HADMÉRNÖK
VÉDELEMINFORMATIKA
17. évfolyam (2022) 2. szám 205–216.
DOI: 10.32567/hm.2022.2.14

Mátyás Ináncsi[1]

Cybersecurity Challenges of the Civilian Unmanned Aircraft Systems

Nowadays unmanned aircrafts are widely available at a reasonable price for civilians. This change in the market raises cybersecurity related concerns. In this paper we are focusing on three aspects of the cybersecurity challenges: data protection element, cyberattack element and general concerns over drones from the Asian market. The first element is extremely important when it comes to ethical and rightful drone use. A drone fitted with a camera or a video recording device can easily violate personal data. The cyberattack element aims to make sure the user understands that their device can be hacked, and not just simply the drone itself but various devices connected to them. Lastly, we are focusing on raising awareness of using drones from the Asian market. These types of products sometimes get into the spotlight due to built-in cyberissues. This part is aimed to raise general awareness over data protection coming from third party device use.

Keywords: **cybersecurity, drones, UAV, data protection, civil drone use**

1. Introduction

In the past years, unmanned aerial vehicles (UAVs, or more commonly drone(s), or unmanned aircraft) are getting more and more popular in the civilian and commercial sector. UAVs are part of unmanned aircraft systems (UAS). The UAS regarding civilian use consists of the following elements:[2]

- unmanned aircraft
- ground control station
- communications data link
- + payload

The unmanned aircraft is the actual aerial vehicle that the user controls, in the civilian sector the customer often uses a rotary wing drone. The main reason why these types

[1] University of Public Service, Doctoral School of Military Sciences, e-mail: inancsi.matyas@uni-nke.hu
[2] Ismael Colomina – Pere Molina: Unmanned Aerial Systems for Photogrammetry and Remote Sensing: A Review. *ISPRS Journal of Photogrammetry and Remote Sensing,* 92 (2014). 80.

are more common is because that they require less infrastructure to deploy, (they only need a reasonably flat surface to take off from), and their goal is not to cover a large distance in a short period of time. The user often has visual contact with the vehicle and from a technical standpoint, the communications data link(s) are short range-based methods. The ground control station is the actual device that the user operates to control the vehicle. In the civilian aspect, this word in my opinion is excessive because it indicates a higher level of infrastructure (that might be seen in commercial or military use). The ground control station, in this case is often a remote, or a controller, or as an alternative a controller plus a smartphone, so in this paper, I would refer to the ground control station as a remote or controller. The communications data link is the telemetry[3] between the unmanned aircraft and the remote. Often it is a Wi-Fi connection, but in the short future when 5G networks become more and more available they might transition to 5G use. Payload is an additional element in the civilian aspect that is considered as an extra to the UAV, while in commercial/military use it is a quintessential part. The payload is the element that the drone either carries or delivers. It could be a sensor, a video camera, a package, or a missile (in military use). But civilians use UAVs for entertainment, and for fun, so having a payload is not important. However, if a payload is carried, it is usually a video camera and mostly available on the higher-end drones.

The wider availability, more options, and in general the more affordable price expand the user amount of these vehicles. Currently (2020) if we are looking at the state of the drone market we receive reasonably different numbers, from 20.4 billion USD[4] to 24.72 billion USD.[5] The market analyses indicate rapid growth in the industry. Some market predictions even say that by the end of 2026 the UAV market could potentially reach 58.4 billion USD.[6] The technology is in rapid expansion, especially in the commercial and civilian aspects. In this paper, we are going to focus on civilian use and the cyber challenges arising from day-to-day use. The goal of this article is to highlight the potential cybersecurity-related risks and challenges and to spread awareness regarding non-commercial UAV use. A relevant research question in this paper is: what are the important cybersecurity elements of the civilian drone use that a hobby user must keep in mind during normal operations. From this perspective, three major aspects should be highlighted.

The key aspects of this paper are:

- the data protection factor of the civilian UAV use (in the EU)
- the cybersecurity factor of the civilian UAS use regarding cyberattacks
- general concerns of non-EU certified drone use

[3] Telemetry: An automatic data link in between two or more devices to transfer and receive data between a remotely operated machine and a control station.

[4] Mordor Intelligence: *Drones Market – Growth, Trends, Covid-19 Impact, and Forecasts (2021–2026).*

[5] Allied Market Research: *Unmanned Aerial Vehicle (UAV) Market by Type (Fixed Wing, Rotary Wing, and Hybrid), Application (Military & Defense, Civil & Commercial, Logistics & Transportation, Construction & Mining, and Others), and Weight (Less Than 50 Kg, and More Than 50 Kg): Global Opportunity Analysis and Industry Forecast, 2021–2030.*

[6] Markets and Markets: *Unmanned Aerial Vehicle (UAV) Market by Point of Sale, Systems, Platform (Civil & Commercial, and Defense & Government), Function, End Use, Application, Type, Mode of Operation, MTOW, Range, and Region: Global Forecast to 2026.*

2. Data protection regarding civilian UAV use (in the EU)

In cybersecurity, data privacy is a key item that comes from data protection measures. Often if we are talking about data privacy and data protection regarding drones, we are considering these a system, for example part of the IoT[7] systems. Regardless of this approach, the key issue is the same: drones have a high mobility and if they are equipped with video camera, they are capable of monitoring and following an individual violating his or her privacy.[8] In this section, the focus will be on the individual operator level, more precisely: what actions should a drone operator keep in mind if he/she operates a UAV to avoid violating privacy.

The European Union has two regulations regarding Unmanned Aircraft Systems:

- Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on Unmanned Aircraft Systems and on Third-country Operators of Unmanned Aircraft Systems.
- Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the Rules and Procedures for the Operation of Unmanned Aircraft.

However, the only element in these two regulations regarding cybersecurity is in the 2019/945 regulation:

"[…] the Agency and the competent authority shall take the necessary measures to address any safety issues on the best available evidence and analysis, taking into account interdependencies between the different domains of aviation safety, and between aviation safety, cyber security and other technical domains of aviation regulation."[9]

Although the drone related regulations very briefly mention cybersecurity, the actual data protection related rules are found in the: "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation)." The General Data Protection Regulation (GDPR) is the regulation that we should understand and look at if we attempt to unpack the data protection rules of UAS use. As it was mentioned above, the cyber-related issue is the fact that drones can violate someone's privacy. But it is not an unregulated territory, in this section we are going to show the fundamental rules of UAS use regarding data protection. The goal is to answer and raise awareness regarding what is forbidden for the drone operator with respect to privacy and data protection. This section only applies to drones fitted with video cameras, but as they are getting more and more popular, the focus is trying to be ahead of the arising issues.

[7] Internet of Things: Multiple devices connected to each other and communicating with either a main system or together to achieve a flawless user experience regarding real life events.

[8] Laith Abualigah – Ali Diabat – Putra Sumari – Amir H. Gandomi: Applications, Deployments, and Integration of Internet of Drones (IoD): A Review. ***IEEE Sensors Journal,*** 21, no. 22 (2021). 25537.

[9] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on Unmanned Aircraft Systems and on Third-country Operators of Unmanned Aircraft Systems, Article 19.

In the general provisions of the GDPR, the regulation clearly states that personal data can be only processed if clear consent is given:

"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement […]."[10]

This means that if the drone is fitted with a camera and that payload is not only transmitting a video feed, but also records to either internal or external storage (for example: an SD card, or a smartphone's storage) if personal data is being recorded clear consent is needed. The element of this rule is what is personal data. The regulation also clearly states what is considered personal data:

"'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[11]

This means anything could be personal data that makes a person either directly or indirectly identifiable. It is a very limiting rule, because regarding the personal views, lots of things can identify indirectly a person. For example, just by looking at a house or a property we might be able to identify someone, or the same goes for vehicle number plates.

The civilian hobby drone use is often creating a recording, mainly:

- making timelapse
- creating panoramic videos or pictures
- performing stunts
- filming wildlife or city life

However, these recording types do fall into a grey zone of data protection, because having a recording of (a) house(s) do have a potential of being personal data. In that case according and fitting into the GDPR requires a personal clear consent. While this element fairly limits the use of video camera fitted drones in cities or towns, it still provides a good frame to tackle surveillance and monitoring issues. The method of recording (for example: height, focus, aim, etc.) possibly matters a lot regarding a situation like this, but drone operators must keep in mind that data protection highly applies to UAS use as well.

Another key element of the data protection act is processing personal data. Anyone who is managing personal data is considered a processor.[12] Any action that is connected to handling personal data is considered processing,[13] the users often do the following with the recordings:

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation) Introduction 32.
[11] GDPR, Chapter 1, Article 4, point 1.
[12] GDPR, Introduction Article 4.
[13] GDPR, Introduction Article 4.

- store recordings
- edit recordings
- upload to social media

Every action that the user performs with personal data is processing, so these main actions that users do during their hobby work falls within the processing statement. Consequently, from this requirement, principles of data processing must be followed. The principles are requirements which shall not be overlooked, including lawfulness, accurate data collection, security and protection of personal data (from unauthorised parties). Hence if the user is processing personal data, then the requirements must be followed. A major question about this element is: can the personal data be anonymised and used?

GDPR allows and gives opportunity to anonymise personal data.[14] At first, this is a prompting opportunity, because it might implement to UAS users that if they record personal data, and later anonymise it (for example blur out houses, vehicles, faces, etc.) it will no longer be forbidden to keep or upload it. Anonymised data does not require permission to be processed and stored. This issue also falls into a grey zone, because at first, before a data is anonymised it is still considered personal information and still requires a permission from the affected party. So, this article is not a loophole around the issue, but a later opportunity that can be used on a legally stored personal data. All in all, in the UAS use the personal data rule cannot be overridden by this article.

Overall, the data protection act applies to civilian drone uses as well if they are fitted with a video camera and are recording to either internal or external storage. In order to avoid any privacy infringement, drones falling into this category are advised to be used in public spaces where there is little to no traffic (for example: fields, woods and outskirts). The operator must be cautious and ahead thinking before using the device to avoid conflicting the GDPR.

What the user really must follow in our humble suggestion is to avoid recording any personal data. Once personal data is processed, the user must ensure data protection; this includes having the capability of proving the rightful use of personal data.

3. Cybersecurity factor of the civilian UAS use regarding cyberattacks

For the operation of UAS, cybersecurity is a key element to ensure a safe working order of the vehicles. If an element of a UAS is compromised, the UAV creates a high-risk situation to ground personnel, other air vehicles, privacy of other individuals and property security. The key factor is to have a constant unbroken control over the vehicle during use. Even losing control for a small period, has a potential to create a high-risk situation. The motivation for doing a cyberattack on drones is mostly simple: the high reliance on wireless communication, and an attack having a drastic outcome makes drones vulnerable to incursions.[15]

[14] GDPR, Introduction Article 26.

[15] Jean-Paul Yaacoub et al.: Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations. *Internet of Things,* 11 (2020); Kim Hartmann – Keir Giles: UAV Exploitation: A New Domain for Cyber Power. In *2016 International Conference on Cyber Conflict,* NATO CCD COE.

If we aim to achieve a safe environment from cyberattacks, we must step back to the same principles, which is data protection. In the previous aection, data protection was presented from a legal standpoint; however, in this section, the issue is approached from a technical (or to be more precise a practical) standpoint. Information security within cybersecurity is keeping our data safe, the requirement framework for information security is the Confidentiality, Availability and Integrity triad.

This model not only applies to UAS use, but in general for categorising potential attacks regardless of what type of technology is being used. The three pillars are designed to cover all aspects of cyber threats. Confidentiality in this case refers to: only the authorised personnel, or systems can access the protected data.[16] Cyberattacks that endanger the confidentiality of the data fall under this category. Integrity means that the assets can only be modified by either authorised personnel or systems.[17] When a cyberattack mutates or changes stored data, the system integrity is endangered. Availability refers to having constant access and control over the systems.[18] While in general availability is a key element, because any downtime of a system has a potential of losing data, risking the business continuity. In aviation it is even more highlighted, because the drone operator must have a constant connection between the remote and the UAV.

The most extensive example of this model with respect to UAS use comes from an IEEE publication:[19]

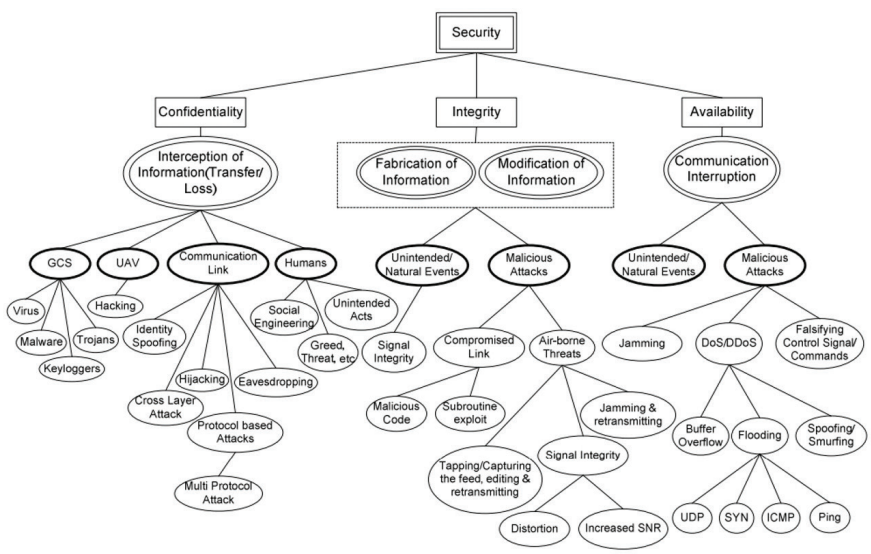

Figure 1: UAS CIA model
Source: Javaid 2012, 588.

[16] Dimitrios Zissis – Dimitrios Lekkas: Addressing Cloud Computing Security Issues. *Future Generation Computer Systems,* 28, no. 3. 586.
[17] Ibid.
[18] Ibid.
[19] Ahmad Javaid Y., et al.: Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. In *2012 IEEE International Conference on Technologies for Homeland Security,* HST 2012. 588.

However, the aim of this paper is to raise awareness about the cyber threats to the UAS, and to make it easier to understand for the average hobby drone user. To make it easier to understand, we simplified this model, while keeping in mind that the focus is the civilian hobby drone use. From this model we created Figure 2, where the attack types are categorised by affected systems and methods with the CIA layer on top of them. The main concept of this figure is keeping it short and trackable for users. One of the challenges of cybersecurity is remaining clear and understandable. By re-organising and simplifying this model, we can get a simpler and more presentable picture of the cyber threats:

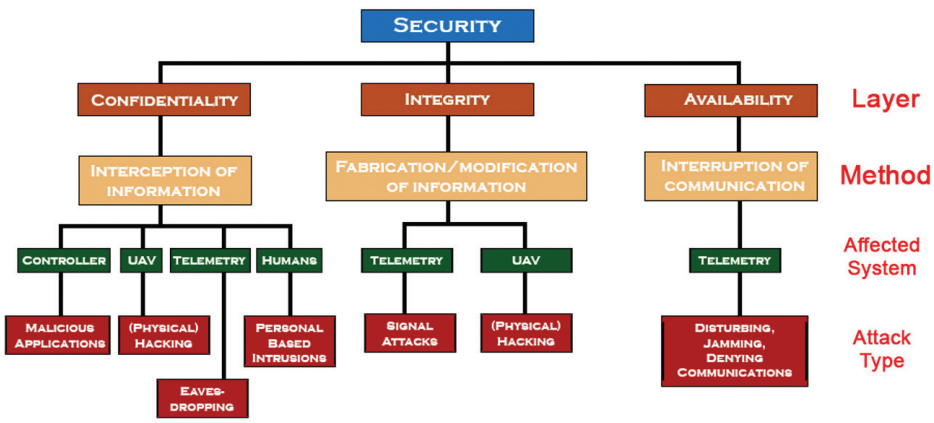

Figure 2: UAS shortened CIA model
Source: Compiled by the author based on Javaid 2012, 588.

The top layers are already mentioned previously, and the methods are concluded from the layers. The first method is interception of information. This means that an attacker has breached into the UAS by any means and has a capability of listening to all information that is being transferred within the system. Interception of information can affect all systems and might be coming from the human factor, as well. The controller, or the remote has a potential of being infected by malicious applications. Normally, in a UAS the controller is a dedicated device, which increases safety and security. However, in the civilian sector this is not always the case. Drone manufactures to stay competitive and to save costs often do not provide a designated controller, but applications that the user can install on his/her phone. This is a risk, because if the device gets infected by a malicious application from even a different application or system, that can affect the safe controlling of the UAV. Often, when hacking comes to play regarding a UAV, it is swapped with the telemetry. When a UAV gets hijacked, not the actual aircraft gets hacked, but the communications network. UAV hacking means physically accessing the device and installing malicious software. Human element is key to ensure cybersecurity. Precisely because of the hobby self-use method, as mentioned in the controller element, the user must pay attention to the risks and potential cyberattack when using the device.

Fabrication or modification of information usually refers to an attacker taking over the UAV. In this case the attacker modifies the information or injects information between the UAV and remote. One of the information types that can be modified or injected is controller inputs. There are multiple methods of carrying out a signal attack, most commonly GPS-spoofing, message injection, message modification, message deletion and deauthentication.[20]

Lastly, the interruption of communication is a much lower level of attack method than the previous two, because here the attacker did not breach into the system and has no control or overview of the information at all. The attacker in this case denies or jams the communication between the remote and the UAV.

All in all, the question is what the user can do. Users do not have access to the state-of-the-art technology that may be present on military drones; additionally, the methods from these devices may not be implemented into the civilian drones without publishing the technology.[21]

Keeping a cyber hygiene high means:

- paying close attention to what applications are installed on the controller smartphone, and it being virus and malicious application free
- running virus scan on the controller device
- before every take-off and during the operation of the device also paying attention to the surrounding area. Are there any devices, or people who have the potential to jam the communications network?
- checking the UAV and the controller before take-off that it was not tampered with and there are no outstanding devices attached to it
- being aware what cyberattacks could happen to the device
- not using the same log-in credentials that is provided both with the device and the network

While it is currently unlikely that a civilian drone will be hacked, the outcome of a hijacked or jammed UAV can be severe. In populated areas, it can pose a high risk to damaging buildings, injuring people, or even colliding with other air vehicles.

4. General concerns of non-EU certified drone use

When it comes to cybersecurity, a foreign made product always raises concerns, because during the manufacturing process backdoors or potential security breach methods could be implemented. The key issue usually is data protection and privacy. We can see in news outlets that phone and other telecommunication manufacturers get into a highlight due to this. In the United Kingdom, implementing a Huawei device within a 5G infrastructure is about to be forbidden.[22] A similar element can be seen with Google. Last year, in 2020, due to the United States Government placing a ban

[20] Mohsen Riahi Manesh – Naima Kaabouch: Cyber-attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions. *Computers and Security,* 85 (2019). 388.
[21] István Balajti: Az iker drónok zavarvédelme. *Hadmérnök,* 9, no. 1 (2014). 142.
[22] BBC News: *Huawei Ban: UK to Impose Early End to Use of New 5G Kit.* 30 November 2020.

on these types of smartphones, Google applications are forbidden to be pre-installed or sideloaded.[23] In this case, Google mentions the reason for this is data protection and protecting user privacy.

One of the largest drone manufacturers currently is DJI,[24] and the civilian drone market currently is overwhelmed with Asian imports mostly from China. If we look at the current situation, the China based DJI brand dominates the market (Figure 3). Gaining back market for other western manufacturers from this position will be really difficult, even questionable at this point.

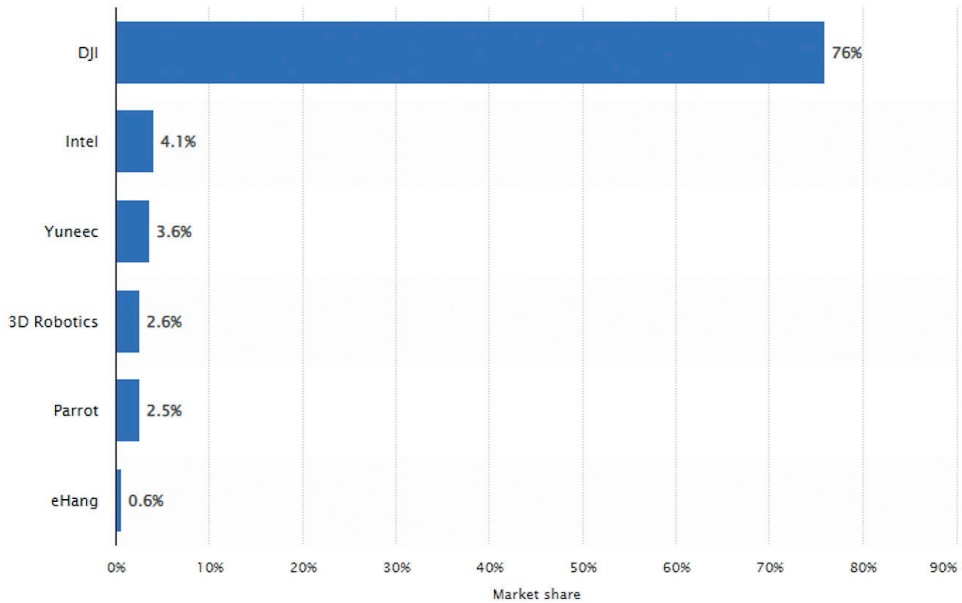

Figure 3: Drone Market share in 2021 March
Source: Statista, 2021.

The governments are already taking steps against DJI, for example the United States Government placed DJI on an entity list, which highly limits the company to be able to work with U.S. bodies.[25] The sense behind this serious action was that the USSOCOM[26] purchased multiple off-the-shelf drones and they all had cybersecurity risks and concerns.[27] Currently, we see no similar actions in the European Union, but it is possible that the EU will also take steps towards cybersecurity.

[23] Tristan O: *Answering Your Questions on Huawei Devices and Google Services.* 21 February 2020.
[24] Global Brands: *Top 10 Drone Companies in the World – 2020;* Business Insider: *Here Are the World's Largest Drone Companies and Manufacturers to Watch.* 22 December 2020.
[25] U.S. Department of Defense: *Department Statement on DJI Systems.* 23 July 2021.
[26] U.S. Special Operations Command.
[27] U.S. Department of Defense (2021): op. cit.

However, banning a technology is not always a good solution to the issue, because if there is no other company to cover the dropped out brand, the prices will rise. Banning a technology is a short-term solution, and if the market is one-sided like in this case, a total ban of the products could result in empty shelves. One of the longer period solutions is supporting local manufacturers where the whole production line is transparent to the governmental bodies. At first, it is a difficult task to overcome the disadvantage (from technology, manufacturing capability, logistics and supply standpoint), but to ensure the safety of drones (even if only about user privacy), it is extremely important, and one of the fundamentals of aviation.

5. Conclusions

In this paper our goal was to highlight the three main elements of cybersecurity and raise awareness about the ongoing concerns and challenges from the user standpoint.

One element of this is the data protection layer. Even if the user has a secure device, he/she still must pay close attention to where and how the device is deployed. Because there is a very soft line in the GDPR between not violating privacy and infringing it. The users must also be aware of the privacy limitations of their devices, and the personal data question outlines this and places it in a boundary. Additionally, knowing the boundaries of personal data may assist ethical and rightful drone usage. The data protection factor is also discussed by Hankó's[28] publication, where she draws a similar conclusion regarding data protection: the use of civilian drones may easily violate privacy.

The cyberattack factor is also a complex issue that a user must be aware of. A drone that is out of control has a potential of colliding with other air vehicles, buildings and people. The whole use of drones is a high-risk operation, and a user must be aware that cyberattacks can happen to his device, as well. The attacks might not target the vehicle at first, but other systems connected to it. The user must also know and understand, other vulnerable systems can affect their drone use.

Other element comes from the manufacturing standpoint of these devices. If the governments have no overview of the whole manufacturing process of these devices, they might be raising concerns over them. That happened in the smartphone industry and now is unwrapping in the drone commerce, as well. However, as mentioned before, the solution is not as easy as just to ban these devices. That leaves a market gap and hurts customers. It is a general truth that competition must happen, and support for transparent companies are needed.

[28] Viktória Hankó: A drónokkal kapcsolatos kockázatok és kezelési lehetőségeik [Risks and their Treatment Options Associated with Drones]. *Hadmérnök,* 16, no. 3 (2021). 189–202.

References

Abualigah, Laith – Ali Diabat – Putra Sumari – Amir H. Gandomi: Applications, Deployments, and Integration of Internet of Drones (IoD): A Review. *IEEE Sensors Journal,* 21, no. 22 (2021). 25532–25546. Online: https://doi.org/10.1109/JSEN.2021.3114266

Allied Market Research: *Unmanned Aerial Vehicle (UAV) Market by Type (Fixed Wing, Rotary Wing, and Hybrid), Application (Military & Defense, Civil & Commercial, Logistics & Transportation, Construction & Mining, and Others), and Weight (Less Than 50 Kg, and More Than 50 Kg): Global Opportunity Analysis and Industry Forecast, 2021–2030.* Online: www.alliedmarketresearch.com/unmanned-aerial-vehicle-market-A09059

Balajti, István: Az iker drónok zavarvédelme. *Hadmérnök,* 9, no. 1 (2014).

BBC News: *Huawei Ban: UK to Impose Early End to Use of New 5G Kit.* 30 November 2020. Online: www.bbc.com/news/business-55124236

Business Insider: *Here Are the World's Largest Drone Companies and Manufacturers to Watch.* 22 December 2020. Online: www.businessinsider.com/drone-manufacturers-companies-invest-stocks

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on Unmanned Aircraft Systems and on Third-country Operators of Unmanned Aircraft Systems.

Colomina, Ismael – Pere Molina: Unmanned Aerial Systems for Photogrammetry and Remote Sensing: A Review. *ISPRS Journal of Photogrammetry and Remote Sensing,* 92 (2014). 79–97. Online: https://doi.org/10.1016/j.isprsjprs.2014.02.013

Global Brands: *Top 10 Drone Companies in the World – 2020.* Online: www.globalbrandsmagazine.com/top-10-drone-companies-in-the-world-2020/

Hankó, Viktória: A drónokkal kapcsolatos kockázatok és kezelési lehetőségeik [Risks and their Treatment Options Associated with Drones]. *Hadmérnök,* 16, no. 3 (2021). 189–202. Online: https://doi.org/10.32567/hm.2021.3.11

Hartmann, Kim – Keir Giles: UAV Exploitation: A New Domain for Cyber Power. In *2016 8th International Conference on Cyber Conflict,* NATO CCD COE. Online: https://doi.org/10.1109/CYCON.2016.7529436

Javaid, Ahmad Y. – Weiqing Sun – Vijay K. Devabhaktuni – Mansoor Alam: Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. In *2012 IEEE International Conference on Technologies for Homeland Security,* HST 2012. Online: https://doi.org/10.1109/THS.2012.6459914

Manesh, Mohsen Riahi – Naima Kaabouch: Cyber-attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions. *Computers and Security,* 85 (2019). 386–401. Online: https://doi.org/10.1016/j.cose.2019.05.003

Markets and Markets: *Unmanned Aerial Vehicle (UAV) Market by Point of Sale, Systems, Platform (Civil & Commercial, and Defense & Government), Function, End Use, Application, Type, Mode of Operation, MTOW, Range, and Region: Global Forecast to 2026.* Online: www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html

Mordor Intelligence: *Drones Market – Growth, Trends, Covid-19 Impact, and Forecasts (2021–2026).* Online: www.mordorintelligence.com/industry-reports/drones-market

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation).

Statista: *Global Market Share of Consumer and Commercial Drone Manufacturers in March 2021, Based on Sales Volume.* Online: www.statista.com/statistics/1254982/global-market-share-of-drone-manufacturers/

Tristan O: *Answering Your Questions on Huawei Devices and Google Services.* 21 February 2020. Online: https://support.google.com/android/thread/29434011/answering-your-questions-on-huawei-devices-and-google-services?hl=en

U.S. Department of Defense: *Department Statement on DJI Systems.* 23 July 2021. Online: www.defense.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems/

Yaacoub, Jean-Paul – Hassan Noura – Ola Salman – Ali Chehab: Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations. *Internet of Things,* 11 (2020). Online: https://doi.org/10.1016/j.iot.2020.100218

Zissis, Dimitrios – Dimitrios Lekkas: Addressing Cloud Computing Security Issues. *Future Generation Computer Systems,* 28, no. 3. 583–582. Online: https://doi.org/10.1016/j.future.2010.12.006