23rd RSEP International Economics, Finance & Business Conference – Virtual/Online
25-26 November 2021, University of Washington Rome Center, Rome, Italy

www.rsepconferences.com **CONFERENCE PROCEEDINGS/FULL PAPERS** **ISBN: 978-605-70583-5-5/December 2021**

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

Preventive cybersecurity steps to enhance drone usage

Mircea Constantin Șcheau[a], Larisa Găbudeanu[b], Iulia Brici [c], Alexandru-Lucian Vîlcea[d]

[a] *Researcher, European Research Institute, Babeș-Bolyai University, Cluj-Napoca, Romania & Researcher, Faculty of Automation, Computers and Electronics, University of Craiova, Craiova, Romania*
E-mail: mircea.scheau@ubbcluj.ro , mircea.scheau@edu.ucv.ro
[b] *PhD student, Babeș-Bolyai University, Cluj-Napoca, Romania*
E-mail: larisa.gabudeanu@ubbcluj.ro
[c] *PhD student, Doctoral School of Economics and Business Administration, Babeș-Bolyai University, Cluj-Napoca, Romania*
E-mail: iulia.brici@ubbcluj.ro Corresponding Author
[d] *PhD student, Doctoral School of Economic Informatics, Bucharest University of Economic Studies, Bucharest, Romania*
E-mail: lucian.vilcea@ie.ase.ro

Abstract

Cyber threats regarding drones have increased in the previous years due to the extended use and to the lack of proper preventive measures, not necessarily in the military domain, but in various civil sectors. The legal requirements in place and the best practices in the IoT or drone specific field emphasize specific cybersecurity requirements, however, currently do not view the need for cybersecurity in an integrated matter throughout the drone's life, but rather only for specific parts of the drone life cycle. This research focuses on the entire ecosystem related to drone usage and the need for a correlated and holistic approach to preventive measures against cyber-attacks and exploitation of vulnerabilities, given the position of each stakeholder to contribute to the security of the drone hardware, software, communication mechanisms and not only. In addition, this research also applies this approach for the entire lifecycle of the drone, from creation to decommissioning, (given the changing of cyber threats and cybersecurity landscape). This leads to an increased trust in drone usage in various economic and commercial purposes from both drone users and their customers. The conclusions drawn in the research are validated with a quantitative assessment by way of a questionnaire outlining reactions towards cybersecurity and the main needs of drone users. The questionnaire was chosen as methodology because this type of research method on this particular topic was not approached by the existing literature of the field. Thus, the research includes a multi-disciplinary approach encompassing legal, economic and technical angles of the topic that aims to pave the way for integrated research in terms of all involved stakeholders.

Keywords: security by design, cybersecurity management, cost-benefit analysis, cyber-attack prevention, sustainability, certification, accountability, responsibility

Jel Codes: O14, O33, L15, K24

1. Introduction

In the recent decades, the digital transformation is going on a parallel road with the passing of time. The general orientation is towards efficiency and minimum cost, but also the comfort of the client who is requesting for a product or service. Drones represent an important means in the process of digitalizing several areas. In particular, they are very often used in the military field, but also other civil sectors. The unmanned vehicles industry has grown exponentially in the last 10 years, finding its utility in multiple industries. Precisely for this reason, the forecasts for the use of these devices are on an upward trend.

Being an innovation, it attracts both advantages and disadvantages. In terms of the benefits that these innovations bring, drones represent very useful ways to facilitate many processes, but unfortunately there are a number of downsides. These are due to the increasingly frequent cyber threats of recent years. As the use of these new technologies increases, so does the risk of unwanted events and damages caused to property or to individuals. The main reason for these situations is the lack of a set of preventive measures in order to anticipate possible problems and meet them with immediate solutions.

Cybersecurity is a key element for this topic. It is imperative to develop a legislative framework targeting drones, with all processes, from production and covering the period throughout the use of the drone. Based on the existence of a legislative basis, certain conditions of use can be imposed. These could very effectively prevent the aspects that we previously called inadvertent. Our research supports the development of the best practices and practical

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

approaches concerning preventive security measures in this regard, trying to capture the opinion of users about the most common threats and vulnerabilities in the use of drones and identifying measures to prevent their occurrence in the future.

2. Overview of the existent literature

The specialized literature comes to support these ideas. In most of the studied bibliographic references, we can observe that the authors mentioning and analyzing the use of unmanned vehicles in several fields of activity, but, on the other hand, they also detect shortcomings that those attract. Some authors present case studies of cyber-attacks, others detect hacking methods, and others propose solutions. In the following, we will try to synthesize some of the most interesting sources read in order to inform on the approached topic.

In a 2015 material, Dulo classifies vulnerabilities into several categories: safety, security, privacy, payload, administrative, 2nd amendment. The study also identifies where attacks can occur, namely: embedded UAS Systems, Soft / Hardware or combinations between them.

In 2015, Yağdereli et al. talk in their study about the dependence of today's world on technology in all the fields of activity. In the same sense, they notice the tendency of vulnerability and exposure to errors due to cyber-attacks. Unmanned vehicles face such technical errors and hacker attacks. The authors propose that these limitations and vulnerabilities be identified and classified in order to create a mitigation strategy.

These two studies contribute to the taxonomy of cyber-attacks and types of vulnerabilities.

In 2017, Chang et al. address the issue of commercial and personal regulations regarding security, respectively privacy in the use of drones. The authors raise some problems, in this regard, in the United States. The case study of this paper describes the experience of 20 drone users. They had to evaluate the activity of the devices and report the identified issues. The results of this experiment led to the formulation of recommendations for improving safety regulations in the use of drones. This shows the user perspective and user requirements.

In 2018, Lagkas et al. emphasize the multiple utility of drones and expose the new technologies under development that will work within them. On the other hand, it also detects the disadvantages that appear in connection with cybersecurity, but also with the management. The paper aims to list and detail new areas in which UAV devices will be active, but also reviews the general requirements to be met in order to prevent security or privacy issues. The paper proposes a protection of drones within an IoT architectural network.

In 2019, Zhi et al. address the issue of security and privacy issues of UAVs. In this paper, the authors report that a drone is guided by certain sensors during flight. Small changes in these sensors can completely compromise such a device. First of all, the sensors can receive wrong information, and as a result, the drone will act wrongly. Second, these sensors can be damaged. The flow of information between the drone and the ground control station is based on a type of communication that is very easy to compromise. In terms of privacy, there are aerial photos that can capture private information (location, time).

In 2020, Yaccoub et al. talk about the ability of drones to successfully meet human needs, but also about malicious use, respectively cybercrime. The paper presents a realistic cyber-attack scenario to highlight the ways of hacking. This simulation represents more than a bibliographic reference for the review of the specialized literature. It allows the adoption of new techniques for detecting and protecting unmanned vehicles.

Also in 2020, Raja et al. approach the drone safety issues. The authors believe that intervention is needed in advance. Raising security standards will also have disadvantages. Among the most common enforcement measures is unauthorized reinforcement, a unique time-based password. The simulation results proposed by the authors show that the LTOTP (Logistic map-based Time-dependent One Time) algorithm enhances the reinforcement.

In 2021, Yahya et al. address the issue of increased use of drones in various fields of activity, such as: military, journalism, filming, photography, transportation, delivery, etc. In particular, the role of drones in the Malaysian construction industry is highlighted. In this case, the drones encountered privacy and security issues. The authors suggest that government support is useful in promoting the use of unmanned vehicles, as well as in informing the population about the aid those devices bring, but also about the existing risks.

The above set of articles underline the important role of drones for successfully and efficiently performing certain activities, together with specific use cases of cyber-attacks or vulnerabilities identified in their case studies (both at the source code level and the software architecture level).

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

Also in 2021, Iqbal addresses the issue of cybersecurity and the challenges that will exist over time. The author emphasizes the importance of drones in several fields of activity, as we find in Yahya's study. Despite the opportunities that the use of drones creates for the industry in which they operate, there are also many threats related to security and privacy. This study also suggests the help of the government in regulating the use of drones.

In 2021, Yahuza et al. are writing a very interesting article about the Internet of Drones (IoD) which is a decentralized network that connects drone access to controlled airspace and guides devices from one location to another. This type of network is what Lagkas had thought in 2018 that it would be very helpful if it were implemented. This IoD is a network vulnerable to security and privacy challenges. This paper captures the need for methods of defense against these situations. The authors believe that an examination of the secure IoD architecture is needed to identify what compromises the security and privacy of drones. The purpose of their article is a list of performance evaluation methods used by these techniques.

In another study from 2021, Abdelmaboud emphasizes the idea that drones are a very smart technique for managing problems in many areas of activity. With the existence of IoD, certain aspects related to security, privacy and communication related to IoD remain to be resolved. The paper summarizes the main security and privacy requirements and presents an IoD taxonomy. Also, the paper is based on commercial case studies, proposing solutions for each problem detected.

Also in 2021, Al-dhaqm et al. address another niche of drone vulnerabilities, namely crime, which is closely linked to security issues. The authors propose the detailing of forensic models using the Design Science Research method. The results of this study highlighted both topics for future research and challenges in the circle of drone incidents. The authors also propose a generic model of investigation. Following the results obtained, the study represents a background for a future international standardization in drone crime.

This set of articles focuses on identifying frameworks, standardization point and methodologies to be followed in order to provide governance of the drone lifecycle and, to this end, focus on particular aspects that were identified in the respective research and which should be included in drone governance or the economic impact of cybercrime (Achim & Borlea, 2020).

The studies we have considered to create an overview of the chosen topic led to some common issues. The presence of the risks of cyber-attacks in the use of drones is widely identified. Some authors look for solutions to identify them, others to characterize them, others to solve them, and still others to prevent them. The reviewed literature analyses the issue in silos, without analyzing the entire ecosystem that involved unmanned vehicles such as drones. The topic offers a generous research horizon because the approaches can be diverse. This article brings a holistic view on the topic, by outlining the role of each stakeholder in the ecosystem and in preventing cyber-attacks. In addition, the article analysis the main types of preventive security measures that can be implemented and the opportunity of various types of implementations of the preventive security measures. Our approach is includes as well in the form of a questionnaire to help us identify which are the main vulnerabilities that users accuse and which are the prevention methods that seem relevant to each case.

In the following sections of our study we will address, as follows: Section 2 - Existing vulnerabilities and prevention methods (describes all problems identified in terms of cybersecurity or privacy and proposes a series of solutions to prevent these problems or at least to act in time to stop existing problems), Section 3 - Respondents view (includes processing of the answers obtained in the questionnaire) and in Section 4 - Conclusions and future research directions.

3. Proposals concerning prevention of threats and vulnerabilities

According to Zeng et al. (2016), drones are prone to a variety of attacks that can compromise the data, as well as the physical state of the UAV itself. Since most of the available drones in the consumer sector are not always designed with information security in mind, the threats that drones face are diverse.

Each of the parties involved in building, programming and operating the drone can introduce vulnerabilities that can range from the physical flaws introduced by the manufacturer of the drone to a wrong exploitation of the aircraft by the end-user.

During this section, we are trying to capture all categories of existing threats or vulnerabilities that we have mentioned above and synthesize how are these can be done and what implications can have.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

3.1. Design vulnerabilities

Potential vulnerabilities of an unmanned aircraft can be found in the design of the device itself. Intentionally or not, drone manufacturers can introduce design vulnerabilities to their products, such as rootkits, kill-switches or backdoors.

A rootkit is a piece of software that allows privileged access to a device by subverting the operating system, while remaining undetected from the administrators. It uses an existing system vulnerability to install itself on the device to gain root-level access to the operating system. After gaining privileged access, it can run unauthorized software, intercept data or even modify the functionalities of the infected system. This way, attackers can steal confidential information processed by the drone or even take control of the aircraft.

Rootkits can even take advantage of some dangerous, but legitimate functionalities of the aircraft. For example, most consumer drones have a built-in kill-switch that instantly cuts the power of the propellers to prevent a potential disastrous scenario while in the air. A possible usage of a rootkit is to exploit such functionalities, with the intended purpose of crashing the drone.

Manufacturers can also introduce vulnerabilities voluntarily by creating backdoors. The backdoors are implemented at design-time and lets the manufacturer access the system without the users' consent. Unlike kill-switches, backdoors are rarely noticed, since they do not affect the functioning of the drone itself. Also, they are much harder to detect since most of the times these backdoors are implemented at hardware level.

3.2. Data vulnerabilities

At the data connection level, the drone itself can present some design and security flaws. Since most of the data transmitted between the drone and ground station must be done fast and with a minimal loss, often the exchange channel is not encrypted, since this kind of operation would involve heavier computing and, implicitly, a slower data exchange speed. A variety of encryption techniques were tested, but their own flaws are making this problem even harder.

By using symmetric encryption, the probability of an attacker to decipher the encrypted data is extremely small. Algorithms such as AES are very powerful. Since its minimum key length is 128 bits, brute-forcing a total number of 2128 possible key combinations is not feasible (at least not in a limited amount of time). Also, there is no known mathematical property that can compromise the S-box substitution mechanism used internally by the AES algorithm. The only known vulnerability of the algorithm is related to timing attacks, but the implementation of such systems is costly and not very time efficient. Still, AES encryption comes with a downside: the exchange of the encryption key itself. This poses a problem, since the key must be sent as plain text to the other party, thus in a non-secure way. (Al Hasib et al, 2008)

Asymmetric encryption is not a viable option either. Even though the problem of securely exchanging the encryption key is solved, the high computational power required by asymmetric encryption is very high. Since it relies heavily on randomly generated very large prime numbers, the computational power required to perform such operation is big. As well as AES, an asymmetric algorithm like RSA is very strong against brute-force attacks, provided that the encryption key is of a reasonable size. Usually, a 2048-bit key is used for RSA encryption. However, the longer the key is, the greater the computational power that is required to encrypt/decrypt data. The mathematical properties of RSA make the algorithm vulnerable to attacks, if the chosen encryption key is not big enough. Since the algorithm relies on multiplying prime numbers, a poorly chosen encryption key will facilitate the factorization of the cipher-text, although this operation is also computationally expensive.

A possible way of encrypting data in a secure and fast way can be done using a combination of both symmetric and asymmetric algorithms. Since the symmetric algorithms, although fast, pose the problem of not being able to securely exchange the encryption key, while the asymmetric algorithms rely on public keys, but are very slow, it can prove beneficial to use algorithms such as RSA only to securely exchange the encryption key of a symmetric algorithm, such as AES, then using the exchanged encryption key to send secure messages using only the symmetric algorithm. Figure 1 describes how this process could be implemented.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

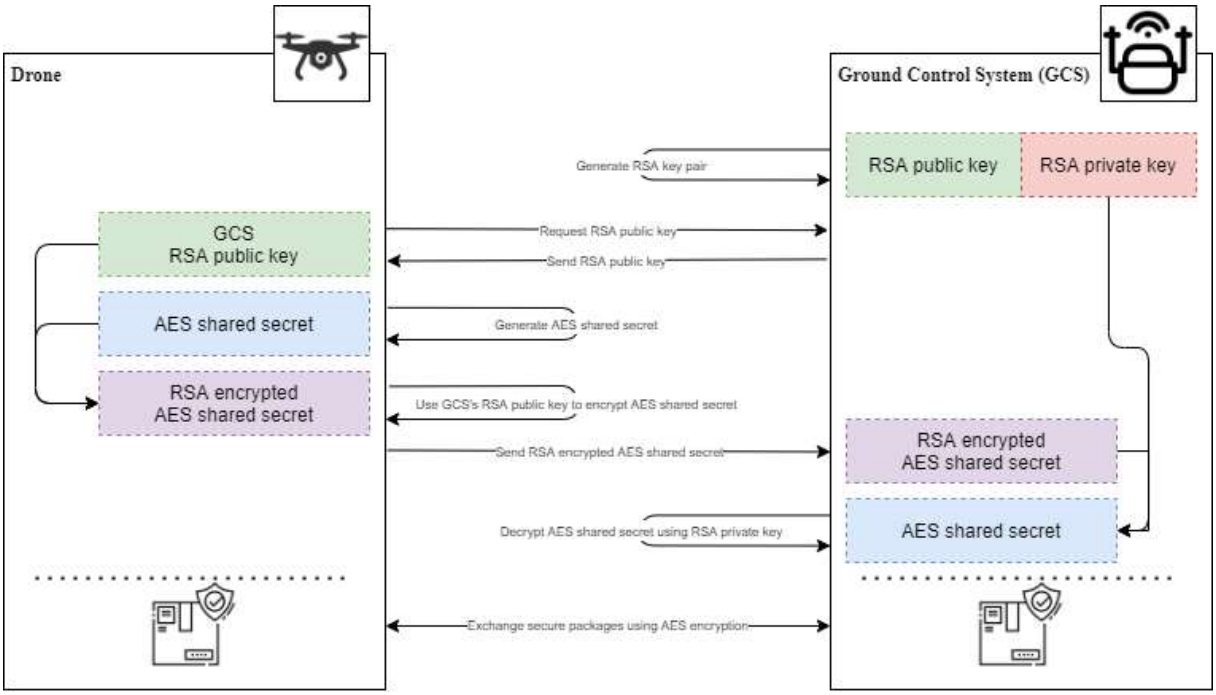

Figure 1. Hybrid symmetric/asymmetric encryption in UAV communication

Source: Author's processing

3.3. Authentication vulnerabilities

Many times, the user itself is responsible for a variety of security issues, by either unwillingly exposing valuable information to a potential attacker or by not protecting its own data strongly enough.

Weak authentication is one of the most exploited types of attacks. According to Data Insider, in 2017 an extensive study related to users' habits related to password management revealed that most of the consumers have risky behavior. In the United States alone, each e-mail address is associated with 130 password protected accounts, while 72% of the respondents admitted storing their passwords in a non-secure environment (paper, a file on their computer etc.) or even reusing the same password for multiple accounts. This can lead to a potential security issue, since hacking a single platform can expose passwords that some users may reuse for different authentication processes, including the ones that are related to drones' usage. This way, attackers can try to authenticate using passwords that the users might reuse. Rainbow tables attacks are also very common when attackers exploit a weak authentication scenario.

However, the same study showed that nearly 65% of the respondents are considering security more important than convenience and they choose complex passwords that are not reused across multiple platforms. Also, more than 93% of the respondents admitted using somewhat complex or very complex passwords, while 48% of the respondents also use a multi-factor authentication scheme for their accounts.

Another common way used by attackers to exploit users' negligence is social engineering. By addressing the right questions or using data that users share on different environments, attackers can deduce what is the password that protects a certain account. A study conducted by the British National Cyber Security Centre revealed that 15% of the British people use their pet's name as a password for online accounts, 14% use a family member's name, while 13% include an important date in their life in their passwords. This kind of information enables attackers to deduce possible passwords that protect an account.

To counter possible breaches due to weak authentication, the drone manufacturer, as well as 3rd party providers can enforce a stronger password policy, as well as providing the users the possibility to use multifactor authentication. From a user's point of view, it is recommended to avoid reusing the same password for more than one service, as well as protecting their accounts with a second mean of authentication (for example, one-time passwords, physical tokens or biometric authentication) (Yildirim et al. 2019). Also, it is imperative to store the passwords in a secure location, like password vaults.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

3.4. Operational vulnerabilities

Users are also responsible for a variety of operational mistakes that can lead to potential security issues. A common mistake is not paying enough attention to the atmospheric conditions. Flying in very low temperatures has a direct effect on the drone's battery life, reducing the flying time, as well as inducing malfunctioning in the aircraft's sensors. Most manufacturers recommend avoiding flying when the air temperature drops below -10ºC, while the battery's internal temperature should never drop under 20ºC. Also, flying in temperatures greater than 40ºC can have an effect on the internal components of the drone, increasing the risk of plastic components melting. Also, high temperatures are often associated with a high humidity, which can damage the electronic components of the aircraft. Wind speed is also often disregarded, especially the higher altitude winds. Since the air currents find less resistance as the altitude increases, their speed also increases, even though at ground level the wind is not perceived to be too strong. Air currents that exceed 40km/h are considered too dangerous for safely operating a UAV.

Also, a poorly maintained battery can lead to unwanted situations. Lithium-polymer (LiPo) batteries are sensitive to temperature changes and can easily be a fire hazard when handled improperly. The usage of LiPo batteries while still being warm from charging or charging a LiPo battery right after its usage might affect the internal structure of the battery, due to the longer amount of time that the battery is kept at a high temperature. In the case of multi-cell batteries, charging or discharging a LiPo battery with improper equipment that do not balance the amount of charge available in each cell might lead to dangerous situations, making the battery unstable and prone to internal short-circuiting.

To avoid most of the operational issues, a pre-flight checklist is always necessary. This way, the users can make sure that all the required conditions in order to safely operate the UAV are met. 3rd party software that can provide information about weather in a particular location or the applicable flight restrictions in the area are also very helpful. Some drone manufacturers include in their software features that can help the user identify a restricted or no-fly area that can also decide whether the drone should take off or not.

4. Methodology and data

For this paper, we have elaborated and used a questionnaire, using the online platform QuestionPro, in order to identify the views of drone stakeholders in terms of prevention mechanisms. The questionnaire was distributed via internet, using e-mail addresses and social media platforms, such as Facebook, Twitter and LinkedIn. The survey was distributed both to specialists in the field and to non-specialists. The survey was conducted from May to July 2021. We considered useful for interpretation the field of activity of the respondents and did not consider useful demographic information such as age group, education level or gender.

The questionnaire contains 17 questions, 15 of them refer to the topic we study and the other 2 questions were added in order to detect and categorize our sample. The survey was designed and distributed in both English and Romanian. For this reason, some of the following interpretations can be interpreted separately for each language category and then concluded for total responses.

The questionnaire was completed by a total of 233 respondents, 37 for the English version and 196 for the Romanian version. For the English version, the distribution of answers is explained in Figure 3. The vast majority of respondents came from Romania (44.12%), followed by answers from the Netherlands (10.29%), Italy (8.82%), Portugal (5.88%), Belgium (4.41%), the United States and Bangladesh (2.94% each), but also India, Bulgaria, Serbia, Canada, Luxembourg, Turkey, Germany, Latvia, Greece, Malta, Croatia, Hungary, Poland and Israel (1.47% each of them). For the Romanian version, 93% were answers completed by Romanian citizens, and the remaining 7% were answers from Spain, Greece, Romania, Great Britain and other countries where there are Romanian speakers or maybe Romanian citizens working in those countries.

The main purpose of the questionnaire was to see the manner in which respondents view the need for measures to prevent cyber-attacks on drones and drone users, together with the stakeholder they view responsible for implementing and monitoring such preventive measures.

5. Results and discussions

Therefore, this section concentrates on the business, operational and legal role of the entities in the drone ecosystem in order to identify the best approach in terms of operativity of the production/distribution/maintenance process

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

and of balance between profit and investment of such entities. This analysis assists with views on implementing the preventive measures proposed in the previous section and the effectiveness verification for such preventive measures.

Question 6 of the questionnaire was *"Which of the following do you consider useful preventive measures to prevent damage / hacker attacks in cases of modifications made by the user to drone software? (1 to 5 scale, 1 representing total disagreement and 5 total agreement).* The answer options for this question can be found in the legend of the table below.

Table 1. Question 6 responses – preventive measures, software changed by user

Answer/Scale	1	2	3	4	5	Average score
Any change to the drone software should be approved by the drone software producer	34	10	26	35	158	4.04
A certification mechanism should be in place to perform a cyber security review of any change in the drone software	23	11	33	59	137	4.05
Users should not be able to change the drone software	36	27	41	23	136	3.75

Source: Author's processing

One reason for multiplication of vulnerabilities is the mixing of existing software with new software not created by the same entity. In these questions we analyzed the case of software created by the user of the drone. As in the case of other devices (either internet of things devices, laptop or mobile telephones), there are various manners of ensuring that no cyber-attacks take place (European Commission, 2017), out of which we have explored three in this question.

The question we are posing goes beyond the identification of cyber-attacks and emphasizes the need for preventive measures. If for most laptops and mobile telephones, the identification of cyber-attacks may be sufficient as it does not generally hinder the using of the device, in case of internet of things devices (and, especially, drones) the identification of cyber-attacks may lead to damages to both the device and the environment/people around it. For this reason, in case of the latter (and, especially, drones) supplementary mechanisms have to be implemented.

It is interesting to see that respondents generally prefer to have mechanism of verification in place (either by the producer or a specialized independent entity) rather than no verification mechanism. This is in line with existing legislation in other sector that include a certification of quality. Further, the respondents consider the governance of changes brought by users as a better approach than the prohibition of change. Nevertheless, in the rating of the responses, the prohibition of changes is classified as third (with an average score of 3.75).

The first option chosen by the respondents is the verification to be performed by the drone software producer. This can be considered a good option in terms of entity that knows best knows the structure of the software and the potential vulnerabilities that new software can generate. From an operation perspective, a mechanism can be design in the form of an app store whereby proposed application are submitted for review before they can be safely deployed on the drone of the user (or, even, place in the app store for other users to deploy). From an operational perspective, this can be cumbersome on the drone software producer, as it will require significant resources to analyze all the requests coming from all over the world. Of course, a fee can be implemented in order to finance the review process. Nevertheless, having a single entity (who is also the producer) review changes can generate subjective reviews given the limitations/vulnerabilities of the existing drone software.

For this reason, the secondly ranked option, having independent entities to audit/test the proposed application in order to give them a certification can be useful in terms of segregation of duties and guarantee of independence. The idea of app store can still be implemented, with a specific platform on which all certification entities can act. From an operational perspective, this can be easily implemented and is widely used in other sectors in terms of certification.

The third option that prohibits the change to the existing drone software limits development and keeps the drone ecosystem closely tied to the drone producers for any new features. This can have anti-competitive consequences. Further, there have been similar discussions in the last years with respect to software embedded on the internet of things devices and lack of possibility for users/other entities to change it or to include security features into it. The

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

discussions are currently in the sense that this prohibition is not beneficial from a competition perspective, from the point of view of advancing science and from a security perspective.

Question 7 was *"Who is liable in case the drone software contained vulnerabilities from the outset and these permitted a hacker to control the drone and generate damages? (Multiple choice question)"*. The answer options for this question can be found in the legend of the figure below.

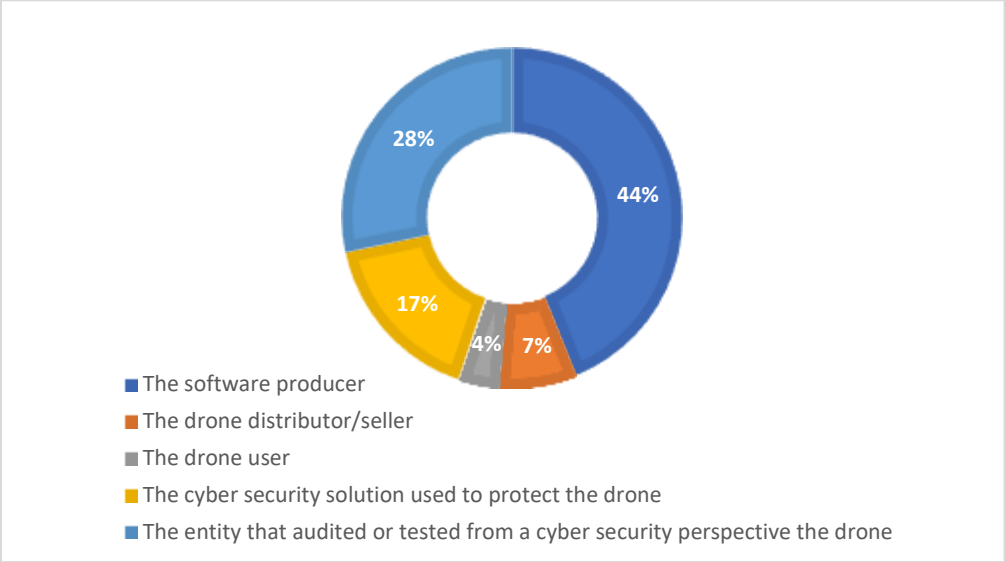

Figure 2. Question 7 responses – liability in case of outset vulnerabilities

Source: Author's processing

This question is aimed at identifying the best place to include additional controls in terms of drone vulnerability verification. Further, this gives additional clarification on how the preventive security measures, such as the ones included in the previous section, can be implemented within the drone ecosystem, from its production to the moment it is sold to/used by the user.

The responses are interesting in the sense that the entity that audited or tested from a cyber security perspective is considered by 28% responsible, while the software producer is considered responsible by 44%. Of course, this depends in practice on the manufacturing process. Current legislation, including the EU Product Liability Directive and general tort law generally view the producer as liable for the vulnerabilities it embedded in the drone software/hardware. Nevertheless, there may be instances in which other stakeholders in the drone ecosystem may be considered as having a significant role in particular aspects that can lead to these stakeholders being considered liable. Such aspects have also been analyzed briefly in the relevant literature, include in (Bassi E., 2019).

In terms of distinction between the software producer and the entity that audited/tested from a cyber security perspective, there are a couple of points to consider. On the one hand, the general legal doctrine and responsibility matrix views the producer as liable for the products it has created, even if these are certified or analyzed by other entities before they are placed on the market. On the other hand, the entity auditing/testing the drone should be held liable for not identifying certain types of vulnerabilities that should have been identified based on known standards at the time.

One proposed approach can include the general liability of the producer, with the auditing/testing entity being a check point. In terms of liability, the producer could, in a litigation, request certain damages from the auditing/testing entity only if the auditing/testing methodology were not properly applied and, thus, certain vulnerabilities were not identified. Otherwise, holding the auditing/testing entity liable for all vulnerabilities may be excessive for its role in the drone ecosystem and may incentivize the producer not to invest in the security of drones. Thus, a balance must be stoked in order to keep all entities involved in the drone ecosystem engaged in the cyber security measures improvement process.

The percentage of respondents considering the cyber security solution as liable (17%) is quite high. This response should be further analyzed in order to understand the reasoning of the respondents. On the one hand, it may entail that the respondents do not fully comprehend the role of a cyber security solution that generally aims at actively

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

rejecting cyber-attacks or detecting intrusion of threat actors in the system. Thus, the role of the cyber security solution is more a reactive one that does provide security against zero-day attacks, for instance. Consequently, the cyber security solution can be held liable for not identifying the infections or not preventing the cyber-attacks it could have been prevented based on known indicators of compromise, threat signatures and attack mechanisms. However, it cannot be held liable for not detecting zero-day attacks or vulnerabilities that can be exploited. On the other hand, this high percentage shows that respondents consider that there should be other entities, independent ones from the producer, in the drone ecosystem that should ensure the security of the drone, aside from the producer.

Around 7% of the respondents consider the drone distributor as responsible. This can be generated especially by situations in which the drones are produced outside the country where they are sold (e.g. for the EU market the drones are produced outside of the European Union). In order to address this case, two mechanisms can be implemented. The initial EU/national distributor that brings the drones on a specific market is the one certifying the drones at the EU/national level and it remains liable for all consequences, with the possibility to request the payment of damages from the drone producer. However, this creates a more complex ecosystem in case vulnerabilities are found and should be addressed in order to enhance security of the drone. Another, more practical mechanism, is for the distributor not be liable for selling the drone provided by the producer and for the producer to obtain all certifications and address all vulnerabilities identified during the certification process or afterwards, with the distributor having no role in this respect.

It is interesting to see that there are 4% of respondents that users are responsible for cyber-attacks. This entails that these respondents consider that there is a minimum set of cyber-hygiene actions that a user should implement and respect, as a typical form of using the drone. Lack of compliance with these results in a causality effect between the lack of compliance and the consequences in case of a cyber-attack. Thus, even if the percentage of respondents having this view is low, this can be taken into account when outlining the preventive security measures to be implemented by various entities in the drone stakeholders.

Thus, it seems that respondents are viewing a shared responsibility in case of cyber-attacks. This can be transposed in a shared responsibility in terms of verification and improvements to the drone software. Of course, this has to have a long-term implementation, as new cyber threats and vulnerabilities can appear based on technology advancement.

As it can be seen from the preventive measures section above, it seems that, from a technical perspective, the approach is similar. There are certain improvements that can be performed by the producer of the drone, certain vulnerabilities that can be identified in practice by other stakeholders in the drone ecosystem and certain rules that should be implemented by users, with partial/silos identification of such aspects in existing literature such as (Bouhcer P., 2014). Nevertheless, the legislation and operational process does not fully address these aspects and should be adjusted in order to balance the responsibility with the best placed stakeholders to address the risks, while not providing excessive cumbersome obligations on a particular stakeholder.

The eighth question was *"Which of the following are useful preventive measures in case of software vulnerabilities included from the outset in the drone software? (1 to 5 scale, 1 representing total disagreement and 5 total agreement).* The answer options for this question can be found in the legend of the table below.

Table 2. Question 8 responses – preventive measure for outset vulnerabilities

Response/Scale	1	2	3	4	5	Average score
Cyber security auditing before the drone is placed on the market	7	9	31	41	165	4.38
Periodic cyber security auditing to be performed by the user in order to be allowed to fly the drone	34	26	52	45	96	3.57
Failsafe mechanisms in case the drone is taken over by hackers in order to safely land the drone and alert the user	14	9	30	48	152	4.25
Cyber security software to be included in the drone to prevent intrusions and respond to them	6	8	25	37	177	4.47

Source: Author's processing

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

This question addresses specific types of preventive measures to be implemented in order to identify vulnerabilities and to prevent negative consequences in case these are used by threat actors during a cyber-attack.

The respondents view as very important real-time cyber security solutions and cybersecurity auditing before placing drones on the market, with these two security measures being ranking first and second in terms of their utility.

Further, additional technical mechanisms such as a failsafe mechanism that can ensure safe landing and shut down of the drone are also consider highly desirable. This show that, in addition to real-time responses to cyber-attacks, respondents consider the need for ensuring lack of negative consequences on property and people when a cyber-attack occur when the drone is flying.

One aspect worth further analyzing is the fact that periodical auditing is not considered useful by respondents. This should be further analyzed, as vulnerabilities can be identified in time and not at the outset, when the drone was placed on the market. The use of cyber security software may not be sufficient in this respect, with additional checks in terms of penetration testing and vulnerability management being required. Thus, it may be that the respondents did not view this distinction between the scope of cyber security software and independent security verifications. Alternatively, it may be that they consider there is a need for more frequent vulnerability scans/penetration testing exercises and not just annual ones. This aspect can be further analyzed to understand the expectations of the users and of the other stakeholders.

The aim of corroborating adequately the above mechanisms together with the other preventive security measures mentioned in the previous section is to ensure a better resilience in time (through continuous monitoring as well). The concept of resilience has been in focus in past decade, including in the context of drone usage, as detailed, for example, by Coopmans C. (2014).

The fourteenth question was *"Do you think there will be improvement generated by drone usage in the field of activity they are used for?"*. The answer options for this question can be found in the legend of the figure below.

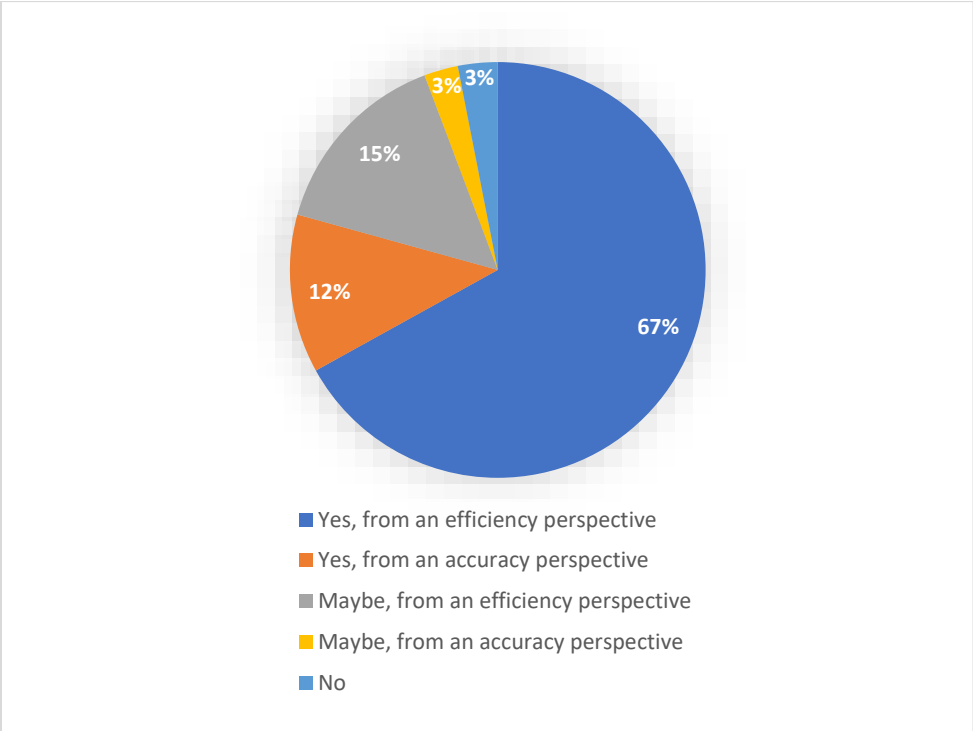

Figure 3: Question 14 responses – drones utility in improving activity field

Source: Author's processing

The question aims to understand the view of the respondents in terms of utility of drone in various sectors. The majority (79%) consider the drones useful in terms of improvement brought to existing manners of approaching

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

the same issue. In terms of advantages brought by the drone, the majority (67%) consider the drones bring efficiency to existing processes, whereas 12% consider they provide accuracy in terms of performance of the tasks.

This entails that there is general positive feedback in terms of using drones, with the security concerns being set aside by the respondents by reference to the benefits their use can bring.

It is interesting to see that around 18% of respondents have mentioned that drones maybe can bring advantages. This lack of confidence can be explored further in order to understand the fears of the respondents in terms of using drone. One angle can be that they are concerned with using drones in certain specific sectors or activities and for these they are reluctant on the usefulness of drone. Another angle can be that they are not confident on the actual usability of drones or on their security against attacks or bugs. Further, in certain cases, it may be that the respondents are not familiar with the benefits of using drones in certain activities and their reluctance comes from lack of familiarity with the technology and the process.

Nevertheless, the results show positive feedback in terms of drone usage, as was the case for the press release issued by public authorities, including (European Commission, 2014). This is also reflected by the responses to the other questions within the questionnaire, which show that, even though respondents have certain concerns on the operational side, have a general view that drone usage can be integrated in daily life.

5. Conclusion and future research directions

The article shows that there are various types of preventive security measures that can be implemented to prevent cyber-attacks on drones. Such prevention mechanisms are becoming more important given the wide use of drone in terms of industry sectors, territorial reach and activities for which they are used, as detailed in (SESAR Joint Undertaking, 2017). These can fall within two main categories: technical and organizational. The organizational aspects have to be taken into account when setting-up the creation of security measures and the roles and responsibilities in this respect.

As shown in the results to the questionnaire, each stakeholder in the drone ecosystem has a specific role, which has to be taken into account when designing the entities responsible with the implementation of the security measures or with supplementary controls to verify existing vulnerabilities.

In terms of entities responsible for cyber-attacks, the respondents have the same view of shared responsibility among the entities involved in the drone ecosystem. One additional aspect to be had in mind is the constant monitoring of the need for security measures. On this point, the respondents were divided, as some of them did not view periodical reviews of the drone software as useful, with an instant vulnerability scanning solution being preferred. This shows once again that the cyber threat landscape is ever changing and that very swift adapting must take place in order to prevent cyber-attacks.

Regardless of the security issues that may arise and the need for additional implementation of preventive measures both in legislation and in practice, the respondents view the use of drone in various sectors as positive in terms of the efficiency of performing certain tasks and in terms of the accuracy of the results obtained in various tasks. Additional clarity is brought by the overview provided in this paper than in the existing literature identified relating to the preventive security steps that can be taken, as is the case for (Novaro Mascarello L. and Quagliotti F., 2017).

As next steps and future research, it is essential to determine clearly the role of each stakeholder in the ecosystem in terms of quality assurance and cyber security. This entails a balance between the liability of the particular stakeholder and its role in preventive active actions, as such balance has been hinted in literature such as (Carlsen, Christopher, Tarr, Julie-Anne, 2021). Further, this can assist with identifying the view of all stakeholders involved in the drone ecosystem and with the manner in such to have an integrated approach towards preventive security measures in order to increase the trust of users and of stakeholders in the use of drone.

Author Contributions: Conceptualization, M.C.S., L.G.and A.L.V.; Methodology, M.C.S., L.G. and I.B.; Formal analysis, L.G., I.B. and A.L.V.; Investigation, M.C.S., L.G. and A.L.V.; Resources, I.B and A.L.V.; Data curation and analysis, I.B. and L.G.; Writing—original draft preparation, L.G., I.B. and A.L.V.; Writing— review and editing, M.C.S., L.G., I.B.and A.L.V.; Visualization, M.C.S., L.G., I.B., and A.L.V.; Supervision, M.C.S.; Project administration, M.C.S.; Funding acquisition, M.C.S and I.B.

All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a grant from the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174, within PNCDI III.

Data Availability Statement: Data used in this analysis is not public, but available upon request.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

Abdelmaboud, A. (2021), The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. *Sensors 21(17)*, 5718.

Achim, M. V., Borlea, S. N. (2020), Economic and financial crime. Corruption, shadow economy, and money laundering. *Springer Nature Switzerland AG.*

Al-dhaqm, A., Kebande, V. R., Adeyemi, I. R., Razak, S. A. (2021). Research Challenges and Opportunities in Drone Forensics Models. *Electronics 10(13)*, 1519.

Bassi, E. (2019). European Drones Regulation: Today's Legal Challenges. *2019 International Conference on Unmanned Aircraft Systems (ICUAS).*

Boucher P. (2014). Civil Drones in Society: Societal and Ethics Aspects of Remotely Piloted Aircraft Systems. EUR 26824. *Luxembourg (Luxembourg): Publications Office of the European Union*. JRC91671.

Carlsen, Christopher, Tarr, Julie-Anne (2021). Drone Law and Policy. Chapter Product liability. *1st Edition, Routledge.*

Chang, V., Chundury, P., Chetty, M. (2017, May). "Spiders in the Sky": User Perceptions of Drones, Privacy, and Security. *CHI '17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6765-6776). Denver Colorado USA, Association for Computing Machinery.

Communication from the Commission to the European Parliament and Council (2014). A new era for aviation: Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner. *Brussels, 8.4.2014*.

Coopmans C. (2014). Architecture requirements for ethical, accurate, and resilient unmanned aerial personal remote sensing. *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, 1–8.

Dulo, D. A. (2015). Unmanned Insecurity: The Safety and Privacy Issues of Unmanned Aircraft Information Assurance. *Unmanned Aircraft Safety & Security Society, Inc. Aviation / Aeronautics / Aerospace International Research Conference*, 10.

European Commission (2017). Study on techniques addressing security and privacy aspects of civil operations of drones in Europe.

Hasib, A. A., Haque, A. A. M. M. (2008). A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography. *2008 Third International Conference on Convergence and Hybrid Information Technology* (pp. 505-510). Busan, Korea (South), IEEE.

Iqbal, S. (2021). *A Study on UAV Operating System Security and Future Research Challenges. IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 0759-0765.

Lagkas, T., Argyriou, V., Bibi, S., Sarigiannidis, P. (2018). *UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things". Sensors 18(11)*, 4015.

Lord, N. (2020). Uncovering Password Habits: Are Users' Password Security Habits Improving? (Infographic), *Digital Guardian*.

National Cyber Security Centre. (2021). Paws-word change recommended on National Pet Day.

Novaro Mascarello L. and Quagliotti F. (2017). The civil use of small unmanned aerial systems (sUASs): operational and safety challenges. *Aircraft Engineering and Aerospace Technology, Vol. 89, no. 5,* 703-708.

www.rsepconferences.com CONFERENCE PROCEEDINGS/FULL PAPERS ISBN: 978-605-70583-5-5/December 2021

Scheau, M.C. , Gabudeanu, L. , Brici, I. & Vilcea, A.L. pp.106-118

Raja, G., Anbalagan, S., Kottursamy, K., Aparna, G.S., Kumaresan, J., Ihsan, M. (2020). *Authorized arming and safeguarded landing mechanism for drone. Conference or Workshop Item.*

SESAR Joint Undertaking (2017). European Drones Outlook Study. Unlocking the value for Europe.

Yaacoub, J. P., Noura, H., Salman, O., Chehab, A. (2020). *Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things*, *11*, 100218.

Yağdereli, E., Gemci, C., Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *Journal of Defense Modeling and Simulation Applications, Methodology, Technology*, 1-13.

Yahuza, M., Idris, M. Y. I., Ahmedy, I. B., Wahab, A. W. A., Nandy, T., Noor, N. M., Bala, A. (2021). Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. *IEEE Access*, *9*, 57243 – 57270.

Yahya, M. Y., Shun, W. P., Yassin, A. M., Omar, R. (2021). The Challenges of Drone Application in the Construction Industry. *Journal of Technology Management and Business, 8 (1)*, 20-27.

Yıldırım, M., Mackie, I. (2019). Encouraging users to improve password security and memorability. *Int. J. Inf. Secur. 18*, 741–759.

Zeng, Y., Zhang, R., Lim, T. J. (2016). Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Communications Magazine*, Vol. 54, no. 5, 36-42.

Zhi, Y., Fu, Z., Sun, X., Yu, J. (2019). Security and Privacy Issues of UAV: A Survey. *Mobile Networks and Applications, 25*, 95-101.