Developing Guidance on The Responsible Use of Drones by Private Security Companies

MINT 317 Applied Research Project

Submitted in fulfilment of the requirements for the
Master in International and Development Studies

by
Leo Colonnello, Alice Iynedjian, Ebrima Touray

Faculty Lead: Souhaïl Belhadj-Klaz

Partner Organization: International Code of Conduct Association (ICoCA)

Geneva

May 16th 2025

Index

LITERATURE REVIEW

Introduction

The rapid advancement of Information and Communications Technologies (ICTs[1]) is transforming the private security sector, with Private Security Companies (PSCs) increasingly adopting new technologies, including drones, to expand and enhance their service offerings. However, the impact of these technological shifts on the private security sector is not fully understood, particularly in terms of the potential human rights implications. As ICTs, such as drones, are integrated into security practices, they introduce new risks, including privacy invasions and broader concerns about the impact of automated and data-driven technologies on individuals' rights (Buzatu, 2022). This is why this study seeks to address the following research question: **How are PSCs using drones, and what legal and regulatory frameworks govern their operations and current practices?**

The work will be divided into three main parts responding to the following research sub-questions:

1. How are PSCs utilizing drones?
2. What legal implications arise from drone use by PSCs?
3. What best practices, guidelines, and regulations currently exist regarding drone usage by PSCs?

These three sub-questions were originally outlined in ICoCA's mandate. However, for the purposes of scientific research, we reframed them into a single, overarching research question. This reframing also enabled us to formulate our central hypothesis: that the current operations and practices of PSCs involving drones are subject to minimal regulation at both national and international levels.

Although there is research on drone use by Private Military Companies, no studies have been focusing on their use by PSCs. Moreover, regulations specific to drone use by PSCs are currently scarce. This is why this study will address a critical gap in the literature, with the collection of primary data playing a key role in advancing understanding in this area. Through this research, we will examine the ways in which drones are employed by PSCs, evaluate the associated human rights risks, and highlight gaps in the regulatory landscape. By analysing existing legal frameworks and human rights standards and engaging with stakeholders involved in drone operations and governance, the study aims to provide insights into the responsible use of drones and propose recommendations for enhancing oversight and accountability in the private security sector.

[1] In the mapping study on the Use of Information Communications Technologies (ICTs) in Security Services provided by Commercial Actors (2022), ICTs are defined "as a diverse set of technological tools and resources used to capture, transmit, store, create, secure, damage, delete, share, analyze or exchange information. These technological tools and resources include but are not limited to their use in computers, the Internet and internet connected devices, software and apps used for intelligence gathering and analyzing, risk reduction/prevention and other security purposes, devices to capture biometrics, video surveillance, robotics, drones and telephony (fixed or mobile, satellite, GPS)" (Buzatu, 2022).

1. Definitions and Clarifications of Concepts.

1.1. Private Military Companies (PMCs).

Private Military Companies (PMCs) are corporate entities specializing in the provision of military services. Such firms operate as private businesses contracted by states, international organizations, corporations or Non-State-Actors (NSAs) to support or enhance military capabilities.

PMCs engage in roles such as military logistics, training for local and national forces, be it military or police, intelligence gathering, land, sea and air reconnaissance, manned or unmanned flight operation, material and technical support, and, in some cases, direct combat services. Examples include providing support for complex military machinery and the operation of sophisticated systems like missile defences (Analysis and Research Team, Council of the European Union, 2023; Arduino, 2023; Singer, 2005; Saner and al., 2019).

PMCs activities are not limited to defensive roles; they can also be contracted for offensive operations, which has been the case with Russian PMCs like Wagner in Ukraine (Analysis and Research Team, Council of the European Union, 2023) or Turkish PMC SADAT in Syria and in Nagorno-Karabakh (Arduino, 2023).

1.2. Private Security Companies (PSCs).

A useful characteristic to distinguish them from PMCs is their (geographical) area of operation, as PSCs typically operate in non-combat, defensive capacities and territories; they are used to guard installations, protecting personnel, and offering risk assessments. PSCs are businesses that offer protective and security services, focusing on the safety of individuals, property, and assets, particularly in volatile or high-risk environments. Their scope may also cover surveillance, intelligence for security purposes, and transport security, even in high-threat environments.

Even though the distinction between PMCs and PSCs can be useful, it is important to note how it can blur; indeed, many of these companies can offer both military and non-military security services. Moreover, many operations carried out by Security Companies, such as border control or protection of personnel, involve the use of military-grade equipment and gear, even in areas not classified as combat zones. A great example of such hybrid, multi-function equipment is drones, which can be modified so that they can take up both strictly military and non-military functions, regardless of their manufacturers' scope. This hybrid nature aligns with the broad scope of activities outlined in the International Code of Conduct for Private Security Service Providers (ICoCA, 2021, p.3), which acknowledges the role of PSCs in both civilian and military contexts, stating that these companies often support "relief, recovery, and reconstruction efforts, commercial business operations, diplomacy and military activity." (Arduino, 2023; Csernatoni, 2018; Saner and al., 2019).

1.3. Drones.

Unmanned Aerial Vehicles (UAVs), or drones**,** are remotely controlled or autonomous aircrafts equipped with advanced technological capabilities, including surveillance tools, weapons, and data collection devices, to support military, security, and civilian operations. Designed primarily for military use, drones are now used for a range of applications, from combat missions to intelligence gathering, due to their ability to operate without direct risk to human operators and perform tasks in hazardous environments. These machines blur the traditional boundaries between civilian policing and military combat, exemplifying the “war-police nexus” (Neocleous, 2013, cited in Csernatoni, 2018) by operating across different security contexts. They incorporate advanced sensors such as high-definition cameras, thermal imaging, and even facial recognition, allowing prolonged and discrete monitoring (Buzatu, 2022; Arduino, 2022; Cavoukian, 2012).

1.4. Internet of Things (IoT).

Drones are part of the broader Internet of Things (IoT), where "things" refer to devices and machines equipped with information-sensing technologies that allow them to be identified, tracked, and controlled through Internet connectivity (Tzafestas, 2018). Besides drones, machines also include robots, vehicles, and wearable sensors. Although IoT lacks a universally accepted definition (Rose and al., 2015), it generally describes an expansive ecosystem of "smart objects", devices, sensors, and machines that extend computational and network capabilities to a variety of physical and digital objects in fields such as industry, commerce, and personal use. Given the continuous expansion of this ecosystem, the need for increased regulation of smart objects has become more pressing, as well as more challenging. This research seeks to provide recommendations for specific regulations governing the use of drones.

By connecting through the internet and wireless networks, IoT devices can identify, track, communicate, and interact with one another and their surroundings, often requiring minimal human input (Rose and al., 2015; Ammar and al., 2018). IoT is a socio-technical system consisting of three main environments: (1) the physical environment, made up of human and non-human entities linked through a pervasive network; (2) the technological environment, encompassing hardware, software, networking technologies, and integrated platforms that enable data exchange and interaction; and (3) the socioeconomic environment, involving stakeholders such as business leaders, industry associations, government bodies, and consumers, who shape IoT’s growth, set standards, and ensure interoperability and security (Krotov, 2017). Together, these elements create a dynamic network that transforms static objects into intelligent agents capable of generating, sharing, and responding to real-time data, enhancing applications across sectors and enabling deeper integration with the physical world (Guillemin, 2009, as cited by Baldini and al.,2018; Tzafestas, 2018).

2. Use of Drones by PSCs.

2.1. The use of drones by PSCs.

PSCs utilize drones to perform a wide range of functions, including but not limited to aerial surveillance, mapping, inspection tasks, real-time monitoring, patrols, crowd control, event security, access control, intruder detection, search and rescue operations, evidence collection, decontamination, asset protection, facility security, traffic and route monitoring, crime detection and prevention, information sharing, and border surveillance and protection (Granieri, 2024). Granieri also highlights how, in the last ten years, advancements in drone technology have been quite remarkable, resulting in their extensive integration into various sectors and contexts that were previously not considered viable for their use. Moreover, PSCs are increasingly providing surveillance technologies and services, including surveillance-for-hire, which are marketed to both government agencies and private clients globally (Understanding Private Surveillance Providers and Technologies, DCAF-Geneva Centre for Security Sector Governance, 2024).

The influence of PSCs extends beyond operational roles. According to Lemberg-Pedersen (2013, as cited by Csernatoni, 2018), PSCs have played a pivotal role in shaping the governance and militarization of EU borders. This influence has raised critical concerns, such as the opacity of border security budgets, the challenges faced by public authorities in reversing border militarization driven by private actors, and the potential humanitarian repercussions for migrants. While these points do not specifically address drones, they underscore the significant role of PSCs, particularly those leveraging advanced technologies, in shaping border security policies and infrastructure. This likely entails deploying drones and other surveillance technologies in border management to identify migrants and collect and store their biometric data without obtaining consent.

Regarding the use of drones, as we will see in the following paragraphs, existing literature highlights that their increasing availability, particularly those equipped with lethal capabilities, has lowered the threshold for their deployment, including in scenarios involving the use of deadly force. This trend raises critical ethical and legal considerations surrounding their use by PSCs.

2.2. The human rights and ethical implications of the use of drones by PSCs.

Drones are capable of handling complex tasks, enhancing security, conducting surveillance, and collecting valuable information. However, their deployment may breach international and national regulations, such as : Article 17 of International Covenant on Civil and Political Rights (OHCHR, n.d.); Article 12 of the Universal Declaration of Human Rights (Nations, 1948); Article 16 on the Convention on the Rights of the Child (Convention on the Rights of the Child, 1990); Article 8 of the European Convention on Human Rights (European Court of Human Rights, 1953); General Data Protection Regulation (General Data Protection Regulation (GDPR) – Legal Text, 2016/679) which aims to protect data of EU citizens. These conventions and laws set standards and protection for the collection, processing and storing of peoples' data and stipulate the rights of people whose data are being utilized. They also provide a framework for member states for the formulations of legislatures and regulations that aim to protect and safeguard the rights of their citizens. These rights include right to privacy, family life and protection of personal data (Kutynska & Dei, 2023). Despite the existence of various domestic and international regulations, none specifically address PSCs or provide guidance on the regulation of their drone usage to prevent potential human rights violations.

The increased access and usage of drones comes with privacy and cyber security concerns. The backdrop of such concerns led to discussions and formulations of both legal and ethical standards to restrict and limit violations specific or attached to the usage of drones by various sectors for diverse reasons by both international and state authorities. Integral or constitutive to this crusade, is the International Civil Aviation Organization (ICAO), which is a specialized UN Agency assigned to handle the Convention on International Civil Aviation, commonly known as the Chicago Convention (Granieri, 2024). The importance of this study lies in its examination of available information on PSCs, focusing on specific human rights violations or risks associated with their use of drones. It also aims to develop targeted legal and ethical frameworks to regulate and monitor this use effectively.

2.2.1 Human rights implications of the use of drones by PSCs.

The widespread application of drones has been adopted in many spheres of human endeavours, including PSCs. However, due to the prolific usage of this technology concerns have been raised about the potential implication it may have on human rights. Kutynska and Dei (2023) point out that the primary issue with drone usage lies in its potential to violate privacy. Drones can record videos or collect personal data without an individual's consent, thereby creating significant risks to human rights.

Indeed, drone usage presents several potential risks to fundamental rights, including infringements on privacy and the protection of personal data, both of which are safeguarded by numerous international legal frameworks.

The right to privacy is recognized by both the UN General Assembly and the UN Human Rights Council as a fundamental element of a progressive democratic society. Although privacy is not an absolute right, it remains a critical one, and its violation can have a ripple effect on other essential rights, such as the right to a fair trial, and the freedoms of assembly and expression. It is protected under Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Therefore, all states that are signatories to such conventions or treaties are obliged to enact domestic laws that protect the right to privacy against any unauthorized or unsolicited interference without prior consent. According to DCAF (2024):

> *"The UN General Assembly highlighted that the rapid pace of technological development enables individuals all over the world to use new information and communications technologies, and at the same time, it enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular, the right to privacy."*

The use of drones by PSCs is no exception to the violations or potential violations of individual's rights - not only the right to privacy, but also the rights to freedom of expression, assembly, a fair trial, anonymity, and even the right to life, which is an absolute right guaranteed under both the ICCPR (Article 6) and the ECHR (Article 2). These concerns about the potential for human rights abuses associated with new technologies underscore the urgent need for robust scrutiny and regulation of such technologies, including drones, to ensure compatibility with international human rights standards.

In conclusion, the risk of actual or potential human rights violations through the use of drones is well-documented across a range of sources. The most prominent concern is the right to privacy and data protection, whose infringement often leads to further violations of other fundamental rights, such as freedom of expression, freedom of assembly, the right to life, and the protection of property. As noted in the DCAF report: "The rise of surveillance technologies and the increasing use of them by both the state and private surveillance companies pose a significant threat to the right to life" (Understanding Private Surveillance Providers and Technologies, DCAF - Geneva Centre for Security Sector Governance, 2024).

Although many human rights implications of drone use have been identified, there is a notable lack of research specifically examining the implications of drone usage by PSCs. The findings of this review suggest that most of the identified concerns are equally applicable to private security providers, indicating that their use of drones raises similar issues. A comprehensive review of existing literature revealed a clear gap in scholarly work focused on the human rights implications of drone use by PSCs. This underscores the importance and value of our assigned task in addressing and filling this gap in knowledge.

2.2.2. Ethical implications.

Drone surveillance, along with other forms of long-distance monitoring, raises a number of ethical concerns that must be considered throughout the execution process. This practice often leads to the objectification of surveillance targets by creating physical, moral, and ethical distances between the observer and the observed. Such distancing contributes to the bureaucratization and gamification of surveillance (Asaro, 2013; Coeckelbergh, 2013), which implies a lack of human empathy and the erosion of moral and psychological norms, issues that are particularly salient in the context of drone operations. Scholars such as Holmqvist (2013) have examined how drone surveillance reshapes humanity’s perceptions of both drone operators and the individuals being monitored. Marcuse (1998, as cited in Csernatoni, 2018) offered a critical perspective on this phenomenon, referring to a "happy conscience" among drone operators, a state in which guilt is successfully suppressed or forgotten. This detachment is facilitated by technological rationality, which enables individuals to carry out potentially harmful actions without remorse, as though they are immune from accountability and able to proceed unaffected (Csernatoni, 2018).

The involvement of drone technicians in border surveillance is shaped by techno-cultural mediation, influenced by operational instructions and scientific interpretation (Johnson, 1999). This reliance on drone technology is often perceived as a form of “scientific objectivity” (Haraway, 1991), fostering a belief in technological omniscience. However, such an understanding can obscure ethical concerns by institutionalizing “forms of blindness” (Johnson, 1999), where the assumption of technological rationality overrides essential human values. The ethical implications stem from this reliance, as the heavy dependence on drone surveillance risks dehumanizing those being monitored. It may diminish empathy and lead to decision-making driven primarily by data, often detached from moral accountability and considerations of justice. This dynamic increases the likelihood of reinforcing programmed biases and undermining the critical human judgment required in high-stakes environments such as border control (Csernatoni, 2018).

In combat and military operations, the accessibility and deployment of drones present a deeply troubling ethical and strategic landscape. As Peter Rudolf (2014) notes, drones pose no physical risk to their operators, thereby lowering the threshold for their use and increasing the likelihood of targeting individuals beyond those who strictly meet the criteria of necessity and proportionality. In contexts such as Yemen, for example, killings facilitated by the ease of drone strikes may occur in situations where alternatives (such as arrest) would require greater effort, coordination, and resources. The convenience and detachment associated with drone usage contribute to a morally ambiguous space, making it easier to justify actions that might otherwise be deemed unacceptable. This detachment from immediate human accountability fosters ethical complacency and a weakening of moral and legal constraints. These perspectives collectively underscore a significant concern: that drones, despite their technological sophistication and operational efficiency, can promote a disregard for the principles of proportionality, human dignity, and accountability. In both surveillance and military contexts, an overreliance on such technology risks undermining foundational ethical standards that are essential to preserving humanity in conflict and security operations.3. The existing regulatory framework on the use of Information and Communications Technologies (ICTs) by PSCs.

The use of advanced drone technologies brings up ethical and human rights issues, particularly concerning privacy, bias, and accountability (Buzatu, 2024). Despite these pressing issues, there is currently a notable lack of specific regulations governing drone usage by PSCs, leaving a significant gap in oversight. This underscores the urgent need for comprehensive research in this area. Our study is both timely and essential, as it seeks to address these regulatory and ethical voids. By examining the deployment of drones by PSCs, identifying associated human rights risks, and exploring regulatory shortcomings, our research aims to fill a critical gap in academic and policy discourse. Furthermore, this study will provide valuable insights to support the development of guidelines for the responsible and ethical use of drones by PSCs, fostering greater accountability and adherence to human rights standards.

3.1. The International Regulatory Framework.

Based on the literature analysed, it appears that no comprehensive body of international law or regulation specifically addresses the use of drones by PSCs. However, several legislative and regulatory frameworks do govern the use of Internet of Things (IoTs) and Information and Communication Technologies (ICTs) more broadly, as well as the protection of human rights and privacy, which are applicable to drones and their use by PSCs (Buzatu, 2024).

These regulations include, but are not limited to, the United Nations Guiding Principles on Business and Human Rights (UNGPs), the Voluntary Principles on Security and Human Rights, International Human Rights Law (IHRL), and International Humanitarian Law (IHL**)**, which provide a foundation for addressing human rights concerns in security operations (Buzatu, 2024).

Moreover, both international and national bodies have introduced legislation aimed at safeguarding data privacy and security. For instance, the EU’s General Data Protection Regulation (GDPR) imposes stringent requirements on the collection, processing, and storage of personal data, principles that are highly relevant to the use of drones for surveillance or data gathering by PSCs. These frameworks highlight the importance of protecting individuals' rights when ICTs are employed in security operations (Buzatu, 2024).

In addition to these legislative frameworks, multi-stakeholder initiatives such as the International Code of Conduct for Private Security Service Providers aim to regulate PSCs more directly. These initiatives advocate for accountability, transparency, and adherence to human rights standards within the private security sector, creating voluntary guidelines that PSCs can adopt. For example, the International Code of Conduct for Private Security Service Providers (ICoC) emphasizes the importance of privacy protections and the ethical use of surveillance technologies, principles that align with the broader regulatory needs for drones (ICoCA, 2021).

The present study, conducted in partnership with the International Code of Conduct Association (ICoCA), directly supports these objectives by providing a detailed analysis of drone use by PSCs, identifying human rights risks, and proposing recommendations to strengthen governance and accountability in alignment with ICoCA's mandate to promote responsible practices within the private security sector.

Nevertheless, none of the bodies of regulation specifically addresses the use of ICTs or drones by PSCs, leaving significant gaps in the international regulatory framework. This underscores the necessity of our study in addressing these gaps and contributing to the development of responsible and rights-respecting practices within the private security sector.

3.2. National Regulatory Framework.

National regulatory frameworks for drones differ significantly between regions. In the U.S., data protection regulations such as the California Consumer Privacy Act (California Consumer Privacy Act (CCPA) – State of California – Department of Justice – Office of the Attorney General, 2018) underscore the growing importance of privacy and security. Drone regulation involves federal, state, and local authorities, with local municipalities leveraging police power for regulatory functions. Federal definitions, such as the FAA Modernization and Reform Act of 2012, guide states like Indiana, which defines drones as human-operated UAS capable of remote or autonomous flight. The Federal Aviation Administration (FAA) oversees drone regulations, permitting recreational and commercial uses within federal and local boundaries. In Europe, the EU 2018/1139 framework, shaped by collaboration between the European Commission, EASA, and other aviation actors, establishes Europe as a global leader in comprehensive drone regulations. These ensure safe and sustainable operations across member states.

Literature on drone regulations predominantly focuses on civilian applications, with limited attention to PSCs. It remains unclear whether existing frameworks adequately address the use of drones by PSCs, highlighting a gap in regulatory discourse (Granieri, 2024; Brobst, 2020).

In conclusion, looking at the literature one can realize that only a limited number of research articles and studies about the use of drones by PSCs have been published, especially studies concerned on the activity of PSCs outside of armed conflicts. Furthermore, there appears to be no existing regulatory framework governing their use, whether national or international, suggesting that PSCs likely have significant freedom in how they deploy drones.

These gaps underscore the critical role of our project, which aims to assess the specific ways in which drones are utilized by PSCs, analyse the associated human rights risks, and identify the regulatory shortcomings in current frameworks. Building on this foundation, our methodology includes conducting interviews with industry representatives and human rights experts, as well as performing qualitative analyses to propose actionable guidelines. This comprehensive approach will not only address the academic void but also contribute to the development of responsible practices and governance models tailored to the unique challenges posed by drone technology in private security.

METHODOLOGY

The methodology was structured into three main phases. The initial phase included a continuous literature review conducted throughout the research process to contextualize the study, clarify its contribution to addressing the research question, and highlight the added value it will bring to three key areas: (1) academic research, (2) our partner ICoCA, and (3) the regulation of drone use by PSCs. Additionally, the literature review offered a critical analytical framework for the study. The second phase included interviews with both academic and policy experts from the field of human rights and international humanitarian law, as well as industry representatives from PSCs to collect primary data from those with insights into drone use and drone regulations. The third phase entailed qualitative analysis of the collected data, followed by the development of a final report with policy recommendations regarding the responsible use of drones.

1. Literature Review.

The academic and policy literature on drone use by PMSCs, along with the existing regulatory framework on the use of ICTs by PMSCs and PSCs, established the foundation for our research, informed the interview guide, and supported the development of guidelines on the responsible use of drones by PSCs for our partner ICoCA.

2. Data Collection (Interviews)

Given the scarcity of prior research on drone use by PSCs and the limited availability of guidance on their responsible application, we conducted 11 semi-structured interviews between February 25th, 2025, to April 3rd, 2025. Our experts came from different fields, mainly academic and policy experts in human rights and/or international humanitarian law, technology experts and industry representatives with direct knowledge of drone use within the PSC operations. This purposive sampling strategy was designed to gather primary tailored insights addressing our research objectives. Semi-structured interviews provided flexibility for participants to elaborate on both the operational and ethical dimensions of drone deployment. The selection of interviewees was informed by Buzatu's mapping study (2022), which identified key individuals with relevant expertise, and by a network that we developed both through referrals from initial interviewees and by participating in in-person events, such a consultative workshop on private security and ICTs hosted by ICoCA on March 26th 2025.

2.1. Recruitment Process and Coordination Challenges

Initially, we contacted participants via email invitations. However, we faced challenges in reaching some of the participants due to incorrect or missing email addresses and difficulty in securing responses. To improve the response rate, we contacted them through LinkedIn Premium to follow up with potential participants. This approach significantly increased engagement and allowed us to schedule key interviews that would have otherwise been missed.

To maintain logistic and communication efficiently, we used an Excel table to track:

- Contact status (invited, responded, confirmed, completed)
- Roles and affiliations
- Interview status and follow-up difficulties

These interviews provided qualitative insights into the use of drones, legal considerations, and ethical challenges of drone use and integration into the security service delivery of PSCs.

2.2. ICoCA Consultative Workshop on the Theme: “Ensuring the Responsible Use of Technology in Private Security”

ICoCA convened a two-day event comprising a consultative workshop which took place on the 26th and a Webinar on the 27th of March 2025 under the theme “Ensuring the Responsible Use of Technology in Private Security” which brought together legal, security and tech experts to hold discussions around the urgent need to develop better governance and regulations on the use of technology in the private security sector. The expert roundtable, featuring representatives from Think Tanks, Civil Society, Swiss Government Officials, Private Security Industry and independent legal experts, provided valuable insights into the evolving use of technology in the private security field. The event reinforced our research focus by highlighting the growing reliance on technology in private security operations, the associated human rights risks (especially around privacy and surveillance), the regulatory gaps across jurisdictions, the lack or insufficient definition of PSCs and their use of emerging technologies and digital transformation. The discussions were varied and revolved around new options for ICoCA, such as the possibility of expanding the definition of private security providers to tech companies and also explored the development and application of the ICoCA/ ICT4Peace toolkit as a practical guide for ethical use of technology in private security. These insights directly complement our interview findings.

Commentato [A1]: Add the main debates that took place during the workshop. for example one of them was : should ICoCA expend the definition of security services provider to tech companies

2.3. Interview Process and Data Handling: Ethical Protocols and Tools Utilised

Each interview lasted between 30 and 60 minutes and was conducted virtually via Webex or Zoom, recorded and then transcribed generated via *descript.com*. All this was done with written consent by the interviewees. The interview protocols were designed around the core themes of the research, with different sets of questions for each group (policy/academic experts and industry representatives) as outlined in the appendix. The initial questions were refined to be more discursive and thought provoking. Before each interview consent forms were provided and interview questions were handed to the interviewee, outlining the purpose of the research, their rights to anonymity and confidentiality, and the voluntary nature of their participation. Before analysing the transcripts, we have made use of ChatGPT to rephrased sentences that appeared unclear. On the other hand, NVivo was used in the qualitative analysis of the data and in assigning codes to categorise and discover themes, patterns and main concerns.

3. Data analysis.

This phase involved qualitative content analysis of the interview transcripts using the framework proposed by (Starks & Brown, 2007), involving decontextualization and recontextualization. First, the data is summarized and important parts highlighted and organized into themes. Then patterns across interviews were identified and restructured to align with the research question.

Each interview was first analysed separately from others, as each offered different perspectives and were asked distinct questions based on the group that the interviewee belongs to (academic/policy experts in human rights and/or international humanitarian law, technology experts and industry representatives). Insights from industry representatives mainly addressed the first research sub-question: *How are PSCs utilizing drones?* Conversely, inputs from human rights and policy experts widely informed the two remaining research sub-questions: *What legal implications arise from drone use by PSCs?* and *What best practices, guidelines, and regulations currently exist regarding drone usage by PSCs?*

Throughout our qualitative analysis, several key themes emerged, reflecting expert concerns and priorities around drone technology and its governance. For instance, experts frequently highlighted the need for better future regulations of drones in the private sector, expressed their concerns over the possible human rights violations of drone use and noted the lack of current regulatory systems.

FINDINGS

The final analysis provides insights to develop policy recommendations for the responsible use of drones. The final report will also include a practical guidance document to support PSCs in ethical and compliant drone use.

1. Use of Drones by PSCs.

1.1. Case study of South Africa's largest commercial drone service provider.

We will provide a detailed and relatively extensive depiction of the use of drones by PSCs using the case study of UAV & Drone Solutions (UDS), South Africa largest commercial drone service provider. Their Chief Operating Officer, Mr. Heiko Kühn, was kind enough to give us a deep overview of their operations (personal communication, April 7th, 2025). This contribution was particularly valuable, as South Africa is a country in which PSCs thrive, as they are used both for civilian protection and patrolling the vast mining complexes in the country. UAV & Drone Solutions works by providing and operating drones on behalf of other PSCs.

According to Mr. Kühn, drones are used to patrol state owned enterprises, pipelines, mines, railway infrastructure, lifestyle residential estates, industrial areas.

Drones have various advantages, including cost savings, better efficiency, getting access to roads that are not accessible by security vehicles, allowing them to survey larger areas, and diminishing the risk of collusion (e.g. foot patrollers accepting bribes by criminals).

Each client has its own privacy governance policy that the PSC follows in terms of data storage on the drone and in terms of the livestream data that they push through their closed servers. The drones they are using have standard built-in safety features, and they fly with geofences (mandated by the South African civil aviation).

Mr. Kühn presented two types of drones' training practices: piloting training which is part of the mandatory civil aviation training, followed by an internal safety training certified by PSIRA (South Africa's private security industry regulator). The drone training's aim is to teach pilots how to fly drones and how to react in case of an emergency. The safety training is meant to teach the pilots to understand their surroundings while they are flying, so that pilots know how to proceed when they encounter suspects. Concerning the civil aviation guidelines, drones' pilots are only allowed to fly over properties in areas where they have the landowner's permission. Any data that they received and any persons that appearing in the footage must remain the property of their client and may not be circulated.

We also discussed the AI integration into their drones' operations. Since most of their work comes from patrolling large mining areas, especially during the night, they believe the current state of AI technology is insufficient for their needs. They use facial recognition for special operations, and the only automated technology they currently use regularly is automated flight path planning for perimeter monitoring. Nevertheless, predicting that they will integrate AI into their operations more and more, as the technology evolves, they are currently involved in research and development focused on AI for object detection, particularly using thermal data to detect people and vehicles. Their collaboration for research is particularly resourceful, as their drones collectively fly 18,000+ hours a month, generating a significant amount of analytical data, not just footage, but metrics like crime timing, location, number of people involved, etc. This data can be fed into a database to develop predictive models.

1.2. Counter Drones Activities.

PSCs often must implement counter-drones' operations, because criminals have also begun using drones to identify the positions of security teams and locate valuable assets. Drones have also been deployed by other, less threatening actors, e.g. to capture footage of a VIP that a PSC oversees protecting. Due to legal restrictions, the technology PSCs can use is often limited to detection only. They are not allowed to jam signals or forcibly bring drones down, as this is a prerogative of the military or police forces. This is the case both in Europe and in South Africa, while in China, as pointed out by Dr. Arduino (personal communication, April 3rd, 2025), PSCs are hired by the police to do counter-drone activities in very crowded areas, where they also have the option of jamming drones.

According to Dr. Martins, senior researcher at the Peace Research Institute Oslo (personal communication, March 28th, 2025), counter-drone technology is generally divided into three categories.

1. Systems (such as radar and sensors) designed to detect whether a drone is trespassing a certain area.
2. Systems that not only detect drones but also act on the threat (most commonly through signal jamming).
3. Systems that neutralize drones through a kinetic use of force (typically restricted to law enforcement).

Even though PSCs are not allowed to bring drones down, the common practice behind counter-drones activities raises the question of the actual practices of PSCs and the blurring lines between law enforcement, military and PSCs' roles as security providers. Leander (2007) for example highlighted that security and military services in conflict situations could not be easily distinguished from one another. This is why she argues that "the institutional regulation covering the role of specialists in violence in public debate" should be revised (Leander, 2007, p.59). As will be pointed out later in the report, many experts share this concern.

1.3. Ukraine as a Laboratory of Drones.

As Dr. Martins highlighted, the war in Ukraine has been a major turning point in the use and development of drone and counter-drone technologies, particularly by private actors. According to him and to various reports, companies (particularly from the US) that produce drones and counter-drone technologies are actively using the Ukrainian battlefield to test and improve their systems. By deploying their tools in a live combat zone, they not only can refine them after they have been tested, but they also can advertise their products as "combat-tested," significantly boosting their market value.

This phenomenon usually works with companies “gifting” new technologies, such as drones, to the Ukrainian armed forces, and sending their own experts to operate these systems, which are often complex and difficult to handle. Therefore, many drone manufacturers, though not security providers in the traditional sense, are now effectively providing security functions on the ground in Ukraine. They do so under the guise of humanitarian or military support, often framed as donations, but with the actual goal of product testing and improvement. This points to the necessity to start considering drones manufacturers and other tech companies as security providers in the ICoC.

1.4. Drone Use in China.

Our interviews with Dr.Zhanggui, director of Institute for Overseas Safety and Security and ICoCA observer (personal communication, March 18th, 2025), and with prof. Alessandro Arduino (personal communication, April 3rd, 2025), affiliate lecturer at Lau China Institute King's College London and expert on Chinese private security, led us to include a small section on the use of drones in China. According to Dr. Zhanggui, drone usage in China is highly differentiated depending on the operator. While government and military actors operate with broader discretion, PSCs are subject to far stricter oversight: for instance, only one state-owned PSC in each of China’s 34 provinces is authorized to carry firearms and perform sensitive tasks such as bank security or money transport. Privately owned PSCs are usually not allowed to use weapons, but they utilize drones for purposes like surveillance and patrol, although restricted to designated zones pre-approved by the Department of Public Security.

In China, drones and robots (often fully autonomous and AI driven) are widely used, and they are often operated by PSCs. As prof. Arduino noted, this means that vast amounts of data, including visual recordings and operational metrics, is gathered and stored by PSCs. However, these activities typically involve significant governmental oversight; in China, every company with more than 600 employees is required to host a Chinese Communist Party cell, meaning that even nominally private enterprises are closely linked to the state. Therefore, the Chinese government is actively trying to integrate this massive amount of data, which is now of critical importance to their national security.

While we are not devoting a section on this topic, we want to highlight that both Prof. Maslen (personal communication, March 17th, 2025) and prof. Arduino have both emphasized the use of drones in maritime settings. Maslen noted that recent technological advances have made drones particularly valuable for maritime protection of commercial vessels, especially in regions like the Gulf of Aden, where many companies rely on PSCs despite the continued presence of state-operated security.

2. Legal implications of the use of drones by PSCs

2.1. Insights on Risks Associated with Integrating Drones into PSCs Operations.

As noted by Charlie Mayne (personal communication, March 5th, 2025), the human rights implications of drone use largely depend on their function and whether they are operating in peacetime. Whether drones are armed with lethal or less-lethal capabilities, or used solely for surveillance, each application raises distinct concerns. While all forms of drone use involve important issues, the most serious arise when PSCs deploy drones to use force, due to the potential for civilian harm, an increased likelihood of violence, and possible violations of the right to life and the right to protection from inhuman or degrading treatment.

When drones are used for surveillance, our interviewees emphasized privacy-related concerns. In this section, we will examine both categories of issues in greater detail.

Regarding the use of drones by PSCs for force, Dr. Clapham stressed that such use could heighten the likelihood of violence, as drone operators do not face personal risk. Consequently, they may be more prone to using force than personnel on the ground, as they are detached from the immediate consequences of their actions. Dr. Clapham also argued that drones cannot perceive the fear of death they provoke. In essence, sending a human being to carry out an execution or a massacre is fundamentally different from remotely operating a drone from thousands of miles away.

In connection with the fear of death, many of our interviewees expressed concern about the psychological impact of drones. Dr. Zhanggui noted that in certain regions, particularly in parts of Africa, drones provoke widespread fear and apprehension among local communities. These fears highlight broader risks, especially in areas with histories of violence or weak governance.

On privacy-related concerns, Mr. Mayne pointed out the risk of data misuse when drones capture footage of individuals going about their daily lives. He emphasized that even in conflict-related operations where companies are not directly engaged in combat, the use of such technologies still presents significant ethical and legal risks.

Another risk, highlighted by Dr. Arduino, involves cross-border data management. He explained that if a Chinese PSC uses Chinese-manufactured drones in Africa, stores the data on Chinese servers, and a third-party international company accesses that data, the situation could be considered a form of espionage.

Finally, although every human rights expert we interviewed acknowledged the cost-saving benefits of drones, they also cautioned that replacing local security personnel with unmanned systems introduces significant operational and ethical challenges.

2.2. Integrating AI into PSC Drone Use and Emerging Risks.

The use of AI in PSCs' drones can exacerbate privacy issues by enabling more sophisticated surveillance and data collection without consent. AI-powered drones can gather detailed information about individuals and locations, raising significant privacy concerns. Furthermore, the opacity of AI decision-making creates a "black box" environment in which the system's responses are not fully understood, posing additional risks.

Dr. Martins described predictive AI as a form of artificial intelligence that forecasts future events based on past patterns. While he acknowledged that AI could facilitate facial recognition, and thereby, in theory, support the principle of distinction, a key tenet of international humanitarian law requiring differentiation between civilian and non-civilian targets, it also carries the risk of reinforcing existing biases, both in civilian contexts and in conflict zones. He referenced the European Union's AI Act, which classifies AI technologies along a risk spectrum. The Act imposes varying levels of regulation depending on the assessed risk, ranging from minimal oversight for low-risk AI to outright bans on high-risk applications. For Dr. Martins, this approach underscores the need for nuanced, risk-based governance in the development and deployment of AI systems.

A doctoral researcher specialized in the civilian regulation of drones (personal anonymous communication, March 17th, 2025) explained the technical distinction between automation and autonomy in drone systems. Automation involves pre-programmed actions, where the drone follows a set of instructions without human intervention, and its behaviour is predetermined. Autonomy, by contrast, incorporates an element of self-determination: the drone is granted the flexibility to make certain decisions independently, especially in response to unforeseen situations, based on incoming data. Autonomous systems can learn from the patterns and data they collect, adjusting their behaviour accordingly. This learning capacity is central to autonomy, whereas automation does not necessarily involve any learning, it is more rigid and predefined.

However, categorizing drone systems as either automated or autonomous is challenging. Machine learning models can enable self-determined actions characteristic of autonomy, while other AI techniques support automation. This complexity blurs the lines between the two categories. In the commercial drone industry, this leads to confusion and sometimes misleading marketing. Companies often advertise their drones as fully autonomous, but these systems remain heavily pre-programmed, with only limited autonomous capabilities. The label "autonomous" is marketable, even when it does not accurately reflect a drone's actual functionality.

The same interviewee also highlighted risks related to drone sensors. Drones rely on a multitude of sensors, and the more sensors they contain, the greater the number of potential failure points or entry points for intrusion. Additionally, the use of radio frequencies raises telecommunications challenges, such as spectrum allocation and interference, which may result in cyber vulnerabilities.

Given the high risks associated with AI in drone systems, ICoCA should consider recommending that its member companies buy long-range, high-tech video cameras for routine surveillance tasks instead of drones. These cameras are generally less alarming to local populations, as they are stationary, pole-mounted, and more familiar, thus less intrusive. However, the primary barrier is cost (D. Brooks, personal communication, March 5th, 2025): while a high-quality drone costs approximately $4,000, a long-range thermal camera typically starts at around $20,000 (C. Mayne, personal communication, March 5th, 2025).

3. Existing best practices, guidance and regulation on the use of drones by PSCs

3.1. Existing Legal and Regulatory Frameworks.

PSCs operate under varied legal systems, often within grey areas. As outlined in our literature review and supported by expert interviews, there is no comprehensive international legal framework specifically regulating drone use by PSCs. Instead, applicable rules must be pieced together from legislation on civil aviation, data privacy, and AI, an approach made clearer through the two national cases studied.

3.1.1. China.

As Dr. Zhanggui explained, China's 2024 Interim Regulations on the Flight Management of Unmanned Vehicles cover drone classification, flight permits, and pilot registration. Like similar EU laws, this applies broadly to commercial drones, not PSC-specific use. A step towards regulating PSCs specifically came in 2023 GBT 42765/2023 (a modified adaptation of ISO 18788:2015), aimed at improving management systems and professionalization across PSC operations.

Similarly, China adopted the Cybersecurity Law and Personal Information Protection Law, closely modelled on the EU's GDPR. According to Dr. Zhanggui, these laws reflect an effort to align with global privacy standards.

3.1.2. Italy and the EU.

Senior officials from the Milan Police Department (personal communication, March 25th, 2025) shared insights into their drone program. In Italy, both police and commercial drone use fall under national and EU aviation and data laws. Aviation wise, operators must comply with ENAC (Italy's Civil Aviation Authority), which enforces EASA (European Union Aviation Safety Agency) regulations. Relevant EU regulations include Delegated Regulations 2019/945 and 2019/947.

In Europe, drones are divided into three categories – Open, Specific and Certified. Each category requires different certifications, and they are further split into seven classes (C0 - C6) by weight and scope of use. Generally, drones are restricted from flying over large crowds. Drone use by PSCs is also regulated by data privacy laws, such as the GDPR, and bodies like the EDPB (European Data Protection Board) and Domestic Data Protection Authorities.

3.1.3. Use of Force.

The legal framework for drone-enabled use of force by PSCs remains unclear and underdeveloped. As Professor Maslen noted, there is no consensus on whether Human Rights Law and International Humanitarian Law apply to PSCs only when contracted by states or also when acting for private actors. In conflict areas, in particular, such dangers mount. As Professor Clapham pointed out, multiple studies have shown how the use of drones in times of conflicts increases the risk of escalation and violence, and this can also lead to breaching Human Rights Law and International Humanitarian Law. At the same time, as seen in the ongoing Ukraine War, cheap drones manufactured for civilian purposes can be easily modified to be combat-ready, for example by enabling them to carry IEDs on their payload.

3.1.4. Recommendations.

ICoCA's current scope does not sufficiently address technology. Interview data suggest the Code of Conduct should be updated to cover drones, AI, and other surveillance technology, in order to cover the existing legal gaps. We also recommend expanding the definition of Private Security providers to include those companies, such as tech companies, testing warfare technology in conflict areas while providing military aid to the parties in conflict.

PSCs should abstain from drones' modifications and comply with national and international regulations. They should also be aware of the legal risks of having their drones stolen in such scenarios and used for unlawful purposes (Privacy International, n.d., personal communications with various experts, February – April 2025).

3.2. Impact assessment.

3.2.1. Fear-factor on Impacted Communities.

Studies (Edney-Brown, 2019; Hijazi and al., 2018) and experts' opinions guard against the use of drones in conflict and post-conflict areas for patrolling and surveillance purposes. Civilians previously exposed to drone violence often associate drone sounds and visuals with imminent danger, triggering anxiety and fear, sometimes causing them to change their living habits in fear of being targeted. These dynamic risks alienating communities and undermining the legitimacy of PSC operations.

3.2.2. Law Enforcement Mimicry and Overstepping Perimeters.

According to Mr. Mayne, PSCs sometimes emulate law enforcement practices without proper legal authority or oversight. This is more likely to happen where regulations are weak or client instructions and requests are vague, leading PSCs to misinterpret their role or boundaries, thus risking human rights violations.

Numerous interviewees highlighted the risks of PSCs emulating law enforcement's drone practice. The 1990 Basic Principles on the Use of Force and Firearms by Law Enforcement Officials do not cover PSCs, as they do not hold constabulary powers such as arrest or detention. The issue complicates when PSCs are equipped with potentially lethal drone technologies, raising difficult questions about oversight, proportionality, and accountability in both national and international legal frameworks.

A common example involves drones being used for perimeter patrolling, when drones may extend their surveillance outside their clients' property. While EDPB regulations allow incidental capture of passers-by, processing, storing, or sharing such data is prohibited. Images should be blurred and promptly deleted. In our opinion, this regulation creates room for misuse, and it raises concerns about the retainment and deletion of the footage and the data. In such cases, PSCs should adopt human rights best practices and consult relevant guidelines (e.g. Buzatu, 2022).

3.2.3. Recommendations.

Prior to deployment, PSCs should assess the psychological and contextual impact of drone use. Failure to do so may lead to human rights violations and legal consequences. Moreover, engagement with local communities and civil society is advised to assess the real-world impact of drone operations and mitigate potential harm. Where existing regulations are unclear or absent, PSCs and regulatory bodies like ICoCA could develop dedicated operational standards, rather than relying on law enforcement models that may be legally and ethically inappropriate.

3.3. AI Use and Best Practice.

Due to current limitations of the technology, such as false positives, AI should be used by PSCs to support, not replace, human decision-making. AI tools (e.g., for object detection or perimeter alerts) can assist operators, but final decisions should rest with trained personnel.

Fully and semi-autonomous systems should not operate in particularly high-risk or populated environments, where errors could lead to serious consequences. Facial recognition or behavioural analysis should not be conducted onboard drones. Instead, data should be encrypted and transmitted to secure ground stations. This approach reduces the risk of unauthorized data access and ensures compliance with data protection regulations such as the GDPR.

As noted by Dr. Martins, many systems marketed as “autonomous” are in fact only partially automated. PSCs must accurately disclose the capabilities and limitations of their systems to clients or regulators. Clear documentation should be maintained for all AI tools, including their training data sources, limitations, and known error rates. PSCs may use AI to analyse aggregated drone data to identify crime trends or security vulnerabilities (e.g., peak times for trespassing or theft).

However, as facial recognition and behavioural analysis still have noticeable failure rates, and AI systems can be hacked to enforce malicious biases, these systems must be carefully monitored and handled, and PSCs must monitor AI outputs and avoid over-policing based on flawed data.

Indeed, AI-integrated drones are part of a vulnerable Internet-of-Things (IoT) ecosystem. Robust cybersecurity measures are necessary and should be checked with the manufacturer, such as encrypted communications, secure firmware and regular updates and protection against jamming, data hacking and remote interferences.

3.4. Other Best Practices.

3.4.1. Operator Training.

Operator training must be mandatory and legally grounded. For commercial purposes, the UK, South Africa and EU require licensed pilots with extensive training, this could be a global best practice. Ethical and privacy considerations should also be included in the training.

Responsible use of drones training should emphasize avoidance of surveillance creep, wildlife harm, and privacy violations, as well as acknowledging and preventing psychological harm from the "fear factor", especially in post-conflict zones (personal communications with various experts, February - April 2025).

Recommendations: ICoCA and related bodies could create modular training guidelines addressing drone-specific risks, ethical code of conducts and procedures to deal with operators breaching such policies (B. Martins, personal communication, March 28th, 2025).

3.4.2. Transparency.

Experts lament that there is little to no reporting on PSCs drone incidents, especially regarding Human Rights violations. Internal accountability appears to be weak, and whistleblowing is rare (C. Mayne, personal communication, March 5th, 2025). Moreover, companies often are not clear whether they use drones or anti-drones' technology, in which settings and how they manage them.

Recommendations*:* ICoCA's partner companies should be more transparent on their use of drones and AI related technologies, as well as their data handling and purposes. This allows for greater accountability and control.

3.4.3. Manufacturing Standards.

Companies should be encouraged to carefully consider their drones' manufacturers. A lot of issues that can arise from the use of drones can be prevented by certain design features, which should be robust enough to prevent hacking and overriding attempts. ICoCA could create a list of required manufacturing standards for its partners, with features including (but not limited to):

- **Geofencing**: Geofencing prevents drones from entering restricted areas, which might include out-of-perimeter zones, areas with crowds or critical infrastructure; if an operator tries to breach a restricted area, the attempt should also be automatically recorded and sent to the authorities.

- **Encryption and Logging**: Drones should encrypt their data and maintain flight logs for forensic investigations. As demonstrated by both private security providers and law enforcement agencies, all onboard data, such as footage saved to SD cards should be encrypted to prevent unauthorized access if a drone is lost or compromised. Sensitive data processing (e.g., facial recognition) should never occur on the drone itself. Instead, as used in secure deployments, footage should be transmitted via intranet or secured telemetry to a central control room for processing and storage. In cases where internet streaming is necessary, it must go directly to the client's encrypted, password-protected server, bypassing third-party or operator systems, to minimize security vulnerabilities and ensure compliance with data protection regulations.

- **Fail-safes and monitoring**: Drones should have return-to-home functions and real-time monitoring capabilities to minimise accidents, ensure accountability and damage control when malfunctioning occurs.

CONCLUSION

This seminal research project was launched under the clearly defined mandate of identifying the best practices for the use of drones by PSCs; its declared goal was informing recommendations that the International Code of Conduct Association (ICoCA) might offer to its members, as well as potential updates to its Code of Conduct. From inception to execution, the project was therefore designed to be practical, grounded, and policy-relevant, shaped by ICoCA's commitment to accountability, oversight, and human rights in the private security sector.

What began as a focused inquiry into drone operations has evolved into a broader exploration of how emerging technologies - from artificial intelligence to automation - are entering the commercial security domain. In this sense, drones, our research object, revealed themselves as a gateway technology: emblematic of the wider challenges and regulatory gaps associated with digital transformation in private security. Through literature review, primary interviews, and expert consultation, the research has outlined both promising practices and critical risks, particularly in relation to data governance, psychological impacts, regulatory vacuums, and blurred boundaries between law enforcement, military, and private actors.

While the scope of the inquiry has expanded in insight and recommendation potential, it remains preliminary. It is not intended to resolve broader or more philosophical questions about the future of security technology - such as whether drones should be banned, or whether AI-based surveillance should be strictly curtailed. These are legitimate, urgent debates, and many of our findings intersect with them. However, such questions fall outside the intended scope of this study.

Instead, this research offers an initial, applied contribution: a foundation for targeted ethical and operational guidance, tailored specifically to the needs and responsibilities of PSCs and the regulatory frameworks - current and potential - that govern them. As technologies advance, so too must the frameworks for accountability. In this current environment, given the scarcity of specific regulation on drone use by PSCs, the role of regulatory bodies like ICoCA - especially given its multi-stakeholder composition - is crucial in ensuring and promoting respect for human rights without alienating those who yield the greatest influence over the adoption of best practices. We hope this project serves as a useful step in that direction.

**Word count: 9396*

REFERENCES

1. AI-powered tools

In the development and writing of this research, AI-powered tools were used to support the refinement of language and ensure grammatical accuracy. The use of these tools was intended to improve the clarity and coherence of the writing, without impacting the originality or analytical content of the work. The follow tools were used:

- OpenAI – ChatGPT was used to rephrase some sentences to enhance flow and grammar. This helped make the research clear, easy to read, and professionally presented.
- Descript.com was used to generate the transcripts from the recordings of the interview.

The core research ideas, methodologies, analyses, and conclusions remain entirely the authors' original work. Any text generated by AI was critically reviewed and modified by the authors to align with the specific goals and requirement of the ARP.

2. Primary Data

Analysis and Research Team, Council of the European Union. (2023). *The Business of War – Growing risks from Private Military Companies*.

Buzatu, A.-M. (2022). *From boots on the ground to bytes in cyberspace: A mapping study on the use of ICTs in security services by commercial actors*. Geneva: ICT4Peace Publishing.

Buzatu, A.-M. (2024). *Tool 8: Emerging technologies and future trends in private security* (ICoCA, ICT4Peace). Geneva: ICT4Peace Foundation. https://ict4peace.org/activities/launch-of-toolkit-from-boots-on-the-ground-to-bytes-in-cyberspace/

California Consumer Privacy Act (CCPA) | State of California—Department of Justice—Office of the Attorney General. (2018). https://oag.ca.gov/privacy/ccpa

Convention on the Rights of the Child. (1990). OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

European Court of Human Rights. (1953). *European Convention on Human Rights*.

General Data Protection Regulation (GDPR) – Legal Text. (2016). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

ICoCA. (2021, December 10). *INTERNATIONAL CODE OF CONDUCT.* https://icoca.ch/the-code/

Nations, U. (1948). *Universal Declaration of Human Rights*. United Nations; United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

OHCHR. (n.d.). *International Covenant on Civil and Political Rights*. OHCHR. Retrieved December 2, 2024, from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Privacy International. (n.d.). *Drones Surveillance*. https://privacyinternational.org/learn/drones-surveillance

Understanding private surveillance providers and technologies | DCAF – Geneva Centre for Security Sector Governance. (2024). https://www.dcaf.ch/understanding-private-surveillance-providers-and-technologies

3. Secondary Data

3.1. Books.

Arduino, A. (with McFate, S.). (2023). *Money for Mayhem: Mercenaries, Private Military Companies, Drones, and the Future of War* (1st ed). Rowman & Littlefield Publishers, Incorporated.

3.2. Academic articles.

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications, 38*, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

Analysis and Research Team, Council of the European Union. (2023). *The business of war – Growing risks from private military companies*.

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical design in the Internet of Things. *Science and Engineering Ethics, 24*(3), 905–925. https://doi.org/10.1007/s11948-016-9754-5

Brobst, J. A. (2020). Enhanced civil rights in home rule jurisdictions: Newly emerging UAS/drone use ordinances. *West Virginia Law Review, 122*, 741–782. Available at SSRN: https://ssrn.com/abstract=3575216

Cavoukian, A. (2012). *Privacy and drones: Unmanned aerial vehicles*. Office of the Information and Privacy Commissioner of Ontario.

Csernatoni, R. (2018). Constructing the EU's high-tech borders: FRONTEX and dual-use drones for border management. *European Security, 27*(2), 175–200. https://doi.org/10.1080/09662839.2018.1481396

Edney-Browne, A. (2019), The Psychosocial Effects of Drone Violence: Social Isolation, Self-Objectification, and Depoliticization. Political Psychology, 40: 1341-1356. https://doi.org/10.1111/pops.12629

Granieri, F. (2024). Navigating the skies: A cross-country exploration of drone policies in Europe, USA and China, unveiling privacy and cybersecurity challenges. *Journal of Law, Market & Innovation, 4*(2). https://doi.org/10.13135/2785-7867/10740

Hijazi, Alaa & Hall, Harold & Hovee, Mark & Ferraro, Feliciano & Schreiber, Sher. (2019). Psychological Dimensions of Drone Warfare. Current Psychology. 38. 10.1007/s12144-017-9684-7.

Krotov, V. (2017). The Internet of Things and new business opportunities. *Business Horizons, 60*(6), 831–841. https://doi.org/10.1016/j.bushor.2017.07.009

Kutynska, A., & Dei, M. (2023). Legal regulation of the use of drones: Human rights and privacy challenges. *Journal of International Legal Communication, 8*(1), 39–55. https://doi.org/10.32612/uw.27201643.2023.8.pp.39-55

Leander, A. (2007). Regulating the role of private military companies in shaping security and politics. In S. Chesterman & C. Lehnardt (Eds.), *From mercenaries to market: The rise and regulation of private military companies* (pp. [insert page range if known]). Oxford University press. https://doi.org/10.1093/acprof:oso/9780199228485.003.0004

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: An overview*. Internet Society.

Saner, R., Uchegbu, A., & Yiu, L. (2019). Private military and security companies: Legal and political ambiguities impacting the global governance of warfare in public arenas. *Asia Pacific Journal of Public Administration, 41*(2), 63–71. https://doi.org/10.1080/23276665.2019.1622325

Singer, P. W. (2005). Outsourcing war. *Foreign Affairs, 84*(2), 119–119.

Starks, H., & Brown Trinidad, S. (2007). Choose your method: A comparison of phenomenology, discourse analysis, and grounded theory. *Qualitative Health Research, 17*(10), 1372–1380. https://doi.org/10.1177/1049732307307031

Tzafestas, S. G. (2018). Ethics and law in the Internet of Things world. *Smart Cities, 1*(1), Article 1. https://doi.org/10.3390/smartcities1010006

Appendix.

A. Semi-structured interview guide for policy/academic experts in human rights

Interview details

1. Interviewee Name
2. Position/Role
3. Date
4. Interviewer Name

Introduction:

Thank you very much for accepting our invitation so quickly and for generously sharing your expertise with us. We are truly grateful for your participation.

To briefly introduce our Applied Research Project, we are conducting a study mandated by the International Code of Conduct Association (ICoCA), with Professor Vincent Bernard serving as our stakeholder representative. During the previous semester, we developed our literature review and research methodology. From this initial phase, we identified a significant gap in existing research concerning the use of drones by PSCs. The scarcity of available studies has led us to conclude that collecting primary data will be essential to understanding this emerging practice. Our data collection focuses on two key groups:

- Industry representatives - to gain insights into how drones are currently used within the private security sector.
- Academic and policy experts in human rights, international humanitarian law and defense technology - to gather expert opinions on the responsible and ethical use of drones by PSCs.

In reviewing the existing literature, it became clear that very few academic articles or studies specifically address the use of drones by PSCs, particularly in contexts outside of armed conflicts. Moreover, no comprehensive regulatory framework, whether national or international, seems to exist to govern their use. This regulatory void suggests that PSCs may currently enjoy considerable flexibility in how they deploy drone technology.

These gaps underscore the importance of our project. Our primary objectives are to:

- Assess the specific ways drones are used by PSCs.
- Analyze the associated human rights risks.
- Identify regulatory shortcomings in current legal and policy frameworks.

Interview Questions:

HUMAN RIGHTS EXPERTS

1. Challenges of PSC Drone Use & IoT Integration – What are the main risks associated with integrating drones into PSCs operations, and their broader implications, including potential ethical, security, and societal concerns? What role can organizations like ICoCA play in mitigating these risks?

2. Legal & Regulatory Gaps – What international and national legal frameworks currently govern PSC drone operations, and where do you see the most significant gaps or ambiguities?
3. Best Practices & Accountability – What concrete measures (technical, operational, or training-related) are essential to ensuring that PSCs use drones responsibly and transparently? For example, what do you think about operators keeping in mind the fear factor associated with drones in conflict or post-conflict areas?
4. Comparative Insights – How do PSC drone practices differ from military or law enforcement drone operations, and what lessons can be drawn to improve private security standards?
5. Reform & Future Directions – What key reforms (legal, technological, or operational) would you propose to enhance the ethical and responsible use of drones by PSCs?

INDUSTRY REPRESENTATIVES

1. Does your company currently use drones? For what specific activities or tasks are they employed (e.g., surveillance, perimeter security, logistics), and what advantages do they bring?
2. What advantages does drone technology bring to your operations? What risks does it bring?
3. Which regulatory frameworks guide your drone operations (international, national, or self-regulatory), both from an aviation and privacy point of view? Do you have to modify your operations with drones depending on the country of operation?
4. How do you address data protection and privacy concerns, especially if your drones record personal or sensitive information? Do you have internal policies on storing, sharing, or deleting such data?
5. What does drones operators' training entail in terms of safety protocols, and especially legal/ethical guidelines? Would you be comfortable with sharing your training protocol, if existing, with us?
6. Have you ever had any incident concerning drones that you feel comfortable sharing? Do you have specific grievance mechanisms? Could you talk us through it?
7. Do you think that the industry needs further and stricter regulation to ensure human rights best practice on drone use? What would be the first steps in terms of internal regulations or ICoCA Implementation? Are there particular gaps, such as data privacy, operator training, or public transparency, that you feel need more attention?
8. What obstacles do PSCs face in adopting best practices for drone operations, and how can these challenges be overcome?

AI/TECH EXPERTS

1. How does the use of AI in PSC drones exacerbate issues of privacy rights?
2. What about human rights abuses, particularly in areas with weak regulatory oversight?
3. To what extent does AI-powered drone surveillance risk reinforce biases in security operations? Would you make a distinction between conflict/post conflict/high risk areas and safer areas?

4. How vulnerable are AI-powered drones to hacking, data breaches, or manipulation, and what could be the worst-case scenarios if these systems are compromised?
5. Are current AI regulations and ethical guidelines sufficient to prevent abuse in PSC drone operations, or is there a risk of AI-driven surveillance outpacing legal protections?
6. What key reforms (legal, technological, or operational) would you propose to enhance the ethical and responsible use of drones by PSCs?

B. List of Interviewees

Actors/Individuals	Position	Reason for inclusion	Time of the interview
Andrew Clapham	Professor of International Law at the Geneva Graduate Institute, Former Member of Advisory Group of ICoCA.	Prof. Clapham is an expert in International Human Rights Law, International Humanitarian Law, Laws of War.	February 25th 2025
Stuart Maslen	Visiting Professor at the University of Johannesburg.	Prof. Maslen is an expert in Human Rights Law, International Humanitarian Law, disarmament law, jus ad bellum, international criminal law, and the protection of civilians under international law.	March 17th 2025
Zhou Zhanggui	Member of Advisory Group of ICoCA and Director of Institute for Overseas at Zhejiang University.	Dr. Zhou is an expert in overseas safety and security, security risk assessment, hydro-politics, energy security, as well as other non-traditional security issues.	March 18th 2025
Doctoral researcher specialized in the civilian regulation of drones.	Research Institute situated in Europe.		March 17th 2025
A senior cybersecurity and cyber threat expert	University located in Switzerland.		March 31st 2025
Doug Brooks	Special Advisor/Responsible Business Practices at The Fund for Peace.	Mr. Brooks has thorough experience with private sector in security firms.	March 5th 2025
Charlie Mayne	Former Member of Advisory Committee at ICoCA, Former CEO and co-founder of VSC Security Solutions, Managing Director of Omnio Services.	Former industry board representative. For 8 years, Mr. Mayne, as CEO of VSC, was providing responsible security solutions in complex environments in line with ICoCA.	March 5th 2025
Senior Officers from Milan Police Department, Italy	Police Department of Milan, Italy.	These officers were interviewed due to their involvement into the newly formed drones' program for Italian police to provide insights into the police use of drones.	March 25th 2025
Bruno Oliveira Martins	Senior Researcher at the Peace Research Institute Oslo and associate researcher at the Institute of National Defense in Lisbon.	Dr. Martins is working on different projects on emerging security technologies.	March 28th 2025

Alessandro Arduino	Advisory Committee Member of ICoCA, Affiliate lecturer at Lau China Institute, Visiting Professor King’s College London.	Prof. Arduino is an expert in private military and security companies, cyber security combat UAVs, and China’s political economy in Africa, the Middle East, and Central Asia.	April 3rd 2025
Heico Kühn	Chief Operation Officer at UAV & Drones Solutions.	Mr. Kühn is an industry representative.	April 7th 2025