Co-operative Doctoral Program of the Ministry of Culture and Innovation financed from the National Research, Development and Innovation Fund.

National Research, Development
and Innovation Office

References

Arteche, David – Chivers, Kenneth – Howard, Bryce – Long, Terrell – Merriman, Walter – Padilla, Anthony – Pinto, Andrew – Smith, Stenson – Thoma, Victoria (2017): *Drone Defense System Architecture for US Navy Strategic Facilities.* Naval Postgraduate School, Monterey, USA.

Balestrieri, Eulalia – Daponte, Pasquale – Vito, Luca de – Lamonaca, Francesco (2021): Sensors and Measurements for Unmanned Systems: An Overview. *Sensors,* 21(4), 1518. Online. https://doi.org/10.3390/s21041518

Bhattacharya, Sourabh – Başar, Tamer (2010): Game-Theoretic Analysis of an Aerial Jamming Attack on a UAV Communication Network. In *Proceedings of the 2010 American Control Conference,* Baltimore, MD, USA, 2010, 818–823. Online: https://doi.org/10.1109/ACC.2010.5530755

Blyskal, Tomasz – Fong, Richard – Thompson, LaMar (2019): *Scalable Effect Net Warhead.* US Patent (Application Number: 10,197,365).

Borja, Lauren (2023): High-Energy Laser Directed Energy Weapons: Military Doctrine and Implications for Warfare. In Gruszczak, Artur – Kaempf, Sebastian (eds.): *Routledge Handbook of the Future of Warfare.* London: Routledge, 353–363. Online: https://doi.org/10.4324/9781003299011-37

Brust, Matthias – Danoy, Grégoire – Stolfi, Daniel – Bouvry, Pascal (2021): Swarm-Based Counter UAV Defense System. *Discover Internet of Things,* 1(2). Online: https://doi.org/10.1007/s43926-021-00002-x

Castrillo, Vittorio – Manco, Angelo – Pascarella, Domenico – Gigante, Gabriella (2022): A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. *Drones,* 6(3), 65. Online: https://doi.org/10.3390/drones6030065

Chamola, Vinay – Kotesh, Pavan – Agarwal, Aayush – Naren – Gupta, Navneet – Guizani, Mohsen (2020): A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Ad Hoc Networks,* 111, 102324. Online: https://doi.org/10.1016/j.adhoc.2020.102324

Cline, Travis (2020): *Mitigating Drone Attacks for Large High-Density Events.* PhD Thesis. Purdue University. Online: https://doi.org/10.25394/PGS.13341860.v1

Curpen, Radu – Bălan, Titus – Micloş, Ioan Alexandru – Comănici, Ionut (2018): Assessment of Signal Jamming Efficiency against LTE UAVs. In *2018 International*

Conference on Communications (COMM), Bucharest, Romania, 2018, 367–370. Online: https://doi.org/10.1109/ICComm.2018.8484746

Csengeri, János (2019): Counter-Drone Activity as a System. *Security & Future,* 3(1), 31–34.

Da Silva, Douglas – Machado, Renato – Coutinho, Olympio – Antreich, Felix (2023): A Soft-Kill Reinforcement Learning Counter Unmanned Aerial System (C-UAS) with Accelerated Training. *IEEE Access,* 11, 31496–31507. Online: https://doi.org/10.1109/ACCESS.2023.3253481

Dey, Vishal – Pudi, Vikramkumar – Chattopadhyay, Anupam – Elovici, Yuval (2018): Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study. In *31st International Conference on VLSI Design and 17th International Conference on Embedded Systems* (VLSID), Pune, India, 2018, 398–403. Online: https://doi.org/10.1109/VLSID.2018.97

Esteves, José Lopes – Cottais, Emmanuel – Kasmi, Chaouki (2018): Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV. In *International Symposium on Electromagnetic Compatibility,* (EMC EUROPE), Amsterdam, Netherlands, 2018, 48–52. Online: https://doi.org/10.1109/EMCEurope.2018.8484990

Ficco, Massimo – Palmiero, Raffaele – Rak, Massimiliano – Granata, Daniele (2022): MAVLink Protocol for Unmanned Aerial Vehicle: Vulnerabilities Analysis. In *2022 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress,* (DASC/PiCom/CBDCom/CyberSciTech), Falerna, Italy, 2022, 1–6. Online: https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927895

Huang, Ke-Wen – Wang, Hui-Ming (2018): Combating the Control Signal Spoofing Attack in UAV Systems. *IEEE Transactions on Vehicular Technology,* 67(8), 7769–7773. Online: https://doi.org/10.1109/TVT.2018.2830345

Jahangir, Mohammed – White, Daniel (2021): Good Practices and Approaches for Counter UAV System Developments – An Industrial Perspective. In Clemente, Carmine – Fioranelli, Francesco – Colone, Fabiola – Li, Gang (eds.): *Radar Countermeasures for Unmanned Aerial Vehicles.* E-book. Online: https://doi.org/10.1049/SBRA543E_ch12

Kang, Honggu – Joung, Jingon – Kim, Jinyoung – Kang, Joonhyuk – Cho, Yong Soo (2020): Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems. *IEEE Access,* 8, 168671–168710. Online: https://doi.org/10.1109/ACCESS.2020.3023473

Krajnc, Zoltán (2018): A drónok elleni stratégia és eljárások. *Repüléstudományi Közlemények,* 30(3), 139–148.

Li, An – Wu, Qingqing – Zhang, Rui (2018): UAV-Enabled Cooperative Jamming for Improving Secrecy of Ground Wiretap Channel. *IEEE Wireless Communications Letters,* 8(1), 181–184. Online: https://doi.org/10.1109/LWC.2018.2865774

Martins, Bruno – Holland, Arthur – Silkoset, Andrea (2020): *Countering the Drone Threat: Implications of C-UAS Technology for Norway in an EU and NATO Context.* PRIO Paper, Peace Research Institute Oslo.

McFadden, Johnjoe (2021): *Life Is Simple: How Occam's Razor Set Science Free and Unlocked the Universe.* New York: Basic Books.

Palik, Mátyás (2013): A pilóta nélküli légijárművek katonai alkalmazása. In *Pilóta nélküli repülés profiknak és amatőröknek.* Budapest: Nemzeti Közszolgálati Egyetem, 281–298.

Pärlin, Karel – Alam, Muhammad – Moullec, Yannick (2018): Jamming of UAV Remote Control Systems Using Software Defined Radio. In *2018 International Conference on Military Communications and Information Systems* (ICMCIS), Warsaw, Poland, 2018, 1–6. Online: https://doi.org/10.1109/ICMCIS.2018.8398711

Pistoia, Daniela (2021): Counter UAS Systems Overview. In Clemente, Carmine – Fioranelli, Francesco – Colone, Fabiola – Li, Gang (eds.): *Radar Countermeasures for Unmanned Aerial Vehicles.* Scitech Publishing, 21–43. Online: https://doi.org/10.1049/SBRA543E_ch1

Rodday, Nils – Schmidt, Ricardo – Pras, Aiko (2016): Exploring Security Vulnerabilities of Unmanned Aerial Vehicles. In *NOMS 2016 – 2016 IEEE/IFIP Network Operations and Management Symposium,* Istanbul, Turkey, 2016, 993–994. Online: https://doi.org/10.1109/NOMS.2016.7502939

Rudys, Saulius – Laučys, Andrius – Ragulis, Paulius – Aleksiejūnas, Rimvydas – Stankevičius, Karolis – Kinka, Martynas – Razgūnas, Matas – Bručas, Domantas – Udris, Dainius – Pomarnacki, Raimondas (2022): Hostile UAV Detection and Neutralization Using a UAV System. *Drones,* 6(9), 250. Online: https://doi.org/10.3390/drones6090250

Sander, Jennifer – Kuwertz, Achim – Mühlenberg, Dirk – Müller, Wilmuth (2018): High-Level Data Fusion Component for Drone Classification and Decision Support in Counter UAV. In *Proceedings of Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation,* Orlando, SPIE 10651. Online: https://doi.org/10.1117/12.2306148

Sliti, Maha – Abdallah, Walid – Boudriga, Noureddine (2018): Jamming Attack Detection in Optical UAV Networks. In *20th International Conference on Transparent Optical Networks* (ICTON), Bucharest, Romania, 1–5. Online: https://doi.org/10.1109/ICTON.2018.8473921

Taillandier, Maximilian – Peiffer, Richard – Darut, Gabriel – Verdy, Charles – Regnault, Reneé – Pommies, Miles (2023): Duality Safety – Efficiency in Laser Directed Energy Weapon Applications. In *Proceedings of SPIE, High Power Lasers: Technology and Systems, Platforms, Effects,* Amsterdam, Netherlands, 2023. Online: https://doi.org/10.1117/12.3001871

Wentzel, Alexander – Cornils, Jan – Valentin, Marco – Heynicke, Ralf – Scholl, Gerd (2024): *Compact Counter-UAS System for Defeating Small UAV in Complex Environments, Detection, Tracking, ID and Defeat of Small UAVs in Complex Environments.* (STO-MP-SET-315).

Willner, Byron (2009): *Methods and Apparatuses for Detecting and Neutralizing Remotely Activated Explosives.* US Patent (Application Number: 12/126,570).

Zhao, Chen – Wang, Xuesong – Xiao, Shilin (2009): Cooperative Deception Jamming against Radar Network Using a Team of UAVs. *IET International Radar Conference,* Guilin, China, 2009. Online: https://doi.org/10.1049/cp.2009.0418