applied sciences

MDPI

Review

Legal, Economic and Cyber Security Framework Considerations for Drone Usage

Mircea Constantin Șcheau [1,2], Monica Violeta Achim [3,*], Larisa Găbudeanu [4], Iulia Brici [5] and Alexandru-Lucian Vîlcea [6]

[1] European Research Institute, Babeș-Bolyai University, 400084 Cluj-Napoca, Romania; mircea.scheau@ubbcluj.ro or mircea.scheau@edu.ucv.ro

[2] Faculty of Automatics, Computer Science & Electronics, University of Craiova, 200585 Craiova, Romania

[3] Department of Finance, Faculty of Economics and Business Administration, Babeș-Bolyai University, 400084 Cluj-Napoca, Romania

[4] Faculty of Law, Babeș-Bolyai University, 400084 Cluj-Napoca, Romania; larisa.gabudeanu@ubbcluj.ro

[5] Faculty of Economics and Business Administration, Babeș-Bolyai University, 400084 Cluj-Napoca, Romania; iulia.brici@ubbcluj.ro

[6] Faculty of Cybernetics, Statistics and Economic Informatics, Bucharest University of Economic Studies, 010374 Bucharest, Romania; lucian.vilcea@ie.ase.ro

* Correspondence: monica.achim@ubbcluj.ro

Abstract: Drones have been used in recent years more and more in various economic sectors (e.g., military, agriculture, retail, transport), but also for personal use and entertainment. The current legislative framework and cyber security standards do not fully address the identification of liable stakeholders in the drone ecosystem for cyber-incidents and the requirement to implement preventive cyber-security measures. The aim of this paper is to investigate how the usage of drones fits in the context of the digital economy. For this purpose, we use a complex questionnaire which was sent to a total of 233 respondents from May to July 2021. The responses are analyzed from a qualitative and quantitative perspective. Our results highlight the areas of improvement in the existing legislation and find the following: (1) respondents are willing to pay additional direct and indirect costs related to cyber security to benefit from more secure drones, (2) the entire ecosystem involved in drone production, distribution, and usage is responsible for ensuring the prevention of security breaches, and (3) respondents perceive a shared liability of stakeholders for certain types of cyber-attacks depending on the role of the stakeholders in the drone ecosystem and the type of vulnerability exploited by the cyber-attack. The details on the specific cyber-attack use cases detail each of the above for each type of cyber-attack. Finally, we make proposals to accommodate the new types of use cases brought by the use of drones in various economic contexts. The results of this research paper assist policy makers in terms of improvement to existing legislation in terms of the drone ecosystem. In addition, they increase visibility for stakeholders in the drone ecosystem in terms of aspects to focus on in order to increase the trust of clients in drone usage.

Keywords: impact; responsibility; security by design; continuous security

Citation: Șcheau, M.C.; Achim, M.V.; Găbudeanu, L.; Brici, I.; Vîlcea, A.-L. Legal, Economic and Cyber Security Framework Considerations for Drone Usage. *Appl. Sci.* **2022**, *12*, 4663. https://doi.org/10.3390/app12094663

Academic Editor: Mauro Lo Brutto

Received: 4 April 2022
Accepted: 3 May 2022
Published: 6 May 2022

1. Introduction

Unmanned aerial vehicles or, in simpler terms, drones are the most important innovation in the military field in the last decade, but also have important applications in other fields. Although, until recently, drones were used only in the theatres of war, their use in the civilian field has quickly expanded, with the drone industry experiencing rapid growth worldwide, given the extremely useful and immediate applications of these technologies in other domains.

The tendency in the past decade has been to use digital solutions in military operations and in various economic sectors, as well as by consumers, mainly in order to reduce costs and to increase the convenience of services rendered. This tendency has been enhanced by artificial intelligence, the digitalization of the public sector, Internet of Things devices and, more recently, also drones. In this context, it is mandatory to think about and develop a legislative but also an institutional framework in Romania regarding the production, marketing, registration and use of drones in the national airspace, in order to align with European and international trends, taking into account the possible future evolution of these technologies and integrated safeguards related to liability in case of economic damages and prevention of cyber-attacks.

From a legislative perspective, until this moment, the national and European legislation has focused on the usability of the drones from multiple perspectives: who can drive them, what types of drones (by reference to their weight) can be used, the altitude to which they can fly, the geographic locations in which they can fly and the possibility to take photographs or video while flying [1]. The need for such rules emerged from the fast growing selling of drones in the European Union and the interest of companies and consumers alike in using them in various activities (either economical or personal in nature). However, these represent the first step in providing a proper regulatory framework for drone usage in various economic sectors and by consumers.

The next steps refer to clarification throughout the ecosystem, from the creation of the software and hardware to distribution and use, by reference to potential threats that can lead to economic damages caused to or by the drone. As in the case of cars or other types of vehicles, the economic damages that a drone can cause are generally greater than those which the average IoT can cause. For this reason, the legal requirements aimed at preventing economic damages (especially caused by cyber-attacks) and those aimed at clarifying liability in case of incurred economic damages are essential [2]. Both types of legal requirements have as their goal the clarification of a stakeholder's role in the drone ecosystem and, thus, encouraging the safe usage of drones and, consequently, the increased wish of customers/companies to use drones in their day-to-day activities.

A lack of clear legal provisions in terms of the prevention of cyber-attacks and liability for certain economic damages caused by a drone (e.g., caused by a cyber-attack) can impact the manner in which drone usability in various sectors of the economy is viewed by consumers and entities operating in those sectors [3]. The main issues refer to the lack of specific legislation and reliance on general tort law [4]. Tort law has in mind certain criteria for identifying the liable entity which may not reflect the specificity of the drone ecosystem [5]. In addition, the product liability legislation may be considered for certain aspects [6]. This article includes references to the pain points for the above in terms of legislative gaps and potential approaches that can be taken for such cases.

This lack of legal requirements is also reflected in the literature, which addresses in a limited manner the aspects of liability and preventive measures in the case of drones. The relevant literature focuses more on the authorization part, on specific technical cyber-attack detection and on cyber-attack prevention.

Furthermore, from an economical perspective, the relevant literature focuses more on the economic benefits of using drones and their functionality in various domains, rather than the cost–benefit analysis of having cyber-attack prevention mechanisms (organizational or technical) in place.

In order to develop our research paper, we analyzed the existing legislation and relevant literature based on the abovementioned three angles (legal, technical and economical). For the identified gaps, we proposed certain ways forward and validated these through a quantitative analysis (a questionnaire whereby we identified the view of the respondents based on the three main aspects: liability in case of cyber-attacks, choice of type of cyber-attack prevention mechanism and cost–benefit analysis of respondents for implementing such prevention mechanisms). The results of this questionnaire were analyzed from a quantitative perspective, while taking into account the various forms of cyber-attacks and prevention mechanisms, as detailed in the below sections.

Three main conclusions are the result of our research, as detailed below.

In terms of liability for cyber-attacks, we found that this is considered by respondents as being shared between stakeholders in the drone ecosystem, starting with the drone software producer, the distributor, the auditors/certification bodies and the drone user. This depends on the type of cyber-attack and on the role of the stakeholder. The questionnaire results identify particularities of liability for each type of cyber-attack analyzed.

Prevention mechanisms also depend on the role of the stakeholder, especially for continuous monitoring and improvement of security posture. Respondents are of the view that the entire ecosystem related to drone production, distribution and usage is responsible for a part of the security measure design and implementation.

Given the responses in terms of enhancing cyber-security technical and organizational measures, it can be concluded that respondents are willing to pay additional direct and indirect costs in order to benefit from more secure drones. The direct costs refer to various periodical maintenance or costs for security services/certifications. The indirect costs reflected in the price of the drone refer to steps taken by the stakeholders on the supply chain before the drone is used by the user.

This article introduces an innovative view to the analysis of the aspects concerning civil liability and approaches to prevent economic damages (economical and other types) and clarify the person/entity responsible for specific situations that can occur, especially in the case of cyber-attacks, by identifying a correlation between the type of cyber-attack, legal implications and economic implications. The legal information technology and economical research is also supported through a questionnaire on the analyzed topics. The questionnaire has respondents from multiple areas of activity, with more than a quarter of the respondents working in the field of information technology, followed by those who work in the legislative field.

The use cases presented in the questionnaire have in mind both the scenario of owning a drone and that relating to the renting of a drone. Furthermore, this article refers to the use of drones for personal use (by consumers) or for economic use (by employees of private entities for their business purposes). The situation of liability of an employer for its employee is not detailed in this article, as the general civil liability rules are clear in this respect.

The innovative aspect of this article stems from this correlation of threat categories and legal approach concerning liability in case of cyber-attacks (materialization of such threats) and the prevention of these threats, together with the views of drone users in terms of incorporating these aspects into their cost–benefit analysis when purchasing/renting a drone.

The novel approach presented by this article is to outline the cases in which the legislation has to adapt to the recent social reality involving drone usage.

The rest of the paper is organized as follows. Sections 2 and 3 present the literature review in the field of drones from a legal, cyber security and economical perspective and also state the hypotheses and objectives. Section 4 describes the data and methodology. Sections 5 and 6 are dedicated to presenting our results and discussions around them. Section 7 presents the conclusions of our research, the limitations of our study and future research directions.

2. Literature Review Analysis

The literature in the field of drone use has employed several perspectives. These three perspectives—legal, cyber security and economical—are also reflected in this research paper and in the questionnaire supporting this research paper.

The usefulness of drones in various fields is outlined in the reviewed literature and is also reflected by the responses to our questionnaire.

2.1. Legal Perspective

The first of these perspectives is represented by regulations. Previous research papers have generally concentrated on the authorization process for flying drones. Thus, there is limited literature in terms of the liability in case of cyber-attacks and, moreover, for the correlation between cyber-attacks and prevention measures to be taken and regulated in legislation. From this point of view, several authors have tried to summarize issues related to the legal use of drones. In 2015, the European Aviation Safety Agency developed material regarding the concept of drone operations [7]. This paper is a risk-based approach to the regulation of unmanned aircraft. In this material, we can find the idea that drones should be part of the aviation system and be considered an opportunity for innovation in the industry because it attracts many benefits, including economic growth or raising the number of jobs. Regulation of the use of drones is needed to set a level of safety for the environment. Therefore, regulation must follow a risk-based model, and thus the established rules will follow industry standards. However, no emphasis is placed on preventive measures by reference to cyber-attacks.

In 2016, a comparative study on the regulation of drone use was conducted in an article presented by The Law Library of Congress, Global Legal Research Center [8]. It includes policies in areas such as Australia, Canada, China, Japan, South Africa, and New Zealand, but also European countries such as France, Germany and Poland. This is an extremely useful study, as it captures the efforts of many countries and areas of the world that are concerned with meeting the standards for the legal use of drones. They are under the analysis of the International Civil Aviation Organization, which issued material in 2011 called Unmanned Aircraft Systems. This was the starting point for adapting the legal framework for the use of drones. This mainly focused on authorization mechanisms.

In 2018, the Food and Agriculture Organization of the United Nations developed a study on the regulation of drone use in agriculture [9]. We can already see the first proof of their usefulness in several activities. This material summarized the main advantages of introducing drones to support agricultural activity. These include operability, data confidentiality and much easier connectivity. This study also included a small summary table of the regulations of several countries on the usefulness of using drones, but only from an authorization perspective.

In 2019, the European Investment Bank developed advisory material on investments in drone use at the European level [10]. In 2015, the European Commission developed an aviation strategy in Europe, a guide for future regulations. The European Investment Bank noticed the upward trend in the use of drones and predicted a sharp increase in the number of these devices until 2022. Following a conference held in Amsterdam in 2018, the European Innovation Partnership on Smart Cities and Communities was issued. Based on the two mentioned documents, a platform was created in order to support the use of unmanned aircraft. It facilitates access to European Union support, thanks to the services that drone use will bring. Here, we can exemplify financial consulting services or financial products. This emphasizes the desire of personal and corporate users to commence using drones in various activities.

2.2. Cyber Security Perspective

Secondly, we approached our chosen issue from the perspective of cyber security. Currently, the regulation of the use of drones is still an area of interest, which is why the literature is more present than ever, in an attempt to reach a balanced form of legal provisions for governing the use of these devices.

In this regard, in 2021 [11], Klauser empirically explored expectations regarding the purchase of a police drone in Switzerland. This study, from the perspective of security, referred to the interactions between power and space in a three-dimensional and cross-ontological manner. However, the study mainly focused on aspects concerning the authorization of drone usage and not cyber-attack prevention mechanisms.

Another concern in this area is the cyber security perspective, reflected, for instance, in a study by Yaacoub et al. (2020), which emphasized the need for correlation between governance and technical requirements [12]. Their study analyzed security elements, such as attack possibilities and limitations of drone use, which came with the development or their use. This study examined preventive measures for drone cyber-attacks. However, it did not identify clear legal aspects to be implemented. Similarly, Huawei, in their 2017 study, reflected on the cyber security aspects of connected drones [13], as the continuous connectivity adds to the attack surface and to the complexity of cyber-attacks and cyber preventive measures.

2.3. Economic Perspective

The third crucial perspective of drone use is the economic one.

We outline below a few representative studies from this perspective. These generally analyze only the economic advantages, without analysis of the impact of cyber security and the clear identification of liability regarding the use of drones.

Additionally, in 2017, material on the new economic era was presented at the United Nations Conference on Trade and Development (UNCTAD) [14]. It shows all the ways in which the economy has changed, becoming digital, but attracting a multitude of benefits with this transition. It also presents business models, along with the strengths and challenges of their implementation.

This point is reflected by other studies published in recent years, such as those mentioned below. In 2018, Zaychenko et al. [15] discussed the development of the digital economy, with an emphasis on the use of drones in the field of construction. Similarly, Deloitte, in their study [16], addressed similar aspects and went further in terms of the role of drones in the infrastructure sector. In 2020, Amukele addressed similar issues concerning the use of drones in the medical field [17]. These studies emphasized only the usefulness of drones from the viewpoint of the economic sector’s need for efficiency in operations. However, they do not address other angles that should be held in mind when deciding on the use of drones in a particular sector, including cyber-attack prevention, the role of each stakeholder in the drone ecosystem concerning the proper functionality and cyber security of the drone.

Furthermore, each of the below studies presents certain specific aspects to take into account when designing the information security preventive measures (based on the used technology) and, given each particular IT solution, liability in the case of cyber-incidents can be determined differently.

In 2019, Li et al. [18] described the idea of developing drones that transmit a network for radio coverage in crowded urban areas, touching upon the quality of service of drone usage and, briefly, ensuring the availability of drones. This entails enhanced and complex algorithms, including neural networks detailed by Amer et al. in 2019 [19], while taking into account specific Internet of Things aspects, as detailed by Alsamhi et al. in 2019 [20]. Whereas these availability aspects are important, confidentiality and integrity principles should also be analyzed. A step in this direction has been made in the literature concerning evolution of IT solutions, including in 2020, when Șcheau et al. described and developed an analytical framework for secure IT evolution [21]. Prevention and control methods are analyzed, while highlighting the role of IT infrastructures in the context of technological development. Nevertheless, for the drone ecosystem, the specifics of its creation and maintenance have to be taken into account when designing cyber-attack liability and prevention mechanisms.

Thus, the use of drones can vary significantly, depending on location in the world and on the economic field. The above studies concentrate on the usefulness and efficiency of drones for activities that are currently being performed by humans or other automation mechanisms. Nevertheless, they do not investigate the reasoning for the increased usage of drones in certain geographic areas or economical areas, especially in terms of a cost–benefit analysis taking into account the cost of drone purchase and maintenance, cyber security during the lifetime of the drone and the clear identification of drone liability in case of incidents.

As a conclusion to the literature review performed from multiple angles (legal, technological and economy), the usefulness of drones is an indisputable phenomenon, based on the number of studies that attest to the great results they have in their actions. The legal framework is an aspect that will be constantly evolving, because the conditions of use are changing at approximately the same rate as the device upgrades. In this respect, the legal research has generally focused on the authorization process of drone and in certain specific liability issues for damages caused by drones in specific situations.

3. Hypothesis and Objectives

The research presented above encompasses the risks and preventive measures concerning drone usage from only one vantage point: security, legal, or economy, without analyzing the interplay between these different angles. The use of drones creates certain cyber-attack risks that can be addressed from a technical, economical or legal standpoint. To this end, the existing research does not analyze the impact of preventive technical measures on the legal and economic aspects or the legal provisions on the economic and technical aspects.

In this paper, we build on the existing literature and explore further and in depth this interplay between the tree angles in order to provide useful solutions to creating drones (and a drone lifecycle) that lead to reduced cyber security risks and increased trust of users/business entities in the use of drones in a wide spectrum of sectors and activities.

To this end, the objective of this article is, after correlation between types of cyber-attacks, legal and economic implications thereof, to include the description of gaps in legislation that should be addressed (for preventive measures and liability in case of cyber-attacks). This proposal also reflects the view of respondents with regard to a questionnaire on these aspects relating to liability for economic damages and preventive measures to be taken. This entails the following research objectives:

Objective 1 (O1). *Identify the view of the respondents in terms of liability for certain types of cyber-attacks.*

Objective 2 (O2). *Identify the view of the respondents on preventive measures for the actions covered under Objectives 1 and 2.*

Objective 3 (O3). *Identify the costs drone users consider useful to incur (either directly or indirectly) in order to ensure safe usage of drone in terms of preventing cyber-attacks and mitigating cyber-attack damages.*

For the above objectives, the below hypotheses are explored in this research paper:

Hypothesis 1 (H1). *(Regarding O1)—For preventing DDoS attacks, the drone cyber security solution is considered liable.*

Hypothesis 2 (H2). *(Regarding O2)—A failsafe mechanism to land the drone safely is considered the best option for preventive measures in case of a DDoS attack and other exploitation of vulnerabilities.*

Hypothesis 3 (H3). *(Regarding O2)—A certification mechanism should be implemented for any changes made by the user to the drone software.*

Hypothesis 4 (H4). *(Regarding O1)—The drone user is liable for any changes it makes to the drone software.*

Hypothesis 5 (H5). *(Regarding O2)—The drone should automatically install needed updates when on the ground and should not fly without these.*

Hypothesis 6 (H6). *(Regarding O1)—The drone software producer is liable for not installing updates timely and properly.*

Hypothesis 7 (H7). *(Regarding O1)—The drone software producer is liable for vulnerabilities in the drone software.*

Hypothesis 8 (H8). *(Regarding O3)—Respondents are of the view that certain technical and organizational measures have to be implemented by the stakeholders involved in the drone production/distribution cycle even if these may be reflected as an indirect cost in the drone purchasing and maintenance cost.*

Hypothesis 9 (H9). *(Regarding O3)—Respondents are of the view that certain organizational measures are to be taken by the drone users for the cyber-safety of the drone, even if this adds to the usage complexity and may impact timing for drone usage.*

4. Methodology and Data

For this paper, we formulated and applied a questionnaire, using the online platform QuestionPro, a free online survey software belonging to Survey Analytics LLC (Seattle, WA, USA), in order to identify the challenges related to drone production and exploitation. The questionnaire was distributed via the Internet, using e-mail addresses and the most common social media platforms, such as Facebook, Twitter and LinkedIn. The survey was distributed both to regular people but also to professionals in the field. The survey was conducted from May to July 2021. We did not consider useful for interpretation demographic information such as age group, education level or gender, but instead we did request information about the field of activity. The questionnaire contained 17 questions; 15 of them referred to the topic under 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.

After filtering the answers, checking for the invalid ones or for missing questions, we identified a total of 233 questionnaires which were fully completed, 37 for the English version and 196 for the Romanian version. For the English version, the distribution of answers is explained in Figure 1. 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 from Spain, Greece, Romania, Great Britain and other countries where there are Romanian speakers or possibly Romanian citizens working in those countries.

The below responses analyzed include the context of the respondents with regard to the questionnaire, as well as the economic aspects concerning drones, as these are shown in the responses.

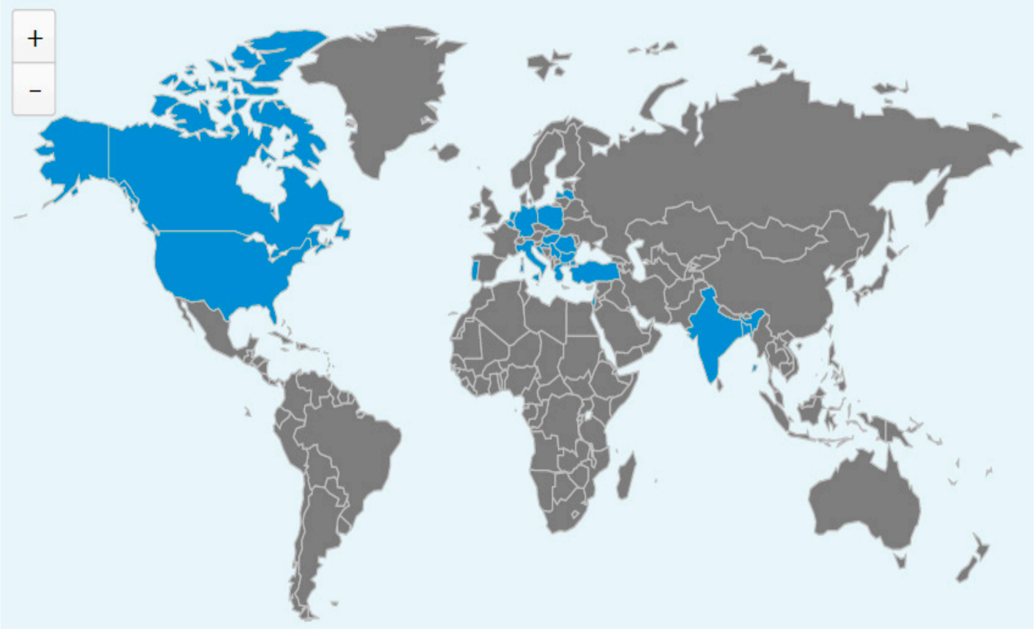

Figure 1. Response distribution (blue color represents respondents' countries of origin). Source: QuestionPro Analytics.

The responses were analyzed for the following use cases in the context of cyber-attacks that generate cyber-risks: use of vulnerabilities, the process for patching vulnerabilities, drone user-created software and distributed denial of service.

Each use case was analyzed from two perspectives: liability for materialized risks and best placed stakeholder to implement security measures.

The qualitative and quantitative analysis was followed by policy enhancement recommendations for each use case mentioned above.

The questionnaire included questions addressing three angles concerning the use of drones.

The first set of questions referred to the liability of stakeholders in the use cases mentioned concerning cyber-attacks. These questions were aimed at identifying the view of respondents in terms of the responsibility of a stakeholder or shared responsibility between multiple stakeholders. From an economical perspective, this showed the expectation of paying damages in case of cyber-attacks.

The second set of questions referred to preventive measures to be taken by certain stakeholders in the drone ecosystem. These were aimed at identifying policy proposals that match the expectations of drone users and that also reflect the costs expected by respondents for ensuring the increased cyber security of drones.

The third set of questions included specific details on utility of drones and the specific sectors in which drones are most useful. These questions are aimed at identifying the specifics to be had in mind for certain sectors in which drones are used. The presentation of the questionnaire is found in Appendix A.

5. Results

This study addressed the drone utility and improvements in existing processes to set the scene for the specific liability and cyber security prevention mechanisms. Furthermore, the study analyzed the sectors in which drones are considered to be useful in order to emphasize the need for specifics in such a sector in terms of cyber-threats and legal requirements for operating drones.

The relevant question of the questionnaire in this respect was "How useful drones are in the following sectors: (1 to 5 scale, 1 representing total disagreement and 5 total agreement)? Answer options: Agriculture, Industrial, Military, Public Order, Topography, Rescue missions, Retail, Transport or None".

Table 1 shows the number of responses by sectors of activity, on a scale from 1 to 5, as well as the average score of these responses (the number of answers weighted with the chosen level on the scale). Judging things from the point of view of the average score, we can see that the military field stands out first. Most of the level 5 responses were recorded in this sector, and so it is considered the domain in which drones are the most useful. At the opposite pole, we can find the retail sector, where only 75 respondents consider drones a facility brought to the field. The usefulness of drones is also highlighted by the small number of level 5 responses to the "none" category. We can conclude that our respondents generally consider drones useful.

Table 1. Usefulness of drones by sectors of activity.

Industry/Scale	1	2	3	4	5	Average Score
Agriculture	7	5	32	51	222	4.50
Industrial	16	21	65	68	146	3.96
Military	16	2	8	18	273	4.67
Public Order	25	23	45	49	175	4.03
Topography	16	15	24	39	222	4.38
Rescue missions	6	5	17	33	255	4.66
Retail	65	52	71	53	75	3.07
Transport	41	33	74	55	113	3.53
None	282	7	9	2	12	1.25

Source: Author's processing.

Another relevant question was "Do you think using drones will lead to an improvement in the field of activity they are used for?".

The answer to this question was overwhelming, as can be seen in Figure 2 below. A very large proportion of respondents, namely 67%, believe that the use of drones is a beneficial aspect for the field of activity in which they operate. Having the role of facilitating, supervising or intermediating some processes, the drones will only bring benefits.

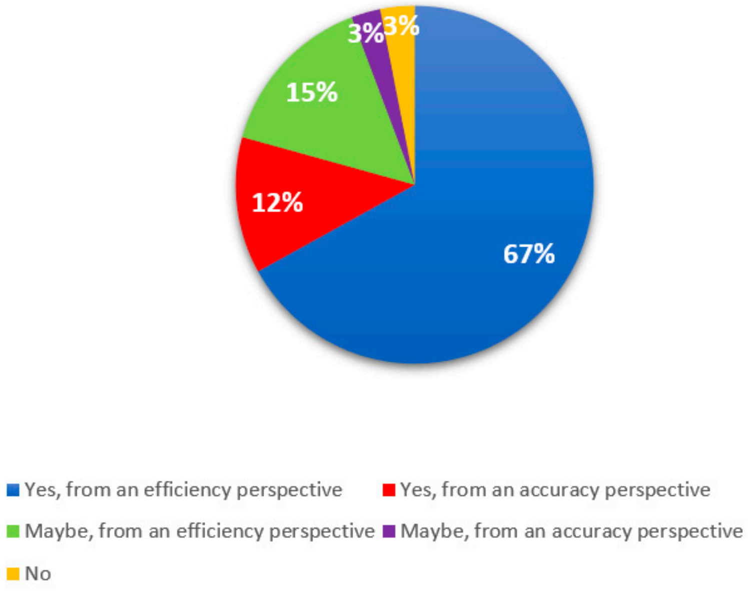

Figure 2. Drones' utility in improving the field of activity. Source: Author's processing.

In addition, the following question is relevant on this topic as well: "Do you think using drones will lead to economic growth?". According to Figure 3, the majority of respondents answered this question affirmatively (61%). Respondents' answers can certainly be supported by concrete arguments. As can be seen in the literature review section, there are many studies that attest to the usefulness of using drones in the economic field. The reason for their creation and use was precisely to facilitate certain processes, as we already specified. The result can only be positive if the technical and legal structure is appropriate. Thus, drones help to strengthen the economy, bringing an additional advantage.

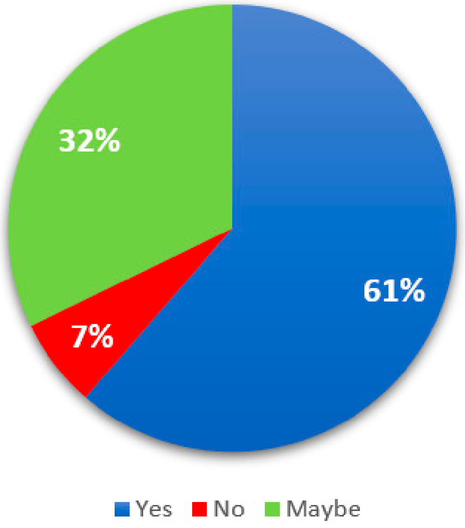

Figure 3. Drones' utility for economic growth. Source: Author's processing.

5.1. Existing Vulnerabilities

Vulnerabilities can be identified from the outset of software creation or can appear throughout the lifetime of the software, either for the source code created by the drone producer or by a third party in the supply chain. Even if legislation is not clear on the liability for vulnerabilities and obligation for establishing security measures, given this timeline, there are certain stakeholders that can practically be involved in the prevention of vulnerability exploitation and the fixing of vulnerabilities.

The questionnaire addressed this topic in two questions: the first concerning the liability angle and the second the preventive security angle.

The following question addressed this topic "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.

As expected, the answers in Figure 4 show that, if there were certain manufacturing problems, the software producers would be responsible for the caused inconvenience. It is interesting to see that the drone distributer/seller is also considered to have a role in this respect. This is especially useful in cases where the drone is produced in another country than it is sold. This clarifies the issues around the applicability of different legislation and different legal requirements around the world. Furthermore, 17% of respondents consider that security should be the responsibility of a dedicated security solution, which does not necessarily belong to the drone producer. This view is reflected in the ranking of the preventive measures detailed below.

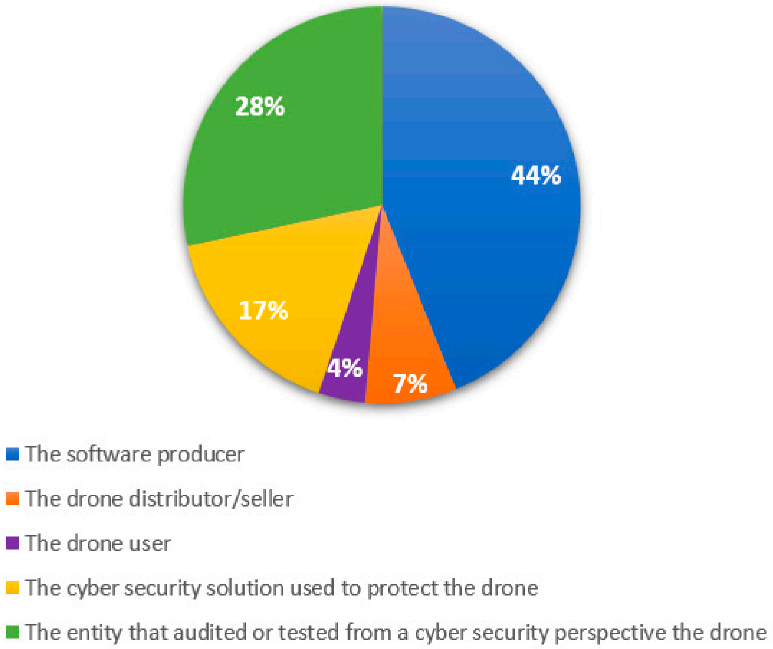

Figure 4. Liability in case of outset vulnerabilities. Source: Author's processing.

H7 is validated, as the majority of respondents view the drone software producer as liable for the vulnerabilities in the drone software, with 44% of the responses. However, it is worth noting that 45% of the respondents view as liable two stakeholders that are involved in the auditing/verification of the drone software, respectively—17% consider the cyber security solution installed on the drone as liable and 28% consider the auditor/tester of the drone cyber security as liable. This suggests that the respondents view the cyber security checkpoints as liable for not properly identifying such vulnerabilities in a similar percentage as the drone software producer.

In addition, the following question addressing this topic 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). Answer options: Cyber security auditing before the drone is placed on the market, Periodic cyber security auditing to be performed by the user in order to be allowed to fly the drone, Failsafe mechanisms in case the drone is taken over by hackers in order to safely land the drone and alert the user, Cyber security software to be included in the drone to prevent intrusions and respond to them".

If there are vulnerabilities in the drone software, the largest part of the respondents consider that the best preventive measure is for the information security software to be included from the factory onwards in the drone. Thus, it can act quickly and respond to existing reported problems (Table 2).

Table 2. 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.

The respondents consider the entrance into the market as the first point for vulnerability management. Furthermore, even higher in ranking is the need for a dedicated cyber security software to be installed on the drone in order to prevent attacks and to be able to respond to them. This is seen as more useful than periodic auditing of the drone, where real-time responses in case of vulnerabilities are essential.

H2 was invalidated for the preventive measures on vulnerabilities. The hypothesis considered that the failsafe mechanisms for landing the drone in the case of exploited vulnerabilities will be chosen as a preventive measure. However, the respondents view cyber security solutions installed on the drone as the highest form of preventive measures with a score of 4.47, with the second highest being the auditing of the drone before it is placed on the market, with a score of 4.38. The failsafe option was third, with 4.25. This entails that the respondents view the immediate response to a cyber-attack as important, rather than just ensuring the safe landing of the drone.

H8 is also validated, as the respondents consider useful payment of additional services for auditing and cyber-security solutions in order to ensure cyber-safety of the drone in terms of vulnerabilities.

5.2. Proper Patching of Software

Once vulnerabilities are identified and their criticality categorized, there are additional steps to be taken in terms of mitigating risks in terms of vulnerabilities, such as the proper installation of such patches.

The questionnaire addresses this topic from two angles: the liability angle and the effective preventive measures angle.

The following question addressed this topic "Who is liable in case a software update is available for the drone software and the drone user did not install this update?" (Multiple choice question). The possible answer options can be found in the legend of the figure below.

The results of the survey, from Figure 5, show us that 45% of the respondents consider that the drone user is the one who has the obligation to install an available update. Otherwise, you will be liable for damages caused by not installing that improvement. Meanwhile, 36% of respondents believe that the software manufacturers are also responsible and should impose the need to download the update.

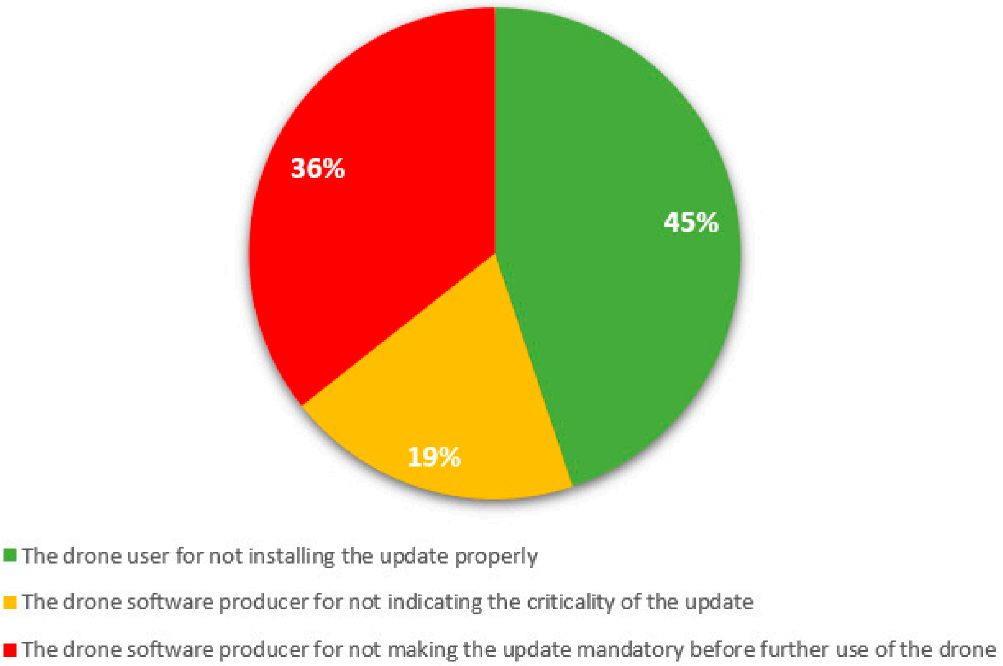

Figure 5. Liability in the case of not installing an available software update. Source: Author's processing.

Regarding update patches, the respondents are divided between the role of the software producer to make updating mandatory before flying (36%) and the users (45%). This type of preventive measure is outlined in Section 5, with emphasis on the mandatory updating of critical updates.

H6 is validated, as 55% of respondents consider the drone software liable for software updates (with 36% for not indicating the criticality of the update and 19% for not making the update mandatory before drone usage). By comparison, 45% of respondents view drone users as liable for not performing the update.

The following question addressed this topic: "Which of the following are preventive measures for ensuring software updates are properly and timely installed on drone software? (1 to 5 scale, 1 representing total disagreement and 5 total agreement). Answer options: The drone should not fly without the latest updates installed (either automatically or manually), The drone should automatically install the updates when it is on the ground within the timeline provided by the drone software producer, The drone should fly irrespective if the new updates are installed or not, The drone software producer should highlight to the user the criticality of the update and the user should decide when to install it".

From Table 3, we can see that, depending on the average score, most respondents believe that drones should automatically install updates when they are on the ground within the range mentioned by the software manufacturer. Again, in this situation, the software manufacturers must anticipate possible asynchronization or incorrect installations and initiate an automatic verification of them while the drone is not yet launched.

H5 is invalidated as the respondents view it as important to update drone software only when the drone is on the ground, with a score of 4.20, but the score for not flying without this update is only 4.07. Thus, the lack of flying is not viewed as important by the respondents by reference to the potential risks in flying an un-updated drone software.

Thus, in terms of H9, referring to the costs of users by not flying the drone unless it has the latest updates, the respondents consider this type of time cost as not adding a significant value in terms of a cost–benefit analysis.

Table 3. Preventive measures for proper install of updates.

Response/Scale	1	2	3	4	5	Average Score
The drone should not fly without the latest updates installed (either automatically or manually)	20	14	35	34	141	4.07
The drone should automatically install the updates when it is on the ground within the timeline provided by the drone software producer	13	14	33	36	148	4.20
The drone should fly irrespective if the new updates are installed or not	131	37	22	24	30	2.12
The drone software producer should highlight to the user the criticality of the update and the user should decide when to install it	34	22	42	41	105	3.66

Source: Author's processing.

The responses outline that the role of the user is not viewed as important as that of the producer in this case. Thus, at least for the vulnerability management, the respondents consider the producer more equipped to prevent incidents than the users. This is in line with the automation of preventive measures as much as possible, which is the general approach in the information security industry.

5.3. User Modified or Created Software

Once the drones have been placed on the market, users start to wish to customize them either themselves or by using third party software. This can bring certain risks if proper governance is not created for this modification. The questionnaire addressed the liability aspects in order to see how the role of other stakeholders than the drone users are viewed by respondents, followed by addressing preventive measures for cyber risks in this use case.

The following question addressed this topic: "Who is liable in case the drone software was modified by the user and this modification generated the damages or drone crash or possibility of hacker to take over the drone? (Multiple choice question)". The response options can be seen in the legend of the figure below.

As we can see in Figure 6, respondents mostly consider the user as liable for modifying the drone software followed by in-flight incidents or hacker attacks. In this regard, the competent authorities should provide some appropriate sanctions. Additionally, in order to avoid this kind of situation, it would be necessary to specify a warning notification in the operating instructions of the device.

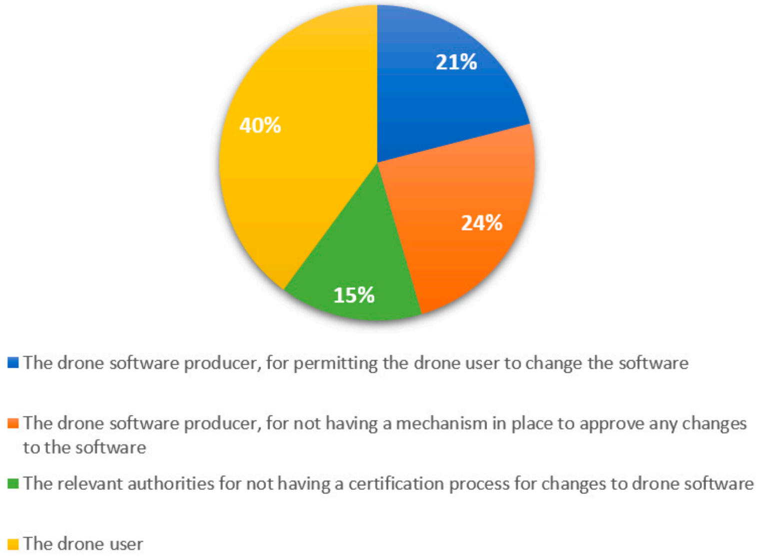

Figure 6. Liability for software changes made by the user. Source: Author's processing.

Thus, the main perception of the respondents (60%) is that other entities (rather than the drone user) are liable for the software changes made to the drone. This outlines the view that preventive measures are essential and that these have to be integrated in a conjunct effort between drone software producers and authorities.

This invalidates H4, which stated that drone users are liable for drone software changes. The majority of respondents (60%) consider the software producer liable for not having in place a mechanism to handle such situations, and only 40% considered the drone user to be liable.

This demonstrates that specific mechanisms should be in place in order to prevent that drone users can make any changes to the drone software. The exact ranking of the preventive measures is outlined in the responses to Question 6 below.

The following question addressed this topic "Which of the following are useful preventive measures to prevent damage/hacker attacks in cases of drone software being modified by the user? (1 to 5 scale, 1 representing total disagreement and 5 total agreement). Answer options: Any change to the drone software should be approved by the drone software producer, A certification mechanism should be in place to perform a cyber security review of any change in the drone software, Users should not be able to change the drone software."

In the case of this question, as can be seen from Table 4 below, the proportions are very close for two of the three answer options. Firstly, respondents believe that a certification mechanism should be implemented to review any changes to drone software in terms of information security. Immediately following this, at 0.01 difference from the average score, was the proposal that any modification of the drone software must be approved by the manufacturer. As a conclusion to this question, we can summarize that the software manufacturer is the only one who can assume such duties.

Table 4. 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.

H3 is validated in the sense that a score of 4.05 was obtained for having a certification mechanism in place. However, a very similar score, 4.04 was also obtained for the preventive measure of approval by the software drone manufacturer. Thus, the respondents view the two options as equally important and complimentary.

Furthermore, H8 and H9 are validated in the sense that additional actions of authorities/certification bodies/drone producers are considered essential to ensure the cyber security of software changed by the drone user, even if this entails additional organizational steps for the drone user and additional costs.

The responses indicate that there should be limited changes permitted to the drone software, with clear analysis thereof prior to implementation and prior to any flying taking place. This is in line with the shortcomings identified in the current legislation and outlined in Section 5. It is interesting to see how closely ranked the regulation of changes and total prohibition of changes rank. This indicates that the respondents consider any changes made by the user very risky and, thus, should be treated in a clear and structured manner.

5.4. Distributed Denial of Service

A distributed denial of service can involve drones both in terms of targets and parts of the botnet. The questionnaire addressed two angles: prevention steps that may be taken and initial response in case of such a type of cyber-attack.

The following question addressed this topic "What steps should be taken when a drone is subject to a denial-of-service attack (which entails that the drone can no longer receive commands from its user, as it is flooded by commands from a hacker)? (Multiple choice question)". The possible answer options can be found in the legend of the figure below.

According to Figure 7, 40% of the respondents in our sample believe that in the event of a denial-of-service attack on the drone, there should be an automatic mechanism to help the device reach the ground safely. A very similar proportion answered that it would be desirable to have an information security solution to identify the problem in a timely manner. Such cases must be premeditated and must be intervened in before a precedent is set.

For the denial-of-service attack, the views of the respondents are in line with the responses given for the software vulnerabilities. The technical approach of prevention is preferred, with the automatic response (e.g., failsafe mechanisms) and the specific technical solution for information security ranking a close second. This means that the respondents view cyber security as a continuous and real-time requirement that can be addressed only by swift identification and response, with periodical audits being too far apart in terms of timing to properly address all issues. In practice, in order to ensure the proper working of failsafe mechanisms and cyber security solutions, periodical review or audits are also required.

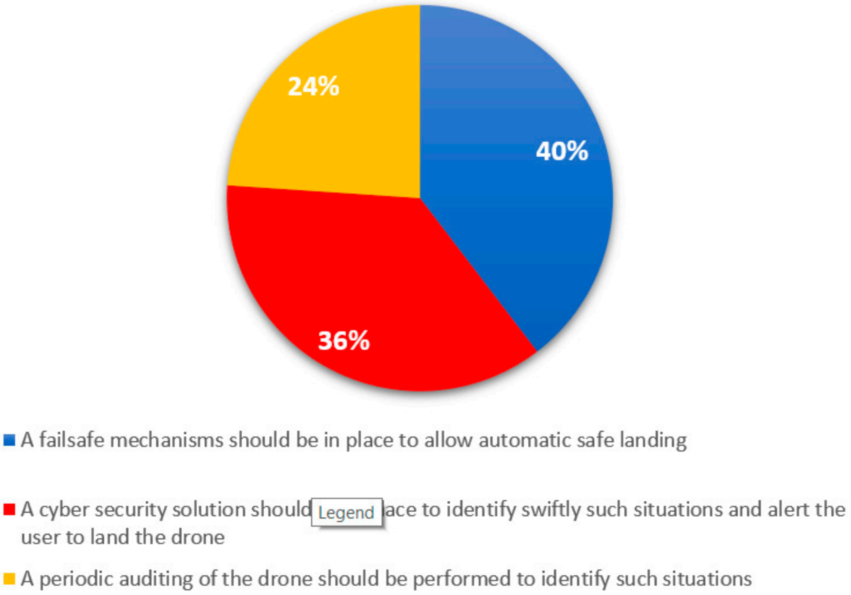

Figure 7. Steps to take in case of a denial-of-service attack. Source: Author's processing.

H2 is validated for DDoS, with 40% of respondents considering the failsafe mechanisms for landing in case of a DDoS attack essential, compared to 36% of respondents considering a cyber security solution essential. It is worth noting that, given the type of attack targeting availability, the cyber security solution applied to drones may not be, from a technical perspective, effective.

H8 is validated in the sense that respondents take into account that such additional requirements are going to impact the manufacturing and maintenance costs and consider the cost–benefit analysis results in favor of having such security measures in place.

The following question addressed this topic: "Who is responsible for preventing a drone from being used as a sender of commands in a denial of service attack towards other IT systems (e.g., as a cyber or physical weapon)?—e.g., the drone being part of a botnet. (Multiple choice question)".

The answers to this question (Figure 8) are divided into almost equal proportions. However, the most consistent part of the answers is the responsibility of the drone software manufacturers. In such situations, much more efficient solutions should be implemented. If the responsibility goes to the software producer, then they should manage these types of situations by developing a system that detects the purpose of using a drone.

In terms of the prevention of denial-of-service attacks, the responses were divided between the multiple stakeholders. It is worth noting that the certification body proposal obtained 28% (almost as much as the cyber security solution, which obtained 29%). This underlines that the public view is that the main stakeholders in the drone ecosystem are jointly responsible for preventing attacks. Thus, aside from the drone software provider and cybersecurity solution, the respondents view the role of an independent certification body as being as useful as that of the previous two stakeholders. It is interesting to see that there are 12% of the respondents who also view responsibility for attack prevention as being with the users themselves. This can be analyzed together with the requirement to maintain a cyber security solution and to perform regular reviews of the drone. This is also in line with the prevention mechanisms proposed in Section 5 that reflect this cooperation between multiple stakeholders in order to ensure swift assistance in case of attacks.

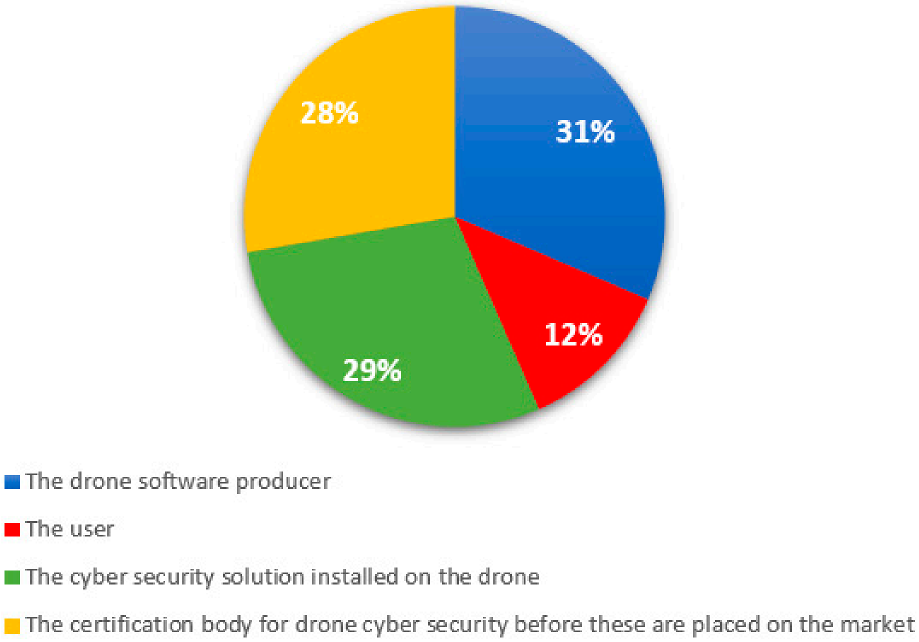

Figure 8. Responsible for preventing DoS attacks. Source: Author's processing.

H1 is invalidated, as the cyber security solution only received 29% of responses, with the drone producer having 31% and the certification body 28%. In the case of DDoS attacks, the essential aspect is for the lack of availability not to create damages in terms of, for example, the drone falling and causing damages. In this case, the responders were not certain whether the stakeholder was best suited to handle preventive measures for such attacks.

Nevertheless, H8 and H9 are validated in the sense that respondents understand that such cyber security measures entail additional costs for the drone user.

Cyber-attacks and cyber-incidents can have multiple causes. The responses show the view of the respondents towards liability and efficient preventive measures for the use cases.

Therefore, for all analyzed types of cyber-attacks, the respondents generally view stakeholders involved in the production, maintenance or certification/auditing as being responsible for cyber-attacks and being best placed to prevent such cyber-attacks from occurring. The user is viewed as a person not specialized in this field who should be protected and guided by the other stakeholders when purchasing and using the drone.

6. Discussions

The respondents to the questionnaire generally consider the first steps in the drone lifecycle (such as production, operation systems, safety systems) to be the responsibility of the drone producer.

The elements related to the use and maintenance of the device in their original form are generally considered the responsibility of the user or of cyber-security solutions installed on the drone.

The drone, as a device, represents a benefit in every field of activity in which it intervenes. The use of drones in the economic field will definitely help the economy grow by making things go faster and easier. Being a part of the digitalization process, it also comes with a package of risks, but this situation provides specialists with reasons to keep on performing research in order to find solutions.

The use cases considered in this section refer to flaws in the vulnerability management process. In terms of vulnerability identification, we analyzed the lack of identification in Section 5.1 (for general confidentiality or integrity vulnerabilities, reflecting H2 and

H7) and Section 5.4 (for the availability vulnerabilities, reflecting H1 and H2) below. Furthermore, for the vulnerability identification and analyzed phase, for human error on the user/client side, Section 5.3 considers software changes or user-created software installed on the drone, reflecting H3 and H4. For the response phase, we analyzed the lack of proper addressing of vulnerabilities (either in lack of proper created patches, lack of timely patches or lack of proper patch applying to the drone software, in Section 5.2 and reflecting H5 and H6).

There are various reasons for which an attack on a drone can be successful. This depends on various actions of the stakeholders involved in the drone ecosystem, from the producer of the hardware to the producer of the software and the user.

According to Choudhary et al., attacks on drones can target different security concepts [22], as follows: (a) privacy, which includes traffic analysis, interception, data capturing or location tracing; (b) integrity, where the most common types of attacks are substitution or alteration of the information, access control point modifications, man-in-the-middle and message forgery; (c) confidentiality, which can be compromised by identity spoofing, replay attacks or eavesdropping; (d) availability, which is prone to physical attacks, denial-of-service and distributed denial-of-service attacks, GPS spoofing or wi-fi jamming; and (e) trust, when the UAV components that rely on third party software or hardware are affected by malware infection, firmware replacement or other types of user's agreement violations. The motivation for the cyber-attack may differ (e.g., hacktivism, state cyber-attacks, commercial cyber-attacks on the drone producer or company using the drone). The purpose of this paper is to identify the civil liability angles and potential preventive steps that can be taken to minimize damages caused by cyber-attacks. This outcome is applicable irrespective of the motivation of the cyber-attack.

Below, we outline the main use cases that can occur, with analysis of the liability that can be established under the current legal provisions and the proposal for clarification in terms of liability and in terms of obligation to ensure preventive measures against cyber attacks. The below are applicable also for the software within the drone, but also for the software on the user side handling the drone.

6.1. Existing Vulnerabilities

One use case relates to the software within the drone to contain vulnerabilities that can be exploited by attackers.

Annex IX of Regulation (EU) 2018/1139 [23] on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency includes a general requirement for the mitigation of risks pertaining to privacy and security, including privacy by design and security by design. Nevertheless, such requirements are rather general and do not address the need for a continuous monitoring of the threat landscape, similar to those in Regulation (EU) 2019/945 [24].

This existing legislation refers to obligations pertaining to the producer of the drone and the entity performing marketing for the drone. Such obligations also include, in article 77 (h) of Regulation (EU) 2018/1139, an obligation for the dissemination of any vulnerabilities or security issues. This can be better reflected in the legislation specific for drones with specific processes for direct communication to users (not just public communications) and can involve a specific authority (such as EASA-European Union Aviation Safety Agency) for setting up the process efficiently.

There are discussions on the applicability of other specific legislation on machinery and radio equipment to drones [25,26]. However, the machinery directive contains only general health and safety requirements and liability, with a general reference to using a risk-based approach (including faulty hardware and software) and requirement for the emergency stopping of the drone in the case of cyber-attacks. Currently, a revision proposal from the EU is awaited in order to address new technologies.

In this case, under existing civil tort law, the liability can be considered to pertain to the drone hardware or software producer if a direct liaison can be made between a specific vulnerability and the cyber-attack, provided the user properly handled the drone throughout its life. The liaison and the latter condition on proper usage is difficult to prove in practice. There are situations in which disclaimers can be made by the producer from the outset, such as a period of usability without maintenance of the drone, a lack of liability in cases where the drone is connected to personal devices of the user used also for other activities, etc. This type of liability is a fault-based liability specific for civil law, with common law jurisdictions having a slightly different perspective, but having as its starting point the same principle.

The tort liability is generally difficult to establish in cases where there is inactivity of an entity (e.g., the producer of a drone), especially if there are no specific legal obligations for such entity with respect to the respective inactivity [27]. This can be the case for many instances in which vulnerabilities appear in time due to evolution in technology or improper development of drones even when current best practices have been implemented. In such cases, as there is no specific legal requirement for identifying and fixing the vulnerability in a timely manner, tort liability may not be applicable to many situations. Details regarding the proposed recommendations in terms of timing and response are included in Section 5.2.

Furthermore, in terms of the burden of proof, under civil law, this belongs to the injured party. In this respect, by having clear strict liability for certain aspects, the burden of proof shifts to the other responsible entities. Nevertheless, strict liability may inhibit the progress and testing of drones. Furthermore, it may limit the entrance into the market of new players. Thus, having preventive steps in place may aid in this respect. This entails adding more clarity to the legal requirements mentioned above about privacy and security technical functionalities in order to include a risk assessment process and a continuous monitoring of risks and communication between stakeholders.

This is closely related to the approach mentioned recently by studies performed by the European Union in relation to the product liability EU directive [28]. Currently, this mentions certain technical specifications that must comply with specific industry standards and, if such standards do not exist, with state of the art in the field. This approach is not in line with technical changes that occur throughout the lifetime of the drone. Even if the software is considered state of the art when it is created, aside from inherent vulnerabilities in the software, changing technology and threat actor methods and techniques can generate new vulnerabilities to previously secure software. For this reason, continuous monitoring and analysis of the drone vulnerabilities is essential. This reflects that an exemption provided by the liability for defective products directive may be applicable (including that under Article 7(b) of the liability for defective products EU directive).

Excessive liability rules without prevention and maintenance mechanisms in place may lead to withdrawal from the market of versions that are found to have critical vulnerabilities, which can lead to loss of profit either for the buyer or for the producers. This would distort the drone market and, thus, preventive steps and close monitoring of cyber-risks can prevent this from occurring [29].

The choice of jurisdiction is also essential for this use case. It depends on the specifics and the national legislation where the damage is caused. This also entails, in certain cases, cross-border liability under the 1952 Rome Convention. In addition, generally, irrespective of the location in which the drones are produced, placing a drone on the EU market makes it subject to the requirements (including health and safety) under EU law. Further, the liability rules become applicable as well. Nevertheless, we are not analyzing this angle in this paper.

Training for flying in case of malfunctioning or cyber-attack can be also a preventive measure to be implemented, together with insurance held by users of the drones (similar to the automotive sector). Currently, there is an obligation under European law to hold insurance for drones weighing more than 20 kg, with certain EU member states opting for additional situations in which insurance should be held.

These two measures add to the trust level in the drone usage for commercial purposes, and their costs should also be integrated in the cost–benefit analysis upon implementation.

The view of the respondents is similar for the vulnerabilities existing in the drone software. Overall, 44% of respondents mentioned the drone producer as being responsible for any consequences of exploited vulnerabilities, whereas 28% of respondents view the entity that audited the drone as being responsible, validating H7. This is correlated with the preventive measure ranked primarily by the respondents as being useful in this case, followed by periodical auditing and including a cyber-security solution in the drone to detect and prevent cyber-attacks. H2 is invalidated for the vulnerability part, as the fail-safe prevention measure is not the highest rated option.

As expected, the software producer is considered mainly responsible by the respondents, with the entity that audited the drone being considered accountable as well. Thus, additional clarification in this respect may also be taken by the legislator. Such clarification has a beneficial effect on drone usage, as clarity in terms of liability brings trust into the ecosystem.

As it was identified in the questionnaire, the respondents consider the most important point in time to address vulnerabilities as being the entrance into the market. Nevertheless, continuous monitoring of vulnerabilities is of highest concern to the respondents. This is closely tied to the liability for vulnerabilities, as it brings into play the stakeholders from the ecosystem that can bridge the cybersecurity gap by identifying and addressing vulnerabilities.

6.2. Proper Patching of Software

Furthermore, related to the first use case, if the vulnerability is identified by the producer and the producer publishes a patch, there are various steps that can be taken and, depending on the actions taken by each stakeholder and the legal obligations, the liability can shift between the various stakeholders involved [30].

Currently, legislation is not specific on handling vulnerabilities identified after the drone has been placed on the market. Aside from the specific drone legislation, general security requirements under Article 32 of the GDPR may be applicable if the drone holds personal data. If drones are used for critical infrastructures or NIS Directive operations, additional requirements become applicable. Introducing a clear process for vulnerability handling is essential to ensure trust on the drone market, to handle data swiftly and efficiently and to handle security measures properly throughout the lifecycle of the drone. EU Directive 2019/771 on the sale of goods includes a general obligation in Article 7 in terms of updates (including security updates), but without details on its implementations, as analyzed in the questionnaire question mentioned below.

There are two main requirements for this aspect. The first is that of the timing for creating patches. Timing is essential and should be as soon as practically possible. The second concerns the deployment of patches. For this case, an impact assessment is to be performed on the most efficient technical solution, depending on the type of patch. One option that can ensure the limitation of risks is that of not allowing the flight of drones without implementation of the most recent patches. Of course, the obligations on the producer side can be correlated with training on the side of the user, as part of the training and certification.

Furthermore, the angles concerning liability mentioned in Section 5.1 are applicable for patching as well. This is relevant especially if there is no express legal requirement to analyze identified vulnerabilities and patch them. Furthermore, if no timeframe for patch creation and patch dispatch is provided under the law, liability may be difficult to establish.

Similar to the measures under Section 5.1, the measures in this section have an impact in terms of costs on the producer side. The security advantages have to be taken into consideration along with the benefits they bring in a cost–benefit analysis of the level of security measures to be implemented [31].

Furthermore, they can have an impact on usability, as the maturity of users concerning cybersecurity measures is relevant in order to understand the need for patching and the manner in which this is performed. Of course, it can be extended to the notification of any identified vulnerabilities. This can be achieved through training and including cyber security components in the certification process. This maturity level increases users' acceptance of drones for day-to-day commercial activities and any increase in costs due to security prevention measures.

Similarly, for updates on drone software, 55% of respondents consider the producer liable in the case of the lack of proper updating of drone software, with H6 being validated. Furthermore, their view is that the drone producer should implement technical measures to make the updating mandatory before flight or to indicate the criticality of updates in order to alert and inform the user properly. H5 is invalidated, as the respondents do not view lack of flying without all updates as a necessary preventive measure.

6.3. User Modified or Created Software

In certain cases, the drone producer may allow users to modify the existing software or add their own software within the drone. In such cases, the liability can shift, as there are multiple entities/persons that can generate vulnerabilities within the drone that can result in a cyber-attack.

The angles mentioned in the previous use cases are valid for this one as well. This use case is closely related to the one for identifying and remediating vulnerabilities. For this use case, modifying existing software or creating new software for a drone may, on the one hand, generate risks associated with the existing software and, on the other hand, can include in itself vulnerabilities that can be exploited by threat actors.

The liability aspects are much clearer under existing legislation, as the liability pertains to the entity creating software. However, in terms of preventive security measures, proper analysis of this new software (changes to software) is essential in order not to extend the vulnerability landscape of the drone. Even if such a measure is not directly related to the actions of the drone producers, from a public safety perspective, it is mandatory to limit the applications used in production to those created by certified developers and analyzed prior to entrance into production.

Proposals in this respect include development by a developer certified for drone software creation. Furthermore, vulnerability analysis and penetration testing of the new application and the drone where the new application is deployed before the new application are used in production and periodically afterwards.

In cases where the user makes changes to the drone software, respondents primarily view the producer/authorities (60%) and the user (40%) as being liable for any cyber-attacks caused by such changes, invalidating H4, which stated that drone users are considered liable. In this case, the respondents considered that the authorities (e.g., through the certification body) and the producer are best placed to prevent vulnerabilities from being included in the drone software, which validates H3. Thus, their view correlates the liability with the entities that can properly implement preventive measures, even if there is no legal requirement in this respect.

6.4. (Distributed) Denial of Service

As in the case of other IoT devices, denial of service attack and distributed denial of service attack can lead to significant economic damages. The first scenario involves a denial of service attack on the drone itself.

The second scenario involves a denial of service attack on other IT systems in which the drone plays the part of attacker, as part of a botnet.

In both cases, the third party attempting to perform the distributed denial of service is relying on vulnerabilities identified within the drone [32].

Thus, the recommendations proposed in Section 5.1 are applicable. In addition, a mechanism for monitoring the drones in order to identify such types of attacks (or others) may be useful. This can be created either at the individual level of the drone or at the level of multiple drones (either by the drone producer, a public authority or authorized security operations centers).

The questionnaire analyzed both roles of drones, as attacked devices and the attacking device.

For the prevention of DoS and DDoS, the situation is similar. Overall, 31% of the persons belonging to the sample consider the drone producer to be responsible for the drone being used as a bot, 28% consider the certification entity to be responsible, and 29% consider the cyber-security solution to be responsible, with H1 being invalidated as it referred to the cyber security solution. Only 12% consider the user responsible. In the case of a (D)DoS attack on the drone, H2 for the DDoS part is validated, as 40% believe that the drone should have a failsafe mechanism, while 36% state that the cyber-security solution should prevent the attack.

H8 and H9, referring to the fact that respondents choose additional features, prevention mechanisms and organizational aspects (e.g., certifications, training) are necessary and are generally validated as detailed below. Thus, from a cost–benefit analysis, the respondents view that the additional features/measures should be implemented by the relevant stakeholders (from producers, certification bodies, cyber security solutions, drone users, etc.) in view of ensuring cyber security and, thus, from a cost–benefit analysis, such additional payments and time spent is a proper tradeoff for the prevention of cyber-attacks and damages.

6.5. Main Considerations on Correlation between Cyber-Attack Prevention Measures and Liability

Even if there are certain general legal rules around the safety of devices/products (including some specific for drones), these are not specific enough given the current threat landscape and the high impact of any incident affecting drones. Furthermore, they do not provide a continuous analysis of cyber risks and risk-addressing mechanisms. [33] This should be applicable for any applications or amendments introduced into the drone software/hardware by users.

Thus, a first step in creating trust in drone usage for users is having a process in place for prevention.

In addition, from a technical perspective, safety measures can be contemplated in order to ensure safe landing of the drone in case of a cyber-attack (e.g., by creating a separate read only area for safety source code), especially in case of a distributed denial of services [34].

Furthermore, in terms of navigation of drones, practical training, especially for actions in the case of cyber-attacks and preventive cyber-security measures, can be contemplated to reduce cyber-risk and costs associated with damages resulting from cyber-attacks.

In addition, specific liability legal provisions should be implemented for specific situations, including the above, in order to clarify the entities that should be responsible for certain parts of the drone functionalities, security and maintenance. This ensures that the relevant entities are aware of the steps they should take and responsibility they have, giving users the confidence that any damages can be easily addressed and resolved.

The above measures increase the complexity of actions to be taken by all stakeholders (from the hardware producers, software producers, distributors, authorities, users) involved in the drone usage process. Furthermore, these include additional costs and time for most of the stakeholders. When establishing the level of details and frequency of these measures, the costs associated with them and the time impact on the drone usage have to be considered. Nevertheless, the benefits of preventing damages and litigation have to be placed into balance. In this respect, a cost–benefit analysis may be the foundation for the impact assessment of the above preventive measures [35].

In cases where the attackers are state players or drones are used for state-targeted cyber-attacks, additional legislation comes into play in terms of liability and can also impact the civil liability aspects. These aspects are not the subject of this article, but it is worth noting that, in certain cases, the attribution of a cyber-attack can have an impact on the establishment of responsible entity for incurred economic damages.

7. Conclusions

For all analyzed types of cyber-attacks, stakeholders involved in the production, maintenance or certification/auditing are viewed as being responsible for the occurrence of a cyber-attack. Furthermore, they are considered best placed to implement security measures that prevent such attacks. This analysis is closely linked to O1 and has been reflected by the analysis of H1, H4, H6 and H7.

There are two angles to consider in this respect. The first is for the legislation to reflect the factual situation described in this paper in terms of involvement of the stakeholders in the drone ecosystem (in terms of liability and obligations to implement preventive measures). The second is to identify the best placed stakeholder for each situation identified in this paper (and any subsequent investigations on the role of each stakeholder).

For both of these two angles, the economic impact of cyber-security and clarification of liability in legislation is related to a cost–benefit analysis for each stakeholder in the drone ecosystem and a balancing of rights and obligations.

On the cost increase side, the producer, public authorities and the user/owner can incur additional costs, as detailed in the analysis of O2 and reflected by the analysis of H2, H3 and H5. Firstly, the producer may increase prices of drones if it needs to address additional technical, organizational or certification steps to ensure prevention of economic damages. This cost can increase if the steps have to be taken throughout the lifetime of the drone, as is the requirement in similar legislation concerning medical devices. Secondly, the public authorities may request various fees for services provided in relation to authorization, certification or auditing of drones. Thirdly, the user/owner of the drone may need to pay additional maintenance fees, periodical verifications/audits of the drone or insurance to cover economic damages caused by the drone.

On the benefits side, the technical, organizational and certification steps can decrease the likelihood and/or impact of economic damages caused by cyber-attacks or other triggers mentioned above. Furthermore, having these in place together with clear legislation can assist in resolving litigious situations swiftly (without time consuming litigation) and in a clear manner that increases the trust in using drones as a safe and time-efficient manner to address economic needs of companies and of consumers.

From a legal perspective, establishment of liability in certain situations relating to malfunctioning or cyber-attacks relating to drones is not clear in the current legislation, irrespective of external or internal factors responsible for the incurred economic damages. Of course, this is closely tied with other relevant aspects, such as liability for economic damages concerning privacy or lack of compliance with privacy requirements. The analysis of O3 and of the hypotheses H8 and H9 reflects the general view of the respondents that certain preventive measures are essential in limiting subsequent damages caused by cyber-attacks. Thus, generally, the cost–benefit analysis resulted in the undertaking by the respondents in terms of costs and additional timing delays in using drones for the benefit of cyber security.

As detailed above, generally, there are certain criteria that can be used in order to identify, under current aviation legislation, civil tort law or producer liability legislation, the responsible entity within the complex ecosystem concerning drones [36]. Nevertheless, there are certain situations in which clearer legislation reflecting the actual input of each stakeholder in the ecosystem should be adopted and these have been outlined throughout the article.

In addition, there are certain preventive measures that can be implemented in the production, distribution and use phases of the drone ecosystem that can assist in limiting future economic damages from both internal and external factors, as these have been detailed above.

Author Contributions: Conceptualization, M.C.Ș. and L.G.; Methodology, M.C.Ș., M.V.A. and L.G.; Formal analysis, L.G., I.B. and A.-L.V.; Investigation, M.C.Ș., L.G. and A.-L.V.; Resources, I.B.; Data curation and analysis, I.B. and L.G.; Writing—original draft preparation, L.G., and I.B.; Writing—review and editing, M.C.Ș., M.V.A., L.G., I.B. and A.-L.V.; Visualization, M.C.Ș., M.V.A., L.G., I.B., and A.-L.V.: Supervision, M.C.Ș.; Project administration, M.C.Ș.; Funding acquisition, M.V.A., A.-L.V. 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. This paper was co-financed by The Bucharest University of Economic Studies during the PhD program. This paper was also co-financed by the Babes-Bolyai University of Cluj-Napoca during the PhD program.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data used in this analysis are 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.

Appendix A

Questionnaire

1. Do you find drones useful for economic activities?
   Yes
   No
2. How useful drones are in the following sectors? (question 1 from the manuscript)
   A. Agriculture (1–5)
   B. Industrial (1–5)
   C. Military (1–5)
   D. Public Order (1–5)
   E. Topography (1–5)
   F. Rescue missions (1–5)
   G. Retail (1–5)
   H. Transport (1:5)
   I. None (1:5)
3. Who is liable for negligent flying of drones that results in damages incurred by objects on the ground or in the air?
   A. The user of the drone, because he/she should be careful while flying
   B. The user of the drone, because he/she did not comply with the requirements in the drone manual
   C. The producer of the drone software
   D. The entity that assembled the drone software and hardware
4. Which of the following are useful preventive measures to prevent damages caused by negligent flying?
   A. Automatic responses of the drone to prevent certain types of crashes/incidents (1:5)

B. Periodical training to be completed by the professional drone users (1:5)
C. Obtaining a drone driving license after a number of training hours for drone driving (1:5)

5. Who is liable in case the drone software was modified by the user and this modification generated the damages or drone crash or possibility of hacker to take over the drone? (question 8 from the manuscript)

   A. The drone software producer, for permitting the drone user to change the software
   B. The drone software producer, for not having a mechanism in place to approve any changes to the software
   C. The relevant authorities for not having a certification process for changes to drone software
   D. The drone user

6. Which of the following are useful preventive measures to prevent damages/hacker attacks in case of drone software being modified by the user? (question 9 from the manuscript)

   A. Any change to the drone software should be approved by the drone software producer (1:5)
   B. A certification mechanism should be in place to perform a cyber security review of any change in the drone software (1:5)
   C. Users should not be able to change the drone software (1:5)

7. 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? (question 4 from the manuscript)

   A. The software producer
   B. The drone distributor/seller
   C. The drone user
   D. The cyber security solution used to protect the drone
   E. The entity that audited or tested from a cyber security perspective the drone

8. Which of the following are useful preventive measures in case of software vulnerabilities included from the outset in the drone software? (question 5 from the manuscript)

   A. Cyber security auditing before the drone is placed on the market (1:5)
   B. Periodic cyber security auditing to be performed by the user in order to be allowed to fly the drone (1:5)
   C. Failsafe mechanisms in case the drone is taken over by hackers in order to safely land the drone and alert the user (1:5)
   D. Cyber security software to be included in the drone to prevent intrusions and respond to them (1:5)

9. Who is liable in case a software update is available for the drone software and the drone user did not install this update? (question 6 from the manuscript)

   A. The drone user for not installing the update properly
   B. The drone software producer for not indicating the criticality of the update
   C. The drone software producer for not making the update mandatory before further use of the drone

10. Which of the following are preventive measures for ensuring software updates are properly and timely installed on drone software? (question 7 from the manuscript)

    A. The drone should not fly without the latest updates installed (either automatically or manually) (1:5)
    B. The drone should automatically install the updates when it is on the ground within the timeline provided by the drone software producer (1:5)

C. The drone should fly irrespective if the new updates are installed or not (1:5)
D. The drone software producer should highlight to the user the criticality of the update and the user should decide when to install it (1:5)

11. Who is liable in case of a malfunctioning of hardware components in the drone?

A. The hardware producer for the component
B. The entity that integrated the hardware and software of the drone
C. The software producer for the drone software
D. The drone user
E. The drone distributor/seller
F. The entity that audited or tested from a cyber security perspective the drone
G. The cyber security solution used to protect the drone

12. What steps should be taken when a drone is subject to a denial-of-service attack (which entails that the drone can no longer receive commands from its user, as it is flooded by commands from a hacker)? (question 10 from the manuscript)

A. A failsafe mechanisms should be in place to allow automatic safe landing
B. A cyber security solution should be in place to identify swiftly such situations and alert the user to land the drone
C. A periodic auditing of the drone should be performed to identify such situations

13. Who is responsible for preventing a drone from being used as a sender of commands in a denial of service attack towards other IT systems (e.g., as a cyber or physical weapon)?—e.g., the drone being part of a botnet (question 11 from the manuscript)

A. The drone software producer
B. The user
C. The cyber security solution installed on the drone
D. The certification body that

14. Do you think using drones will lead to an improvement in the activity they are used for? (question 2 from the manuscript)

A. Yes, from an efficiency perspective
B. Yes, from an accuracy perspective
C. Maybe, from an efficiency perspective
D. Maybe, from an accuracy perspective
E. No

15. Do you think using drones will lead to economic growth? (question 3 from the manuscript)

A. Yes
B. No
C. Maybe

16. Country of provenience:

17. Field of activity

A. Information technology
B. Engineering
C. Legal
D. Economist
E. Medical
F. Banking
G. Retail field
H. Real estate area
I. Academic
J. Other

References

1. Comandé, G. Product liability in Italy. In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*; Machnikowski, P., Ed.; Intersentia: Cambridge, UK, 2016.
2. Konert, A.; Kotliński, M.; U-Space—Civil Liability for damages caused by Unmanned Aircraft. *Transp. Res. Procedia* **2020**, *51*, 304–312.
3. Vacek, J.J. the Next Frontier in Drone Law: Liability for Cyberse-curity Negligence and Data Breaches for UAS Operators. *Campbell Law Rev.* **2017**, *39*, 135.
4. Alunaru, C.; Bojin, L. *The Tort Law Provisions of the New Romanian Civil Code*; De Gruyter: Boston, MA, USA, 2011.
5. European Group on Tort Law. *Principles of European Tort Law: Text and Commentary*; Springer: Vienna, Austria, 2005.
6. Borghetti, J.-S. Product liability in France. In *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies;* Machnikowski, P., Ed.; Intersentia: Cambridge, UK, 2016.
7. European Aviation Safety Agency. Concept of Operations for Drones. A Risk Based Approach to Regulation of Unmanned Aircraft. 2015. Available online: https://www.easa.europa.eu/sites/default/files/dfu/204696_EASA_concept_drone_brochure_web.pdf (accessed on 6 July 2021).
8. Regulation of Drones. The Law Library of Congress, Global Legal Research Center. 2016. Available online: https://irp.fas.org/congress/2016_rpt/lloc-drones.pdf (accessed on 22 August 2021).
9. E-Agriculture in Action: Drones for Agriculture; UAS Regulations, Policies & Privacy; Sustainable ICTs for Agriculture; Regional Training on the Use of Drones, Satellite Imagery and GIS for Agriculture. 2018. Available online: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/Drones-in-agriculture/asptraining/Drone%20regulations,%20policies%20and%20privacy.pdf (accessed on 26 August 2021).
10. European Drone Investment—Advisory Platform, European Investment Bank. 2019. Available online: https://www.eib.org/en/press/news/commission-and-eib-announce-launch-of-european-drone-investment-advisory-platform (accessed on 22 August 2021).
11. Klauser, F. Policing with the drone: Towards an aerial geopolitics of security. *Secur. Dialogue* **2021**, *16*, 2661.
12. Yaacoub, J.-P.; Noura, H.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218.
13. Connected Drones. A New Perspective on The Digital Economy. Huawei. 2017. Available online: https://www.huawei.com/en/technology-insights/industry-insights/outlook/mobile-broadband/xlabs/insights-whitepapers/connected-drones-a-new-perspective-on-the-digital-economy (accessed on 22 August 2021).
14. UNCTAD. The «New» Digital Economy and Development, UNCTAD Technical Notes on ICT for Development, United Nations Conference on Trade and Development. 2017. Available online: https://unctad.org/system/files/official-document/tn_unctad_ict4d08_en.pdf (accessed on 26 August 2021).
15. Zaychenko, I.; Smirnova, A.; Borremans, A. Digital transformation: The case of the application of drones in construction. In Proceedings of the International Scientific Conference Environmental Science for Construction Industry, Ho Chi Minh City, Vietnam, 2–8 March 2018.
16. Deloitte, Department of Infrastructure, Transport, Regional Development and Communications, Economic Benefit Analysis of Drones in Australia, Final Report, Deloitte Access Economics. 2020. Available online: https://www.infrastructure.gov.au/sites/default/files/documents/economic-benefit-analysis-of-drones-to-australia-final-report.pdf (acessed on 23 July 2021).
17. Amukele, T. *The Economics of Medical Drones*; Johns Hopkins School of Medicine: Baltimore, MD, USA, 2020.
18. Li, X.; Wang, J.; Yao, H.; Xu, X.; A Near-Optimal UAV-Aided Radio Coverage Strategy for Dense Urban Areas. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9098–9109.
19. Amer, K.; Samy, M.; Shaker, M.; ElHelw, M. Deep Convolutional Neural Network-Based Autonomous Drone Navigation. In Proceeding of the Thirteenth International Conference on Machine Vision. International Society for Optics and Photonics, Vienna, Austria, 11–13 February 2021.
20. Alsamhi, S.; Ma, O.; Ansari, M.S.; Gupta, S.K. Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization. *Drones* **2019**, *3*, 13.
21. Șcheau, M.C.; Rangu, C.M.; Udroiu, C. Secure IT Evolution Short Analysis. *Rom. J. Inf. Technol. Autom. Control* **2020**, *30*, 95–108.
22. Choudhary, G.; Sharma, V.; Gupta, T.; Kim, J.; You, I. Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives, Networking and Internet Architecture, Computer Science. In Proceeings of the 3rd International Symposium on Mobile Internet Security (MobiSec'18), Cebu, Philippines, 29 August–1 September 2018; pp. 1–13.
23. European Union Aviation Safety Agency. Regulation (EU) 2018/1139. Available online: https://www.easa.europa.eu/document-library/regulations/regulation-eu-20181139 (accessed on 2 September 2021).
24. Commission Delegated Regulation (EU) 2019/94 of 12 March 2019 on Unmanned Aircraft Systems and on Third-Country Operators of Unmanned Aircraft Systems. 2019. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0945 (accessed on 23 July 2021).
25. European Comission. European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Guide to Application of the Machinery Directive 2006/42/EC. Available online: https://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en (accessed on 22 August 2021).
26. European Comission. Guide to the Radio Equipment Directive 2014/53/EU. 2018. Available online: https://ec.europa.eu/docsroom/documents/33162(accessed on 22 August 2021).

27. Clarke, R.; Moses, L.B. The regulation of civilian drones' impacts on public safety. *Comput. Law Secur. Rev.* **2014**, *30*, 263–285.
28. Thomson Reuters, Practical Law. Directive 85/374/EEC on Liability for Defective Products. Available online: https://uk.practicallaw.thomsonreuters.com/w-013-0379?transitionType=Default&contextData=(sc.Default)&firstPage=true (accessed on 2 September 2021).
29. European Commission. Commission Staff Working Document, "Liability for emerging digital technologies", Accompanying the Document "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions", Artificial Intelligence for Europe. Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018SC0137 (accessed on 2 September 2021).
30. Sehrawat, V. Liability Issue of Domestic Drones. *Santa Clara High Tech. Law J.* **2018**, *35*, 110.
31. Du, H.; Heldeweg, M.A. *Responsible Design of Drones and Drone Services—A Synthetic Report*; SSRN: Rochester, NY, USA, 2018.
32. Pyzynski, M.; Balcerzak, T. Cybersecurity of the Unmanned Aircraft System (UAS). *J. Intell. Robot. Syst.* **2021**, *102*, 35.
33. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13.
34. Konert, F.A.A.; Balcerzak, B.T.; Legal and ethical aspects of rules for the operation of autonomous unmanned aircraft with artificial intelligence. In Proceedings of the International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 15–18 June 2021; pp. 602–609.
35. HSD Securitydelta.nl. Final Report: Technical Aspects Concerning the Safe and Secure Use of Drones. 2016. Available online: https://www.thehaguesecuritydelta.com/uavs-drones (accessed on 2 September 2021).
36. Hodgkinson, D.; Johnston, R. *Aviation Law and Drones: Unmanned Aircraft and the Future of Aviation*; Routledge: Milton Park, UK, 2018.