ILLÉS HORVÁTH

# The newest aspect of industrial espionage. Cyber threats from UAVs to non-state actors

Az ipari kémkedés legújabb aspektusa. Az UAV-k általi kiberfenyegetés a nem állami szereplők tekintetében

DOI: HTTPS:// DOI.ORG/10.53793/RV.2024.2.5

***Abstract***

*The crime of industrial espionage to obtain trade secrets is as old as the dawn of commerce. With the development of modern technology, the techniques for obtaining secrets, or in modern terms, data, have been constantly evolving. With the advent of drones on the market, physical and cyber-attacks against critical infrastructure and non-state actors have increased significantly. The relative ease of modification of UAVs (Unmanned Aerial Vehicle) has led to the emergence of spy vehicles capable of acquiring sensitive data without the ground controller entering the area. Critical infrastructure is protected at the state level, with military and/or national security at the global level, but non-state actors are vulnerable to attack. The aim of this paper is to show how non-state actors are affected by the threat and what options they have to defend themselves. Whether EEA countries are threatened by this form of espionage.*

KEYWORDS: CYBER ESPIONAGE, NON-STATE ACTORS, CRITICAL INFRASTRUCTURE, LAW, UAV MITIGATION

***Absztrakt***

*Az üzleti titok megszerzésére irányuló ipari kémkedés bűncselekménye mondhatni egyidős a kereskedelem megjelenésével. A modern technológia fejlődésével a titok, vagy modern kifejezéssel élve az adat megszerzésére irányuló technikák folyamatosan új arculatot öltöttek. A drónok piaci forgalomba kerülésével a kritikus infrastruktúra, valamint a nem állami szereplők ellen irányuló fizikai- és kibertámadások jelentős mértékben megnövekedtek. Az UAV-k (Unmanned Aerial Vihicle, magyarul pilóta nélküli légi jármű) meglehetősen könnyű modifikációja miatt olyan kémkedésre alkalmas egységek jelentek meg, melyek úgy képesek megszerezni a szenzitív adatokat, hogy a földi irányító nem lépi át a területet. A kritikus infrastruktúra állami szinten védett, az elhárítást globális szinten a katonaság, és/vagy a nemzetbiztonság végzi, azonban a nem állami szereplők védtelenek a támadásokkal szemben. Jelen tanulmány célja bemutatni, hogy a fenyegetés milyen formában érinti a nem állami szereplőket, milyen lehetőségeik vannak a védelemre, illetve fenyegeti-e a kémkedés fenti formája az EGT országokat.*

KULCSSZAVAK: KIBERKÉMKEDÉS, NEM ÁLLAMI SZEREPLŐK, KRITIKUS INFRASTRUKTÚRA, JOG, UAV MITIGÁCIÓ

It's probably not an exaggeration to say that corporate espionage is as old as commerce. In the surviving sources of the ancient world, from China (Tőkei trans 1995), Persia Empire (Briant 2009) and the Greek polisis to the Roman Empire (*speculatores, exploratores*), we find a wealth of references to the workings and tasks of military and economic intelligence specialists (Russel 1999; Syvänne 2016). To put it cautiously, the sources of the Byzantine Empire almost give us a model of an advanced intelligence service, in which spies (*ακριβείς κατάσκοποι*) obtained information in the interests of the state's security from the civilian population (*άμαχοι*), especially from market players (*έμποροι*), both inside and outside the borders of the empire (Theotokis 2018). When the strategic aspects of the empire required it, spies often used disinformation and its varied tools to gain significant military and economic advantage. Apart from the state, non-state actors of the time also played their part in espionage, mostly in the competitive sphere. In modern terms, rivals sought to discover each other's corporate secrets in order to gain an advantage over competitors. More fundamentally, the medieval commercial sector was not immune to the crime of industrial espionage.

Italian cities, especially Venice and Florence, stood out from their competitors not only for the advanced attributes of their spies, but also for their manipulative strategies (Prajda 2015; Iordanou 2018). Venice's republicanism gave rise to a number of institutions typical of the modern state, such as the Council of Ten (*Consiglio dei Dieci*) and the State Investigatory (*Inquisitori di Stato*), which also organised the network of informers and the police. The international intelligence role of the lagoon city should not be underestimated, if only in the context of the early modern information revolution (Pilch ed. 1936; Ágoston 2014; Preto 2016). It is no coincidence that Venice provided the model for the procedures and tasks of modern intelligence services.

In a globalised world, one of the most important materials is undoubtedly knowledge and the information that builds it. It has become increasingly true that the constant acquisition of knowledge, and the acquisition of knowledge from competitors, even if it is often illegal, is an inherent part of the market economy and the key to maintaining the competitiveness of some companies. In industrial espionage, a firm or individual seeks to obtain the secrets of its competitors by illegal means in order to increase its own market advantage. The object of the crime is information, which can be formal or informal, white, or black. Industrial espionage can take the form of sabotage methods aimed at obtaining or destroying information. Information gathering methods are divided into active and passive methods. Active methods require physical personal presence and influence. It means physical intrusion, access to various electronic systems, theft, copying of confidential documents, copying to a data recorder. Passive methods include electronic eavesdropping, interception of conversations in public and closed places. The *social engineering* aspect is also included as a separate category (Deák 2019).

In the Hungarian legal environment, industrial espionage does not appear in the Criminal Code as an independent offence, which is mainly due to the fact that industrial espionage has various aspects. (Nasheri 2014) The acquisition of data can take several forms. Consequently, there are several elements in the criminal law which focus on secret data unknown to the individual. The term "*trade secret*" is defined in Article 1 (1) of Act LVI of 2018 on the Protection of Trade Secrets as *"a trade secret is a fact, information, other data and a compilation thereof, which is related to an economic activity, is secret, is not known in its entirety or as a set of elements or is not easily accessible to the persons engaged in the economic activity concerned, and therefore has a pecuniary value, and is not known to the public or is not easily accessible to the persons engaged in the economic activity concerned, and therefore the holder of the secret acts in a manner that is generally expected in the given situation in order to keep it secret."* As can be seen, a trade secret must be indispensably linked to the economic activity of the company. Thus, information relating to the activity in question is in any event covered by the trade secret. The criterion for the information discussed above is that it must not be public knowledge or easily accessible. At the same time, it is clear that the law imposes an obligation on the holder of the secret and states that the information is only considered a secret if the owner of the secret ensures its protection. A specific condition is that the acquisition, use, disclosure, or disclosure of the information by unauthorised persons would harm or jeopardise the economic or market interests of the right holder. Thus, for information to be classified as a secret, it is sufficient that one of the above conditions is fulfilled, no harm or threat to the interest is required (Schubert 2019).

The domestic legal environment regulates the *know-how* as a completely separate category, i.e. proprietary knowledge, as this concept enjoys the same legal protection as trade secrets. According to the above-mentioned law, *"know-how is technical, economic or organisational knowledge, solutions, experience or a compilation thereof, which is a trade secret, and which is recorded in an identifiable manner."* As defined above, know-how is primarily not data, but knowledge or experience. It may also be a combination of these. Due to the legal context, industrial espionage can be carried out not only by infringing trade secrets, but also by infringing other data and information, including private, confidential, confidential correspondence and trade secrets. In extreme cases, the offences of illicit acquisition of data or misuse of personal data may also exist. The form of industrial espionage is espionage as defined in Article 261 of Act C of 2012 on the Criminal Code. Industrial espionage is covered by this offence, in particular if the target is a state or a company with direct links to the state. This can understandably be damaging not only to economic life but also raises national security concerns. On this basis, the penalty can range from two to eight years, and from five to fifteen years for top secret data. Given the emergence of new forms of espionage with the development of modern technology, it is essential that the legislative environment to curb industrial espionage is constantly evolving and being supplemented. At the same time, the legislator should also consider the introduction of a specific offence, which would effectively prevent the forms of the offence from being carried out.

In recent years, technological progress has given rise to a particular form of industrial espionage. With the commercialisation of UAVs, or *vulgo dicitur*: drones, and

the extremely rapid expansion of the market, the devices have become readily available to the civilian population (Dillow 2011; Schneider 2016). Their widespread use and their versatility of application have quickly brought them to the forefront of criminals' minds and often made them a means of committing crimes. The crimes committed with drones in recent years cover a very wide spectrum. From crimes against aviation, to espionage, to terrorist attacks (Rassler 2016; Hartmann–Giles 2016), they play an extremely important role. Thanks to their power and their easy modification, they can also be used as a payload to carry and operate weapons and various electronic devices. The latter equipment is specifically targeted at obtaining forbidden or protected data, which often includes the theft of bank card details, attacks against social media profiles and attacks to obtain the data files of various messaging software. In addition to crimes against individuals, the business sector has also become vulnerable to drone attacks. This form of attack is not without precedent (Wendt 2020).

In 2011, a U.S. Air Force engineer and cybersecurity contractor collaborated at the Black Hat and Def Con Security Conference in Las Vegas to unveil a 14-pound, 6-foot-long UAV-WASP (Unmanned Aerial Vehicle - Wireless Aerial Surveillance Platform) fixed-wing spy drone. In creating the drone, its creators, Mike Tassey and Richard Perkins, were in fact trying to draw attention to the fact that by commercialising drones, the state and manufacturers have given too much access to technologies that are a quasi-potential threat to private individuals, the state, and non-state actors. In demonstration of this finding, their units are constructed strictly from commercially legally available materials. The model is based on the U.S FMQ-117B. military UAV. The body is made of EPO foam, with an E-Flite 90 carbon brushless motor, a CP 85 HV ESC, and 2x6 22.2v 5000mAh LiPo batteries. The control consisted of a JR Spectrum Dx6i transmitter and receiver (2.4 GHz), DIY Ardu Pilot, Servo, Xbee Pro Ada Fruit adapter, while the so-called payload; Via Epia Px5000eg Pico-ITX, USB 4G, XBee Pro module, and a Universal Serial Radio Peripheral (USRP). While the BaseStation was made up of a Gumstix Overo Earth, DIY ArduStation, an Asus WL-330gE Wi-Fi Access Point, an Inter P4 3.06 GHz HT processor, 4 Gb Ram, 500 GD HDD, and an Nvidia GTX 470. During the test flight of the aircraft, the controllers were able to intercept several phone calls, collect a significant amount of data, and hack into various Wi-Fi networks (Tassey–Perkins 2011).

In 2015, 4Armed introduced the DJI Phantom 2 Vision+ drone, a user-friendly drone equipped with a Rasberry Pi and an omni-directional antenna. The connection between the UAV and the ground controller was provided by a Huawei 3G dongle, which minimized the detection capabilities of the device. During the flight, significant data was collected using Snoopy-ng, the detected networks were hacked using Aircrack-ng, (Clarity From Above) and finally the target's system was penetrated by exploiting a security flaw in Microsoft Windows MS08-067. The total cost of the drone and modification was roughly $1,200. (Greenwood 2015) In the same year, the Singaporean marketing company AdNear used a modified DJI Phantom with very similar equipment to the aforementioned UAVs to target the phones of the Los Angeles victims (Kumar 2015), specifically to collect data to flood potential customers with unwanted advertising on their phones (Paráda–Tóth 2020).

In 2017, BishopFox's Danger Drone mUAV (multirotor UAV) was unveiled at Def Con. The Danger Drone's frame is 3D printed. The brain of the unit, so to speak, was an Erle Brain 2, equipped with an Ublox Neo-M8N GPS, a Turnigy TGY-i6 LE 4x MN2213 Motor, HKPilot tansceiver Telemetry Radio Set V2 (915 MHz), Flouren 4S 35C 14. 8V 5500mAh Li-Polymer RC Battery Pack, Andoer 4 Pcs Simonk 30AMP regulator, RipaFire F450 4-Axis multirotor, Eriocco Power Supply Module w/BEC APM 2.5 APM, and a PPM Encoder Module HKPilot 32 has been fitted. The so-called utility box consisted of a SENA UD100 USB, Bluetooth 4.0 USB, Wi-Spy DbX Pro Sprectrum Analyzer, Wifi Pineapple Nano, TP-Link TL-WN72N, Asus USB-N53, a Crazyradio 2.4GHz nR24LU1+USB radio dongle, and Atmel - ZigBee hacking gear. The total cost was just over $ 500.The 4G communication system made the device capable of evading the latest jammers, approaching the target undetected and breaking into the system. By building the device, the company wanted to highlight the importance of protection and vulnerability. In their presentation, Francis Brown and David Latimer highlighted that the weak defence architecture of IoT Home & Office (Internet of Things) systems makes it easy for UAVs like Danger Drone to enter the network and take control of devices (Bramlette 2019). In this respect, they also sought to highlight the particular importance of taking physical and cyber defence measures, especially for large enterprises (Brown–Latimer 2017).

In the latest and most dangerous form of corporate espionage, the perpetrators most often use UAVs. As can be seen from the above, drones are extremely easy to use to carry out physical and cyber-attacks. They are readily and legally available commercially (Findings 2018). Due to their technical attributes, they can also be modified to be able to steal company secrets and customer information. But they are also capable of allowing the perpetrator to monitor the target

permanently while keeping his identity hidden. In the past, the traditional techniques of industrial espionage were based on bugging, wiretapping and infiltration, but today this form of crime has almost entirely moved into cyberspace (Holland 2020). With the advent of the information society and cloud technology, the perpetrator can now successfully carry out espionage without physically crossing the company's premises. This leaves companies almost defenceless against cyber-attacks by UAVs, as current legislation essentially does not allow them to legally and legitimately take action against a spying UAV. At global level, there is a general belief that counter-interception (C-UAS) is the exclusive competence of civil or military national security services. Private individuals and non-state actors must take their own measures to protect their data stored in cyberspace.

In July 2020, drones were spotted over chemical plants in Louisiana, prompting the Federal Bureau of Investigation (FBI) to report on the potential for espionage and terrorism involving critical infrastructure (Barnes 2020). According to the report, obtained by CNN, the FBI wrote that such flights could be an effective way to monitor critical infrastructure. Security and law enforcement forces at the facility have limited ability to detect and deter the threat. On July 29, 2020, observers saw two drones fly over the facility, split in two a few feet above the facility and continue flying in different directions. The FBI, taking measures to protect the facility, notified the U.S. Department of Homeland Security, which has counterintelligence authority, and involved the Cybersecurity & Infrastructure Security Agency (CISA) in organizing the protection (Protecting against the threat 2020). On 8 March 2021, security again discovered a drone near the plant's pipelines. Subsequently, for security reasons, the FBI encouraged managers of critical infrastructure facilities to contact the agency's field office immediately in the event of a drone detection. The Department of Homeland Security has also issued a briefing on the incident, warning that drones are extremely useful tools, but in the wrong hands they can also be used as explosive weapons or for espionage. Therefore, the State has taken steps to enhance the protection of critical infrastructure (Sands 2022). The FBI's field office and CISA have issued a new report on the incident, underlining that the detection of drones poses a major problem in finding the pilot on the ground. he critical infrastructure protection system may not be able to find the pilot, nor can it assess what information has been obtained from the espionage activity. The FBI added to the statement that a drone that crashed near a power station in Pennysylvania in 2020 was investigated and there were strong suspicions that the device was used to damage infrastructure, so the National Counterterrorism Center was involved in investigating the case. Overall, the above example shows that in the event of physical and cyber-attacks against critical infrastructure, the state will seek to extend its protection to the infrastructure under attack using all means at its disposal (Sneath 2021).

Currently, in the United States, this form of espionage is most prevalent among large non-state corporations such as General Motors Company, Gillette Company, Google LLC, HP Inc, Microsoft Corporation, Tesla Inc, Meta Platforms Inc, and Apple Inc. A major problem is that cyber espionage allows perpetrators to obtain data in cyberspace without companies ever realising that they have been the victims of an attack. At the same time, if an attack is identified, it is very difficult to determine how much damage has been done to the company as a result of the crime. The investigation is further complicated by the fact that, for example, as the company is globally responsible for protecting trade secrets, it must itself take care of the protection of sensitive proprietary data. In this regard, in the United States, in the course of an investigation, the authorities must carefully consider (i) the extent to which the secret information obtained was known outside the company, (ii) the extent to which it was known by employees, (iii) the extent to which the information was kept secret, (iv) the advantage the information may have over competitors, (v) and what the company involved in the espionage did to protect the information. Taking all the above into account, it is common that if the company detects the threat in time and its information is leaked, it will not report it (Rowe 2016). Thus, no criminal prosecution is initiated. There is no way to detect the crime. Another fundamental problem is that companies are unable to estimate the potential damage caused by a crime in such cases (Kosseff 2020; Scott 2021).

We can only cautiously infer that Apple Inc, Meta Platforms Inc, and Tesla Inc, may have been victims of UAV spying in the past, as they have taken the initiative to declare their campuses as "No Drone Zones" due to the numerous illegal flights detected. Of these companies, Apple Inc. was perhaps the most affected. The construction of their campus in Cupertino, California, USA, has attracted drone pilots. During the illegal flights, the company's construction site was constantly monitored, and there were even attempts to hack into the newly installed network. For this reason, Apple Inc. management first designated the campus area as a No Drone Zone (Aisight report), trusting that commercially available drones would be stopped by geofencing (Marketwatch report 2018). Word soon spread on the internet that it was no longer possible to

fly into the campus. But that didn't deter adventurous pilots and the company's rogue pilots. In 2018, the company's security team decided to take action to protect its trade secrets against the UAV threat. In April 2018, a young pilot attempted to fly onto the campus to take photos of the construction site but was warned by Apple's security team to leave the area in less than ten minutes. Otherwise, they will be forced to take action. The pilot turned his UAV around and landed away from the campus. According to unconfirmed sources, Apple Inc. may have purchased a detection and defeat system marketed by Dedrone Holdings to protect its business secrets and infrastructure (Marketwatch report 2018).

In 2020, two researchers used a drone-mounted Wi-Fi to show how to hack a Tesla car in the Pwn2oown hacking competition. The hackers used security vulnerabilities in Tesla's infotainment system to penetrate the vehicle's system and take control (Kovács 2019). The attack allowed them to modify the basic functions: music playback, air conditioning, steering, and acceleration modes, as well as unlock the doors (Kovács 2020). But not remote control. Nevertheless, the attack has shown that using Wi-Fi and the right software, an attacker can hack into the systems of any Tesla Model S, 3, X, and Y from up to 100 meters away and open the vehicle's doors, which obviously makes it easier to steal the vehicle. After the race organisers informed the manufacturer of the results, the bug was fixed in October 2020. However, it has emerged that the Connman component is widely used in the automotive industry and similar attacks could be launched against other manufacturers' vehicles. The attack on Tesla's vehicle systems is not the first. In 2020, Tesla researchers attacked their own car to address the weaknesses of the Advenced Driving Assistance System (ADAS) (Nasi et al. 2020). The tests confirmed the vulnerability and manipulability of the system. Volke Automotive in Germany has also built its detection and defeat system partly to prevent industrial espionage and partly to protect vehicles from industrial espionage. Volke is known as one of the world's leading technical developers in automotive design. Protecting the company's intellectual property is therefore a priority (Dedrone/Volke).

The examples above show that in the case of state actors, state bodies extend their protection to all critical infrastructure institutions, but non-state actors can only legally protect data stored in cyberspace. In the face of external physical and cyber-attacks from the air, the company is defenceless. Current technological tools allow the use of drones to steal proprietary and confidential trade secrets that give competitors and adversaries an unwarranted advantage. In addition, it can be seen that illicit data mining against companies by drone poses a potential threat not just to one region, but globally, even to European companies. Consequently, since the legal environment only gives the state the right to counteract, non-state actors are trying to discourage corporate espionage by alternative or currently less legal methods. As the above is a very new practice of spying, the legislator should consider the possibility of granting the state's economic partners the right to detect and intercept data, even if limited, in addition to designating economic areas as No Drone Zones. Domestic practice is fully analogous to US legislation. Government Decree 4/1998 (I. 16.) on the use of Hungarian airspace 9/A. § (2) of the Hungarian Act of 19/19/1978 on the use of Hungarian airspace, any unmanned aircraft engaged in air traffic which a) violates the laws on air traffic and the operation of unmanned aircraft, and thereby endangers the safety of air traffic or the inviolability of privacy, may be intercepted, identified, its operation may be electronically interfered with, and it may be required to land, and it may be forced to land by electronic or mechanical means; b) which constitutes a threat to the security of the protected installation; c) which is used for an unlawful purpose; d) which has reasonable grounds to believe that its flight is being used for the illegal transport of various substances, in particular weapons or drugs, or for the improper transport of dangerous substances; e) which makes unauthorised use of Hungarian airspace. Pursuant to paragraph (3) of the Act: the Hungarian Defence Forces, the Military National Security Service, the Office for the Protection of the Constitution, the National Security Service, the Information Office, the Counter Terrorism Centre, the Parliamentary Guard, and the designated law enforcement agencies performing law enforcement tasks under the control of the Minister of the Interior shall be entitled to take measures pursuant to paragraph (2). In reality, these tasks are carried out by the Military National Security Service and the Specialised National Security Service with the full range of counter-intelligence resources. Obviously, there are types of C-UAS systems that can cause unforeseeable damage in unqualified hands, and it is therefore necessary to limit their use moderately. Consideration should be given in the future to the possibility of using licensed systems that can only 'soft kill' an unauthorised unit flying into an economic area, relying strictly on jammer and drone gun devices. Nevertheless, it is necessary to make companies aware of this threat and the possibilities for self-help as a preventive measure (Scott 2021).

## Bibliography


Ágoston, G. (2014) Információszerzés és kémkedés az Oszmán Birodalomban a XV-XVII. században. Európa és az Oszmán Hódítás. Budapest.

Barnes, S. (2020) Real and present danger: Industrial plants face a new level of threats from drones, cyberattacks and corporate espionage. 1012industryreport. https://www.1012industryreport.com/safety/real-and-present-danger-industrial-plants-face-a-new-level-of-threats-from-drones-cyberattacks-and-corporate-espionage/ [Accessed: 02.02.2024.].

Bramlette, C. M. (2019) *Cyber-Attack Drone Payload Development and Geolocation via Directional Antennae*. (Thesis.) Faculty Department of Electrical and Computer Engeneering Graduate School of Engineering and Management Air Force Institue of Technology.

Briant, P. (2009) 'Le thème de la « décadence perse » dans l'historiographie européenne du XVIIIe siècle: remarques préliminaires sur la genèse d'un mythe'. In: L. Bodio–V. Mehl–J. Oulhen–F. Prost–J. Wilgaux (eds.) *Chemin faisant: mythes, cultes et société en Grèce ancienne. Mélanges en l'honneur de Pierre Brulé.* Presses universitaires de Rennes, Rennes. pp. 19–38.

Brown, F.–Latimer, D. (2017) *Game of Drones* – Putting the emerging „Drone Defense" Market to the test. Las Vegas, Def Con.

Bunker, J.–Sullivan J. P. (2021 eds) Criminal Drone Evolution: Cartel Weaponization of Aerial IEDs. XLibibris US.

Bunker, R. J. (2015) Terrorist and Insurgent Unmanned Aerial Vihicles: Use, Potentials, and Military Implications. Strategic Studies Institute, US Army War College. pp. 1–55.

Cafarella, J.–Dunford, J.–Land, M.–Wallace, B. (2020) *Turkey Commits to Idlib.* – Institute for the Study of War, 18 March 2020. https://understandingwar.org/backgrounder/turkey-commits-idlib [Accessed: 03.02.2024.].

Clarity From Above: PwC Global report on the commercial applications of drone technology. https://www.pwc.pl/pl/pdf/clarity-from-above-pwc.pdf [Accessed: 01.02.2024.].

Crino, S.–Dreby, C. (2020) Drone Attacks Against Critical Infrastructure: A Real and Present Threat. Atlantic Concuil, May 1. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/drone-attacks-against-critical-infrastructure-a-real-and-present-threat/ [Accessed: 27.10.2023.].

Deák, V. (2019) Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle*, Vol. 12. Nr. 3. pp. 95–111.

Dedrone Official site, Customers https://www.dedrone.com/customers/volke [Accessed: 02.02.2024.].

Dillow, C. (2011) "A DIY UAV That Hacks Wi-Fi Networks, Cracks Passwords, and Poses as a Cell Phone Tower". *Poplular Science*, 2011. [Online]. https://www.popsci.com/technology/article/2011-07/diy-uav-hacks-wi-fi-networks-cracks-passwords-and-poses-cell-phone-tower [Accessed: 31.01.2024.].

Findings, K. (2018) Cybersecurity risks Posed by Unmanned Aircraft Systems. Homeland Security. National Protection and Programs directorate. Office of Cyber and Infrastructure Analysis. https://www.hsdl.org/c/view?docid=825402 [Accessed: 03.02.2024.].

Greenwood, J. (2015) The Phantom Menace - Weaponising a Consumer Drone. https://www.4armed.com/blog/phantom-menace-weaponising-drones/ [Accessed: 03.02.2024.].

Hartmann, K.–Giles, K. (2016) *UAV Exploitation: A New Domain for Cyber Power*. 2016 8th International Conference on Cyber Conflict. https://www.researchgate.net/publication/305871943_UAV_exploitation_A_new_domain_for_cyber_power [Accessed: 05.01.2024.].

Holland, A. M. (2020) Unarmed and Dangerous. The Lethal Applications of Non-Weaponized Drones. https://dronecenter.bard.edu/files/2020/03/CSD-Unarmed-and-Dangerous-Web.pdf [Accessed: 04.02.2024.].

Iordanou, I. (2018) The Spy Chiefs of Renaissance Venice: Intelligence Leadership in the Early Modern World. Washington.

Kosseff, J. (2020) Hacking Cybersecurity Law. *University of Illinois Law Review*, 2020. https://ssrn.com/abstract=3331350 or http://dx.doi.org/10.2139/ssrn.3331350 [Accessed: 04.02.2024.].

Kovács, E. (2019) Pwn2own 2019: researchers Win Tesla After Hacking Its Browser. *SecuritWeek.Cybersecurity News*, Insights & Analysis. https://www.securityweek.com/pwn2own-2019-researchers-win-tesla-after-hacking-its-browser/ [Accessed: 02.02.2024.].

Kovacs, E. (2020) Tesla Car Hacked remotely From Drone via Zero-Click Exploit. *SecuritWeek.Cybersecurity News*, Insights & Analysis. https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit/ [Accessed: 02.02.2024.].

Kumar, M. (2015) Drones Spying on Cell Phone Users for Advertisers.

https://thehackernews.com/2015/03/drone-cell-phone-spy.html [Accessed: 31.01.2024.].

Nasheri, H. (2004) *Economic Espionage and Industrial Spying*. Cambridge University Press, Cambridge.

Nassi B.–Nassi, D.–Netanel, R. B.–Mirsky, Y.–Drokin, O.–Elovici, Y. (2020) *Pahntom of the ADAS: Securing Advenced Driver – Assistance Systems from Split-Second Pahntom Attacks*. ACM SigSac Conference on Computer and Communications Security. 2020. pp. 293–308. https://dl.acm.org/doi/10.1145/3372297.3423359

Paráda, I.–Tóth, A. (2020) A Metasploit tulajdonságai egy biztonságos FTP démon exploit tükrében. *Hadmérnök*, Vol. 15. Nr. 3. pp. 219–230.

Pilch, J. (ed 1936) A hírszerzés és a kémkedés története. Budapest.

Prajda, K. (2015) *Justice in the Florentine Trading Community of Late Medieval Buda*. Mélanges de l'École française de Rome-Moyen Âge. https://journals.openedition.org/mefrm/2716 [Accessed: 03.02.2024.].

Preto, P. (2016) I servizi segreti de Venezia. Spionaggio e controspionaggio ai temo delle Serenissima. Milano.

*Protecting against the threat of unmanned aircraft systems (UAS)*. An Interagency Security Committee Best Practice. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Integracy Security Committee, 2020.

Rassler, D. (2016) Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology. Combating Terrorism Center, No. October. https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/ [Accessed: 05.01.2024.].

Rassler, D. (2018) *Drone Games, Terror Drone Diffusion, and Near-Term Threats*. The Islamic State and Drones: Supply, Scale, and Future Threats. https://www.jstor.org/stable/resrep21486.7 [Accessed: 27.10.2023.].

Rassler, D. (2018) *The Islamic State Drones*. Supply, Scale, and Future Threats. Combating Terrorism Center at West Point.

Report (2022) FBI Warns of drone risk after detections at Lousiana chemical facilities. Report Staff. 1012industryreport. https://www.1012industryreport.com/technology/fbi-warns-of-drone-risk-after-detections-at-louisiana-chemical-facilities/ [Accessed: 02.02.2024.].

Rowe, E. A. (2016) *Rats, Traps, and Trade Secrets*. 57 B.C. L. REV 381 (2016) https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1769&context=facultypub [Accessed: 20.03.2024.].

Russel, F. S. (1999) Information Gathering in Classical Greece. Michigan.

Sands, G. (2022) FBI warns drones pose potential risk to critical infrastructure after some spotter over Louisiana chemical facilities. https://edition.cnn.com/2022/09/30/politics/drones-risk-critical-infrastructure-spotted-louisiana-chemical-facilities/index.html [Accessed: 02.02.2024.].

Schneider, M.–Lichte, D.–Witte, D.–Gimbel, S.–Brucherseifer, E. (2021) *Scenario Analysis of Threats Posed to Critical Infrastructures by Civilian Drones*. 31st European Safety and Reliability Conference, ESREL pp. 520–527. Research Publishing Services. Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021), Angers, Frankreich. doi: 10.3850/978-981-18-2016-8_234-cd. ISBN 978-981182016-8.

Schubert, B. (2019): Az ipari kémkedés megjelenése a magyar büntetőjogban – a Huawei-ügy tükrében. Ars Boni. https://arsboni.hu/ipari-kemkedes-a-huawei-ugy-tukreben/ [Accessed: 30.01.2024.].

Scott, C. (2021) Corporate Espionage by Drone: Why Corporations Need Better Physical and Legal Protections. https://ssrn.com/abstract=3772434 or http://dx.doi.org/10.2139/ssrn.3772434 [Accessed: 04.02.2024.].

Sneath, S. (2021) *Gov. Edwards gets bill that doubles maximum punishment for flying drones over critical infrastructure*. Petrochemical facilities, pipelines, and grain elevaturs are no-fly zones for drones. Louisiana Illuminator. https://lailluminator.com/2021/06/09/gov-edwards-gets-bill-that-doubles-maximum-punishment-for-flying-drones-over-critical-infrastructure/ [Accessed: 02.02.2024.].

Syvänne, I. (2016) The Eyes and Ears: The Sasanian and Roman Spies ca. AD 222-450.

*Historia I Swiat*, Nr. 5. pp. 107–131.

Tassey, M–Perkins, R. (2011) *Wireless Aerial Surveillance Platform*. DEFCON 19, 2011. https://www.defcon.org/images/defcon-19/dc-19-presentations/Tassey-Perkins/DEFCON-19-Tassey-Perkins-Wireless-Aerial-Surveillance-Platform.pdf [Accessed: 31.01.2024.].

Theotokis, G. (2018) Byzantine Military Tactics in Syria and Mesopotamia in the 10th Century. Edinburgh.

Tőkei, F. (trans 1995) *Szun-Ce. A hadviselés törvényei*. Budapest.

WatchMArker Report (2018) https://www.marketwatch.com/story/apple-cracks-down-on-drone-pilot-who-shoots-epic-apple-campus-videos-2018-04-16 [Accessed: 02.02.2024.].

Wendt, P.–Voltes, A.–Suau-Sanchez, P. (2020) Estimating the costs for the airport operator and airlines of a drone-related shutdown: an application to Frankfurt International Airport. *Journal of Transportation Security*, Vol.13. Nr. 1. pp. 93–116.