Article

Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar's Mega Sporting Events

Khalifa AL-Dosari *, Ahmed M. Deif , Murat Kucukvar , Nuri Onat and Noora Fetais

College of Engineering, Qatar University, Doha P.O. Box 2713, Qatar; adeif@qu.edu.qa (A.M.D.); mkucukvar@qu.edu.qa (M.K.); onat@qu.edu.qa (N.O.); n.almarri@qu.edu.qa (N.F.)
* Correspondence: 200704317@qu.edu.qa; Tel.: +44-97455815856

Abstract: Unmanned aircraft vehicles (UAVs) are now used to support security precautions in search and rescue operations to track and evaluate critical services, to provide cybersecurity measures by transporting security supply chain management (SCM) to sports events, and to aid efforts to safeguard the spectators from attacks. A drone may quickly fly over sports grounds, scan the area for potential dangers, and offer aerial footage and still photographs. Although UAVs provide benefits to their operators, there is a possibility that they may also pose cybersecurity threats. This guide offers recommendations for best security practices, intending to assist sports operators in protecting their networks, materials, and staff for Qatar's mega sporting events. The literature comprises several theoretical frameworks and conceptual models for security supply chains. Unfortunately, there is no practical model for measuring the behavioral intentions of professional IT and security experts. Therefore, this study conducted research in two stages. In the first stage, an in-depth systematic literature review was conducted to identify the factors and themes of UAV-based SCM for security measures. In the second phase, a survey questionnaire (N = 712) was implemented, comprising the themes and items from the literature review among professional IT and security experts. Exploratory factor analysis (EFA) was carried out with IBM SPSS, and confirmatory factor analysis (CFA) was employed with IBM AMOS. This study proposed and developed a UAV-based SCM model to provide security for Qatar's mega sporting events, which comprised five factors: traceability, security and privacy, trust, acceptability, and preparedness. This study also confirmed the validity and reliability of the newly developed scales, offering practical and proposed implications for the IT and security industries. The key findings of the study are: (1) a valid and reliable UAV-based cybersecurity framework for FIFA mega sporting events was developed; (2) five critical factors were identified, including traceability, security and privacy, trust, acceptability, and preparedness; (3) all factors were significantly and positively correlated, highlighting the complexity of managing security systems in mega sporting events.

Keywords: UAVs; supply chain management (SCM); scale development; Qatar's mega-sporting events

check for updates

Citation: AL-Dosari, K.; Deif, A.M.; Kucukvar, M.; Onat, N.; Fetais, N. Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar's Mega Sporting Events. *Drones* **2023**, *7*, 555. https://doi.org/10.3390/drones7090555

Academic Editor: Diego González-Aguilera

Received: 12 April 2023
Revised: 3 May 2023
Accepted: 6 May 2023
Published: 28 August 2023

1. Introduction

Emerging information technologies (EITs) and significant ongoing problems have resulted in the digitalization process acting as a complement to the adoption of digital supply chain management (SCM) and more cutting-edge strategies [1]. In today's globalized era, a supply chain perspective has emerged as the primary unit serving as an organizational principle [2]. This SCM perspective faces multiple challenges, including cybersecurity, which companies have to properly and progressively manage to be able to broaden their SCM activities beyond their borders [3]. Cybersecurity in SCM has recently gained considerable relevance because unmanned aerial vehicles (UAVs) make it possible for supply chain stakeholders to gather, transport, store, and analyze a massive quantity of data at a low cost while also being able to share facts and information [4–6]. In addition, UAV implementation in SCM operations exhibits a significant improvement in process capability, a decrease in costs, and an enhancement in the quality of decision-making in order to improve cybersecurity practices. Cyber threat intelligence and advanced analytics techniques are embedded to successfully anticipate cyberattack trends in cyber SCM [5].

UAVs are increasingly utilized for security and protection at mega sporting events such as those held in Qatar [7], enhancing spectator participation [8]. Effective cybersecurity management at these events is crucial for creating a positive atmosphere and achieving event goals [9]. Cybersecurity risks involve attempts to disrupt digital systems, steal data, or damage resources [7,10]. The 2014 FIFA World Cup revealed the potential impact of cybersecurity issues on sporting events, such as IT system intrusions, phishing emails, cyberattacks, and cyber espionage [11]. Although security threats have gained more attention after tragic incidents in 2015 [7,12], cybersecurity at sporting events has often been overlooked. Rapid technological advancements and their integration into event planning contribute to cybersecurity concerns [13]; Yaacoub et al. [4] explored these in the context of technology use in SCM. In addition, Ardito et al. [1] examined the integration of digital technologies into SCM and marketing, which they argued was essential for organizations to transition towards Industry 4.0. In addition, Tiwari et al. (2018) [2] and Patnayakuni et al. [3] conducted studies of big data analytics in SCM between 2010 and 2016, aiming to provide insights into industry applications. The authors highlighted the increasing importance of big data analytics for enhancing decision-making, improving operational efficiency, and reducing costs in SCM.

Fernández-Caramés [14] declared that unmanned aerial vehicles are used to store, process, and exchange data with equipment stationed in a facility and with SCM. Hopkins [15], Raji et al. [16], and Haji et al. [17] reported on UAVs and drone aircraft for the shortest delivery in the supply chain system, particularly security issues. Abbas et al. [18] presented a blockchain-based SCM of a secure SCM to trace the drug distribution process, handle difficulties relating to faking, and make delivery times shorter; this could be because businesses are digitizing their internal systems through door-to-door SCM so that they can later use UAVs as part of SCM [1,19]. Furthermore, using UAVs, IT professionals track and monitor the security conditions in the supply chain, as well as the upstream, midstream, and downstream data and substitute them into an evaluation model to assess UASs. Using the latest technology of IoT and artificial intelligence (AI), UAVs are now used to handle the SCM of city security [20], particularly in relation to cybersecurity challenges for the SCM of mega sporting events. The chain of valuing UAVs in SCM is based further upstream in the SCM levels, while the point further downstream tracks the information and data operations that are already happening or are going to occur downstream [21,22]. Under the circumstances of UAV supply chain management, even though it is possible to maintain the stability of upstream operation costs, this would result in high-security equipment carrying costs downstream whenever errors are expected or markets are altered. As such, the quality of services would be compromised [21]. On the contrary, SCM is more involved in the real world, and each operation of the upstream, middle, and downstream stages can supply one another [23,24]. Therefore, UAVs help in three SCM stages: upstream, midstream, and downstream. When used at mega sporting events, UAVs present several challenges that should be solved in each SCM stage (Figure 1).

Problems further upstream are referred to as "upstream" problems, which arise before an event. The regulatory framework for UAVs is one of the most significant upstream challenges. There needs to be more harmonization among the regulations governing UAV use at mega sporting events. The regulations vary from country to country [25], which results in uncertainty for both the event organizers and the UAV operators, ultimately affecting the planning and execution of UAV operations. Issues that arise in the middle of an event are called "midstream problems." One of the most significant issues during the midstream concerns the security of UAV operations. According to Lopez et al. [26], the use of UAVs in crowded and confined spaces, such as stadiums, can pose a safety risk to the spectators and players, or could collide with other UAVs or objects. Another issue that needs to be addressed in the middle of the process is the potential for cyberattacks that target UAVs or the data they collect [27]. Meanwhile, downstream problems arise because of the event that has already taken place. The protection of the spectators' and players' personal information and privacy is one of the most significant issues that arise due to this. Using UAVs to record video footage and collect data can result in privacy concerns, mainly if the data needs to be adequately secured or used for purposes that are not authorized [27]. Whether or not using UAVs at mega sporting events is cost-effective raises another issue further down the line. The cost of purchasing and operating UAVs, in addition to the cost of training and certifying operators, can be a significant investment for event organizers. The proposed SCM perspective to manage cybersecurity challenges at mega sporting events is shown in Figure 1.

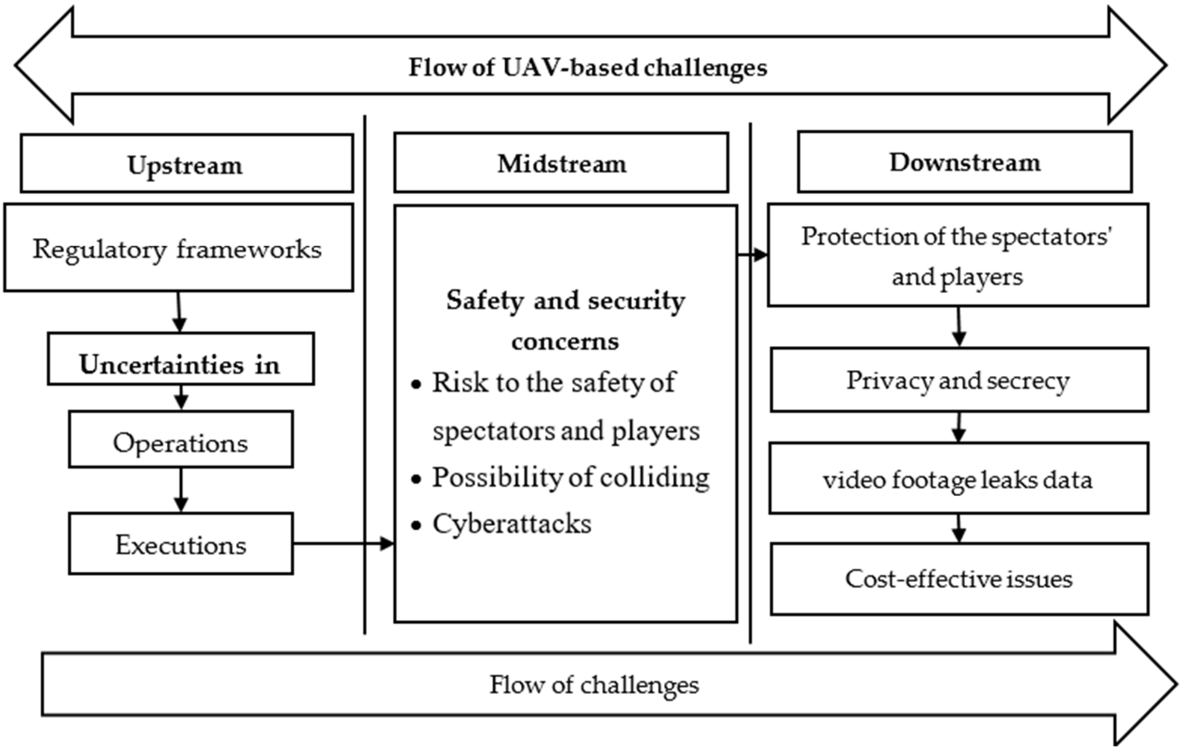

Figure 1. Stages of supply chain management (SCM) challenges.

The use of UAVs at mega sporting events offers many benefits, including providing new perspectives, analyzing data in real time, and improving the overall experience for both players and spectators. In contrast, it imposes several challenges upstream, midstream, and downstream that must be resolved. A coordinated and harmonized regulatory framework, advanced safety measures, and robust privacy and data protection policies are required to guarantee the safe, secure, and efficient use of UAVs during mega sporting events. The use of UAVs in the SCM stages is growing, and with it comes advantages for sports and games. However, it increases the complexity of scalability and cybersecurity, as well as the SCM of security and preventive measures for sporting events. Each of these streams in the security of mega sporting events is simultaneously responsible for managing security measures (i.e., cameras, sensors, and flying capacities), safety assurance, and information using UAVs. This procedure calls for an integrated supply chain strategy to handle the difficulties that exist throughout the entire chain and to increase the efficiency of complicated supply chain networks [28]. The best way to capture the factors behind the difficulties and possibilities in cybersecurity ahead of the impact of future mega sporting events is to understand the motives that lead Qatar to organize such an event. Talavera et al. [12] conducted a study on Qatar's mega sporting events and found several challenges in providing measures to secure these events. As a result, the most important challenge for public policy is to enhance cybersecurity by eliminating the present drawbacks inherent to the cybersecurity issues that link Qatar to mega sporting events [29]. Therefore, Ganji [29] offered an "unmanned aerial system (UAS)" for automating cybersecurity measures in order to secure mega sporting event processes. This system can detect cybersecurity threats and cyberattacks more quickly than human operators can, and can locate objects in a warehouse based on the signal from their tags.

Due to the growing need for more modern security measures, using unmanned aerial vehicles (UAVs) for cybersecurity purposes at large athletic events, concerts, and playgrounds has received much attention recently. Several nations' event management procedures have incorporated UAV-based cybersecurity strategies, which have been adopted and implemented. According to Cooper et al. [10], unmanned aerial vehicles (UAVs) in the United States have been used to deliver real-time situational awareness and threat identification around the perimeter of large-scale events such as the Super Bowl. Similarly, law enforcement agencies in the United Kingdom have begun using unmanned aerial vehicles (UAVs) to monitor security at high-profile events such as the Glastonbury Festival and the London Marathon [27]. This has increased both public safety and improved coordination among security professionals. According to Abbas et al. [18], the New South Wales Police Force in Australia has successfully integrated unmanned aerial vehicles (UAVs) into its security measures for large events such as the celebrations held in Sydney on New Year's Eve and the Australian Open. Even if SCM practices are becoming increasingly commonplace, the cybersecurity of UAVs is still a challenge [30]. Investigators at Johns Hopkins University have discovered vulnerabilities in UAV technology, including those that might be exploited by hijackers, man-in-the-middle attackers, and injection hackers during sporting events [29]. Because of this, numerous challenges regarding the safety, security, and dependability of using UAVs for SCM have been voiced. As a result, there is a need to alleviate the concerns regarding the safety and security of UAVs via monitoring their every movement in the cybersecurity supply chain.

This study relied on UAV-based cybersecurity to bring drones back to sporting events if they began to deviate from their intended path. We identified the challenges in implementing a proper UAV framework and have proposed opportunities to handle security issues and cyberattacks in the SCM at mega sporting events. In particular, we developed a new UAV-based cybersecurity framework that assesses the performance of UAVs at mega sporting events. This UAV framework offers the possibility of the SCM of cybersecurity supplies. In addition, UAVs may fly on their own using the digital security and safety built into them or can be controlled remotely using a controller. This study developed a testable UAS-based security model to enhance the SCM-carrying UAVs that guarantee the supply of security and safety measures at mega sporting events. Specifically, we aimed to cover the following objectives when designing a model that measures SCM:

1. To identify the challenges in the SCM process;
2. To propose a research framework for the implementation of UAS-based cybersecurity for SCM at Qatar's mega sporting events;
3. To assess the upstream, midstream, and downstream stages in the implementation of the UAS-based cybersecurity model for SCM at Qatar's mega sporting events;
4. To develop a testable UAV-based security framework for the SCM of security and safety measures.

2. Literature Review

2.1. Diffusion of Innovation (DOI) Theory

This study explored the significance of the diffusion of innovation (DOI) theory for a UAV-based cybersecurity framework to develop a conceptual model for cybersecurity SCM. This allowed us to put more effort into the dark side of UAV-based cybersecurity. A technology, design, method, practice, vision, or attitude that is new to the team that adopts it can be classified as an innovation [31]. DOI is the method by which a technology spreads over various contexts [29]. UAS-based cybersecurity operations are still relatively unexplored in the SCM practices at mega sporting events because implementing UAS-based cybersecurity necessitates using new technology, processes, and resources in addition to incurring financial costs [23,26]. Due to the implementation of cybersecurity, the DOI theory emphasizes technology issues in addition to a system's internal and external qualities [32].

2.2. Cyber Threats and Attacks at Mega Sporting Events

A mega sporting event is typically defined as attracting a large number of spectators, generating significant economic impact, and receiving widespread media coverage. However, events that attract tens of thousands or more spectators and involve multiple venues or locations requiring substantial infrastructure and logistical support, which generate billions of dollars in economic impact, can be considered mega sporting events. Examples of such events include the Olympic Games, FIFA World Cup, and the Super Bowl. Therefore, it is likely that cybercriminals will engage in actions of a similar nature throughout the following few years, given the widespread appeal of the FIFA World Cup, Olympic Games, FIFA World Cup, and Super Bowl, as well as the strong demand for tickets and flights [33]. Understanding these rising events in depth is the only effective strategy to reduce the risk of being targeted by cyberattacks during such occasions. In advance of the arrangements for the World Cup, the Qatar government has already produced a cybersecurity framework, but previous cybersecurity practices did not overcome cyberattacks during other mega sporting events [34,35]. Therefore, this study developed a UAV-based cybersecurity framework that specifies the UAS-based cybersecurity needs to secure national key infrastructure hosting the FIFA World Cup and focuses on the Qatar Nation Vision 2030 [36]. Undoubtedly, security experts will have a better grasp of the potential dangers and will be more likely to protect themselves against them if they receive a steady flow of realistic threat intelligence before and throughout the event. Better security of UAV technology and increased resistance to targeted cyberattacks can be achieved by identifying the potential points of vulnerability and then taking the appropriate steps to resolve them. Users not paying attention to their surroundings have a reduced risk of having their personal information stolen by hackers using this method. It is also possible to decrease the possibility of assaults on a more extensive scale by keeping an eye on and exercising control over the flow of knowledge over these networks.

2.3. Challenges in UAS-Based Security at Mega Sporting Events

UAVs are the ideal complement to ground security due to their speed, size, degree of mobility, and added technological capabilities. They make it possible for security staff to monitor mega sporting events more rapidly and effectively. As a result, UAVs have a competitive edge over sensory cameras because intruders cannot swiftly move out of view. Unfortunately, UAVs can lead the mission to be aborted; many drones automatically return to their main base if communication is lost, or they might be triggered to collapse [6]. In parallel to this, attackers can also compromise the central command system of a drone in order to seize control of the UAV. UAVs are susceptible to both of these vulnerabilities in cybersecurity practices. Nevertheless, we can generally aggregate them into three main consequences that UAVs have on the human psyche: a lack of privacy, feelings of uneasiness and anxiety, and alterations in the mechanics of social interactions [37]. Regarding high-tech items in general, security is almost always an issue, and UAVs are no exception at mega sporting events. Communication between UAVs and their remote operators is frequently encrypted. In contrast, the encoded codes frequently remain the same (that is, static), which makes it an excellent and straightforward target for hijacking [6]. Therefore, there are many challenges in the implementation of UAV-based cybersecurity in SCM measures.

Meanwhile, the efficiency of a supply chain has an immediate and direct impact on organizational performance [38]. Nevertheless, the shift from a linear to a supply chain is difficult for enterprises to undertake [39]. When the challenges surrounding the supply chain are studied from a macro-viewpoint, the primary problem is the need to alter the entire SCM following the fundamental components of supply security. According to Ellen [40], there seem to be three of these components, referred to as serviced business models, enablers, and reverse logistics. Bressanelli et al. [41] noted that it is unlikely that a corporation will restructure their complete SCM all at once; instead, there is a greater possibility of focusing on security issues. This viewpoint is supported by the evidence presented in the previous paragraph. The researchers attempted to identify significant challenges in the supply chain, establishing an interpretative structural model by evaluating their interactions in successfully adopting supply chain practices. Mangla et al. [42] researched the challenges in supply chain management, particularly in emerging economies.

Levering and Vos [43] concentrated on adopting and implementing procedures to attain a supply chain process. They identified the challenges and drivers of supply chain management for four distinct industries by considering the sustainable practices that were already in place. In addition, Saroha et al. [44] carried out a comprehensive literature review on recognizing SCMs' challenges. These challenges were separated into the following categories: regulatory challenges, technical challenges, skills and knowledge challenges, management challenges, social challenges, and marketing challenges. They wanted to provide an initial framework in the hope of a better understanding of SCM challenges. In particular, Pan et al. [45] mainly focused on supply chains and glanced at methods to achieve recycling by concentrating on issues such as waste management and energy needs. They categorized challenges into technological, institutional, financial, and regulatory. (Table 1) offers an overview of the SCM challenges reported in various research works. These challenges come from a variety of sources.

Table 1. Challenges for SCM.

Challenges	Sources
Lack of effective planning and management for CSCM concepts	Mangla et al. [42] Verboeket and Krikke [46]
Lack of management commitment and approach for CSCM adoption	
Lack of implementation of environmental management certifications and systems	
Lack of customer awareness of and participation in CSC activities	
Inadequacy in the knowledge and awareness of organizational members about CSCM initiatives	
Lack of appropriate training and development programs for SC members and HR	
Lack of coordination and collaboration among SC members	
Transportation and infrastructure	Bressanelli et al. [41]
Availability of suitable supply chain partners	
Data privacy and security	
Coordination and information sharing	
Eco-efficiency of technological processes	
Lack of vision	Saroha et al. [44]
Higher investment cost	
Lack of knowledge	
Lack of awareness	
Lack of information sharing	
Technologies made locally available	Pan et al. [45]
Measuring environmental impact (certification)	Levering and Vos [43]
Cost of developing unmanned vehicle alternatives	
Lack of a standard system for performance indicators with regard to measuring supply chains	Govindan and Hasanagic [47]
Unclear vision and lack of trust in technology	
Lack of transparency	
Lack of traceability	
Lack of skills by employees in SCM	
Cybersecurity and international supply threats	Aggarwal et al. [48] Meissner et al. [49]
Security and risk management	
Risk of security threats and vulnerabilities	Sahu et al. [50]

2.4. Unmanned Aerial Vehicle-Based Security and SCM

After conducting research into the various sensing technologies and countermeasures that are now available to defend against the use of drones, previous research on cybersecurity has been expanded upon by incorporating UAVs and drones into the cybersecurity supply chain. Previous studies have determined and assessed several potential attack scenarios involving the use of UAVs. This study's primary objective was to demonstrate the potential dangers to public safety and security posed by the improper use of unmanned aerial systems (UASs) and to suggest appropriate countermeasures and counter-UAS technologies that are both efficient and applicable in UASs to endorse aviation's resilience against cyber threats. Wang, Liu, and Song [6] also framed a model and found that UAVs are used in the supply chain deliveries of healthcare materials and products, but unfortunately, the currently available UASs are unable to provide appropriate computing and power supplies. Vision-based detection can be installed in ground-based stations, UASs, and manned aircraft [6]. UASs, on the contrary, provide substantial difficulties to society in terms of issues relating to safety, privacy, and security [37]. The occurrence of events involving drones in close proximity to cybersecurity facilities is becoming increasingly common in modern times. These occurrences are predicted to increase in frequency, difficulty, and intensity as drones grow in size and capability. Infrastructures need to have appropriate countermeasure technologies, strategies for risk management, and resiliency plans in place in order to be safeguarded from cyberattacks and ensure effective SCM [37].

Security and privacy should always be a primary priority when working with any digital technology [51]. Security is a significantly more pressing issue than usual, given the nature of UAVs and the fact that remote wireless communication can take place. The integrity and privacy of the infrastructure, networking, and information in UAVs are the primary targets of most cyberattacks that can be launched against UAV networks. There is a risk of data being intercepted between UAVs and supply chains due to operations such as keylogging and eavesdropping [52], compromising the confidentiality of the information being transmitted. These kinds of assaults happen because there are not enough stringent transmission and encryption regulations, resulting in illegal access to personal information. The data entered on a computer can be monitored through keyloggers, historically utilized for a variety of purposes, including the monitoring of children's online activities, the monitoring of sensitive information provided by employees, and the monitoring of criminals. These days, keyloggers are explicitly utilized for stealing data, either in the instance of automated teller machines, where keyboard sniffers can retrieve a user's PIN, or in unmanned aerial vehicles, the privacy of communication transferred between numerous UAVs can be breached. Keyloggers can access information directly over the Internet and are undetectable by antivirus software since they store their data in encrypted form. Eavesdropping, also known as illegal monitoring of transmission, is a procedure that can control the communication between many UAVs, as the title suggests.

Because of essential properties such as decentralization, integrity and traceability, data dependability, transparency, security and privacy, and trust may scale up the confidentiality and security of UAV-based SCM; also known as UAV-to-everything [30]. There have been a significant number of problems with data security and privacy problems, and academics from all over the world have proposed many methods to secure data from cyberattacks [30]. The solutions that have been offered protect users' privacy and data while also lowering the cost of data storage and improving the efficiency of the network. While BC ensures the safety and confidentiality of UAVs, it raises the bar for the performance of network characteristics. The protection of users' information and privacy is the primary concern in UAV-based SCM [51]. In order to address concerns regarding cost and latency, Koubaa et al. (2019) merged the cloud computing model with a UAV. However, safety and confidentiality concerns were not handled in Koubaa et al. (2019) or Mozaffari et al. [51] studies. The one disadvantage each of them share is that there is no trust developed among the many stakeholders because the security factor is not addressed at any point [53]. When put into practice, the management of SCM can assist in the identification of compromised

UAVs on the premise of trust policies. According to research, such UAV systems are ideally suited for incorporating artificial intelligence (AI) technology to foster trust among UAVs and provide secure communication. AI technology has the capacity to carry out applications in situations where there needs to be a guarantee of confidence between the various stakeholders. In order to preserve players' trust in one another and their integrity throughout the SCM process, AI technology utilizes smart contracts (SCs) [23,37].

This study focused on knowledge, acceptability, and preparedness to occupy UAV technologies to assist decision-makers in security SCM, cybersecurity operations, and planning. The goal of this study was to begin closing the knowledge gap by identifying a UAV-based cybersecurity framework for mega sporting events. It is necessary to analyze the degree to which local populations accept and are prepared for the utilization of drones to ensure that this will not be a barrier to their efficient use in supply delivery [26,43]. In spite of this, pilot studies carried out in a variety of nations have demonstrated that local populations, when informed about the technology's application area prior to its deployment, tend to welcome the innovation with open arms [54]. For preparedness, it is important to consider not only the price and immediate performance enhancements in SCM, such as speed and adaptability, but also the preparedness of the cybersecurity SCM for mega sporting events. Therefore, this study organized a set of factors and items from the literature review to ensure a UAV-based supply chain that enhances the SCM in Qatar's mega sporting events.

3. Research Methodology

3.1. Research Method

The subject of the study and the research questions determined the different research technique. The research methodology is how researchers gather, evaluate, and explain the study's data [55]. Any discipline should include a review of the systematic literature evaluation [56]. When the process is carried out correctly, with the lowest number of mistakes, the study can produce trustworthy findings and conclusions that can assist decision-makers and academic experts in taking the appropriate actions [57]. This study was conducted in two phases. In the first phase, a literature review was conducted, followed by a comprehensive assessment of the literature review information. This study aimed to thoroughly accomplish a secondary study by analyzing the SLR. The literature review did not show any appropriate UAV-based cybersecurity frameworks for mega sporting events. Therefore, an inductive approach was used to develop a UAV-based cybersecurity framework for cybersecurity-based UAVs to ensure the security of mega sporting events from a SCM perspective. The research issues were mentioned in the SLR, which were then compared to previously published studies to determine if their findings could help us to develop a UAV-based cybersecurity framework that provides a solution for mega sporting events. This study used the Scopus-indexed and Clarivative analytics databases. The synthesis process involved extracting and classifying pertinent data from chosen publications and regarding conclusions. The coder retrieved information from the chosen published articles using inclusive and exclusive criteria [58]. The variable of interest was arranged according to the overall qualities of the articles and the criteria used to assess, measure, and address the SLR's goals. Finally, clustered items from different sources were gathered and summarized into five main factors of cybersecurity-based UAVs in SCM. In the second phase, data from Qatar's IT and cybersecurity experts were gathered to validate the proposed model for the UAV supply chain. This phase followed the empirical testation of the UAV-based cybersecurity framework for mega sporting events.

3.2. Conceptualization of the Measurement Scales

An SLR was conducted in the first phase in order to organize the measurement items (Table A1). The items were selected from multiple sources and contexts, and were operationalized according to cybersecurity-based UAVs for mega sporting events from an SCM perspective. Four items were selected for the traceability of UAVs, three items for security and privacy, four items for trust, five items for acceptability, and four items for the preparedness of UAVs in the security supply chain for mega sporting events. Finally, the model contained five factors: Traceability (four items), security and privacy (three items), trust (four items), acceptability (five items), and preparedness (four items) for security SCM using UAVs.

3.3. Data Collection Procedure

A survey questionnaire was developed using the measurement items identified from the SLR. The information was gathered from various IT and security companies located in Qatar. To gather the primary data, a questionnaire method was used to collect data from the IT experts who are managing security and safety practices at mega sporting events. A five-point Likert scale served as the basis for the development of the tool, as follows: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree. The methodology of a research study refers to the systematic approach taken by researchers to collect and analyze data to answer the research questions or test hypotheses. In this case, the study aimed to develop and propose a new UAV-based supply chain model for companies in Qatar. The researchers used convenience sampling to select the companies included in the study. Convenience sampling is a non-probability sampling method in which the sample is selected based on ease of access or availability. The researchers accessed Qatar's online database and selected the companies that were easily accessible to them. The researchers collected data from the IT and cybersecurity experts of the selected companies. The data collection method used was a combination of surveys and interviews. The researchers developed a questionnaire administered to the experts to collect quantitative data. The questionnaire was designed to collect information on the companies' current supply chain management practices, their use of UAVs in supply chain management, and the challenges they face.

In addition to the questionnaire, the researchers conducted face-to-face interviews with IT and cybersecurity experts to collect qualitative data. The interviews were semi-structured, meaning that the researchers had predetermined questions but were open to exploring other topics that arose during the interview. The interviews were audio-recorded and transcribed for analysis.

To ensure the security and privacy of the information provided by the companies, the researchers obtained a permission letter from the concerned university department. The permission letter explained the purpose of the study and the measures taken to ensure the confidentiality of the information provided. The researchers also ensured the secrecy and privacy of the information by storing the data securely and analyzing it anonymously. After data collection, the researchers analyzed the data using qualitative and quantitative methods. The quantitative data collected from the questionnaires were analyzed using descriptive and inferential statistics. Data were collected in multiple rounds. The online survey questionnaire was distributed to 712 IT experts over the Internet, resulting in a total of 476 complete responses—with a 66.85% response rate. Therefore, 476 sample data were sufficient for exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) because researchers recommend a minimum sample size of 300 for EFA and 200 for CFA [59,60]. (Table 2) outlines the demographic information of the participants.

Table 2. Demographic information.

		Frequency	*Percentage*	*Valid Percentage*	*Cumulative Percentage*
Gender	Male	223	46.8	46.8	46.8
	Female	253	53.2	53.2	100.0
	Total	476	100.0	100.0	

Table 2. *Cont.*

		Frequency	*Percentage*	*Valid Percentage*	*Cumulative Percentage*
Company nature	IT companies	248	52.1	52.1	52.1
	Security companies	228	47.9	47.9	100.0
	Total	476	100.0	100.0	
Company age	1–5 years	176	37.0	37.0	37.0
	6–10 years	261	54.8	54.8	91.8
	11+ years	39	8.2	8.2	100.0
	Total	476	100.0	100.0	
Working experience	Less than 1 year	47	9.9	9.9	9.9
	1–3 years	174	36.6	36.6	46.4
	4–6 years	135	28.4	28.4	74.8
	More than 6 years	120	25.2	25.2	100.0
	Total	476	100.0	100.0	
Number of employees	10–20	58	12.2	12.2	12.2
	21–40	115	24.2	24.2	36.3
	41–60	127	26.7	26.7	63.0
	61+	176	37.0	37.0	100.0
	Total	476	100.0	100.0	
Education level	12 years of education	6	1.3	1.3	1.3
	14 years of education	89	18.7	18.7	20.0
	16 years of education	318	66.8	66.8	86.8
	18+ years of education	63	13.2	13.2	100.0
	Total	476	100.0	100.0	

3.4. Data Analysis

The study employed two key data analysis techniques: exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). Both techniques were used to analyze the data and test the validity and reliability of the factors in the conceptual model [55,56,61]. In this study, EFA was conducted using IBM SPSS software to analyze demographic information and identify key factors [62,63]. The process involved several steps, including data cleaning, ensuring the suitability of data for factor analysis, selecting the extraction method, determining the number of factors to retain, and interpreting the factor loadings [62,63], including:

(1) **Data reduction:** It simplifies data by grouping correlated variables into smaller factors, making it easier to understand and interpret the data;
(2) **Identifying underlying constructs:** EFA helps to reveal the latent factors or constructs that underpin the relationships among variables;
(3) **Construct validity:** EFA provides evidence of construct validity by showing that the variables in a factor are related and measure the same underlying construct.

In addition, CFA was conducted using IBM AMOS software to test the validity and reliability of the factors identified in the EFA [64,65]. This involved specifying the factor model, estimating the model parameters, assessing the goodness-of-fit, and interpreting the results, including:

(1) **Model testing:** CFA tests whether the observed data fit the hypothesized factor structure, which is specified by the researcher beforehand;
(2) **Construct validity:** CFA examines the relationships among the variables and the factors, assessing convergent validity, discriminant validity, and nomological validity;
(3) **Reliability:** CFA evaluates the reliability or internal consistency of the factors by examining the factor loadings, composite reliability, and average variance extracted.

4. Data Analysis and Findings

4.1. Common Method Bias (CMB)

A test for non-response bias was carried out. Following the completion of the various steps of follow-ups, replies were obtained. When the early and late levels were examined using homogeneity of analysis of variance, the findings showed that no scores remained statistically significant. This indicates that there were no big differences between the levels of the variables [62]. The CMB was assessed with the well-known and widely utilized Harman's single-factor testing with five factors. Five factors appeared from the IBM SPSS results, and the overall factors contributed to 32.018% of the total variance, which is lower than the threshold value of 50% and indicates that the dataset was clear from common method bias [63]. Additionally, all Eigenvalues were higher than 1.00; therefore, there were no biases.

4.2. Exploratory Factor Analysis (EFA)

EFA is a well-known method that has been utilized in past studies on SCM [64]. The primary goal of EFA is to reveal the underlying pattern of many variables [65]. The Kaiser–Meyer–Olkin (KMO) and Bartlett tests consider all of the data at their disposal. A KMO value greater than 0.5 and a significant threshold for Bartlett's test less than 0.05 indicate that the data exhibit a significant correlation [64]. In Bartlett's test of sphericity, a correlation matrix that has been observed is compared to the identity matrix [66]. The KMO value was 0.860 (p < 0.05), which, as shown in (Table 3), is higher than the minimum value of 0.60 suggested by Kaiser [67].

Table 3. KMO and Bartlett's test.

KMO and Bartlett's Test		
Kaiser–Meyer–Olkin measure of sampling adequacy		0.860
Bartlett's test of sphericity	Approx. chi-square	4442.060
	Df	190
	Sig.	0.000
a. Based on correlations		

The researchers did not make any preconceived notions regarding the links between the factors [68]; therefore, the validity and reliability of the factors should be ensured. A statistical technique known as factor analysis was employed to describe the variability of a set of observed and correlated factors in terms of a reduced number of unseen variables known as factors. A dimension reduction method was applied by following principal component analysis (PCA) in varimax rotation. The measured variables were modeled as ordered pairs of the possible factors and "error" terms; the principal component analysis could be regarded as a specific example of an errors-in-variables model [69,70]. Numerous studies have reported different values for factor-loading, but this study followed the advanced criteria that the factor loading of each item/observed indicator should be higher than 0.70 [71,72].

A series of dimension-reduction processes were applied to meet the maximum acceptable criteria for factor loading (Table 4). First, a maximum value of 0.6 was ensured, meaning that all lower values were removed automatically. Later, the researchers found that no value was lower than 0.60, so the advanced acceptable criteria of factor loading (value > 0.70) were applied, and it was found that one item of preparedness (PREP = 0.673) and one item of acceptability (ACCEPT = 0.667) had lower factor loadings than 0.70. Therefore, these two items were removed from the model. Finally, 18 items from a total of 20 items were declared valid and reliable for the confirmatory factor analysis (CFA): four items for trust, three items for security and privacy, three items for preparedness, four items for acceptability, and four items for traceability.

Table 4. EFA findings.

Factors	Items	Item Loading	Cronbach's Alpha	Eigenvalues	Cumulative %
Traceability	TRAN1	0.702	0.841	32.890	32.890
	TRAN2	0.795			
	TRAN3	0.827			
	TRAN4	0.803			
Security and privacy	SAP1	0.860	0.825	11.351	44.241
	SAP2	0.800			
	SAP3	0.802			
Trust	TRUST1	0.785	0.890	8.437	52.678
	TRUST2	0.824			
	TRUST3	0.826			
	TRUST4	0.871			
Acceptability	ACCEPT1	0.704	0.753	7.935	60.613
	ACCEPT2	0.718			
	ACCEPT3	0.703			
	ACCEPT4	0.732			
Preparedness	PREP1	0.789	0.807	7.311	67.924
	PREP2	0.763			
	PREP3	0.822			

Additionally, reliability analysis was conducted using Cronbach's alpha approach (Table 4). As a general rule of thumb, a Cronbach's alpha value of 0.70 or higher is considered good, 0.80 or higher is considered better [73,74], and 90 or higher is considered the best [70,71]. As such, this study used the threshold value of Cronbach's alpha > 0.70 [72]. Finally, traceability was found to have good reliability at 0.841, security and privacy at 0.825, trust at 0.890, acceptability at 0.753, and preparedness at 0.807.

4.3. Confirmatory Factor Analysis (CFA)

After EFA, IBM AMOS software was used to conduct CFA (Figure 2). The purpose of CFA is to determine whether or not the observed factors contribute to latent or unobserved indicators. In the vast majority of studies pertaining to the social sciences, CFA is utilized to both validate and determine the reliability of newly developed measurement scales [75]. Checking the validity of items ensures that they measure what they were designed to measure, while checking the reliability of items ensures that they do not contain any errors in the variables that they are measuring [76,77].

Studies have reported that convergent validity includes factor loadings > 0.60 and average variance extracted (AVE) > 0.5, while discriminant validity includes the Fornell–Larcker criteria [78–80]. Herein, CFA was employed, and it was found that the factor loading of each item was higher than 0.6, as per the suggested criteria [78–80]. Meanwhile, the AVE value for each factor was higher than 0.5, with traceability being 0.577, security and privacy being 0.614, trust being 0.676, acceptability being 0.538, and preparedness being 0.589. Finally, the convergent validity of the newly developed scale was demonstrated for the UAV-based SCM of security measures for mega sporting events.

The basic independent groups' model of CFA is typically utilized in estimating composite reliability. When conducting exploratory research, composite reliability values between 0.60 and 0.70 are considered acceptable; however, when conducting research at a more advanced stage, these values must be more than 0.70 [76]. Therefore, a score greater than 0.90 is not preferable, and a value of 0.95 or higher is undoubtedly not preferable [77]. Finally, this study ensured good composite reliability (CR) for each factor (Table 5).

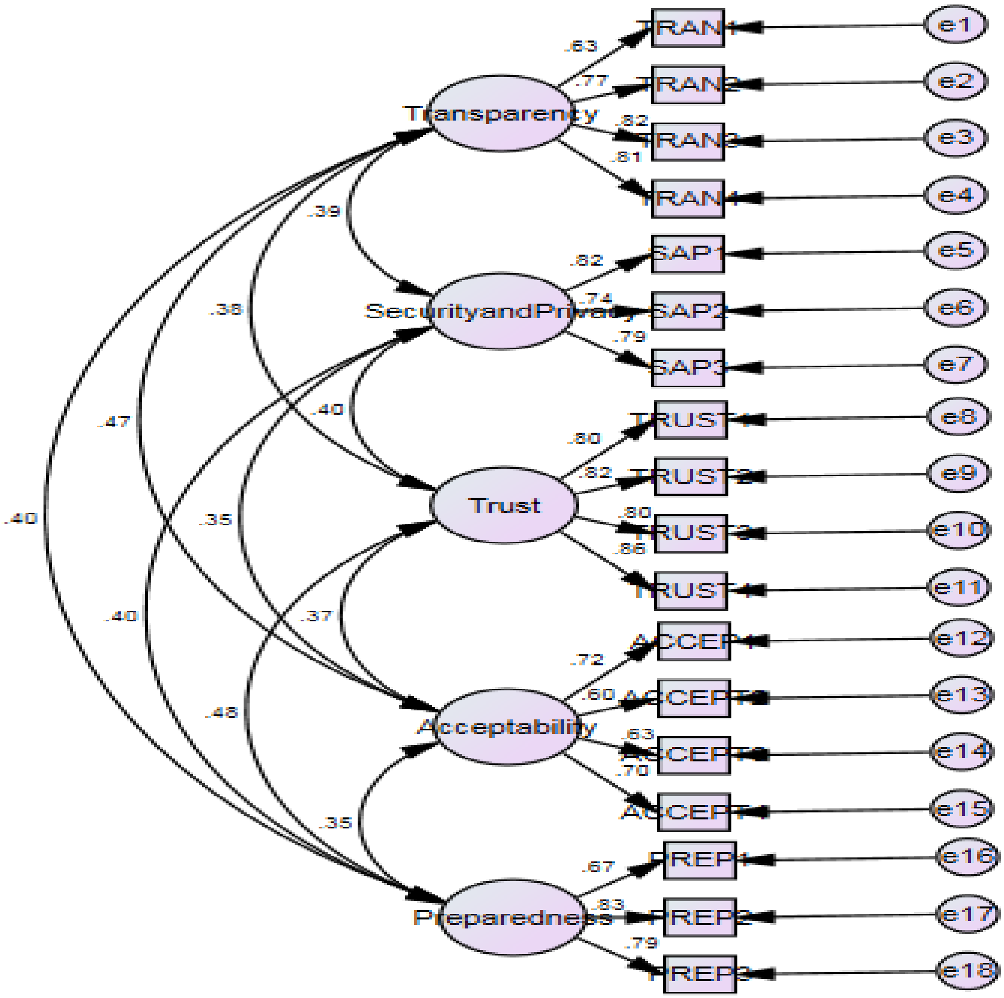

Figure 2. Confirmatory factor analysis (CFA).

Table 5. CFA results.

Factors	Items	Item Loading	Composite Reliability	Average Variance Extracted (AVE)
Traceability	TRAN1	0.627	0.844	0.577
	TRAN2	0.769		
	TRAN3	0.819		
	TRAN4	0.807		
Security and privacy	SAP1	0.820	0.826	0.614
	SAP2	0.737		
	SAP3	0.791		
Trust	TRUST1	0.804	0.893	0.676
	TRUST2	0.821		
	TRUST3	0.802		
	TRUST4	0.860		
Acceptability	ACCEPT1	0.717	0.756	0.538
	ACCEPT2	0.603		
	ACCEPT3	0.625		
	ACCEPT4	0.696		
Preparedness	PREP1	0.667	0.810	0.589
	PREP2	0.832		
	PREP3	0.794		

Discriminant validity was also tested using the Fornell–Larcker criteria [81]. In a nutshell, Fornell and Larcker [82] argued that the AVE ought to be higher than the variation between the construct in question and the other constructs included in the model (i.e., the squared correlation between two constructs). In this study, it was found that each factor of the UAV-based SCM had a higher value itself than the other factors in the same column, meaning that the discriminant criteria were also met (Table 6).

Table 6. Fornell–Larcker criteria.

	Preparedness	Traceability	Security and Privacy	Trust	Acceptability
Preparedness	**0.768**				
Traceability	0.404	**0.759**			
Security and Privacy	0.403	0.389	**0.783**		
Trust	0.480	0.380	0.395	**0.822**	
Acceptability	0.345	0.468	0.352	0.373	**0.662**

4.4. Model Fit Indices

Different values for the UAV-based supply chain model's fitness were determined. Some examples of fit indices are the comparable chi-square statistics (CMIN), the comparative fit index (CFI), the Tukey–Lewis index (TLI), and the root mean square error of approximation (RMSEA). The CFI is a confirmatory fit index, meaning values of CFI $\geq$ 0.95 and TLI $\geq$ 0.95 are the most frequently applied standards to determine whether or not a given model is a good fit [83,84]. Meanwhile, a CMIN value less than 0.03 indicates an excellent fit. According to one line of thinking, RMSEA values that fall between 0.05 and 0.08 are regarded as satisfactory, those that fall between 0.08 and 0.1 are considered marginal, and those greater than 0.1 are considered unacceptable [85]. (Table 7) meets the model fit indices, so there was good model fitness.

Table 7. Model fit indices.

Multi-Dimensionality of the UAV-Based SCM Model							
Indicators	***CMIN***	***RFI***	***NFI***	***TLI***	***CFI***	***RMSEA***	***p*-Value**
18	2.716	0.898	0.915	0.932	0.944	0.060	0.000

Notes: χ^2/df = chi-square ratio; GFI = goodness-of-fit index; CFI = comparative fit index; RMR = root mean; RMSEA = root-mean-square error approximation; NFI = normed fit; FL = factor loading.

5. Discussion

UAVs are now used to capture FIFA World Cup games in countries such as Qatar. The purpose of this study was to develop a UAV-based cybersecurity framework in order to ensure the SCM of security and safety measures in FIFA mega sporting events. The study was conducted in two stages, with the first stage focused on SLR and the second on developing and testing a UAV-based cybersecurity framework in FIFA mega sporting events. Using a survey questionnaire, the 66.85% response rate to the drone security survey indicates significant interest and relevance among IT professionals. The high rate may be due to the growing importance of drones in various industries and the need for robust security measures. The 33.15% non-response could be due to reasons like time constraints or lack of interest, or these individuals may not view drone security as a priority. The survey provides valuable insights into IT experts' opinions and experiences related to drone security. Understanding these perspectives is crucial for developing effective policies and practices as drone usage increases. Using this UAV-based framework, the potential benefits posed by UAVs will continue to diversify and intensify throughout the upcoming years. In this way, UAVs will frequently avoid detection due to their physical and operational qualities, which presents the community responsible for vital infrastructure with several issues [4,5]. Several studies have been conducted on using technology-based UAVs [7,8,20,21], UAV-based security supplies [4,10,11,15–17], and SCM 4.0 [1,3,5,12,18,21,24]. However, this study developed a valid and reliable UAV-based cybersecurity framework for FIFA mega sporting events. Furthermore, this study investigated the use of UAVs at mega sporting events from a supply chain perspective to explore the cybersecurity challenges at these events. A framework was proposed and developed across two stages. In the first stage, an SLR was conducted to identify the challenges and issues faced by UAVs based on the mega sports event supply chain. In the second phase, an empirical study was conducted using a survey questionnaire based on 20 of the previously identified challenges and issues from the SLR. These 20 items were categorized into five factors: Traceability, security and privacy, trust, acceptability, and preparedness. This study was conducted through statistical analysis that included EFA using IBM SPSS and CFA using IBM AMOS to ensure the validity and reliability of the newly developed framework. All five factors had good validity and reliability.

A good correlation was found among the factors of the UAV-based cybersecurity framework for mega sporting events. Traceability was found to be significantly and positively related to security and privacy (r = 0.389), trust (r = 0.380), acceptability (r = 0.468), and preparedness (r = 0.404). Security and privacy were significantly and positively related to trust (r = 0.395), acceptability (r = 0.352), and preparedness (r = 0.403). Trust was also positively and significantly related to acceptability (r = 0.373) and preparedness (r = 0.480). Finally, acceptability was positively and significantly related to preparedness (r = 0.345). This means that all five factors were significantly and positively correlated with one another, which will determine the security measures employed at mega sporting events. Such dependency also points to the complexity of managing such security systems and the importance of understanding the design and operation of FIFA mega sporting events.

5.1. Managerial Implications

The proposed framework offers some practical and managerial implications across the three stages for implementing UAVs (i.e., upstream, midstream, and downstream) of mega sporting events. They can be summarized as the flow of three stages at mega sporting events.

Upstream—According to the upstream stage, traceability plays the role of identifying weak areas that hackers/terrorists can use for attacks. Because of traceability, quality is necessary at each step of the process, and UAV navigation must have traceability in each activity that pertains to sports areas. UAVs could use such technology to trace cybersecurity threats. UAVs have undergone considerable technological advancements to their control units, sensors, and security options and have experience with significant traceable objects. Thus, UAVs have the potential to assist professional IT and security experts, such as those that must be completed consistently, to determine security needs and to maintain the traceability of a particular area. Using traceability sensors, it is possible to track drones that communicate using radio frequency, while, when using radar detection, it is possible to track drones that have been pre-programmed using GPS to travel to a specific location. The acceptability of UAV technology at mega sporting events for use in security operations is the second factor in the upstream stage, allowing users to implement it as part of the security measures. It has been estimated that delivery UAVs and users have an average acceptance rate of 62% across various industries. Acceptability is at the heart of research using a UAV-based supply chain. It is proposed that a user's perception of the danger posed by the operation of UAVs plays a role in whether or not they will accept the new technology. The results demonstrate that social and economic considerations are components of perceived risk, determining how users feel about using UAV technology as part of the security of mega sporting events. This proposal is pertinent to the present line of research examining social and economic issues regarding the use of UAVs. It implies a relationship between concerns and the adoption of UAVs, which has never been proposed.

Midstream—An analysis of the trust in using UAVs that are subsequently coupled with AI technology was performed with the assistance of a behavior-based and local scheme. Trust in a UAV-based supply chain model determines behavioral and local trust in adopting UAVs in the SCM at mega sporting events. UAVs with higher trust are considered legitimate devices and are granted permission to communicate and carry out surveillance within the network. In addition, the trust factor updates the technology and surveillance network, enabling regular analysis and monitoring of areas [86]. The goal is to establish confidence among all UAVs in the area while simultaneously monitoring the network and power levels of any adjacent UAVs to provide a more in-depth understanding of how security measures based on UAVs assist users and security managers in combating security threats and vulnerabilities caused by hackers, terrorists, and others by improving the core productivity of security practices in the UAV-based supply chain. Similarly, managers can improve their ability to predict supply through UAVs by embedding sensors into their containers, cars, and products. On the other side, the utilization of UAVs will potentially increase the traceability, security, and accuracy of transactions and collaboration between stakeholders in the supply chain.

Downstream—Preparedness is the last factor of the downstream stage, where it is necessary to implement UAVs in the supply chains of security and privacy measures. In this stage, managers and users prepare themselves to tackle the problems faced by sports organizers. This also helps managers to increase measures so that security and privacy measures are provided on time. Furthermore, managers and users ensure the safety and security of the public because they show their preparedness, skills, and capabilities with necessary security measures.

5.2. Limitations and Future Directions

This study has some limitations regarding the generalizability of adopting UAV-based cybersecurity systems at mega sporting events. First, the framework was developed and proposed with high emphasis on Qatar's recent FIFA events and other concerts and religious events, so whether and how it can be used in other contexts of supply and to maintain security practices are very important. Second, the proposed framework included five factors that are not exclusive, and other cybersecurity issues and challenges can be added in future work. This can include testing the behaviors of the public (i.e., satisfaction, awareness, and safety compliance) and the performance of security measures (i.e., sustainability performance, loyalty behaviors, and IT performance). Furthermore, future studies may use different dependent/outcome variables to check the effect of the included factors in the proposed framework. Future studies should be conducted on integrating AI and machine learning algorithms in UAVs, improving threat detection, analysis, and response capabilities, and enabling faster and more accurate real-time decision-making [87]. UAVs also become more prevalent; there is a growing need for counter-UAV systems to detect, track, and neutralize potential rogue drones that pose security threats during mega events [88].

6. Conclusions

The study concludes the findings that examined the UAV-based supply chain management of security measures for mega sporting events. The research utilized various statistical methods to analyze the data, ensuring the validity and reliability of the findings. The results demonstrated that no significant biases were present in the dataset, and the exploratory factor analysis supported the structure of the proposed model. The confirmatory factor analysis confirmed the convergent and discriminant validity of the measurement scale and the composite reliability of each factor. Furthermore, the model fit indices revealed that the proposed model demonstrated a satisfactory fit to the data. These findings contribute to understanding UAV-based supply chain management in the context of security for mega sporting events and provide valuable insights for future research and practical applications.

Author Contributions: Conceptualization, K.A.-D. and A.M.D.; methodology, K.A.-D. and A.M.D.; investigation, K.A.-D. and A.M.D.; writing original draft preparation, K.A.-D.; writing—review and editing, A.M.D.; supervision, M.K., N.O. and N.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data can be shared up on request.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Survey Questionnaire

Table A1. Survey questionnaire.

Demographic Variables		
Gender		1. Male 2. Female
Company nature		1. IT company 2. Security company
Company age		1. 1–5 years 2. 6–10 years 3. 11+ years
Working experience		1. Less than 1 year 2. 1–3 years 3. 4–6 years 4. More than 6 years
Number of employees		1. 10–20 2. 21–40 3. 41–60 4. 61+
Education level		1. 12 years of education 2. 14 years of education 3. 16 years of education 4. 18+ years of education
Survey Items		
Traceability	TRAN1	I support the use of drones for the safety and security of mega sporting events.
	TRAN2	I think drones should be traceable.
	TRAN3	A drone traces the information collected and stored.
	TRAN4	I ensure drones are regulated to ensure traceability.
	TRAN5	Drones share information with authorities or other stakeholders.
Security and privacy	SAP1	I am sure that drone operators respect your privacy during mega sporting events.
	SAP2	I trust the government to regulate drones to protect privacy and security at mega sporting events.
	SAP3	I believe that drones are equipped with privacy and security features, such as the ability to blur faces or license plates.
	SAP4	I am sure that drones are secured against hacking and other cyber threats at mega sporting events.
Trust	TRUST1	I trust drone operators to follow safety and security protocols at mega sporting events.
	TRUST2	I trust the government to regulate drones for safety and security at mega sporting events.
	TRUST3	I trust the technology used in drones to ensure their safe and secure operation at mega sporting events.
	TRUST4	I trust that drones are secured against hacking and other cyber threats.
Acceptability	ACCEPT1	I am comfortable with drones flying near mega sporting events.
	ACCEPT2	I support the use of drones for delivering security tools during mega sporting events.
	ACCEPT3	I keep using drones for search and rescue operations at mega sporting events.
	ACCEPT4	I keep trying to implement drones in international mega sporting events.
Preparedness	PREP1	I am confident that drones can ensure safety and responsibility at mega sporting events.
	PREP2	I am prepared to deal with concerns about using drones at mega sporting events.
	PREP3	I am confident in drones' ability to use technology for search and rescue missions or other emergencies.

References

1. Ardito, L.; Petruzzelli, A.M.; Panniello, U.; Garavelli, A.C. Towards Industry 4.0: Mapping digital technologies for supply chain management-marketing integration. *Bus. Process Manag. J.* **2018**, *25*, 323–346. [CrossRef]
2. Tiwari, S.; Wee, H.M.; Daryanto, Y. Big data analytics in supply chain management between 2010 and 2016: Insights to industries. *Comput. Ind. Eng.* **2018**, *115*, 319–330. [CrossRef]
3. Patnayakuni, R.; Rai, A.; Seth, N. Relational antecedents of information flow integration for supply chain coordination. *J. Manag. Inf. Syst.* **2006**, *23*, 13–49. [CrossRef]

4. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones' systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]
5. Yeboah-Ofori, A.; Islam, S.; Lee, S.W.; Shamszaman, Z.U.; Muhammad, K.; Altaf, M.; Al-Rakhami, M.S. Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access* **2021**, *9*, 94318–94337. [CrossRef]
6. Thakur, K.; Qiu, M.; Gai, K.; Ali, M.L. An investigation on cyber security threats and security models. In Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 3–5 November 2015; pp. 307–311.
7. Theodoropoulou, I.; Alos, J. Expect amazing! Branding Qatar as a sports tourism destination. *Vis. Commun.* **2020**, *19*, 13–43. [CrossRef]
8. Jago, L.; Dwyer, L.; Lipman, G.; van Lill, D.; Vorster, S. Optimising the potential of mega-events: An overview. *Int. J. Event Festiv. Manag.* **2010**, *1*, 220–237. [CrossRef]
9. Greig, A.W.; Guoth, N. Abandon Hope All Ye Who Practice Here: Soccer and Sport Space in 1920s Australia. In Proceedings of the Annual Conference of the Australian Sociological Association (TASA 2011), Newcastle, UK, 28 November–1 December 2011.
10. Cooper, B.; Chen, K.; Feist, Z.; Kapelke, C. *The Cybersecurity of Olympics Sports: New Opportunities, New Risks*; Center for Long-Term Cybersecurity: Berkeley, CA, USA, 2017.
11. Finkelstein, A. Cyber Security at Major Sporting Events. Israel Defense, December 2016. Available online: http://www.israeldefense.co.il/en/content/cyber-security-major-sporting-events (accessed on 7 December 2016).
12. Talavera, A.M.; Al-Ghamdi, S.G.; Koç, M. Sustainability in mega-events: Beyond Qatar 2022. *Sustainability* **2019**, *11*, 6407. [CrossRef]
13. Giulianotti, R.; Klauser, F. Introduction: Security and surveillance at sport mega events. *Urban Stud.* **2011**, *48*, 3157–3168. [CrossRef]
14. Fernández-Caramés, T.M.; Blanco-Novoa, O.; Froiz-Míguez, I.; Fraga-Lamas, P. Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors* **2019**, *19*, 2394. [CrossRef]
15. Hopkins, J.L. An investigation into emerging industry 4.0 technologies as drivers of supply chain innovation in Australia. *Comput. Ind.* **2021**, *125*, 103323. [CrossRef]
16. Raji, I.O.; Shevtshenko, E.; Rossi, T.; Strozzi, F. Industry 4.0 technologies as enablers of lean and agile supply chain strategies: An exploratory investigation. *Int. J. Logist. Manag.* **2021**, *32*, 1150–1189. [CrossRef]
17. Haji, M.; Kerbache, L.; Muhammad, M.; Al-Ansari, T. Roles of technology in improving perishable food supply chains. *Logistics* **2020**, *4*, 33. [CrossRef]
18. Abbas, Y.; Martinetti, A.; Moerman, J.J.; Hamberg, T.; van Dongen, L.A. Do you have confidence in how your rolling stock has been maintained? A blockchain-led knowledge-sharing platform for building trust between stakeholders. *Int. J. Inf. Manag.* **2020**, *55*, 102228. [CrossRef]
19. Roy, M.; Roy, A. Nexus of internet of things (IoT) and big data: Roadmap for smart management systems (SMgS). *IEEE Eng. Manag. Rev.* **2019**, *47*, 53–65. [CrossRef]
20. Büyüközkan, G.; Göçer, F. Digital Supply Chain: Literature review and a proposed framework for future research. *Comput. Ind.* **2018**, *97*, 157–177. [CrossRef]
21. Jahani, N.; Sepehri, A.; Vandchali, H.R.; Tirkolaee, E.B. Application of industry 4.0 in the procurement processes of supply chains: A systematic literature review. *Sustainability* **2021**, *13*, 7520. [CrossRef]
22. Liu, K.S.; Lin, M.H. Performance Assessment on the Application of Artificial Intelligence to Sustainable Supply Chain Management in the Construction Material Industry. *Sustainability* **2021**, *13*, 12767. [CrossRef]
23. Chen, Y.H.; Huang, L.C.; Lin, I.C.; Hwang, M.S. Research on the Secure Financial Surveillance Blockchain Systems. *Int. J. Netw. Secur.* **2020**, *22*, 708–716.
24. Li, X.; Sun, Y. Network Evolutionary Game-Based Diffusion Mechanism regarding the Nonperformance of Farmers in Agricultural Supply Chain Finance. *Discret. Dyn. Nat. Soc.* **2022**, *2022*, 8550974. [CrossRef]
25. Mukherjee, A.; Misra, S.; Chandra VS, P.; Obaidat, M.S. Resource-optimized multiarmed bandit-based offload path selection in edge UAV swarms. *IEEE Internet Things J.* **2018**, *6*, 4889–4896. [CrossRef]
26. Jiménez López, J.; Mulero-Pázmány, M. Drones for conservation in protected areas: Present and future. *Drones* **2019**, *3*, 10. [CrossRef]
27. Na, Z.; Liu, Y.; Shi, J.; Liu, C.; Gao, Z. UAV-supported clustered NOMA for 6G-enabled Internet of Things: Trajectory planning and resource allocation. *IEEE Internet Things J.* **2020**, *8*, 15041–15048. [CrossRef]
28. Aslam, J.; Saleem, A.; Khan, N.T.; Kim, Y.B. Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *J. Innov. Knowl.* **2021**, *6*, 124–134. [CrossRef]
29. Ganji, S.K. Leveraging the World Cup: Mega sporting events, human rights risk, and worker welfare reform in Qatar. *J. Migr. Hum. Secur.* **2016**, *4*, 221–259. [CrossRef]
30. Gupta, R.; Shukla, A.; Mehta, P.; Bhattacharya, P.; Tanwar, S.; Tyagi, S.; Kumar, N. Vahak: A blockchain-based outdoor delivery scheme using uav for healthcare 4.0 services. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 255–260.

31. Bhatti, B.M.; Mubarak, S.; Nagalingam, S. Information security implications of using NLP in IT outsourcing: A Diffusion of Innovation theory perspective. *Autom. Softw. Eng.* **2021**, *28*, 12. [CrossRef]
32. Kolini, F. Two heads are better than one: A theoretical model for cybersecurity intelligence sharing (CIS) between organisations. In Proceedings of the ACIS 2017: The 6th Asian Conference on Information Systems, Phnom Penh, Cambodia, 12–14 December 2017.
33. Nasser, A.L. Identification and prevention of expected cybersecurity threats during 2022 FIFA World Cup in Qatar. *J. Poverty Investig. Dev.* **2020**, *5*, 49–84.
34. Haghirian, M.; Robles-Gil, P. Soft Power and the 2022 World Cup in Qatar: Learning from Experiences of Past Mega-Sporting Event Hosts. *Tajseer J.* **2021**, *3*. [CrossRef]
35. Serdar, M.Z.; Al-Ghamdi, S.G. Resiliency assessment of road networks during mega sport events: The case of FIFA World Cup Qatar 2022. *Sustainability* **2021**, *13*, 12367. [CrossRef]
36. Ponzio, R.; Kiel, R.; Larik, J.; Petcu, C.; Swanson, J. *Reimagining Global Governance in a Multipolar World: Doha Forum 2019*; The Stimson Center: Doha, Qatar, 2019.
37. Lykou, G.; Moustakas, D.; Gritzalis, D. Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors* **2020**, *20*, 3537. [CrossRef]
38. Corona, B.; Shen, L.; Reike, D.; Carreón, J.R.; Worrell, E. Towards sustainable development through the circular economy—A review and critical assessment on current circularity metrics. *Resour. Conserv. Recycl.* **2019**, *151*, 104498. [CrossRef]
39. Schraven, D.; Bukvić, U.; Di Maio, F.; Hertogh, M. Circular transition: Changes and responsibilities in the Dutch stony material supply chain. *Resour. Conserv. Recycl.* **2019**, *150*, 104359. [CrossRef]
40. Ellen Macarthur Foundation. Towards the Circular Economy. 2013. Available online: https://www.ellenmacarthurfoundation.org/assets/downloads/publications/Ellen-MacArthur-Foundation-Towards-the-Circular-Economy-vol.1.pdf (accessed on 12 June 2013).
41. Bressanelli, G.; Perona, M.; Saccani, N. Challenges in supply chain redesign for the Circular Economy: A literature review and a multiple case study. *Int. J. Prod. Res.* **2019**, *57*, 7395–7422. [CrossRef]
42. Mangla, S.K.; Luthra, S.; Mishra, N.; Singh, A.; Rana, N.P.; Dora, M.; Dwivedi, Y. Barriers to effective circular supply chain management in a developing country context. *Prod. Plan. Control* **2018**, *29*, 551–569. [CrossRef]
43. Levering, R.; Vos, B. Organizational drivers and barriers to circular supply chain operations. In *Operations Management and Sustainability*; Palgrave Macmillan: Cham, Switzerland, 2019; pp. 43–66.
44. Saroha, M.; Garg, D.; Luthra, S. Key Issues and Challenges in Circular Supply Chain Management Implementation-A SystematicReview. *Int. J. Appl. Eng. Res.* **2018**, *13*, 91–104.
45. Pan, S.Y.; Du, M.A.; Huang, I.T.; Liu, I.H.; Chang, E.E.; Chiang, P.C. Strategies on implementation of waste-to-energy (WTE) supply chain for circular economy system: A review. *J. Clean. Prod.* **2015**, *108*, 409–421. [CrossRef]
46. Verboeket, V.; Krikke, H. The disruptive impact of additive manufacturing on supply chains: A literature study, conceptual framework and research agenda. *Comput. Ind.* **2019**, *111*, 91–107. [CrossRef]
47. Govindan, K.; Hasanagic, M. A systematic review on drivers, barriers, and practices towards circular economy: A supply chain perspective. *Int. J. Prod. Res.* **2018**, *56*, 278–311. [CrossRef]
48. Aggarwal, A.; Gupta, S.; Ojha, M.K. Evaluation of key challenges to industry 4.0 in Indian context: A DEMATEL approach. In *Advances in Industrial and Production Engineering*; Springer: Singapore, 2019; pp. 387–396.
49. Meisner, M. Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernic. J. Financ. Account.* **2017**, *6*, 63–73. [CrossRef]
50. Sahoo, S.; Mishra, S.; Peng, J.C.H.; Dragičević, T. A stealth cyber-attack detection strategy for DC microgrids. *IEEE Trans. Power Electron.* **2018**, *34*, 8162–8174. [CrossRef]
51. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2334–2360. [CrossRef]
52. Manesh, M.R.; Kaabouch, N. Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Comput. Secur.* **2019**, *85*, 386–401. [CrossRef]
53. Nguyen, T.; Tran, N.; Loven, L.; Partala, J.; Kechadi, M.T.; Pirttikangas, S. Privacy-aware blockchain innovation for 6G: Challenges and opportunities. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
54. Goda, M.P. Blockchain Enabled Vaccine Supply Chain Provenance. Master's Thesis, Penn State University, State College, PA, USA, 2021.
55. Creswell, J.W.; Creswell, J.D. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*; Sage Publications: Thousand Oaks, CA, USA, 2017.
56. Hart, A.G.; Carpenter, W.S.; Hlustik-Smith, E.; Reed, M.; Goodenough, A.E. Testing the potential of Twitter mining methods for data acquisition: Evaluating novel opportunities for ecological research in multiple taxa. *Methods Ecol. Evol.* **2018**, *9*, 2194–2205. [CrossRef]
57. Tranfield, D.; Denyer, D.; Smart, P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *Br. J. Manag.* **2003**, *14*, 207–222. [CrossRef]
58. Shelby, L.B.; Vaske, J.J. Understanding meta-analysis: A review of the methodological literature. *Leis. Sci.* **2008**, *30*, 96–110. [CrossRef]
59. Gorsuch, R.L. Exploratory factor analysis: Its role in item analysis. *J. Personal. Assess.* **1997**, *68*, 532–560. [CrossRef]

60. Kline, R.B. *Principles and Practice of Structural Equation Modelling*; Guilford Press: New York, NY, USA, 2011.
61. Shrestha, N. Factor analysis as a tool for survey analysis. *Am. J. Appl. Math. Stat.* **2021**, *9*, 4–11. [CrossRef]
62. Armstrong, J.S.; Overton, T.S. Estimating nonresponse bias in mail surveys. *J. Mark. Res.* **1977**, *14*, 396–402. [CrossRef]
63. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psychol.* **2003**, *88*, 879. [CrossRef]
64. Bag, S.; Yadav, G.; Dhamija, P.; Kataria, K.K. Key resources for industry 4.0 adoption and its effect on sustainable production and circular economy: An empirical study. *J. Clean. Prod.* **2021**, *281*, 125233. [CrossRef]
65. Osborne, J.W.; Costello, A.B.; Kellow, J.T. Best practices in exploratory factor analysis. In *Best Practices in Quantitative Methods*; Sage Publishers: Thousand Oaks, CA, USA, 2008; pp. 86–102. [CrossRef]
66. Shkeer, A.S.; Awang, Z. Exploring the items for measuring the marketing information system construct: An exploratory factor analysis. *Int. Rev. Manag. Mark.* **2019**, *9*, 87. [CrossRef]
67. Kaiser, H.F. An index of factorial simplicity. *Psychometrika* **1974**, *39*, 31–36. [CrossRef]
68. Polit, D.F.; Beck, C.T. *Resource Manual for Nursing Research: Generating and Assessing Evidence for Nursing Practice*, 10th ed.; Wolters Kluwer, Lippincott Williams & Wilkins: Philadelphia, PA, USA, 2012.
69. Hadi, N.U.; Abdullah, N.; Sentosa, I. An easy approach to exploratory factor analysis: Marketing perspective. *J. Educ. Soc. Res.* **2016**, *6*, 215.
70. Yong, A.G.; Pearce, S. A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutor. Quant. Methods Psychol.* **2013**, *9*, 79–94. [CrossRef]
71. Truong, Y.; McColl, R. Intrinsic motivations, self-esteem, and luxury goods consumption. *J. Retail. Consum. Serv.* **2011**, *18*, 555–561. [CrossRef]
72. McNeish, D. Thanks coefficient alpha, we'll take it from here. *Psychol. Methods* **2018**, *23*, 412. [CrossRef]
73. Trizano-Hermosilla, I.; Alvarado, J.M. Best alternatives to Cronbach's alpha reliability in realistic conditions: Congeneric and asymmetrical measurements. *Front. Psychol.* **2016**, *7*, 769. [CrossRef]
74. Kiliç, S. Cronbach's alpha reliability coefficient. *Psychiatry Behav. Sci.* **2016**, *6*, 47.
75. Bruyn, G.A.W.; Pineda, C.; Hernandez-Diaz, C.; Ventura-Rios, L.; Moya, C.; Garrido, J.; Groen, H.; Pena, A.; Espinosa, R.; Möller, I.; et al. Validity of ultrasonography and measures of adult shoulder function and reliability of ultrasonography in detecting shoulder synovitis in patients with rheumatoid arthritis using magnetic resonance imaging as a gold standard. *Arthritis Care Res.* **2010**, *62*, 1079–1086. [CrossRef]
76. Hair, J.F., Jr.; Sarstedt, M.; Hopkins, L.; Kuppelwieser, V.G. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *Eur. Bus. Rev.* **2014**, *26*, 106–121. [CrossRef]
77. Sarstedt, M.; Ringle, C.M.; Smith, D.; Reams, R.; Hair, J.F., Jr. Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. *J. Fam. Bus. Strategy* **2014**, *5*, 105–115. [CrossRef]
78. Arbuckle, J.L. *IBM SPSS Amos 20 User's Guide*; Amos Development Corporation, SPSS Inn: Crawfordville, FL, USA, 2010; Volume 635, pp. 226–229.
79. Sudarsono, B.; Tentama, F.; Ghozali, F.A. Employability Analysis of Students in Yogyakarta: Confirmatory Factor Analysis. *AL-ISHLAH J. Pendidik.* **2022**, *14*, 1451–1462. [CrossRef]
80. Hisham, R.; Ng, C.J.; Liew, S.M.; Lai, P.S.M.; Chia, Y.C.; Khoo, E.M.; Hanafi, N.S.; Othman, S.; Lee, P.Y.; Abdullah, K.L.; et al. Development and validation of the Evidence Based Medicine Questionnaire (EBMQ) to assess doctors' knowledge, practice and barriers regarding the implementation of evidence-based medicine in primary care. *BMC Fam. Pract.* **2018**, *19*, 98. [CrossRef]
81. Ab Hamid, M.R.; Sami, W.; Sidek, M.M. Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. *J. Phys. Conf. Ser.* **2017**, *890*, 012163.
82. Fornell, C.; Larcker, D.F. Structural equation models with unobservable variables and measurement error: Algebra and statistics. *J. Mark. Res.* **1981**, *18*, 382–388. [CrossRef]
83. Hu, L.T.; Bentler, P.M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Struct. Equ. Model. A Multidiscip. J.* **1999**, *6*, 1–55. [CrossRef]
84. West, S.G.; Taylor, A.B.; Wu, W. Model fit and model selection in structural equation modeling. *Handb. Struct. Equ. Model.* **2012**, *1*, 209–231.
85. Fabrigar, L.R.; MacCallum, R.C.; Wegener, D.T.; Strahan, E.J. Evaluating the use of exploratory factor analysis in psychological research. *Psychol. Methods* **1999**, *4*, 272–299. [CrossRef]
86. Catalini, C.; Gans, J.S. Some simple economics of the blockchain. *Commun. ACM* **2020**, *63*, 80–90. [CrossRef]
87. Bithas, P.S.; Michailidis, E.T.; Nomikos, N.; Vouyioukas, D.; Kanatas, A.G. A survey on machine-learning techniques for UAV-based communications. *Sensors* **2019**, *19*, 5170. [CrossRef]
88. Wang, J.; Liu, Y.; Song, H. Counter-unmanned aircraft system (s) (C-UAS): State of the art, challenges, and future trends. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 4–29. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.