Navigating the Legal and Governance Implications of Private Contractors in Drone Surveillance Operations

Sarah Smith
Legal Specialist, TRIISA Group
October 3, 2024

The use of private contractors in national security operations has raised critical questions in both legal and governance arenas. As emerging technologies such as autonomous drones become integral to military and intelligence functions, the lines between state and private actor roles have become increasingly blurred.

Although these issues continue to evolve, today we discuss legal challenges surrounding the use of private contractors in government-funded drone surveillance operations, exploring the implications for state accountability, liability, and evolving regulatory frameworks.

The Legal Gray Area: State Action and Private Contractors

One of the most pressing legal issues concerning private contractors in surveillance operations is the question of state action. When a private entity receives substantial government funding and conducts operations closely aligned with national security interests, the boundaries between private and state action can become unclear. The key

question is whether these private contractors' activities can be attributed to the state under international law.

Traditionally, international law has focused on the principle of attribution—the process of determining when the actions of a private entity can be considered actions of a state. The International Law Commission's Articles on State Responsibility for Internationally Wrongful Acts (2001) outline when this attribution is possible, especially when private actors are either directly instructed or controlled by a state. However, in practice, the situation is more nuanced.

In the case of private contractors conducting drone surveillance, the traditional tests of effective control (requiring direct oversight over specific actions) and overall control (which might allow for broader influence without direct involvement) often fall short of addressing the complex and fluid nature of private-state relationships. This creates ambiguity for contractors who may not be directly controlled by the government but are still heavily integrated with state objectives through funding, operational overlap, and the use of government-developed technologies.

Emerging legal interpretations, such as the "functional state actor" doctrine, offer an evolving perspective on this issue. Under this approach, private contractors involved in surveillance operations may be treated as functional state actors based on their economic and operational dependence on the government. This analysis acknowledges that, despite a lack of formal control, contractors' activities often align with state objectives and support national security efforts. As a result, even in the absence of explicit state direction, contractors may be held accountable for actions that would typically fall under the state's responsibility.

Legal and Governance Risks: Accountability, Liability, and Compliance

The growing reliance on private contractors for drone surveillance brings with it significant legal and governance risks. First and foremost, if contractors are deemed to

be functioning as state actors, they could face direct liability for violations of international law, such as human rights abuses or breaches of sovereignty. These risks are particularly pronounced in international contexts where contractors operate in foreign territories under ambiguous legal frameworks. For example, contractors may be vulnerable to lawsuits under the Alien Tort Statute (ATS) for alleged violations of international human rights, even if the actions themselves were carried out without direct government oversight.

Additionally, the increasing use of autonomous drones in surveillance operations presents its own set of legal challenges. Autonomous technologies often operate with minimal human intervention, raising questions about the accountability for actions taken by these systems. As drones become more capable of independent action, determining liability for unintended consequences—such as violations of privacy or unlawful surveillance—becomes increasingly complicated.

On the regulatory front, private contractors also face complex compliance challenges. As contractors work with government-funded technologies, they must navigate strict export control laws, dual-use technology regulations, and evolving data protection requirements. Missteps in regulatory compliance could result in significant legal exposure or fines, particularly as international bodies continue to develop frameworks for the governance of emerging technologies.

Mitigating Legal Exposure: Strategic Recommendations for Contractors

Given the evolving legal landscape, private contractors must adopt proactive strategies to mitigate legal exposure and ensure compliance. Key to this effort is maintaining a clear operational separation from government activities. While contractors may receive substantial funding, it is crucial for them to establish frameworks that allow for greater independence in decision-making and operations. For instance, developing independent technological capabilities and decision-making protocols can help mitigate concerns about undue government influence.

Moreover, contractors should actively pursue funding diversification to reduce their reliance on government contracts. By expanding into commercial markets or seeking international partnerships, contractors can help safeguard against risks associated with government dependence.

In addition to operational strategies, legal safeguards such as clear contractual provisions defining the boundaries of government control and ensuring indemnification against potential claims are essential. Contractors should also implement rigorous compliance frameworks, including privacy protocols and human rights impact assessments, to demonstrate their commitment to ethical practices in drone surveillance operations.

Adapting to the Future of National Security and Legal Accountability

As emerging technologies reshape national security and defense landscapes, private contractors are playing an increasingly central role. The legal complexities surrounding their activities require ongoing attention and adaptation. While the question of state action remains unresolved in many instances, evolving legal doctrines such as the functional state actor theory suggest that contractors may be treated as state actors in certain circumstances, carrying significant legal and governance implications.

For contractors, the key to navigating this uncertain terrain lies in adopting flexible strategies that balance operational effectiveness with a commitment to legal and ethical standards. **As the regulatory environment continues to evolve, contractors will need to stay ahead of legal risks by proactively addressing accountability, compliance, and governance challenges in their operations.** By doing so, they can help shape the future of national security in a way that aligns with both technological progress and the rule of law.

As this issue continues to evolve, we must continuously adapt our strategies and legal frameworks to ensure operational effectiveness while also remaining legally accountable and subject to appropriate oversight.

Facing Emerging Tech Challenges? Let TRIISA Group Be Your Guide.

If your organization is grappling with the evolving intersection of technology, law, and operations, TRIISA Group is here to help. Our team provides the insight and expertise you need to navigate the evolving landscape of cyber capabilities, surveillance technologies, and more. From risk assessment and regulatory compliance to operational integration and strategic planning, we offer comprehensive consulting services that guide you through today's most pressing challenges.

Reach out to TRIISA Group today to explore how our expert consulting services can help your organization address the critical issues that are reshaping your industry.