

The CLOSE PROTECTION & SECURITY JOURNAL

Custodi Civitatem Per Sapientiam!

Volume 2, Issue 2

Published by the International Protective Security Board
December 2024



Editor-in-Chief Treston Wheat, PhD (Insight Forward)

Editorial Board Members Charles Randolph (Ontic), Fred Burton (Ontic), Charles Tobin (AT-RISK International), Rachael Frost (Frost ICED), and Samantha Newbery, PhD (University of Salford)

The International Protective Security Board is an independent, volunteer organization devoted to promoting the protection industry's interests and professionalization.



Contents

- Letter from the Editors 3
- Research Articles 6
 - Creating a Discipline: Theory Building and Research Methods for *Private Security Studies* 7
 - Navigating Complexity: A Structured Approach to Travel Risk Management 21
- Professional Articles 41
 - Impact of an Incident: Risk to Executives 42
 - Synopsis of the IPSB’s Risk Intelligence and Protection Symposium, London, 10 October 2024 48
 - T-ray Imaging: Emerging Technologies to Combat Increasingly Dangerous Threats Concealed in Mail and Everyday Items 51
 - Enhancing Last Mile Security: A Guide for Executive Protection Companies Partnering with Secure Global Ground Transportation Services 58
 - The Last Mile: Ensuring Seamless and Secure Execution 59
- Book Reviews 63
 - The Use of Informants on Terrorism in a “Quagmire”. A Review of: Samantha Newbery, *Terrorist Informers in Northern Ireland*, Oxford University Press. 64
 - Book Review - *Beyond States and Spies: The Security Intelligence Services of the Private Sector* by Lewis Sage-Passant, Edinburgh University Press 70
- Submitting to the Journal 75



Letter from the Editors

In December 2024, the International Protective Security Board hosted the Close Protection Conference (CPC) in Nashville, Tennessee. This event took place only a few days after the assassination of the UnitedHealthcare CEO by an individual with a personal grudge and political motivations. Many important conversations were had about that watershed moment and what it meant for the industry. Simultaneously, protectors were responding to media requests about the issue and providing the security profession's perspective. There were also pertinent dialogs on everything from protecting high-net-worth individuals and celebrities to tactical discussions on appropriate equipment to protective intelligence to active shooter data to geopolitics for the security professional.

The Close Protection and Security Journal wants to continue those dialogues and provide relevant information and research that would help prevent senseless violence like that assassination. As always, it is a privilege to bring together the voices of academic researchers and professionals who are shaping the ever-evolving field of private security. This journal exists as a bridge between theory and practice, a space where rigorous research meets the nuanced realities of those working on the front lines of security every day.

The dialogue between academia and industry professionals is vital. Academic researchers offer the analytical tools, frameworks, and long-term perspectives that help us make sense of complex security challenges. Meanwhile, professionals provide invaluable insights from the field, grounded in experience and real-world application. It is through these conversations that we refine best practices, innovate solutions, and elevate the standards of our industry. As security professionals, staying informed about the latest developments in our field is not just beneficial; it is essential. The private security landscape is dynamic, shaped by technological advances, geopolitical shifts, and emerging risks. To navigate these challenges effectively, we must engage with the latest thinking and explore diverse perspectives. That is why we have dedicated space in this edition to book reviews. These reviews highlight recent publications that are not only relevant to private security but also provide valuable insights into broader issues such as risk management, ethics, and organizational resilience.

Thank you for being part of this ongoing conversation. Your engagement—as readers, contributors, and practitioners—ensures that the journal remains a relevant and impactful resource for our community. Together, we can continue to advance the field of private security and address the challenges of tomorrow with insight, resilience, and innovation.

Treston Wheat, PhD
Editor-in-Chief, CPSJ

Charles Randolph
Fred Burton
Charles Tobin
Rachael Frost
Samantha Newbery, PhD
Editorial Staff Members, CPSJ



TAKE A CLOSER LOOK.

AT  RISK

JOIN US AT BOOTH #118

PROTECTION • INVESTIGATIONS • CONSULTING • INTELLIGENCE • TRAINING

at-riskinternational.com

CRISIS24 | PRIVATE
STRATEGIC
GROUP

TOTAL PROTECTION
WITH NO COMPROMISE

UNPACK WHAT IS POSSIBLE. FOCUS ON WHAT MATTERS IN LIFE.
LEAVE THE REST TO US.

www.crisis24.com/psg



Trusted by thousands of individuals, family offices, and enterprise security teams, including **20 of the Fortune 100 companies** in the United States, with their **Digital Executive Protection** needs.

To learn more, contact us at info@360privacy.io

Creating a Discipline: Theory Building and Research Methods for *Private Security Studies*

Treston Wheat, PhD

Introduction

Private security is an old practice, with historical examples ranging from personal bodyguards for monarchs and merchants to mercenary forces employed by city-states. Throughout history, private actors have played critical roles in protecting individuals, assets, and interests in contexts where state authority was weak, absent, or insufficient, especially in the United States. Despite this long legacy, the modern profession of private security remains relatively inchoate, and even more so as an academic discipline. While its practices have grown in sophistication and scale—shaping everything from corporate risk management to conflict zone operations—private security has yet to receive the same level of theoretical development and scholarly attention as public-sector security fields like law enforcement, intelligence analysis, or military studies.

In today's globalized and increasingly privatized security landscape, private security actors are indispensable, addressing risks that state agencies cannot manage alone. The expansion of private security into areas such as close protection, event security, corporate investigations, protective intelligence, and cybersecurity highlights the growing need for structured academic inquiry. Yet, despite its widespread use and economic significance, private security remains understudied, lacking a unified framework to analyze its practices, impacts, and ethical challenges. Therefore, the private security profession needs to establish an independent academic discipline that fills this gap by providing a dedicated space to examine the roles, theories, and research methodologies necessary to understand private security in its entirety.

This essay will outline the foundations of that new discipline, emphasizing the need for its own theoretical frameworks while drawing inspiration from related fields such as international relations, criminology, behavioral threat assessment, intelligence studies, and criminal justice. Additionally, it will explore how qualitative and quantitative research methods can be applied to build a robust body of knowledge. Ultimately, the goal is to establish a discipline as a legitimate and vital field of inquiry that bridges theory and practice, addressing the unique challenges to the industry.

What's in a Name? The New Discipline of *Private Security Studies*

In creating a discipline, the first major step is nomenclature, that is naming the discipline. This is what helps establish the scope of what is being studied. For example, political science is so called because it is the “scientific” study of the political sphere, or one can see the difference between macroeconomics, microeconomics, and political economy. Naming what the industry is and what academics will research is not an easy task, though. Every term within the security profession denotes a particular kind of practice. Consider the extremely small sample of these terms:

- **Close Protection:** Close protection refers to the physical security and personal safety of individuals who may be at risk due to their prominence, profession, or circumstances. It involves deploying



trained security personnel, often referred to as bodyguards, to ensure the safety of the client through risk assessment, planning, and mitigation of threats in real time.

- **Executive Protection:** Executive protection is a specialized form of security focused on safeguarding high-profile individuals such as corporate executives, political leaders, and celebrities. It encompasses close protection but also includes advance security planning, secure transportation, venue reconnaissance, and crisis management to mitigate risks associated with travel, public appearances, or day-to-day operations.
- **Travel Security:** Travel security involves measures and protocols to ensure the safety of individuals while traveling, especially in high-risk regions. It includes pre-travel risk assessments, itinerary planning, secure transportation, monitoring of evolving threats, emergency response planning, and evacuation support if needed.
- **Corporate Security:** Corporate security refers to the strategies and measures an organization implements to protect its personnel, assets, operations, and reputation from risks. This includes physical security (access controls, surveillance systems), cybersecurity, crisis management, risk assessments, business continuity planning, and protection against fraud, espionage, or workplace violence.
- **Intelligence Analysis:** Intelligence analysis is the process of collecting, evaluating, and interpreting information to produce actionable insights. Analysts synthesize data from various sources to assess risks, trends, or threats, enabling decision-makers to make informed strategic or operational decisions.

None of these terms adequately contain all the aspects of what the security profession does, which means that any name established for the discipline would need to be as broad and eclectic as possible. The discipline would need to include the above-mentioned terms along with everything from mail screening, event security, risk management, evacuations, investigations, asset protection, and so many more aspects of security. Therefore, this essay proposes calling the discipline of what this journal studies and assesses *Private Security Studies* to separate it from the other major academic disciplines, such as international relations, security studies, criminology, and intelligence studies.

Private Security Studies is the interdisciplinary academic field focused on the systematic study, analysis, and development of theories, practices, and strategies within the private security sector. This discipline examines the roles, functions, and impact of non-governmental security entities. This discipline examines the roles, functions, best practices, and impact of non-governmental security entities by analyzing their operational practices, strategic importance, and evolving responsibilities in safeguarding individuals, organizations, and assets. Additionally, the discipline investigates their influence on global security dynamics, their contributions to individual, corporate, and humanitarian resilience, and the ethical, legal, and regulatory challenges they face in diverse operational environments. It explores how these entities provide critical services often filling gaps left by public security agencies, including but not limited to close protection, executive protection, travel security, event security, risk management, investigations, corporate security, red teaming, political risk analysis, and intelligence analysis. It integrates knowledge from fields such as criminology, business management, international relations, security studies,



intelligence studies, sociology, psychology, and risk analysis to address the growing complexities of private-sector security in a globalized, risk-prone world.

Why A New Discipline

There are several reasons that *Private Security Studies* ought to become a separate discipline to those that already exist. While public security (law enforcement, military, and government intelligence) has been well-established in academic discourse, the private security sector—which increasingly complements and, at times, surpasses public security efforts—remains under-researched. *Private Security Studies* would provide an academic foundation to explore its role in modern security ecosystems. It would do so by combining frameworks with real-world applications to better prepare professionals, policymakers, and scholars by focusing on evidence-based practices, risk assessments, and innovative solutions to private security challenges.

Interestingly, this is not the first attempt of academics to explore private security as the *Routledge Handbook of Private Security Studies* expertly went through a number of areas where private security was impacted by and impacted military operations, geopolitics, policing, and intelligence. Despite the attempt, though, the volume has issues. As the editors note in their introduction, *Private Security Studies* for them does “not exist as a unified field of study, with clear boundaries between insiders and outsiders, but is instead defined by its diversity and heterogeneity.”ⁱ That is clear from the range of topics in the book that focuses on the privatization of security, policing, and the military which is separate from the discipline for which this essay is advocating. Rather, *Private Security Studies* should not focus on corporations doing the work of governments, but the separate issue of securing private entities (corporations, families, non-profits, and the like).

The private security sector is also one of the fastest-growing industries globally,ⁱⁱ driven by rising security challenges, globalization, corporate vulnerabilities, and evolving threats such as cybercrime, terrorism, and disinformation. Understanding its operational and strategic implications demands rigorous academic study. Modern security threats—whether physical, digital, or reputational—require specialized expertise that often falls outside the jurisdiction of state actors. Academic research can help refine private-sector responses to these threats through training methodologies, new technologies, and strategic partnerships. Finally, the field of private security lacks uniform standards for professional conduct, training, and accreditation. Establishing *Private Security Studies* as a discipline would encourage professionalization, promote ethical standards, and elevate the credibility of private security actors.

What is a Theory?

In academic research, a theory is a structured framework of ideas, concepts, and explanations that helps to understand, analyze, and predict phenomena within a specific field of study. Theories organize observations into a coherent structure, provide explanations for why certain events or behaviors occur, and allow researchers to make informed predictions about future outcomes. Theories are also testable, enabling scholars to validate, refine, or challenge them through empirical research. In essence, theories serve as the "building blocks" of academic research, guiding the way scholars think about problems, formulating research questions, and interpreting findings.



Academic disciplines need theories because they provide a foundation for knowledge, offering shared principles and frameworks that define key concepts, relationships, and the scope of inquiry. Theories guide research and inquiry by informing the questions scholars ask, the methods they use, and the way they interpret results, ensuring that research is systematic rather than fragmented. They simplify complex phenomena, offering explanatory frameworks that help scholars identify patterns and make sense of intricate issues. In applied fields, theories enable predictive analysis, allowing researchers to anticipate trends and future developments, which is particularly valuable in areas like security studies where foresight is critical.

Theories also advance academic disciplines by fostering critique, refinement, and innovation, allowing the field to adapt to new challenges and contexts. They also connect research to practice by providing actionable insights to professionals and policymakers, bridging the gap between academic inquiry and real-world application. Furthermore, theories facilitate cross-disciplinary collaboration by offering shared conceptual tools that allow fields like criminology, international relations, risk management, and business studies to intersect with *Private Security Studies*. Ultimately, theories are essential because they provide structure, explanation, and direction to research. They enable scholars to move beyond isolated observations toward systematic, predictive, and actionable understandings of their subject matter. For emerging disciplines like *Private Security Studies*, developing strong theoretical frameworks is critical for legitimizing the field, advancing knowledge, and addressing real-world security challenges.

Theories in Related Disciplines

Many disciplines have had to go through stages of theoretical development to the present in both the hard and social sciences. International relations, the progenitor of security studies, has gone through several rounds of theory building to refine systemic analysis and those related to sub-disciplines. Take for example the foundational theories of neorealism stemming from the works of Kenneth Waltz. In *Man, the State, and War* and *Theory of International Politics*, Waltz elucidates the “causes of war” in an anarchic system.ⁱⁱⁱ These works articulated a theory that state behavior comes from that anarchic structure, particularly security competition, and that states will seek to balance against each other. Scholars took that theory and tested it to refine neorealism and challenge it. For example, James Fearon would argue for rational choice theory within the international system where actors make decisions on incomplete information while still trying to maximize utility.^{iv} Besides neorealism and rationalism, there are many theories have developed in international relations, including classical realism, neoclassical realism, neoliberalism, democratic peace, constructivism, Marxism, structuralism, complex interdependence, balance of threat, and the English School.

The international relations theories described above are principally to demonstrate how a related academic discipline has developed multiple theories to guide research and analysis. However, *Private Security Studies* will need to draw disciplines that are even more closely related if the discipline wants to understand how to apply theory to the subject. International relations seeks to answer broad questions about state behavior, causes of war and peace, and seeks to explain the global system. *Private Security Studies*, though, is more akin to intelligence studies and criminology in what it seeks to explain.



Peter Gill, Stephen Marrin, and Mark Phythian's *Intelligence Theory: Key Questions and Debates* display the pursuit of theory that will be needed in *Private Security Studies*. In this seminal tome, scholars look at competing aspects of intelligence to theorize about operations and decision making.^v Phythian makes the case in one chapter that intelligence studies should draw from international relations, but other authors take on theory of surprise, organizational theory, and adaptive realism. What separates intelligence theory and international relations theory is what they are trying to explain, and that is why different theories are requisite. Institutions seeking to secure the executive of the company is not the same as institutions seeking to gather human intelligence on a terrorist organization.

Research has continued since the publication of *Intelligence Theory*, and scholars in this discipline have pursued refining theory. *Intelligence and National Security* published a special edition on "Critical Intelligence Studies" in which Hamilton Bean, Peter de Werd, and Cristina Ivan wrote in the introduction that intelligence theory had a reification problem that needed to be addressed.^{vi} In that same vein, Samantha Newbery and Christian Kaunert worked to expand Critical Intelligence Studies to the private sector, offering a new framework for analysis.^{vii} There are many other examples of novel research and theory building in intelligence studies. James Cox researched how human cognition impacts intelligence analysis, deriving a new model for future research.^{viii} Gunilla Eriksson proposed a reframing of the intelligence-policy relation that challenged the long-held theory about the role of intelligence in policy making.^{ix} Jules Gaspard and Giangiuseppe Pili went in an entirely different direction by integrating intelligence theory with philosophy to "instantiate the benefit of philosophy in both the theory and practice of intelligence."^x

These examples proffer potential emulation in theory building for *Private Security Studies*. Importantly, though, private security is different legally and practically from the public sector, which reinforces the need not only for a separate discipline but separate theories as well. That is why *Private Security Studies* will likely need to also draw from other disciplines like criminology.^{xi} Criminology also draws on rational choice, similar to Fearon, but applies the framework to individual decisions.^{xii} Then there are biosocial theories as to the cause of crime.^{xiii} Criminology's sibling is the discipline of criminal justice, and theories there can also inspire *Private Security Studies*.

Private Security Studies will require its own distinct theories to address the unique legal, operational, and practical challenges of non-state security actors. While the theoretical evolution of established fields like international relations, intelligence studies, criminology, and criminal justice offers a roadmap, *Private Security Studies* must develop frameworks that specifically analyze and explain private security's roles, functions, and impacts. International relations, for example, provides a foundational model for theory building, having developed multiple paradigms—such as neorealism, neoliberalism, and constructivism—to explain state behavior and systemic dynamics. However, *Private Security Studies*, being more operational and applied in scope, aligns more closely with disciplines like intelligence studies and criminology. Intelligence studies demonstrates how theory can address practical questions, such as decision-making processes, organizational behavior, and the dynamics of surprise, while still drawing inspiration from broader international relations theories. Similarly, criminology applies frameworks like



rational choice and biosocial theories to explain individual and systemic behaviors, offering methodological approaches that can be adapted to private security contexts.

What distinguishes *Private Security Studies* is its focus on non-state actors, such as private security firms, corporate security systems, and protection services, which operate within legal and ethical parameters distinct from both public security and intelligence operations. This differentiation underscores the need for original theoretical frameworks that can explain phenomena like the commodification of security, risk transfer, professionalization, and legitimacy challenges specific to the private sector. By drawing inspiration from related disciplines while addressing its own unique concerns, *Private Security Studies* can develop theories that are both rigorous and applicable to real-world challenges, solidifying its place as a vital and independent field of academic inquiry.

Potential Theories for *Private Security Studies*

To establish *Private Security Studies* as a robust academic discipline, several theories could guide research, analysis, and education. The following offered theories aim to explain the roles, behaviors, and impacts of private security actors within broader security, social, economic, and political contexts, and they could be used by (or rejected) by researchers in constructing the discipline. They are drawn from already established theories in other disciplines that could be applied to *Private Security Studies*.

- The Complementarity Theory of Security posits that private security operates as a complementary force to public security agencies, addressing gaps where state capacity is limited.^{xiv} Rather than replacing public security, private actors create a "security ecosystem," working alongside the state to safeguard individuals, corporations, and institutions. This theory is particularly relevant for understanding private security's role in conflict zones, fragile states, or in corporate environments where public resources may be overstretched.
- The Marketization of Security Theory explores the privatization of security as a commodity driven by market forces.^{xv} Security, traditionally considered a public good provided by the state, is increasingly subject to supply, demand, and competition in the private sector. This commodification drives innovation and specialized services but also raises ethical concerns about access and equity, as security becomes stratified along socioeconomic lines.
- The Security Governance Theory situates private security within the broader landscape of global security governance, where state, private, and non-state actors share responsibilities for maintaining safety and order.^{xvi} Private security firms not only fill operational gaps but also influence policy, regulation, and risk management frameworks. This theory highlights the decentralized nature of modern security systems, where accountability, legitimacy, and collaboration become central concerns.
- The Risk Transfer Theory explains how individuals and organizations outsource their security needs to private actors as a way of transferring responsibility and liability for managing risks.^{xvii} This is particularly relevant for corporations and NGOs operating in volatile environments, where private security firms serve as intermediaries that assume responsibility for assessing, mitigating, and responding to dynamic threats.



- The Private Security Legitimacy Theory focuses on how private security actors gain, maintain, or lose legitimacy in the eyes of stakeholders, including governments, clients, and the public.^{xviii} Legitimacy is influenced by ethical conduct, transparency, adherence to regulations, and cultural perceptions. Tensions often arise when private actors operate in legal gray areas, use coercive measures, or face scrutiny for their methods, making legitimacy a dynamic and critical area of study.
- The Security Professionalization Theory argues that the rapid growth of the private security sector requires formalized standards for training, accreditation, and ethics.^{xix} This theory parallels the evolution of other professions, such as medicine or law, and emphasizes the importance of professionalizing private security to enhance competency, legitimacy, and accountability. It also advocates for the adoption of standardized global practices to address gaps in regulation and service quality.
- The Dual-State Security Theory proposes that modern security provision is increasingly shared between two "states": the public state, represented by government security agencies, and the private state, composed of corporate and private security actors.^{xx} This theory explains how private security operates as a parallel force, sometimes collaborating with public security and, at other times, competing for authority. The balance of power between public and private actors often shifts depending on governance structures, market forces, and state capacity.

Together, these theoretical frameworks provide a potential foundation for understanding the complexities of the private security sector. They could guide research into its roles, impacts, and ethical challenges while offering insights into its relationships with public security systems, technology, and socioeconomic structures. By applying these potential theories, *Private Security Studies* can develop into a rigorous, interdisciplinary academic discipline capable of addressing real-world security challenges in an increasingly privatized and globalized environment.

Research Methods in *Private Security Studies*

As *Private Security Studies* emerges as a distinct academic discipline, it must adopt rigorous research methods to establish credibility and produce actionable insights. Both qualitative and quantitative research methods are essential for investigating the complex, multi-faceted nature of private security.^{xxi} Qualitative methods allow researchers to explore the human, organizational, and ethical dimensions of private security practices, while quantitative approaches provide empirical data to measure effectiveness, trends, and impacts. Together, these methods will complement each other to advance theoretical development and address practical challenges in the field.

Qualitative Research Methods

Qualitative research methods are particularly well-suited for exploring the behaviors, decisions, and practices of private security actors. This approach seeks to understand "how" and "why" private security operates in specific contexts and environments, providing depth and nuance that quantitative methods cannot always capture. Given the applied nature of *Private Security Studies*, qualitative methods such as



case studies, interviews, focus groups, ethnography, and content analysis can offer critical insights into the motivations, challenges, and impacts of private security actors.

Case Studies

Case studies will be one of the most valuable qualitative methods for *Private Security Studies*. They allow for in-depth exploration of specific events, organizations, or phenomena within private security. For instance, Philip Jett provided an excellent case study in *Taking Mr. Exxon* in which he explores the brutal kidnapping of then Exxon International president Sidney Reso.^{xxii} That became one of the biggest kidnapping investigations in US history and would lead to major shifts in private security, even beyond the energy sector. Those kinds of cases would shed an enormous light on major events and how private security did/could have responded effectively. Case studies can also highlight instances of crisis response, such as private security-led evacuations during political unrest or natural disasters. These investigations can reveal patterns of behavior, ethical dilemmas, and gaps in regulation that might not be visible through quantitative data alone. By comparing multiple cases, scholars can develop theories about the roles and effectiveness of private security actors across diverse environments.

There is also the potential for narrative analysis on the protector side. Private security is often intertwined with individual experiences, especially in close protection, investigations, and risk management. Narrative analysis would allow researchers to study personal accounts, such as interviews or memoirs from private security professionals, to uncover how they perceive and adapt to threats, ethical dilemmas, and operational challenges. This approach can provide unique insights into the psychological and emotional dimensions of private security work, such as stress, decision-making under pressure, or the impact of operating in hostile environments.

Interviews and Focus Groups

Interviews and focus groups allow researchers to engage directly with private security professionals, clients, policymakers, and other stakeholders. Through semi-structured or open-ended interviews, academics can gather insights into the decision-making processes behind security risk assessments, crisis responses, or close protection operations. For example, executives in private security firms might provide valuable perspectives on the challenges they face. Similarly, interviews with NGO staff working in high-risk regions can illuminate how they perceive and rely on private security for protection. Focus groups, on the other hand, encourage discussion and the exchange of ideas among participants, revealing consensus or tensions within the field. This method is particularly useful for understanding emerging challenges, such as integrating new technologies like AI-driven surveillance or addressing cultural dynamics in global operations.

Ethnographic Research

Ethnographic research involves immersive observation of private security operations, offering rich, first-hand insights into their practices, interactions, and challenges. Researchers can embed themselves within private security teams during events, corporate operations, or crisis responses to observe behaviors and decision-making in real time. For instance, an ethnographic study of executive protection services could examine how agents manage threats, navigate cultural sensitivities during international travel, and



coordinate with local security forces. This method can also shed light on the professional culture of private security, revealing norms, hierarchies, and values that shape the industry.

Quantitative Research Methods

While qualitative methods explore the *why* and *how* of private security practices, quantitative research methods provide the empirical evidence needed to test theories, measure effectiveness, and identify trends. Quantitative approaches rely on numerical data and statistical analysis to generate objective, measurable findings. In *Private Security Studies*, these methods are critical for assessing outcomes, identifying correlations, and making policy recommendations.

Surveys and Questionnaires

Surveys are a primary tool for collecting large-scale quantitative data from security professionals, clients, and other stakeholders. Researchers can use structured questionnaires to gather information about the prevalence of private security services, client satisfaction, or risk mitigation outcomes. For instance, a survey might analyze corporate reliance on private security firms for travel security, examining factors such as frequency of use, cost, and perceived effectiveness. Surveys can also assess how security teams view particular issues or subjects, and these are already often used in industry publications.

Statistical Analysis of Security Incidents

Quantitative research can analyze security incident data to evaluate the performance and impact of private security measures. By examining metrics such as incident frequency, response times, and resolution rates, researchers can assess the effectiveness of private security interventions. For example, statistical analysis of event security incidents might reveal patterns of crowd management failures or successes, leading to evidence-based improvements in security planning. The best example of how researchers in this space can perform effective research is Erin Carlin et. al.'s "Workplace Related Shootings and General Strain Theory" in which the researchers collected and analyzed data on active shooters in commercial spaces that then applied general strain theory.^{xxiii}

Risk and Cost-Benefit Analysis

Quantitative methods are crucial for conducting risk assessments and cost-benefit analyses in private security operations. Researchers can use mathematical models to evaluate the likelihood and impact of security threats, helping organizations allocate resources effectively. For example, a cost-benefit analysis might compare the expenses of hiring private security firms for executive protection versus the financial risks associated with a security breach. These analyses can also quantify the value of security investments, providing decision-makers with evidence to justify expenditures on risk management and protection services.

The Need for Both Methods

Private Security Studies, as an emerging discipline, requires a balanced integration of qualitative and quantitative research methods to address its complex and multifaceted subject matter. Qualitative methods, such as case studies, interviews, and ethnographic research, offer valuable insights into the human, organizational, and cultural dimensions of private security. They allow scholars to explore decision-



making processes, ethical dilemmas, and professional practices that shape the industry. In contrast, quantitative methods, such as surveys, statistical analysis, and modeling, provide measurable, empirical data to evaluate effectiveness, identify trends, and inform evidence-based decision-making. By combining these approaches, researchers in *Private Security Studies* can develop rigorous theories, advance academic inquiry, and provide actionable solutions to the challenges faced by the private security sector. This methodological diversity will not only strengthen the legitimacy of the discipline but also ensure its relevance in addressing real-world security needs in a globalized and increasingly privatized security environment.

Potential Research Agenda for Scholars

Now that the need for theory, potential theories, and practical methods has been addressed, the next step would be a research agenda for scholars to pursue in this arena. A possible research agenda for *Private Security Studies* could begin by examining the role and impact of private security within global governance frameworks. Guided by the Complementarity Theory, Security Governance Theory, and Dual-State Security Theory, scholars can explore how private security actors contribute to public safety, particularly in fragile states or during crises, and analyze their partnerships with public security agencies. Regulatory frameworks and case studies on companies operating in humanitarian and post-conflict settings would provide valuable insights into their effectiveness and best practices.

Another part of research could focus on the marketization and professionalization of security, driven by Marketization of Security Theory and Security Professionalization Theory. Research can assess how private security has transformed into a commodity influenced by market forces, analyzing both the economic drivers and ethical dilemmas this raises. Professionalization efforts, such as standardizing training and accreditation, are also critical to understanding how private security can enhance its legitimacy and service quality while addressing global inequalities in access to protection. Risk and crisis management are another focal point, using Risk Transfer Theory to explore how organizations outsource their risk to private security actors. Scholars can analyze private-sector responses to dynamic threats like terrorism, cyberattacks, and disinformation, as well as their role in corporate resilience, global mobility, and humanitarian crises. Case studies of successful evacuations, crisis interventions, and risk mitigation strategies would highlight best practices and areas for improvement.

Then there is potential research that emphasizes the role of technology, innovation, and ethics in private security, applying the Marketization of Security Theory and Private Security Legitimacy Theory. Research in this area can assess the transformative potential of emerging technologies like AI, biometrics, and surveillance systems while addressing ethical concerns such as privacy violations, misuse of force, and regulatory gaps. Comparative studies on technological adoption across different industries and regions will shed light on best practices and responsible innovation. Legitimacy and accountability remain central to understanding private security's evolving role, guided by Private Security Legitimacy Theory and Security Governance Theory. Research can explore how private security firms maintain transparency, gain public trust, and balance operational needs with ethical and legal responsibilities. Public perception studies across various cultural and political contexts will help identify challenges to legitimacy and opportunities for reform.



This research agenda provides a possible roadmap for building a rigorous and interdisciplinary academic foundation for *Private Security Studies*. By addressing critical gaps in theory, ethics, technology, and global governance, scholars can contribute to a deeper understanding of the private security sector's evolving role in today's security landscape. Researchers can take these potential theories and areas of inquiry to design their own studies and contribute to the development of *Private Security Studies* as a discipline.

Academic Institutions

There is a final area that needs to be discussed for *Private Security Studies* to become a distinct discipline: where it should be housed within academic institutions?

Given the interdisciplinary nature of private security, this field touches on a wide range of subjects, including criminology, international relations, business management, intelligence studies, and risk management. As private security encompasses diverse practices—from close protection and corporate security to investigations and event security—there are strong arguments for its integration into multiple academic departments. However, determining the most suitable institutional home for this new field requires consideration of its theoretical foundations, research focus, and the skills it seeks to develop in students and professionals.

One possible home for *Private Security Studies* is within international relations or security studies departments. These departments focus on understanding state and non-state actors' roles in global and regional security, which aligns with certain aspects of private security. The growing role of private security firms in global governance, humanitarian operations, and post-conflict stabilization makes the field relevant to international security scholars. For example, theories of security governance and risk transfer can be examined through the lens of both international relations and private security practices. However, while there is overlap, international relations focuses more on systemic, state-centered dynamics, whereas *Private Security Studies* is more operational and applied, dealing with individual and organizational security at a practical level.

Another logical placement could be within Business Schools. Private security is often a commercial service, and corporate security, risk management, and asset protection are integral to business operations. Business schools already offer programs in risk analysis, crisis management, and organizational behavior, which align with private security's objectives. For instance, a program within a business school could train future security managers to assess corporate vulnerabilities, develop risk mitigation strategies, and manage security teams effectively. However, while private security has a clear business element, its focus on security operations extends beyond the scope of a purely business-oriented education.

Intelligence studies programs also provide an appealing institutional setting for *Private Security Studies*. Both disciplines share an interest in protective intelligence, surveillance, threat analysis, and decision-making under uncertainty. Intelligence studies explores how information is collected, processed, and used to mitigate risks—an essential component of private security operations, particularly in travel security, investigations, and crisis response. Programs could offer cross-disciplinary coursework in protective



intelligence, open-source intelligence (OSINT), and organizational security. Yet intelligence studies primarily emphasize state and national security, while private security operates in corporate, humanitarian, and individual contexts, requiring a broader focus on practical security delivery.^{xxiv}

Criminology departments, which examine the causes, prevention, and management of crime, are another potential home for *Private Security Studies*. Private security directly intersects with criminology in areas such as investigations, surveillance, event security, and crime prevention strategies. The application of criminological theories, such as rational choice and situational crime prevention, aligns closely with private security's goals of deterring, managing, and responding to threats. Criminology also explores the social, ethical, and legal dimensions of security—important areas for understanding the role of private security actors in society.

As such, criminal justice departments offer the strongest alignment with *Private Security Studies*. Criminal justice programs emphasize the practical delivery of security, justice, and law enforcement services, mirroring the applied nature of private security. Both fields share a focus on security operations, investigations, ethics, risk management, and crisis response, making criminal justice departments a natural home for *Private Security Studies*. For example, a *Private Security Studies* program within a criminal justice department could offer courses on close protection, corporate investigations, event security management, and protective intelligence alongside traditional coursework on law enforcement and justice systems. The focus on real-world application in criminal justice aligns well with private security's operational goals, preparing students with the skills needed to excel as security professionals, managers, and analysts.

Criminal justice departments provide a natural home for *Private Security Studies* because they share a practical, applied focus on delivering security services, managing risks, and responding to threats. Both fields address operational realities and the legal frameworks surrounding security, making criminal justice programs well-suited to house and support this emerging discipline. By situating *Private Security Studies* within criminal justice, academic institutions can leverage existing expertise and curricula while creating a dedicated space for the study of non-state security actors, ultimately strengthening the legitimacy and impact of the field.

Conclusion

Private Security Studies represents a critical and timely addition to academia, addressing the growing prominence of non-state security actors in an increasingly complex global security environment. Just as importantly, it would be relevant and offer practical help to the private security profession as the research focuses on real-world and applicable issues. By examining subjects like close protection, corporate security, investigations, risk management, and protective intelligence, this discipline could provide a systematic and academic foundation for understanding the roles, impacts, and challenges of private security. Theoretical frameworks such as Complementarity Theory, Risk Transfer Theory, and Private Security Legitimacy Theory offer the intellectual tools needed to explain private security's functions, while qualitative and quantitative research methods ensure rigorous and practical analysis. As an applied and interdisciplinary field, *Private Security Studies* could draw inspiration from related disciplines like criminology, criminal justice, international relations, and intelligence studies while distinguishing itself through its focus on non-state



security solutions. With a clear research agenda, theoretical foundation, and institutional direction, *Private Security Studies* is poised to become a vital academic discipline, bridging the gap between theory and practice to address the evolving security challenges of the 21st century.

Author: Dr. Treston Wheat is the Chief Geopolitical Officer for Insight Forward, Special Advisor for Geopolitics and Security at Riley Risk Inc., and an adjunct professor at Georgetown University.

Endnotes

- ⁱ Rita Abrahamsen and Anna Leander, "Introduction," in *Routledge Handbook of Private Security Studies*, ed. Rita Abrahamsen and Anna Leander (Routledge, 2016), 4-5.
- ⁱⁱ "Private Security Market Size, Share & Industry Analysis, By Service Type (Manned Security, Cash Services, Electronic Security Services, and Others), By Application (Residential, Commercial, Industrial, and Government), By End User (Manufacturing, Energy & Utilities, BFSI, Infrastructure, Retail, Ports/Airports, and Others), and Regional Forecast, 2024-2032," *Fortune Business Insights*, December 2, 2024, <https://www.fortunebusinessinsights.com/private-security-market-108283>
- ⁱⁱⁱ Kenneth Waltz, *Man, the State, and War: A Theoretical Analysis* (Columbia University Press, 2001). Kenneth Waltz, *Theory of International Politics* (Columbia University Press, 2010).
- ^{iv} James Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379-414.
- ^v Peter Gill, Stephen Marrin, and Mark Phythian, eds., *Intelligence Theory: Key Questions and Debates* (Routledge, 2009).
- ^{vi} Hamilton Bean, Peter de Werd, and Cristina Ivan, "Critical intelligence studies: introduction to the special issue," *Intelligence and National Security* 36, no. 4 (2021): 467-475. Note: For those lucky enough not to have dealt with the concept of reification, it is the Marxist-Hegelian notion of abstract concepts and processes becoming a "thing." Such analysis should not be welcomed in *Private Security Studies* as it is antithetical to good theory building and professionalization of the industry.
- ^{vii} Samantha Newbery and Christian Kaurert, "Critical Intelligence Studies: a new framework for analysis," *Intelligence and National Security* 38, no. 5: 780-798.
- ^{viii} James Cox, "A fundamental re-conceptualization of intelligence: cognitive activity and the pursuit of advantage," *Intelligence and National Security* 37, no. 2 (2022): 197-215.
- ^{ix} Gunilla Eriksson, "A theoretical reframing of the intelligence-policy relation," *Intelligence and National Security* 33, no. 4 (2018): 553-561.
- ^x Jules J. S. Gaspard and Giangiuseppe Pili, "Integrating intelligence theory with philosophy: introduction to the special issue," *Intelligence and National Security* 37, no. 6: 763-776.
- ^{xi} Michael Dow Burkhead, *The Search for the Causes of Crime: A History of Theory in Criminology* (McFarland and Company, 2006). Don C. Gibbons, *Talking About Crime and Criminals: Problems and Issues in Theory Development in Criminology* (Prentice Hall, 1994).
- ^{xii} Travis C. Pratt, "Rational choice theory, crime control policy, and criminological relevance," *Criminology & Public Policy* 7, no. 1 (2008): 43-52.
- ^{xiii} Michael Rocque, "Policy Implications of Biosocial Criminology: Crime Prevention and Offender Rehabilitation," in *The Nurture vs. Biosocial Debate in Criminology: On the Origins of Criminal Behavior and Criminality*, ed. Kevin M. Beaver, JC Barnes, and Brian B. Boutwell (SAGE, 2014).



^{xiv} Byounggu Choi, Simon K. Poon, and Joseph G. Davis, "Effects of knowledge management strategy on organizational performance: A complementarity theory-based approach," *Science Direct* 36 (2008): 235-251.

^{xv} Deborah Avant, "The Implications of Marketized Security for IR Theory: The Democratic Peace, Late State Building, and the Nature and Frequency of Conflict," *Perspectives on Politics* 4, no. 3 (2006): 507-528.

^{xvi} Elke Krahnemann, "Conceptualizing Security Governance," *Cooperation and Conflict* 38, no. 1 (2003): 5-26.

^{xvii} Peijun Shi, Jiabing Shuai, Wenfang Chen, and Lili Lu, "Study on large-scale disaster risk assessment and risk transfer models," *International Journal of Disaster Risk Science* 1 (2008): 1-8.

^{xviii} Jesse Fielder and Kristina Murphy, "A crisis of legitimacy?: The importance of procedural justice in frontline private security provision," *Policing and Society* 32, no. 7 (2022): 846-861.

^{xix} Mel Griffiths, David Brooks, and Jeff Corkill, "Defining the Security Professional: Definition through a Body of Knowledge," Australian Security and Intelligence Conference (2010).

^{xx} Ernst Fraenkel, *The Dual State: A Contribution to the Theory of Dictatorship* (Oxford University Press, 2017). Note: While this theory stems from studying dictatorships, the idea of dual and competing "states" between the public sector and private sector goes back centuries to Edmund Burke's critique of the East India Company. See Treston Wheat, "'A State in Disguise of a Merchant': Multinational Tech Corporations and the Reconfiguration of the Balance of Power in Asia," The Andrew W. Marshall Foundation (2022), <https://www.andrewmarshallfoundation.org/library/a-state-in-disguise-of-a-merchant-multinational-tech-corporations-and-the-reconfiguration-of-the-balance-of-power-in-asia/>.

^{xxi} The research methods discussed below are well established. To help those unfamiliar with them, see the following books. Catherine Dawson, *Introduction to Research Methods: A Practical Guide for Anyone Undertaking a Research Project* (Robison, 2019). Anol Battacherjee, *Social Science Research: Principles, Methods and Practices* (University of Southern Queensland, 2019). Alexander L. George and Andrew Benet, *Case Studies and Theory Development in the Social Sciences* (The MIT Press, 2005). Daniel Stockemer and Jean-Nicolas Bordeleau, *Quantitative Methods for the Social Sciences* (Springer, 2023).

^{xxii} Philip Jett, *Taking Mr. Exxon: The Kidnapping of an Oil Giant's President* (Chronos Books, 2021).

^{xxiii} Erin Carlin, Anna Leimberg, Kirsten England, Alexis Israel, and Kaylynn Sims, "Workplace Related Shootings and General Strain Theory," *The Close Protection and Security Journal* 1, no. 1: 2-18.

^{xxiv} Newbery and Kaunert, "Critical Studies Intelligence: a new framework for analysis."



Navigating Complexity: A Structured Approach to Travel Risk Management

Nathan Ackerman

Abstract

This paper introduces a robust framework for travel risk management, developed by Riley Risk, Inc., based on 20 years of practical experience and refined over the past five years. The six-element ITRIPS framework bridges theoretical approaches and practical application, providing a systematic yet flexible method for addressing complex and evolving threats in diverse environments, particularly higher-risk destinations. Traditional travel risk frameworks often fall short in high-risk settings due to resource constraints, inadequate duty of care, and challenges like sophisticated state surveillance, non-state actors, and rapid crises. Using case studies from executive protection and international development missions in fragile regions, the study highlights how the ITRIPS framework enables organizations to assess, mitigate, and respond effectively to travel risks while maintaining operational flexibility. The methodology has been successfully implemented across multinational corporations and NGOs, proving its scalability and adaptability. Organizations adopting this framework report improved resiliency, better resource allocation, enhanced threat detection, and superior emergency planning. This research equips security practitioners with a practical toolkit for managing travel risks, integrating threat assessments into broader duty of care programs, and ensuring readiness for emergencies, thereby enhancing organizational safety and compliance in global operations.

Introduction

The landscape of global travel risk has undergone significant transformation in recent years, presenting unprecedented challenges for security practitioners. Traditional approaches to travel risk management often fall short when confronted with the realities of modern threats ranging from sophisticated state surveillance to unpredictable non-state actors, and from rapidly evolving health crises to sudden infrastructure collapse. This paper aims to address these challenges by presenting a structured methodology for assessing, mitigating, and responding to travel risks in complex and high-risk environments using a framework that draws well-established practices, yet remains agile enough to support bespoke deployment without sacrificing essential components.

The author draws from over two decades of experience managing travel security across a spectrum of operational contexts—from active conflict zones to complex urban environments, with the presented framework used by the author’s firm for managing a conservative estimate of thousands of global travel risk occurrences for client operations for the past 5 years effectively proving its value. This paper offers insights for practical implementation, presented in a manner which demonstrates structural approach and implementation, as well as noted context when variables based on risk profile, resources, or operational environment dictate added complexity. The methodology presented here has been refined through years of real-world application, providing a systematic approach that remains adaptable to the unique demands of diverse operational scenarios.



As the global risk landscape continues to evolve, security practitioners must move beyond a mere static checkbox approach to travel risk management. Each journey into a complex risk environment demands a tailored strategy yet should have an adherence to a systematic framework to ensure critical aspects are not overlooked during all operational phases of the travel occurrence. This paper presents such a framework, designed to be both comprehensive and flexible with minimal gaps in the essential coverages for a travel risk management program, intended to address the nuanced challenges of modern travel risk management.

Current Operating Environment

Today's security practitioners face a persistently challenging convergence of evolving risks that demand a nuanced approach to travel risk management. Within the past decade, examples include the global COVID-19 pandemic, widespread natural disasters, and escalating government instability.ⁱ Violent coups d'état in Myanmar, Burkina Faso, Guinea-Bissau, Central African Republic, Libya, Thailand, Yemen, Ukraine, Niger, and Mali serve as stark reminders of how rapidly border situations can deteriorate, disrupting travel operations and potentially stranding personnel in high-risk environments.

Ongoing conflicts illustrate the dynamic nature of global security challenges: the war in Ukraine, the expanding Middle East conflict centered on Gaza and the West Bank (with regional implications across Lebanon and Iran), the deteriorating situation in Burma, tensions surrounding Taiwan, and the persistent conflict in Sudan. These situations, often driven by a combination of ideological differences and great power competition, particularly evident across Africa, demonstrate how rapidly seemingly stable regions can descend into chaos, necessitating swift adaptation of security protocols and protective measures.

State actors' surveillance and information-gathering capabilities—and more critically, their intent to use these capabilities—have expanded dramatically in recent years.ⁱⁱ Advanced technologies, including facial recognition systems, social media monitoring platforms, and big data analytics enhanced by artificial intelligence, have significantly increased governments' ability to track and potentially interfere with foreign visitors. This heightened surveillance environment creates evolving risks for travelers, particularly those engaged in sensitive business or diplomatic activities, or those merely associated with persons or organizations of interest.

Simultaneously, non-state actors continue to develop increasingly sophisticated methods to target travelers and organizations. Criminal enterprises have leveraged technology to enhance their operations, making even urban financial centers potentially high-risk environments for unwary travelers.ⁱⁱⁱ Terrorist organizations have further demonstrated adaptability in their tactics while keeping a focus on soft targets that may include business travelers or expatriate communities, they also demonstrated an ability to be more selective on specific targeting, when asked to do so for profit, or for other organizational-based purposes.

In many regions, the traditional distinction between low and high-risk environments has blurred significantly. Historically, organizations have used country-wide risk levels to determine security support



and platform engagement, if any. However, a seemingly routine business trip to an urban financial center can now carry substantial risks from state surveillance or sophisticated criminal enterprises. Higher-risk countries and destinations—or corporate security operations involving executive protection teams deployed based on profile rather than location—typically involve enhanced security protocols and support requirements, as appropriate. With proper preparation and relevant mitigation strategies aligned to identified threats and environmental risk factors, operations in both traditionally low and high-risk environments can be managed effectively, often requiring fewer resources than conventional approaches.

Climate change and environmental degradation introduce additional layers of complexity to the risk landscape. Extreme weather events, water scarcity, and other environmental factors can rapidly destabilize regions, creating new security challenges for travelers and organizations operating in affected areas.

The rapid pace of technological change presents both opportunities and challenges for travel risk management platforms and practitioners.^{iv} While advancements in communication and tracking technologies offer enhanced tools for traveler safety, they also create potential vulnerabilities that malicious actors can exploit. Technology integration into travel risk management programs must prioritize operational value over unnecessary complexity. Security practitioners must develop proficiency in these systems and thoroughly understand the essential components of deployed technologies. This expertise is crucial not only for professional competency but also for building trust with end users—from travelers at airport boarding gates to those managing check-in processes, whether traveling by ground transport, rail, aviation, or maritime means.

In this complex and rapidly evolving risk environment, security practitioners must adopt approaches that are both systematic and adaptable. The following sections outline a structured framework designed to address these challenges, providing a comprehensive yet flexible approach to travel risk management from lower-risk to high-risk environments.

Traditional Travel Risk Management Frameworks: A Critical Analysis

The evolution of travel risk management has produced several established frameworks, each with distinct approaches to addressing organizational security needs. However, as the global risk landscape becomes increasingly complex, the limitations of these traditional frameworks have become more apparent. This section examines existing methodologies and identifies critical gaps that necessitate a more adaptive approach.

Established Frameworks and Their Limitations

ISO 31000 Risk Management Framework

The ISO 31000 framework provides a standardized approach to risk management that many organizations adopt for travel security.^v While comprehensive in its risk assessment methodology, its broad scope often fails to address the specific nuances of travel risk management. The framework's rigid structure, while valuable for systematic analysis, can impede rapid response to evolving threats in dynamic environments.



Traditional Country Risk Rating Systems

Many organizations rely heavily on country-wide risk ratings to determine security measures. However, this approach increasingly proves inadequate as threats become more localized and dynamic. A singular risk rating for an entire country often fails to capture nuanced variations in risk levels between different regions or urban centers within the same jurisdiction. This oversimplification can lead to either inadequate security measures or excessive resource allocation.

Corporate Travel Management (TMC) Models

Traditional TMC-based frameworks typically focus on logistics and compliance rather than comprehensive security management.^{vi} While these models excel at tracking traveler movements and ensuring policy compliance, they often lack robust threat assessment and response capabilities.

Critical Gaps in Current Approaches

Reactive vs. Proactive Stance

Many existing frameworks emphasize response protocols or operational levels rather than addressing threat anticipation.^{vii} This reactive orientation, while necessary for crisis management, inadequately addresses the need for proactive threat identification and mitigation. The growing sophistication of both state and non-state actors requires a more anticipatory approach to risk management.

Resource Allocation Inefficiencies

Traditional frameworks often prescribe standardized security measures based on broad risk categories, leading to inefficient resource allocation. This one-size-fits-all approach fails to account for organization-specific needs and capabilities, potentially resulting in either security gaps or unnecessary expenditure. A lack of collaboration between procurement and security teams can exacerbate this issue. When procurement operates in isolation, there's a risk of selecting security solutions that don't align with the organization's actual needs, resulting in either overprotection or vulnerabilities. Integrating procurement teams into the security management process, alongside those responsible for physical, personnel, and information security, is essential for holistic protection against threats and effective risk management.

Integration Challenges

Existing frameworks frequently operate in silos, creating challenges in integrating travel risk management with broader organizational security programs. This segregation can lead to communication gaps, duplicated efforts, and missed opportunities for comprehensive risk mitigation.

Technological Adaptation Lag

While many traditional frameworks acknowledge technological considerations, they often fail to fully incorporate modern technological capabilities and threats. The rapid evolution of both security tools and cyber threats requires a more dynamic approach to technology integration.

The Need for a New Approach



These limitations in traditional frameworks highlight the need for a more adaptive and comprehensive methodology. Modern travel risk management calls for the below factors, which while not *necessarily revolutionary*, are not always an integral company of the classic model, for a variety of reasons previously outlined:

1. Flexible Framework Structure
 - Ability to scale security measures based on specific threat contexts
 - Rapid adaptation capabilities for emerging threats
 - Integration of both traditional and modern security tools
2. Enhanced Threat Analysis
 - Incorporation of both OSINT and HUMINT capabilities
 - Real-time threat assessment and response mechanisms
 - Better integration of technological tools for threat monitoring
3. Resource Optimization
 - More efficient allocation of security resources
 - Scalable security measures based on actual threat levels
 - Better alignment of security measures with organizational capabilities
4. Stakeholder Integration
 - Improved communication between security teams and organizational leadership
 - Better coordination between various security functions
 - Enhanced information sharing across organizational units

The ITRIPS framework, presented in the following sections, provides a flexible structure to address these critical gaps while maintaining the systematic approach necessary for an effective travel risk management program. By combining structured analysis with operational flexibility, it provides a more comprehensive and adaptive approach to modern travel risk management challenges.

A Structured Approach: The Six-Element Framework

The methodology presented in this paper has been developed and refined through years of practical application across diverse operating environments. It provides a systematic framework for assessing and mitigating travel risks while remaining flexible enough to adapt to specific contexts and requirements.

The framework consists of six interconnected elements, each consistently building upon the others as a foundational layer to create a comprehensive travel risk management strategy, as demonstrated below:

1. Introductory Assessment & Orientation
2. Threat Awareness & Assessment
3. Risk Identification & Assessment



4. Individual and Team Mitigations
5. Plans for Emergency Response
6. Special Considerations

This six-element framework, known as ITRIPS, offers a structured yet adaptable approach to travel risk management. It balances systematic analysis with the flexibility required to address complex and evolving threats, providing security practitioners with a robust toolkit for navigating the complexities of modern travel risk management in high-risk environments. A flow down view of this process can be seen below:

ITRIPS: Travel Risk Process



Figure 1: ITRIPS Travel Risk Management Structure

1. Introductory Assessment & Orientation

The foundation of effective travel risk management lies in developing a thorough, context-driven understanding of the operational environment. This initial assessment goes beyond surface-level country briefings to include:

- Political landscape analysis encompassing both formal power structures and informal influences.
- Social and cultural dynamics that might impact operations.
- Infrastructure reliability and limitations.



- Legal and regulatory environment, particularly regarding foreign visitors.
- Historical patterns of targeting travelers or organizations.
- Seasonal considerations, from weather patterns to political events and more.

This comprehensive orientation provides the informational foundation for all subsequent planning, shaping understanding and awareness while reducing critical gaps in knowledge that could lead to adverse consequences when an incident occurs, often due to escalatory factors.

2. Threat Awareness

Building on the contextual foundation established in the first step, practitioners can effectively identify and analyze specific threats. This process should be dynamic and ongoing, not a one-time assessment, and should be considered an essential component,^{viii} t (*What Challenges Do TMCs Face in Travel-Risk Management?* n.d.), with assessment elements including at minimum:

- Threat Actor Identification: State actors, non-state armed groups, criminal organizations, hostile surveillance threats, environmental and health threats.
- Capability Assessment: Known tactics and techniques, resource availability, historical activities and patterns, geographic areas of operation.
- Trend Analysis: Emerging threats and capabilities, seasonal variations in activity, impact of current events on threat actor behavior, changes in targeting preferences or methods.
- Further Analysis: Further analysis categories can, and should be added to this stage, driven by organizational profile and capabilities.
-

3. Risk Identification & Assessment

This phase involves mapping identified threats against operational vulnerabilities. It requires systematic examination of key operational aspects that, if compromised, could impact safety, security, and mission success. Areas of focus include:

- Travel Profile and Visibility.
- Asset Exposure and Protection.
- Movement Requirements.
- Communication Systems.
- Local Support Networks.
- Medical Considerations.
- Transportation Infrastructure.
- Accommodation Safety and Security.

For each identified risk, practitioners should evaluate both likelihood and potential impact, considering cascade effects and assessing secondary and tertiary consequences. Practitioners should strive to have a firm understanding of foundational risk concepts and understand the practical application and meaning of the words threat, asset, vulnerability as they relate to the overall descriptor of risk.

4. Individual and Team Mitigation Strategy



This phase focuses on developing practical mitigation strategies tailored to the specific operation and the individuals involved. These strategies must be realistic about resource constraints, flexible enough to adapt to changing situations, and clearly understood by all involved parties. Having knowledge of threats and risk matters little if a sound, practical mitigation plan can be established to reduce the risk factors to an acceptable level. The author will add more context to this specific section later, given its importance for applying the concepts to real-world scenarios.

Building Redundancy

Implementing robust backup systems for critical components is essential for effective risk mitigation:

- **Communication Methods:** Establish multiple channels of communication, including satellite phones, encrypted messaging apps, and local mobile networks. Ensure team members are trained in using all available communication tools.
- **Transportation Options:** Identify and vet multiple transportation providers and routes. This includes both ground and air transportation options, considering potential disruptions or blockades.
- **Evacuation Plans:** Develop primary, secondary, and tertiary evacuation plans. Each plan should include different exit routes, modes of transportation, and safe havens.

Leveraging Local Knowledge

Cultivating reliable local source networks is crucial for gaining a nuanced understanding of the operational environment:

- **Informal Power Structures:** Identify and understand local power dynamics that may not be immediately apparent but can significantly impact operations.
- **Unwritten Rules:** Recognize and respect local customs, cultural norms, and informal practices that may affect traveler safety and operational success.
- **Subtle Indicators:** Train team members to recognize subtle signs of changing security conditions that may not be evident to outsiders.

Scenario Planning

Develop and analyze potential future scenarios to anticipate possible threats and their impacts:

- Conduct regular tabletop exercises with the team to explore various "what-if" scenarios.
- Create response plans for each identified scenario, ensuring team members understand their roles and responsibilities.
- Regularly update these scenarios based on evolving threat assessments and changes in the operational environment.

Individual Risk Profiles

Tailor mitigation strategies to the specific risk profiles of individual travelers:

- Consider factors such as the traveler's role, visibility, experience level, and personal characteristics that may affect their risk exposure.
- Provide personalized security briefings and training based on individual risk assessments.



- Develop specific protocols for high-risk individuals, such as executives or those with unique vulnerabilities.

Team Coordination and Communication

Establish clear protocols for team coordination and communication:

- Define clear roles and responsibilities within the team for various risk scenarios.
- Implement regular check-in procedures and establish triggers for escalating concerns.
- Conduct pre-travel team briefings to ensure all members understand the risk environment and mitigation strategies.

Adaptive Decision-Making

Foster a culture of adaptive decision-making within the team:

- Empower team members to make real-time risk assessments and adjustments to plans as needed.
- Establish clear guidelines for when and how to deviate from established plans in response to emerging threats.
- Conduct post-travel debriefs to capture lessons learned and continuously improve mitigation strategies.

By implementing these comprehensive individual and team mitigation strategies, organizations can significantly enhance their ability to manage travel risks effectively. This approach ensures that both individual travelers and teams are well-prepared to navigate complex and potentially high-risk environments, adapting to challenges as they arise while maintaining a strong foundation of preparedness and resilience.

5. Plans: Emergency Response

This critical component involves developing comprehensive emergency response plans that address various potential scenarios identified in the risk assessment phase. In the context of corporate travel risk management, this includes:

- **Evacuation Procedures:** Detailed plans for rapid evacuation from high-risk areas, including multiple exit routes and transportation options.
- **Medical Emergency Protocols:** Procedures for accessing local medical care, emergency medical evacuation, and coordination with international healthcare providers.
- **Crisis Communication Plans:** Clear protocols for internal and external communication during emergencies, including predetermined points of contact and escalation procedures.
- **Business Continuity Measures:** Strategies to maintain critical business operations in the event of a crisis or evacuation.
- **Hostage Situation Response:** Procedures for managing and responding to potential kidnapping or hostage situations.
- **Natural Disaster Response:** Plans tailored to specific natural hazards prevalent in the operating environment.
- **Civil Unrest Protocols:** Strategies for ensuring traveler safety during periods of political instability or civil unrest.



These plans should be regularly reviewed, updated, and practiced, ensuring their effectiveness and relevance to the current risk environment.

6. Special Considerations

The final element addresses unique factors that might not fit neatly into the previous categories but are crucial for successful risk management in the specific operational context. For corporate travel risk management, these may include:

- VIP Travel: Special protocols for high-profile executives or board members who may face increased risks or require enhanced security measures.
- Insurance & Emergency Resources: BTA (Business Traveler & Accidental), specialty risk, EMAP (Emergency Medical & Assistance Provider) coverages and resources should be well-known by leadership when developing and updating a global travel risk management framework and plan. The integration and implementation of resources, duty of care programs, approvals and management needs to factor in existing resources, as well as identify gaps in coverage which can expose further liability.
- Cultural Sensitivities: Consideration of local customs, religious practices, or cultural norms that may impact travel plans or traveler behavior.
- Reputational Risks: Strategies to manage potential reputational impacts on the company resulting from travel incidents or crises.
- Regulatory Compliance: Ensuring travel risk management practices comply with relevant local and international regulations, including duty of care obligations.
- Technology Considerations: Addressing cybersecurity risks and data protection concerns specific to the travel context.
- Long-term Assignments: Special considerations for employees on extended international assignments, including family support and integration into local communities.
- Mental Health Support: Protocols for addressing traveler stress, anxiety, or other mental health concerns that may arise during high-risk travel.
- Diversity and Inclusion: Tailored risk assessments and mitigation strategies that consider the unique risks faced by diverse travelers, including women, LGBTQ+ individuals, or religious minorities in certain contexts.

By systematically addressing each of these previous six elements, security leadership and security practitioners can develop a comprehensive yet flexible approach to travel risk management, capable of addressing the nuanced challenges of diverse and complex operational environments. This framework provides a solid foundation for corporate travel risk management, ensuring the safety and security of employees while enabling business operations in even the most challenging global contexts.

Implementation Process: Continuous Assessment and Adaptation

Security leadership should regularly reassess risks and the effectiveness of emergency plans, threat and risk management platforms, and information resources, to include evaluating and stress testing mitigation strategies. Adapt approaches as new information becomes available or as the operational environment



changes. Establishing consistent feedback mechanism for each travel occurrence from the practitioner and the traveler perspective can provide high value feedback, without extensive effort, leveraging community-driven data and feedback on an ongoing basis.

This framework is designed to be scalable, allowing for rapid deployment in time-sensitive scenarios while maintaining the capability to expand into detailed analysis for complex operations when suitable, and the resources and time permit.

For rapid deployment, each element can be assessed using critical indicators and baseline analysis. This quick-look approach enables security teams to identify and mitigate primary risks when time constraints prevent deeper analysis. However, the same framework seamlessly scales up complex scenarios requiring more resources and preparation efforts.

In-Depth Discussion on Threat Analysis and Risk Identification

Threat Analysis Methodologies

Effective threat analysis in complex environments requires a multi-faceted approach that combines quantitative data analysis with qualitative intelligence gathering. Key methodologies which can be included in the mix are as follows:

- Open-Source Intelligence (OSINT) Gathering: Systematically collecting and analyzing publicly available information from sources such as media reports, social media, and government publications.
- Human Intelligence (HUMINT): Developing and maintaining networks of reliable local sources who can provide context and early warnings about emerging threats.
- Pattern Analysis: Examining historical incident data to identify trends, patterns, and potential indicators of future threats.
- Scenario Planning: Developing and analyzing potential future scenarios to anticipate possible threats and their impacts.
- Geospatial Analysis: Utilizing GIS tools to map threat actors' areas of operation, incident hotspots, and potential vulnerabilities in planned travel routes.

Risk Identification Techniques

Risk identification in high-risk environments requires a systematic approach that considers both obvious and subtle vulnerabilities. Key techniques include, but are not limited to the following:

- Vulnerability Mapping: Systematically identifying potential weaknesses in operational plans, infrastructure, and security measures.
- Threat-Vulnerability Pairing: Matching identified threats with specific vulnerabilities to understand where risks are most likely to materialize.
- Operational Process Analysis: Examining each step of planned operations to identify points where security could be compromised.



- Contextual Risk Assessment: Considering how local cultural norms, social dynamics, and political contexts might create unexpected risks.
- Technology and Cyber Risk Evaluation: Assessing potential vulnerabilities in communication systems, data storage, and other technological infrastructure.

Effective Implementation Strategies

Effective implementation of travel risk management strategies in high-risk environments requires meticulous attention to practical details, continuous adaptation to changing conditions, and comprehensive stakeholder engagement. As an example, Riley Risk’s tailored strategy typically includes the following aspects:

Resource Allocation

Carefully balance competing needs when allocating resources. Staffing levels must account for both routine and compliance requirements, with the ability to support surge capacity during incidents. For materials implementation, equipment and supplies such as communications and medical travel kits need to be appropriate for the environment and consistently available, with distribution as seamless as possible.

Training and Preparation

Conduct thorough pre-deployment briefings with staff focused on specific, relevant information. Implement scenario-based training that reflects real-world conditions and potential complications. Travel briefings structured for both travelers and those charged with providing support during travel, such as executive protection teams, can use the same framework, but should be structured to be relevant to the individual or group category. Briefing for practitioners will generally be more focused on preparing and managing for the travel occurrence, for travelers, it should be about informing of the priority factors, as well as clear guidance for how to respond to potentially adverse incidents. Practitioners and teams should regularly rehearse emergency procedures and processes until responses become automatic.

Continuous Assessment

Implement regular risk reviews that question assumptions and look for emerging threats. Establish clear processes for integrating new information into existing plans and rapidly adapting strategies when conditions change.

Comprehensive Stakeholder Alignment

A critical aspect of successful implementation is ensuring all stakeholders understand their roles and responsibilities within the ITRIPS (Introductory & Orientation, Threat Awareness, Risk Identification & Assessment, Individual & Team Mitigation Strategy, Planning: Emergency Response, Special Considerations) framework. This alignment is crucial for creating a cohesive and responsive risk management program.

- Travel Coordinators: Those responsible for booking travel and managing logistics were briefed on the importance of selecting appropriate accommodation, transportation, and routes based on current risk assessments.



- Vendor Management: Teams liaising with local service providers were trained to recognize potential security concerns and report them through established channels.
- Executive Assistants: These key personnel were educated on the ITRIPS framework to better understand the rationale behind security decisions and to effectively communicate with executives about risk-related matters.
- Advance Personnel: Teams conducting pre-travel assessments were given in-depth training on applying the ITRIPS framework in the field, ensuring consistency in risk evaluation across different locations.

By ensuring each stakeholder understands their role within the ITRIPS framework, a more resilient and responsive risk management system can be developed.

Tailored Communication Protocols

Communication protocols will generally be organization-specific, however, security leadership will be prudent to implement a tiered communication strategy to ensure that critical information flowed efficiently without overwhelming stakeholders with unnecessary details:^{ix}

- Need-to-Know Basis: Information was compartmentalized, with each stakeholder receiving only the details relevant to their responsibilities.
- Regular Briefings: Scheduled updates kept all parties informed of evolving risks and mitigation strategies.
- Emergency Protocols: Clear, concise procedures were established for rapid communication during crisis situations.

Flexible Risk Profiling

The ITRIPS framework was adapted to accommodate various risk profiles, ranging from HNWI executive business travel to multinational entities traveling to extremely risky conflict zones. This flexibility ensured that regardless of the traveler's profile or time constraints, critical risk information was effectively communicated.

Role-Specific Checklists and Action Items

To move beyond generic checkbox approaches while maintaining systematic oversight:

- Customized Checklists: Developed for each role (e.g., travel coordinator, security team, executive assistant) to ensure all critical tasks were completed.
- Dynamic Action Lists: Implemented a system where role-specific action items could be updated in real-time based on evolving risk assessments.
- Centralized Dashboard: Created a live dashboard accessible to travel risk management leadership, providing visibility into completed actions, pending tasks, and requests for information (RFIs).

This approach ensured that while checklists were used for the purpose of compliance with established practices and internal standards, they were fit for purpose and integrated into a dynamic process,



informing a broader global risk management program rather than operating as a segmented and siloed function.

Practical Implementation Measures

- Discreet Transportation: Arranged low-profile vehicles with vetted local providers, varying routes and timing to avoid predictable patterns.
- Distributed Accommodation: Implemented a plan to use multiple, lower-profile accommodations rather than centralized, high-visibility hotels.
- Enhanced Security Measures: Deployed counter-surveillance techniques and secure communication protocols tailored to the local threat environment.
- Adaptive Movement Strategies: Established flexible itineraries that could be rapidly adjusted based on real-time risk assessments.
- Multi-Tiered Evacuation Planning: Developed comprehensive emergency evacuation plans with multiple options and clear activation triggers.

By integrating the above elements into a broader implementation strategy, Riley Risk has been able to create multiple robust, flexible, and responsive travel risk management systems for their clients. This approach ensured that all stakeholders, regardless of their specific role or the traveler's risk profile, were equipped to contribute effectively to the overall security posture.

This comprehensive yet adaptable implementation strategy formed the cornerstone of the firm's ability to navigate complex, high-risk environments successfully for the past 5 years, with far less resources and staffing as compared to more traditional models.

Study Case Application: High-Profile Executive Travel for an International Development Organization

Consider a recent operation by Riley Risk in which the firm supported a high-profile executive travel for an international development organization to a South Asian country experiencing increasing authoritarianism and recent civil unrest. The situation developed further, prompting hurried mass emergency evacuations by most multinational entities operating in the country. By utilizing the six-element travel risk framework, Riley Risk was better equipped to manage the situation effectively.

1. Initial Assessment: The initial travel assessment revealed complex dynamics between government forces and opposition groups, with increased targeting of foreign entities, particularly international development organizations. The country was experiencing rapid political shifts, with the government consolidating power and restricting civil liberties.
2. Threat Analysis Key findings included:
 - Heightened surveillance risks from state security services, especially targeting foreign NGOs.
 - Criminal groups opportunistically targeting high-profile international visitors Potential for rapid escalation of civil unrest, particularly in urban centers.
 - Increased scrutiny and potential interference with international development activities.



3. Risk Identification Critical vulnerabilities identified included:

- Exposure during airport transfers and other ground movements
- Potential security compromises at commonly used expatriate accommodations.
- Communication vulnerabilities due to state monitoring of electronic and cellular networks.
- Risks associated with the organization's public profile and activities.

4. Risk Impact Assessment

Riley Risk evaluated the likelihood and potential impact of various scenarios, including:

- Detention or harassment of personnel by state security forces.
- Violent civil unrest impacting freedom of movement.
- Sudden implementation of travel restrictions or visa cancellations.
- Forced closure of international development projects.

5. Implementation Strategy

The tailored strategy included:

- Arranging discreet transportation with thoroughly vetted local providers, implementing a distributed accommodation plan, and avoiding high-profile hotels.
- Deploying enhanced counter-surveillance measures and secure communication protocols.
- Establishing flexible movement patterns based on real-time risk assessments.
- Developing comprehensive emergency evacuation plans with multiple options and triggers.

6. Continuous Assessment and Adaptation

Ongoing monitoring of:

- Political developments, including informal power dynamics.
- Civil society activities and potential flashpoints for unrest.
- Changes in government attitudes towards international organizations.
- Regional dynamics that could impact the domestic situation.

Special Considerations

- Upcoming local elections and their potential to spark unrest.
- Religious and cultural events affect movement and security posture.
- Complex ethnic and regional dynamics influence security force reliability.
- Recent changes in security services leadership altering established relationships.

Outcome

Due to the structured approach and continuous assessment activities supported by ongoing operational intelligence, Riley Risk identified early indicators of escalating instability. This allowed the firm to advise the executive to conclude their mission, with essential activities completed, and depart the country in an orderly manner, well ahead of the mass exodus that followed. The proactive stance ensured the safety of the executive and maintained the organization's operational continuity, in stark contrast to the hurried evacuations many other entities were forced to undertake.



This case (among many others in the firm's experience) demonstrates how the framework enabled a nuanced understanding of the evolving risk landscape, allowing for proactive travel risk management and timely decision-making in a highly complex and rapidly changing environment.

Lessons Learned

The robust planning proved crucial when civil unrest erupted, requiring rapid adaptation of movement plans and eventual implementation of alternate evacuation routes. Key lessons included:

- The importance of maintaining multiple contingency plans.
- The value of cultivating diverse local support networks.
- The need for real-time information gathering and analysis capabilities.
- The critical role of clear, practiced protocols during crisis situations.

Practical Recommendations

Drawing from the author's own two decades of experience implementing this framework across diverse operational contexts, several key recommendations emerge:

- **Prioritize Flexibility:** While the framework provides essential structure, rigid application can be as dangerous as having no framework at all. Maintain the ability to rapidly adapt plans when ground realities diverge from initial assessments.
- **Leverage Local Knowledge:** Cultivate reliable local source networks to gain nuanced understanding of informal power structures, unwritten rules, and subtle indicators of changing conditions.
- **Focus on Sustainability:** Ensure that security measures can be consistently maintained throughout the duration of operations. Consider long-term impacts on team fatigue, resource availability, and local relationships.
- **Build Redundancy:** Implement robust backup systems for critical components such as communication methods, transportation options, and evacuation plans.
- **Integrate Security with Operations:** Ensure that security measures seamlessly support operational objectives rather than hindering them. Excessive security can be as problematic as insufficient protection.
- **Invest in Continuous Training:** Regularly update and practice security protocols to ensure all team members can execute them instinctively under stress.
- **Embrace Technology Judiciously:** Leverage technological advancements to enhance security capabilities but remain aware of potential vulnerabilities they may introduce. These vulnerabilities may be technical or organic, understanding the integration and providing training can help reduce the latter risk while robust selection and auditing of systems can help minimize the former.

Conclusion

Managing travel risk in complex, high-risk environments demand a systematic approach informed by practical experience. The framework presented in this paper provides a structured methodology for assessing, mitigating, and responding to travel risks while maintaining the flexibility required to address the nuanced challenges of diverse operational contexts.



Drawing from the author's own experience in managing travel security across a spectrum of environments—from conflict zones to complex urban settings, this framework offers a robust foundation for modern travel risk management. The author has personally trained numerous organizations on this framework, ranging from massive international development entities regularly operating in high and extreme-risk locations to executive protection travel teams responsible for one of the world's largest technology CEO's.

This diverse application demonstrates that the framework and process are incredibly simple and efficient, yet scalable to fit the demands of modern travel risk management, regardless of risk profile. As global complexities increase and the distinction between low and high-risk environments continues to blur, the importance of robust travel risk management strategies grows ever more critical. Security practitioners must remain adaptable, continuously refining their approaches as:

- Technological advancements change threat capabilities and create new vulnerabilities.
- Global power dynamics shift, altering the nature of state-based threats.
- Non-state actors evolve their tactics and targeting preferences.
- Climate change and environmental factors introduce new destabilizing forces.

Success in today's dynamic risk landscape hinges on both meticulous planning and effective implementation. The framework in this article addresses the shortcomings of traditional approaches by offering a structured yet flexible methodology capable of confronting modern threats, from state surveillance to health crises. Its simplicity and scalability make it an invaluable tool for organizations of all sizes and risk profiles, from small NGOs to multinational corporations operating in some of the world's most challenging environments.

By combining systematic analysis with adaptable implementation, this framework enables security practitioners to navigate the complexities of modern travel risk management across a spectrum of operational contexts. As global complexities intensify, the need for such robust, systematic approaches becomes increasingly critical. The ITRIPS framework provides a solid foundation for developing effective risk management strategies while remaining responsive to specific operational requirements.

As the protective services community continues to refine and professionalize travel risk management, engagement with both the broader security community and academic researchers is crucial. While this paper demonstrates the practical effectiveness of the ITRIPS framework through operational experience, further academic research is needed to quantitatively validate its components and compare its effectiveness against traditional approaches.

Specific areas which likely warrant scholarly investigation include:

- Comparative analysis of ITRIPS against established risk management frameworks
- Quantitative assessment of the framework's impact on incident prevention and response
- Evaluation of the model's scalability across different organizational contexts



- Investigation of the framework's effectiveness in varying risk environments
- Analysis of resource optimization through structured implementation

The author invites both practitioners to share their experiences and academic researchers to empirically evaluate this framework. Through this dual approach of practical implementation and scholarly validation, we can collectively advance the field of travel risk management while ensuring the continued safety of personnel and the success of missions in an increasingly unpredictable global landscape.

Author: Nathan Ackerman is the President and CEO of Riley Risk, Inc., a security risk advisory firm that engages in extensive protection operations for non-governmental organizations, governments, and private clients. He is a recognized expert on travel security and previously spent sixteen years in military and government service.

Endnotes

ⁱ Andreas Rodman, "Everything You Should Know about Travel Risk Management," Safeture, 2024, <https://safeture.com/everything-you-should-know-about-travel-risk-management/>.

ⁱⁱ "Nation-State Cyber Actors," Cybersecurity and Infrastructure Security Agency, 2024, <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>.

ⁱⁱⁱ Gurpreet Tung, "Technology as a Tool for Transnational Organized Crime: Networking and Money Laundering," *The Journal of Intelligence, Conflict, and Warfare* 4, 1 (2021): 118-127.

^{iv} John Nyaga, "Leveraging Technology for Enhanced Security: Solutions for Modern Challenges," Lauth Investigations, June 23, 2024, <https://lauthinvestigations.com/leveraging-technology-for-enhanced-security-solutions-for-modern-challenges/>.

^v Available at: <https://www.iso.org/standard/65694.html>.

^{vi} Arianne Mizuta, Kathleen Swindler, Les Jacobson, and Steve Kuciemba, "Impacts of Technology Advancements on Transportation Management Center Operations," Department of Transportation, 2013, <https://ops.fhwa.dot.gov/publications/fhwahop13008/fhwahop13008.pdf>.

^{vii} Saradha Balaji, Lolakpuri Shreshta, and K. Sujatha, "A Study on Risk Management in Corporate Business," *Involvement International Journal of Business* 1, no. 3: 197-209.

^{viii} Mike Atherton, "What Challenges do TMCs Face in Travel-Risk Management?," *Mantic Point*, June 1, 2018, <https://www.manticpoint.com/blog/what-challenges-do-tmcs-face-in-travel-risk-management>.

^{ix} Penny Swift, "Crisis Communication: Navigating Turbulent Waters with Clarity," Cerkl, October 17, 2023, <https://cerkl.com/blog/crisis-communication/>.





Your Partner in Secure Global Ground Transportation



Why Choose Eight Black for Secure Ground?

- **Unparalleled "Last Mile" Protection:** Seamless integration of advanced secure driving and meticulous route planning for total safety and comfort.
- **Attention to Every Detail:** From controlled motorcade movements to discreet vehicle selection, every element is tailored to ensure confidence for principals and EP teams.
- **Globally Trained Professionals:** Expert drivers with advanced training to handle high-stakes scenarios with precision and professionalism.
- **Rigorous Training & Real-World Simulations:** Exceptional preparation creates a team ready to exceed expectations, wherever you need us.
- **Making EP Teams Shine:** Our mission is to make you look like rock stars with flawless, secure, and discreet ground services.
- **Redefining Industry Standards:** When safety is non-negotiable, trust Eight Black for excellence in secure transportation.

Eight Black has served numerous Fortune 500 companies, high-profile individuals, and luxury travelers, consistently receiving accolades for our exceptional service, reliability, and attention to detail. We have successfully managed complex transportation and security operations for large corporate events, international travel, and high-security assignments.



Simon Chen
Founder Eight Black
Simon@EightBlack.com



Scott Jones
Director - Global Security
Scott@EightBlack.com

206 S Main St., Ste. 4
Longmont, CO 80501
eightblack.com
1(281)799-1877



EIGHTBLACK.

Secure | Global | Ground

ARE YOUR EXECUTIVES AS SAFE AS THEY COULD BE?

TOO MANY EXECUTIVE SECURITY PROGRAMS DON'T HAVE AN ANSWER FOR A COMMON THREAT VECTOR: MAIL, PACKAGES, AND DELIVERIES.

RaySecur's MailSecur® solution **detects threats** that x-ray and other screening approaches miss, including those responsible for some of the most high-profile incidents and shutdowns.

MailSecur is **the only screening solution** that can detect all nine CBRNE substances and more. **Visit us in Booth #103 at the IPSB 2024 Close Protection Conference to see how RaySecur is helping today's industry leaders keep executives, employees, and facilities safe.**



4 OF THE 5 LARGEST U.S. CORPORATION ARE PROTECTED BY MAILSECUR®



Elevate Your Security Career with ASIS International

Use code **WELCOME75** to get \$75 off membership dues through 2024.

Join Today!



Professional Articles



Impact of an Incident: Risk to Executives

Chuck Tobin

Introduction

Protectors are often expected to provide insights into the threats, vulnerabilities, and risks (TVR) facing their principal. Standards bodies and publications have documented this modeling well. This assessment provides the protector and those assigned to protect a baseline regarding the required protection. Quite often, one question needs to be asked or answered correctly – the question of impact. The answer is quite complicated, and whether you answer this question for a family office, private individual, or publicly traded corporation is different. This article will examine this concept and provide some recommended best practices for protectors.

Risk Matrix

Answers to the questions of risk are based on probabilities. Just how likely is it that the executive will become a victim of targeted violence, a plane crash, or a car accident that forever changes their future? The reality is that the likelihood of many threats we seek to mitigate is relatively low. Of course, this does elevate based on their proximity to threatening conditions or environments, being highly recognizable, or positions that may impact national security, etc. However, when we think about risk and probability, we must also consider impact as a critical aspect. Recognizing that risks exist and may impact the principal does not move the program any closer to decision-making unless we can express the risk in a digestible way. The World Health Organization (WHO) publication Strategic Toolkit for the Assessment of Risk (STAR) elaborates on this concept, noting that once the hazards are identified, the assessor should evaluate the likelihood of an incident and determine the impact. Risk modeling often reflects on a strategic risk severity matrix similar to the one produced by Grace LaConte.¹

Grace LaConte's Strategic Risk Severity Matrix

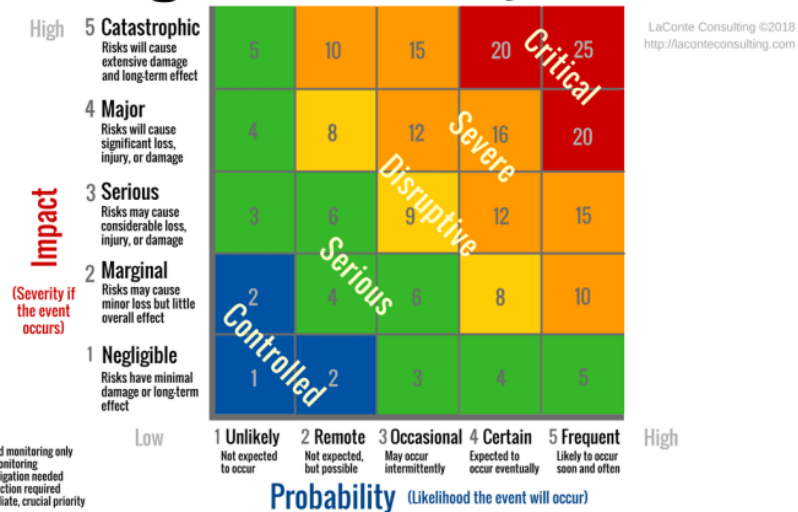


Figure 1

This matrix, utilized by the risk market, correlates the potential impact with the probability of occurrence. This additional step in the threat, vulnerability, and risk modeling process provides much greater context to the assessment. The strategic risk modeling matrix is a five-by-five square with 25 colored boxes that facilitate placing our unlikely-to-frequent events on a grid with our negligible to catastrophic incidents. As we define the impact and probability terms, a greater sense of relevance to the protection program comes to light. Using the probability of a fatal car crash published in Forbes Advisor Car Accident Statistics 2024, one in ninety-three people will be in a fatal accident;ⁱⁱ we could suggest that, at a minimum, a remote possibility exists that the executive could be in a fatal car accident. It is reasonable to suggest that a fatal car accident would prove catastrophic for most organizations in terms of costs, shareholder value, liability, or brand damage, and, of course, certainly for the now-deceased executive. Using the strategic risk severity matrix would place our score at 15. For risk assessment purposes, this would be considered a severe risk that needs to be addressed immediately.

Executive Security and Deaths

Research suggests that approximately seven executives die each year. While most of these are caused by natural causes such as heart attacks, some are the result of preventable incidents, including car crashes. In response, many companies have designed succession plans to help mitigate the impact on the organization. According to research conducted by Behn, Dawley, Riley, and Yang, the length of time it takes for an organization to identify a permanent successor is negatively evidenced in its operations.ⁱⁱⁱ

A myriad of incidents can occur permanently, changing an executive's future. Automobile accidents, plane crashes, abductions, and assassinations have happened, which have forever changed the lives of well-known business leaders and families. Arguably, the highest risk these leaders face occurs every day behind the wheel. Executives often drive themselves to and from work, out to social events, and on road trips to visit family or conduct business. Many will argue that there is no risk, and they can and will drive themselves; there is no need for a trained security driver. But in today's distracted driving world, a three-second glance at a phone to read a text moves a driver 180' at 60 mph. Those lost seconds could result in a driver crossing a line into head-on traffic, running a red light, or striking a pedestrian. The fault does not have to lie with the executive for tragedy to strike. A young, distracted driver could quickly end the life of an executive. Worse even, a distracted executive could strike another driver, killing that driver. Now, not only does the executive face the injuries of the accident and the remorse of their actions but also a massive civil liability, which could quickly be directed to the corporation or family.

Similar losses have been recorded in newspapers and courts around the world. The Walmart franchise has experienced losses due to the driving habits of a family member. Mrs. Walton has reportedly been involved in two notable vehicle accidents. One case resulted in the death of the other driver. The settlement amount is not disclosed, but the lack of subsequent litigation could suggest it was healthy.

Not every incident is the result of distraction or recklessness, though. Sometimes, executives are targeted. As is the case of the abduction and subsequent death of the ExxonMobil CEO, Sidney Reso. Mr. Reso was



abducted from his driveway by a former security guard who intended to take him and obtain ransom. But things went wrong during the abduction, and Mr. Reso was shot. He was taken to a storage unit by his captures, where he was confined without proper medical treatment. He eventually died from his wounds and the confinement.

Other executives have been lost due to violent altercations. During the 2008 Chinese Olympics, Todd Bachman was stabbed to death. Todd's daughter was married to the U.S. Olympic team coach. Todd was stabbed to death by a knife-wielding Chinese male who then jumped from the 130th floor of a building to his death. Todd was the CEO of Bachman's Inc., a home and garden store based in Minnesota. With the sudden loss of their Chairman of the Board/Chief Executive Officer, Todd Bachman, in August 2008, Bachman Industries faced extraordinary circumstances. They now needed to restructure their leadership team to ensure business continuity quickly. Fortunately, Todd had established a detailed succession before his death. Dale Bachman assumed the role of Chairman of the Board/Chief Executive Officer of Bachman's, Inc., with Paul Bachman being named President, and they continued business operations. However, members of the fourth generation of the business, which started in 1885, were faced with burial and succession planning.

In some cases, the nature of the business draws the executive closer to security conditions that make them a target. In one such case, the contract killing of Maurice Spagnoletti resulted in the loss of an executive. Mr. Spagnoletti, working in Puerto Rico at Doral Bank in San Juan, had unknowingly encountered a complex scheme utilizing bank resources. Not only had he come across the trafficking of cocaine and other narcotics, but he also came across a money laundering contract associated with suspicious maintenance contracts at the bank. The organization Mr. Spagnoletti discovered practiced Santeria, a cult-like religion of the Caribbean. When he left his office in San Juan to head home to his beachfront property, he traveled a well-traveled route to his neighborhood in Condado. As Mr. Spagnoletti drove his Lexus onto the busy Expreso De Diego, he came upon traffic. As he sat in the traffic, another car pulled up next to him, shots were fired into the passenger side window, and Mr. Spagnoletti was dead. This killing in 2011 sparked an investigation and prefaced investigations by the U.S. Federal Deposit Insurance Corporation (FDIC), resulting in the bank closing due to shrinking assets. Many of their challenges may have also originated from the associated criminal element of defrauding the bank.

The manager of an Indian branch of a car component company, Graziano Transmissioni, Lalit Chaudhary, was murdered by his former employees. He had been forced to reduce the number of employees due to this mass layoff. Mr. Chaudhary requested a gathering of terminated employees to talk to them. Unfortunately, he was beaten to death by these former employees.

The cement maker, PT Holcim Indonesia also experienced a significant event when their Chief Executive, Tim MacKay, was killed in an explosion in Jakarta at a hotel. This incident resulted in a share loss of more than five percent. These bomb blasts occurred at the JW Marriott and the Ritz Carlton hotels in the business district.^{iv}



When considering the spectrum of incidents that may face an executive, the samples above illustrate that the list is extensive. The threats that face them go beyond risks of targeted violence incidents such as assassination, kidnapping, and abduction. Health crises resulting from transportation-related, medical, and reputational incidents, including compromising their communications and sensitive personal information, are all additional aspects of the threat matrix. The CEO of BMW fainted on stage during a recorded presentation. This incident was reportedly the result of an extreme business and travel schedule that finally caught up to him. Incidents like this, unfortunately, are also recorded in the mortality rates of many executives who pass before their time. Protective programs must be diverse and consider these myriads of threats. Investment in time, personnel, and resources into each threat may vary, but those that have the highest impact, even if a low likelihood, must be addressed.

Quantifying the Risk

Quite often, executives decline protective measures to include security drivers, close protection, or enhanced security around them and their families, indicating the likelihood is too low, and the investment is not justified. The reality is that, while the frequency of these incidents is low compared to other less significant risk factors, the cost is very high. Even if the executive is not concerned about their safety and is confident in the continuity strategies they have put in place, the losses can be significant.

The importance of a CEO has become even more critical in modern times, at least according to the average cost in share price. Research produced by Jordan Reese in 2012 noted that from 1950 to 1969, in the four days before the CEO's death through two days after, the mean CAR rose from 2.8 percent. Comparing this to a 7% average loss during 1990-2009. This study also noted that when measured from the day before death to 30 days after, the mean CAR rose from 7.0 percent during 1950-1969 to 14.7 percent during 1990-2009.

The loss of a CEO typically results in a loss of share value in publicly traded companies if the CEO is considered a strong leader, visionary, or founder. This does not necessarily always occur if the CEO was not considered a strong leader.^v It is difficult to find a mean value when trying to present this in dollars. When the CEO of Herbalife, Mark Hughes, died of an overdose, the company witnessed a 12% share loss. This could suggest that shareholders concerned about the death were also concerned about the nature of his death, raising governance concerns. When Michael Chowdry, CEO of Atlas Air, died on January 24, 2001, in a plane crash, their stocks dropped 4.9%. Similarly, Micron's CEO's death in a plane crash caused a 2.8% stock price loss. Let us use these examples to determine what this meant in dollars:

- Atlas Air's 2022 income statement shows a 4.9% loss equals around \$17.4 million.
- Based on Micron's total revenue for 2024, a 2.8% loss equates to just over \$700K.
- Based on Herbalife's total revenue for 2023, a 12% loss equates to just over \$607 million.

A modest but complete protection program that covers ground and air transportation, close protection, and some residential security enhancement likely costs in the \$2.5 million range and, in many cases, is not considered a perk if supported by appropriate audits. However, this expense certainly can offset a



significant impact event. These programs, if properly administered, also create productivity for the executive.

Beyond the immediate impact on the share value, leaders must consider the effect of a tragic event on retention and recruiting. It is clear that if the CEO of a corporation is assassinated on the job, there will be some difficulties in recruiting a replacement. Once that candidate is identified, their employment contract will likely include enhanced security perks. If their contract does not, the investors certainly will demand it. This likely forced the organization into knee-jerk reaction spending.

However, the impact goes beyond the current vacant position and into the organization's body. Most public corporations include language somewhere in their published risk factors, shared with investors, that their ability to recruit and retain qualified talent is one of their most significant risk factors.

Other Considerations

Another consideration is the impact on employee engagement. Studies have recognized that organizational culture and work environment impact recruiting and retention. Studies have also shown that violence in the workplace has a direct impact on the perceived culture and work environment. In one study of 178 individuals, they found that 88% had experienced some form of workplace violence, and the study suggested a direct negative effect on employee engagement. While no studies have been identified that specifically correlate violent incidents against an executive and their impact on employee engagement, recruiting, or retention, the overall consensus from studies does suggest that the fear of violence does affect the work environment and culture.

Dollars, productivity, and shareholder value aside, the impact on a family in the event of the loss of a family member can be catastrophic. Certainly, the patriarch and matriarch of the family, if lost while leading the family office and business enterprises, can be costly to the organization. Reflecting on the stabbing death of Todd Bachman, CEO of Bachman's Inc. They were fortunate to have planned for succession, and in the end, the business continued to function and benefit the family. Beyond the business' life is the smooth transition of the family office to the next in line. Careful preparation to include a review of reporting, tax, ownership, and transition strategies is essential. But there is no escaping the tragic loss, and the emotional trauma family members went through unnecessarily. While death is inevitable, many high-impact incidents could be mitigated through proper protective strategies.

All of this leads us to the conclusion that executive safety programs must extend the conversation beyond threat, vulnerability, and risk into probability and impact. Threats with a low likelihood but an extremely high impact must be addressed. The organization can then make an informed decision to accept, mitigate, or transfer the risk.



Author: Chuck Tobin is President and CEO of AT-RISK International, LLC. Chuck brings over 25 years of experience in security consulting, executive security, investigations and training. As the Director of Security/Senior Consultant to three Prime Ministers/Presidential Candidates, Chuck has developed a global political campaign security expertise in violence threat assessment, investigations, executive security, and training.

Endnotes

ⁱ Grace Laconte, "How to Calculate the Impact and Probability of Business Risk," La Conte Consulting, December 2, 2018, <https://laconteconsulting.com/2018/12/02/calculate-impact-and-probability/>.

ⁱⁱ Christy J.D. Bieber, "Car Accident Statistics for 2024," *Forbes*, July 30, 2024, <https://www.forbes.com/advisor/legal/auto-accident/car-accident-statistics/>.

ⁱⁱⁱ "S.v. Deaths of CEOs: are delays in naming successors and insider/outsider succession associated with subsequent firm performance? *..," *The Free Library*, Retrieved November 22, 2024, from <https://www.thefreelibrary.com/Deaths+of+CEOs%3a+are+delays+in+naming+successors+and+insider%2foutsider...-a0144015368>.

^{iv} H. Suhartono, "Holcim Indonesia says CEO killed in Jakarta blast," *Reuters*, July 17, 2009, <https://www.reuters.com/article/world/holcim-indonesia-says-ceo-killed-in-jakarta-blast-idUSTRE56G0ZW/>.

^v Tayan Larker, "Sudden Death of a CEO: Are Companies Prepared When Lightning Strikes?," *Stanford Closer Look Series*, 2012, <https://www.gsb.stanford.edu/faculty-research/publications/sudden-death-ceo-are-companies-prepared-when-lightning-strikes>, 2.



Synopsis of the IPSB's Risk Intelligence and Protection Symposium, London, 10 October 2024

Samantha Newbery, PhD

Introduction

The IPSB's second Risk Intelligence and Protection Symposium was held in London on 10 October 2024. Representing the fusion of risk, intelligence, and protection, the day saw IPSB Past President Chuck Randolph set the scene before introducing six panels that provided a wealth of insights, whilst the day also provided networking opportunities. The IPSB is grateful to all the event's sponsors, as well as to speakers, panel moderators, delegates and to the note-takers who supported the production of this synopsis of the Symposium. Conducted under Chatham House rules, what follows are the central issues highlighted by each panel. It is hoped that sharing this synopsis will contribute to the development of best practice and, therefore, to the IPSB's goal of elevating industry standards.

Panel 1. Assassinations and Public Figures

Delegates were taken through a series of case studies from North America, Europe, and Africa, concerning politicians or political candidates who were the subject of assassinations, attempted assassinations or threats that did not make it to such an advanced stage. Motivations of attackers or would-be attackers include seeking fame, local or transnational crime, terrorism or seeking a specific change to policy. There is disagreement in the available literature regarding what signs to look for. Sometimes an explicit threat will be issued, but at other times the threat becomes apparent through one individual sending a large number of communications (such as letters) that individually are not that concerning as they do not issue a direct threat. This is one of many ways in which the available resources become relevant: do you have the resources to sift through all the correspondence received by a politician or the social media posts about them?

This leads to two other points. One is whether campaign staff – who may be volunteers or paid employees – understand what they should be looking for. This applies to other individuals too: an understanding of indicators of risk and the importance of reporting concerns should also be developed amongst the politician, their family, and other staff who are either around them or in their home. The second point is to what extent CP can or should also be investigators. Although there was a difference of opinion in the room on whether an individual could truly be good at both, the need for both was not disputed. Managing who has access to the principal, and whether volunteers in campaign offices for example are vetted, was also discussed, as was where the state stops being responsible for politicians and the private sector becomes responsible instead. The latter is further complicated at events, where there will be event security personnel as well as the principal's own security personnel.

Panel 2. Securing the Backbone: Supply Chains as Critical Infrastructure

Risks to a company can originate anywhere in the company's supply chain. Supply chains should be understood to include (but not be limited to): IT, data centers, contractors, distributors, the transport



infrastructure, Legal, and HR. Risks can be physical or reputational. When a reputational risk is realized, this can in turn damage the company's ability to retain staff. Geopolitics is pertinent to supply chains, not least because of the damage that can be done by working with a company that is owned by a country that starts a war. Companies are better able to understand reputational risk if it is quantified.

When planning to address supply chain risks, decisions on what to focus on should be guided by an understanding of what is likely to have the biggest impact on the company, as well as potential threat actors' most likely motivations and capabilities. Relevant data is voluminous, comes from multiple sources (ranging from teams on the ground to insurance companies), and is not always integrated. Data can also be incomplete, not least due to language or cultural differences when operating internationally. Encouraging security literacy amongst non-security personnel can help ensure they will record and share relevant data. All data has value.

Panel 3. When All Else Fails: Business Continuity and CP

This panel's key message is to be prepared and that being prepared depends upon having knowledge of what could happen. Planning should involve thinking about what can go wrong, for example, if mobile telephones or GPS do not work, or if there is a power cut either locally or regionally. Remember that even if the power is out, you may still be the target of eavesdropping. Ground truth is strategic (this picture changes comparatively slowly), operational (this changes at a medium pace), and tactical (this changes quickly and may not therefore be accurately represented in intelligence reports produced before deployment). Individuals physically present on the ground have access to different information from that available to those conducting intelligence work remotely. Trusted locals can be used to verify information.

Preparations should include lining up multiple alternative methods of communication along with prearranged rendezvous points. In the event of the outbreak or escalation of a conflict, a government may not be able to evacuate you out-of-country, and regular carriers may stop flying: this, too, should be prepared for. However, there is no need to plan for every scenario, but to plan to be able to respond, thereby adopting a resilient mindset.

Panel 4. Resurgence of Geopolitics (and Why it Matters)

Companies may become targets as a result of their associations with a particular country or with a company based in that country. This is illustrated by certain UK banks having paint thrown at their branches because of their associations. While these reputational risks stem from geopolitics, so too do risks to currency, the supply chain, and more. Geopolitics cannot be avoided and drives operational and tactical risks, hence the need for geopolitics to be understood. When operating in a conflict zone, contingencies should be in place in case of damage to transport and energy infrastructure in particular.

When considering the Middle East, this panel highlighted the ongoing cycles of retaliation and possibilities of escalation. In both this context and the Russia/Ukraine context, the panelists emphasized that a country's actions may not necessarily align with its rhetoric or policy. Russia's means of attacking the West include using organized crime rather than its own direct employees because this method is deniable and grants access to any country. A number of recent coups in Africa have deterred investors from making



deals with governments in case that government falls soon after. A final theme within geopolitics highlighted by this panel was the possible impact of the then-upcoming 2024 US Presidential Election both domestically and on delicate global conflicts.

Panel 5. AI: Friend, Foe, and Force Multiplier

Computing has evolved to the point where a machine can be trained to think. What is new about AI is not just the capability itself but that ChatGPT, for example, allows anyone to use AI without needing to be a programmer. AI can be a friend or a force multiplier by scanning and analyzing large amounts of data to find patterns or threats, reducing the workload for humans. Further, it can be used to create reports, speeches, and presentations quickly and to a high standard. While AI itself is not a foe, it can be used by people who intend to cause harm. There are also potential weaknesses in it because of weaknesses in the source data it is based on, as that data may not necessarily be reliable. It can, however, be trained to use only specific sources such as a company's own digital archives. AI is unlikely to stay as cheap as it is now forever, and companies are advised not to risk being left behind by failing to adopt it now.

Panel 6. Element X: Communicating and Coordinating

Breaking down the topic of communication and coordination, this panel explored what to communicate, to whom, by whom, how, and why. Communicating your value to the client should be taken into account rather than assuming they know the value of you as an individual or the value of what your business provides. Preparing for an operation should include ensuring you are aware of who you may need to communicate with on the ground. Who shows up and how they show up affect the building of relationships, as does tailoring your communications and communication style to your audience. Avoiding jargon and taking account of any international dimensions as well as variations in organizational cultures can also aid effective communication.

Coordination depends upon communication. It is also influenced by policies, which need to be practicable, need to be communicated, and need to be understood and learned so they will be used in live situations. The provision of training in coordination can usefully include live exercises, as long as these are set up carefully so they are suited to achieving the end goal. Additionally, the value of communicating information from the ground back to colleagues was articulated. Solving problems is often a team effort, and fixing gaps in intelligence depends upon a culture where everyone is willing and able to share what they know.

Author: Dr. Samantha Newbery is a Read in International Security at the University of Salford and an intelligence analyst and trainer for Optimal Risk Group Ltd. She received her PhD from Trinity College Dublin and recently published the book *Terrorist Informers in Northern Ireland* with Oxford University Press.



T-ray Imaging: Emerging Technologies to Combat Increasingly Dangerous Threats Concealed in Mail and Everyday Items

Alexander Sappok, PhD

Introduction

In 2024, the security community witnessed a continued surge in the sophistication and frequency of mail-based threats, highlighting vulnerabilities that affect the global security landscape. No sector of the industry has been immune to mail-based threats, which span powder threats targeting major corporations, high-profile individuals, critical infrastructure, and government facilities alike. Notably these threats have begun to shift from benign hoaxes containing innocuous powders to the use of more toxic substances including fentanyl and chemically laced paper. Mail has long been a popular attack vector because it offers perpetrators the guise of anonymity, requires little effort to execute, and can be used with minimal expense – in many cases, the cost of a postage stamp.

Why are mail-based threats happening? Recent societal, political, and economic issues continued to take center stage in motivating mail attacks:

- Increasing perception of corporations or high-profile executives deemed symbolic or representative of controversial or polarizing issues.
- Corporate downsizing leading to layoffs, the reversal of remote work policies, labor disputes, and related policy changes increasing the risk of threats from insiders.
- The contentious political landscape in the U.S. has already produced an unprecedented number of mail-based attacks using legitimate threats, including fentanyl-laced mail, targeting government facilities, U.S. election sites, and politicians.
- The ongoing Russia-Ukraine conflict leading to security ramifications for governments, private-sector corporations, religious organizations, and individuals.
- The Hamas attack on Israel and the subsequent war have led to an increase in attacks against religious organizations, educational institutions, and government facilities around the globe.
- The targeting of high-profile individuals and private residences, ranging from athletes as a result of widespread sports betting to entertainers taking public stances on controversial topics.

Each of these issues, among others, have motivated affected individuals to lash out through the mail to express frustration or attempt to effect change. As a result, security spending for key executives by some of the world's largest corporations has increased significantly over the past twelve months.

Comprehensive Insights into Emerging Mail Threats

One of the largest barriers to developing effective strategies to mitigate mail-based security risks is the lack of accurate, timely, and relevant data required to understand the full scope of the problem. There are several government data sources that provide an aggregate view of the prevalence, magnitude, and severity of dangerous mail threats. However, the publication of these official statistics often lags behind current incidents and new and emerging threats by up to twelve months or more. Moreover, mail threats



often go unreported, and those that do make the news cycle are often seen as individual and isolated events.

To provide security practitioners with both a holistic view of the complete mail-borne threat landscape, and access to real-time information on current and emerging threats, RaySecur's 2023-2024 Mail Security Report compiles disparate sources of information from sources such as:

- U.S. government agencies including the United States Postal Inspection Service (USPIS) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).
- International data from the Global Terrorism Index (GTI).
- The RaySecur Threat Data Center (TDC), an informational product prepared using open-source reporting and global analysis of mail incident data in near real-time.

The data presented in the following sections summarizes key findings for the 2023-2024 Mail Security Report and introduces new and emerging technology approaches to address these threats.

Increasing Threats, Risks, and Vulnerabilities: Official U.S. Government Data

Data from official government reports show mail threats eliciting a response from either the USPIS or ATF continuing on a large-scale basis. Key findings are as follows:

- More than 7,000 suspicious mail incidents reported in the United States by both the USPIS and the ATF – more than 20 per day. Although the data is somewhat dated, the 2022 USPIS Annual Report found that the agency responded to more than 1,800 suspicious mail incidents alone.^{i,ii}
- Less than 2% of mail threats result in convictions based on USPIS data. According to the 2022 USPIS report, investigations only led to 21 arrests and 19 convictions, demonstrating the ease of carrying out mail-based attacks with a limited chance of being caught and prosecuted.ⁱⁱⁱ
- 2023 and 2024 saw increased threat activity related to the Presidential Election. The U.S. Department of Homeland Security, FBI, and USPIS all issued specific security alerts. This included the Cybersecurity and Infrastructure Security Agency's (CISA) Election Security Resource Library, which included warnings about the increased use of hazardous materials such as fentanyl, anthrax, and other dangerous substances sent in the mail.^{iv}

These findings also highlight a new change in the behavior and motivation behind mail-based threats. Of particular concern is a shift from benign hoax threats to increasingly harmful attacks. In the past, many white-powder mail threats turned out to be flour, baking soda, or other harmless substances. The ease of procuring highly toxic substances, including fentanyl, has given rise to the use of these substances in targeted mail threats. As a result, more of these threats now contain fentanyl and other dangerous chemicals – reflecting a new intent to cause actual harm as opposed to attempting to simply disrupt operations or intimidate people in power.

Current Events and Emerging Trends: Findings from the RaySecur Threat Data Center

RaySecur's analysis of open-source mail incident data, targeting both public- and private-sector recipients, is consistent with the general trends observed in official USPIS and ATF reports. In 2023, the RaySecur TDC



compiled 223 mail-based threat and smuggling incidents reported in the public domain across the United States and globally in English-language media sources. These events likely represent a small fraction of the total, as many security incidents are handled internally or are reported to local law enforcement but may not make it to the public media. Further complicating reporting is the fact that private- and public-sector organizations are under no legal obligation to report mail-based threats.

Nonetheless, these findings present timely insights into new and emerging trends, targets, and methods used by bad actors to send dangerous mail items to a range of targets. Highlights from the report included key findings and analysis such as:

- 95% of mail threats were delivered via letters or small parcels small enough to be deposited anonymously into a curbside drop box.
- 59% of mail threats contained some type of powder.
- Mail threats resulted in 31 injuries reported in the public domain in the United States.
- 94% of these injuries came from letters.

These insights offer a snapshot into the ongoing and evolving nature of mail threats, reflecting patterns that suggest not only continued risks but also emerging tactics targeting a broad range of sectors. Figure 1 presents a summary of key statistics highlighted in the report.

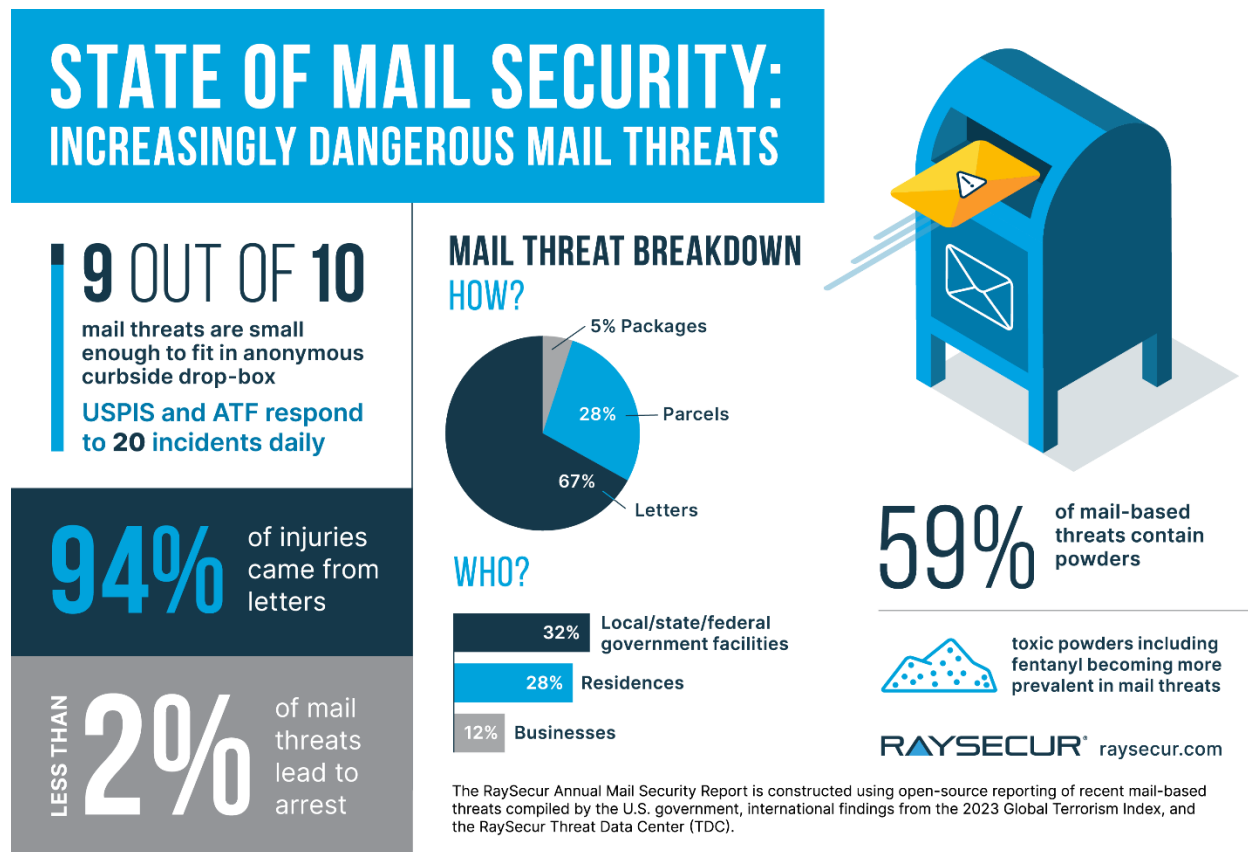


Figure 1. Mail-borne threat statistics cataloged in 2023-2024 RaySecur Mail Security Report.^v



As shown in Figure 1, mail threats continue to affect many organizations from high-profile Fortune 500 companies to small businesses, religious non-profit organizations, and government agencies. Of particular note is the prevalence of threats targeting private residences due both to the ease of obtaining personal address information and the often-lax security measures in place in these locations. Media reports provide additional insights into the mechanisms, targets, impacts, and motivations behind these threats. Understanding these dynamics can help organizations better anticipate, detect, and prevent mail-based incidents in an increasingly complex threat landscape.

What to Expect in the Year Ahead?

The possibility of future threats and hostilities against corporate and government targets, as well as private individuals, are a real concern in light of current events. These include an increasingly polarized political landscape and fallout from the 2024 U.S. Presidential Elections. These developments have already influenced mail threats and will certainly lead to more in the months ahead.

Economic conditions play a role, too. Ongoing uncertainty about inflation, high interest rates, mass layoffs, and unemployment lead to fear, even anger – and have historically resulted in an increase in the total number of threats. In some cases, these threats may be carried out by employees or other insiders, who may have an easier way to access high-profile executives and spokespeople. While the risk of insider threats could be mitigated with more effective and overt mail-screening technologies and procedures, the majority of companies simply aren't as prepared as they should be.

Executives and high-profile figures are now being targeted more than ever in reaction to the public's perception of the company's symbolism or stance on a particular issue or in response to political statements against them in this election year. Large multi-national corporations must also contend with fallout from broader geopolitical events including ongoing wars and regional conflicts. Many of the biggest companies – such as BlackRock, Disney, JP Morgan, and Pfizer, among others – all significantly increased spending on security for their chief executives in 2023 as reported in public disclosures.^{vi}

Finally, the ease of access to extremely potent substances like fentanyl continues to be a real and growing concern as they may be weaponized as threats against high-profile government and corporate targets. Security teams would be well-advised to implement more effective screening approaches, including the adoption of personal protective equipment and safe mail handling protocols, as they face the same tactics and risks.

Terahertz Imaging: Emerging Technologies to Combat Concealed Threats

The mail threats described in the previous section have generally evaded conventional screening and detection approaches to reach their intended targets. While X-ray imaging has been used for over 100 years and is very effective at screening large items such as luggage to detect weapons and explosive threats, conventional X-ray security screening systems are simply not sensitive enough to detect the most common mail threats including liquids, powders, and chemically treated papers.



Unlike the medical industry which has adopted a range of non-invasive imaging technologies to “see inside” the human body including X-ray, magnetic resonance imaging (MRI), and ultrasound, the availability of similar tools and imaging capabilities has lagged in the security space. New and emerging T-ray imaging approaches now offer the security industry similar imaging capabilities to ultrasound in the medical space – specifically real-time, dynamic video imaging – with much higher sensitivity than X-ray to detect small quantities of liquids, powders, and other threats concealed inside mail items.

T-rays, span the Terahertz (THz) frequency range from 100 GHz (0.1 THz) to 10 THz and reside almost right in the center of the electromagnetic spectrum. They have largely been unexploited due to the difficulties associated with developing cost-effective technologies capable of generating and detecting THz signals. This region of the electromagnetic spectrum has long been known as the Terahertz Gap.

At the low end of the electromagnetic spectrum, conventional electronics can readily be used to generate and detect low frequency signals for applications ranging from AM and FM radio to cellular communications and WIFI. On the opposite end of the spectrum, optical technologies can readily be used to generate and detect very high frequency signals including X-ray, infrared and even visible light energy. T-rays reside right in the middle of the spectrum in a region that was previously too costly and complex for either electrical or optical technologies to exploit – this is no longer the case.

Millimeter waves (mmWaves) sit right below the T-ray frequency band, and their applications have grown significantly over the past decade. These applications now span 5G wireless communications to automotive radar systems for autonomous vehicles, and even airport checkpoint security screening systems to detect concealed threats on people, generally operating in the 30 – 80 GHz frequency range depending on the application. These advances in mmWave technologies have paved the way for much lower cost components capable of operating in the THz frequency range.

T-rays are interesting for use in security imaging for a number of reasons. Unlike X-rays which require radiation safety measures, T-rays (like mmWaves) do not generate ionizing radiation. T-rays are safe for screening people and also allow operators the ability to interact with the items they are screening. T-ray screening systems provide a live, real-time 3D video of concealed threats, in comparison to static 2D imaging generated with traditional X-ray screening systems.

Since T-ray imaging systems are generally low power and do not generate ionizing radiation, they can also be up to ten times smaller than comparable X-ray systems, which require heavy lead shielding to contain the X-ray radiation. This allows T-ray systems to be very portable for use in mobile screening applications, including mounted inside vehicles, or in handheld battery-powered systems.

Terahertz imaging also allows operators to directly manipulate objects during screening, enabling real-time 3D imaging that reveals motion inside a sealed object – grains of powder moving inside an envelope for example, or a small quantity of liquid moving inside a closed container. The ability to image in full motion allows for intuitive screening and detection of a wide range of potential threats with less training overhead than may be required for X-ray systems which provide only a static 2D image. The 3D imaging



also provides dynamic insights, allowing operators to rotate items and observe suspicious contents from multiple angles.

Another important aspect of T-rays specific to mail-borne threats is that T-rays offer much higher sensitivity compared to X-rays (up to 300X higher sensitivity) when it comes to detecting complex or low-density materials like powders, liquids, and chemically treated papers. This high sensitivity enables the detection of even very small quantities of hazardous materials at the milligram level concealed within sealed items.

In summary, emerging T-ray imaging technologies now offer security practitioners new capabilities to combat increasingly sophisticated physical security threats concealed in everyday items. Similar to the medical industry which has long benefitted from a range of non-invasive imaging tools, T-ray imaging now provides the security industry with complementary capabilities to X-ray scanners ideally suited to detect small quantities of complex and low-density substances, which have emerged as the predominant threats sent via the mail and readily concealed in a host of seemingly commonplace items.

Summary: Key Observations and Security Implications

Mail-based threats continue to offer malicious actors a straightforward and relatively low-risk way to instill fear, disrupt operations, and, in some cases, cause serious harm on a global scale. Today, 95% of mail threats were delivered in letters or small parcels, allowing them to fit in anonymous curbside drop boxes. New and emerging threats are using more toxic powders, including fentanyl and treated papers, yet low prosecution rates (2% in 2023) make mail a relatively low-risk but high-impact threat.

These threats are often partially successful, especially when the target lacks robust security protocols, or an in-depth understanding of the risks posed. Yet for those that do, the primary method of detecting and preventing mail threats continues to be based on manual screening processes – relying on visual and tactile inspections – that may be supported by X-ray scanners and perhaps canines. Unfortunately, a high number of threats still evade detection with these approaches, even by some of the world’s leading security teams.

T-ray imaging technology offers new and advanced capabilities to mitigate these threats and overcomes many of the limitations of traditional screening methods. This technology provides security teams with an additional layer of defense to detect a wide range of potential threats including powders, liquids, and chemically laced papers concealed inside everyday items, including mail, that might otherwise evade detection. By integrating terahertz screening technologies, security teams can significantly reduce risks, improve response times, and enhance their overall security protocols, creating a more robust barrier against the evolving landscape of mail-based threats.



Author: Dr. Alexander Sappok is the CEO of [RaySecur](#), a company specializing in advanced security imaging technology. Before leading RaySecur, Sappok founded FST, Inc., an MIT spin-out focused on advanced RF sensing technology, which was later acquired by CTS Corporation. He holds over a dozen patents and two R&D100 awards and has both MS. and PhD degrees in Mechanical Engineering from MIT, where he also held the Cummins-MIT Fellowship.

Endnotes

ⁱ The United States Postal Inspection Service, *Annual Report 2022*, 2022, https://www.uspis.gov/wp-content/uploads/2023/07/508_USPIS-ARFY2022-annual-report.pdf.

ⁱⁱ The United States Bomb Data Center (USBDC), *Explosives Incident Report*, 2022, <https://www.atf.gov/resource-center/docs/report/2022-explosives-incident-report-eir/download>.

ⁱⁱⁱ The United States Postal Inspection Service, *Annual Report 2022*.

^{iv} The Cybersecurity and Infrastructure Security Agency (CISA), *Election Mail Handling Procedures to Protect Against Hazardous Materials*, 2024, <https://www.cisa.gov/resources-tools/resources/election-mail-handling-procedures-protect-against-hazardous-materials>.

^v RaySecur, *Annual Mail Security Report 2023-2024*, 2024, <https://www.raysecur.com/state-of-mail-security-2023-2024-raysecur-annual-report/>.

^{vi} Charlotte Gifford, “BlackRock Steps Up Security for Larry Fink after “Anti-Woke” Backlash,” *The Financial Times*, April 21, 2024, <https://www.ft.com/content/c1296bc4-978b-45c3-83db-c798d2439062>.



Enhancing Last Mile Security: A Guide for Executive Protection Companies Partnering with Secure Global Ground Transportation Services

Scott Jones and Simon Chen

Introduction

In the world of executive protection (EP), safeguarding principles are about more than just physical security. It requires careful planning, coordination, and an unwavering commitment to mitigating risks. Among the various stages of travel, the "last mile"—that final stretch of a journey to a principal's destination—presents unique vulnerabilities. Just as an EP team meticulously strategizes every movement, building a strong partnership with a secure ground transportation provider is key to safeguarding the principal throughout this critical phase. This article explores how EP companies can collaborate effectively with specialized firms like Eight Black to enhance last-mile security, focusing on the "first mile" and "last mile" as distinct but interconnected aspects of building an effective partnership.

The First Mile: Establishing Trust and Alignment

"In executive protection, details matter. The trust we build during the planning phase directly impacts the success of the mission," says Simon Chen, Founder of Eight Black. "Our commitment is to ensure that every aspect, from the route to the personnel, is meticulously aligned with the needs of our clients."

A successful partnership between an EP company and a secure ground transportation provider begins with a foundation of trust, clear communication, and mutual objectives. In the metaphorical "first mile," executive protection companies should emphasize the following:

- **Thorough Vetting and Due Diligence:** It's easy to be impressed by luxury vehicles and flashy branding, but true partnership requires digging deeper. Scott Jones, Director of Global Protective Solutions at Eight Black, stresses the importance of prioritizing personnel over vehicles: "What we look for are the right people, the right chauffeurs, and the right security drivers." Due diligence should include investigating the provider's history, safety record, driver screening process, and dedication to ongoing training.
- **Shared Security Culture and Standards:** Secure ground transportation is about more than just safe driving; it requires alignment on core executive protection principles. EP companies should seek partners with a proactive security-first mindset and a strong emphasis on risk mitigation. Jones notes that Eight Black prioritizes drivers who anticipate both client and EP lead needs, highlighting the importance of seamless service integration.
- **Clear Communication and Expectation Setting:** Open communication is the bedrock of a strong partnership. This includes defining roles, preferred communication channels, and expectations for real-time information sharing. EP teams should feel confident in asking about operational procedures, emergency protocols, and driver training, ensuring all parties are on the same page.



- **Logistics and Route Planning Focus:** Secure ground transportation extends beyond getting from point A to point B. It requires detailed route planning, the identification of safe havens, and an understanding of local environments. Eight Black’s drivers are trained to know primary and secondary routes, emergency facilities, and pre-determined safe areas such as embassies or fire stations, ensuring comprehensive preparedness.

The Last Mile: Ensuring Seamless and Secure Execution

Once a strong foundation is established, attention must turn to the “last mile”—the effective execution of secure ground transportation services. This phase involves:

- **Integrated Operations and Communication:** The ground transportation team should be an extension of the EP detail, with shared situational awareness and adaptability to changing circumstances. Eight Black’s use of a world-class global communications platform for real-time tracking and communication exemplifies their dedication to seamless integration.
- **Highly Trained and Discreet Security Drivers:** Security drivers are central to last-mile safety. They must possess advanced driving skills, situational awareness, and the ability to remain composed under pressure. According to Jones, Eight Black aims to strike a balance: their drivers must be highly capable without coming across as overly aggressive, providing both protection and comfort for principals.
- **Proactive Threat Assessment and Mitigation:** The “last mile” often involves travel to predictable locations like hotels or corporate offices, making it a vulnerable phase. It’s crucial for EP companies and ground transportation providers to work together on threat assessments, route analysis, and contingency planning.
- **Strategic Vehicle Selection and Maintenance:** Vehicle choice plays a role in last-mile security but should align with the specific needs of the mission. Whether selecting armored vehicles for high-risk environments or discreet SUVs, Eight Black takes a nuanced approach, understanding that a well-maintained vehicle can be both a transportation tool and a security asset.
- **Continuous Improvement and Debriefing:** Continuous improvement is essential to staying ahead of potential threats. After every mission, debriefs should be conducted to evaluate performance and identify areas for improvement. This collaborative reflection strengthens partnerships and keeps teams agile in responding to evolving security challenges.

Conclusion

In executive protection, the last mile can mean the difference between a secure journey and one fraught with risk. By establishing strong partnerships built on mutual trust, clear communication, and aligned security standards, EP companies can enhance their operational effectiveness and provide a seamless experience for principals. The first mile—where trust is built—and the last mile—where plans are executed—are equally important stages in this critical partnership. By collaborating closely with specialized firms like Eight Black, executive protection teams can elevate their service, ensuring principals are not only protected but also supported with the utmost discretion and professionalism throughout their journey.



Authors: Both authors are key members of the executive protection firm Eight Black. Simon Chen is the Founder of Eight Blacka, and Scott Jones is the Director of Global Protective Solutions at Eight Black.





KEELSON
▶ STRATEGIC

Proven Experience that Facilitates & Empowers Daily Life

We recognize that security is not just a one-size-fits-all solution...

At Keelson Strategic, we understand the importance of selecting a top-tier security firm to protect your Principal and their family. As a global full-service solutions partner with a presence in over 175+ countries, we craft dependable, unparalleled white glove experiences that support and empower ultra-high-net-worth individuals, executives, family offices and corporations, ensuring that protection is seamlessly woven into their lifestyles.

Our approach is rooted in partnership. We prioritize understanding the unique needs of each Principal, creating security programs that adapt to evolving threats. Keelson Strategic provides a comprehensive suite of services, expertly tailored with precision and expertise, designed to safeguard what matters most.

Experience Personalized, World-class Security Services:

-  Executive Protection
-  Transportation Security
-  Global Security Operations
-  Special Event Security
-  Risk, Threat & Vulnerability Assessments
-  Penetration Testing & Red Teaming

At Keelson Strategic, we don't just protect your Principal—we enable peace of mind. Built on a foundation of trust, we are committed to the highest standards of service, continuously raising benchmarks across the industry through innovation, discipline and an unwavering pursuit of excellence. Our focus is to deliver solutions that address immediate risks, while anticipating future vulnerabilities to ensure optimal and lasting serenity.

 info@keelsonstrategic.com


 careers@keelsonstrategic.com



**Veteran Owned
and Operated**




**YOUR TOP TIER PARTNER IN
AUSTRALIA, ASIA AND THE PACIFIC**

 **Executive Protection**

 **Risk Management**

 **Remote Medicine**

 **Transport & Logistics**

 **Infrastructure Security**

panopticsolutions.com
info@panopticsolutions.com



SKOPENOW

**Unlock the power of
open-source intelligence**

for enhanced situational awareness
and internet investigations.

About Skopenow

Skopenow is a comprehensive OSINT platform that enhances security assessment for high-profile individuals. The platform's AI models analyze millions of publicly available data sources in real time, generating alerts and insights that help identify potential threats across the digital and physical landscape. With 1,500+ customers, including law enforcement agencies and corporate security teams, Skopenow provides critical intelligence for proactively safeguarding VIPs against emerging risks and online content that could compromise their security.

Our products

Entity Search

Large-Scale Due Diligence

Situational Awareness

Link Analysis





Get in touch

Feel free to call us at (800) 252-1437 or email us at info@skopenow.com. You can also live chat with a team member for support and sales-related questions. Customer support is available M-F from 9AM-9PM ET.

Try us out



Visit Skopenow.com/try and sign up for our free 7-day pilot.

Follow us:    

Skopenow.com

Book Reviews



The Use of Informants on Terrorism in a “Quagmire”. A Review of: Samantha Newbery, *Terrorist Informers in Northern Ireland*, Oxford University Press.

David Page

This is an impressive, detailed book reflecting the author’s long focus on the use of informants in countering terrorism, primarily in Northern Ireland and to a far lesser extent in the Irish Republic. Terrorism has simply “not gone away” and is unlikely to do so given the history, alongside all the issues and interests involved – even after The Good Friday Agreement (1998) and the end of Provisional IRA activity. An example in 2020 of one informant in The New IRA is also cited.ⁱ

No better illustration of “not gone away” is found in the chapters on the investigations in both nations, into the use of terrorist informers. Only a few days ago the 1989 murder of solicitor Patrick Finucane was back in the press over the glacial pace of having a British public inquiry established.ⁱⁱ It is the only inquiry of five recommended by Canadian Judge Peter Cory QC that has not been held.

Note the author in March 2024 made amendments to incorporate the publication of the Operation Kenova Interim Report.ⁱⁱⁱ In August 2024 it was publicly announced that MI5 (Security Service) had provided new documents, “hundreds of pages” and a review was underway. A BBC News report cited the new Kenova leader, Sir Iain Livingstone: “Our initial assessment is that the files contain significant new material which appears to point to new investigative leads not previously known....However, the material does appear to cast doubt on some of the documents and witness evidence obtained by Kenova and some statements made in the interim report, including information provided by the security service around the dates when they became aware of the agent Stakeknife.”^{iv}

Peter Taylor, a veteran BBC reporter on “The Troubles,” commented (cited in part): “Operation Kenova thought its work was done. Sir Iain and his predecessor, Jon Boutcher, now chief constable of the PSNI, had been assured that they had been given full access to all MI5 files related to Stakeknife. This proved not to be the case. To many on both sides of the border, the revelation of the new files will come as no surprise.”

A key, recurring theme in the book is “the tension between the value of intelligence and the value of convictions” or a conundrum—the tension between the intelligence prism and the law-and-order prism—lies at the heart of this book. At times the scale of violence – for years – meant that criminal law enforcement was not a practical option, and intelligence was given the priority.^v Disruption in many forms occurred, which was based on intelligence, and on many occasions, nothing was done – a number of incidents are referred to.

The UK and Ireland faced a terrorist threat before, during, and after The Troubles from very small groups who pursued their political objectives through the tactic of terrorism – some describe this as political



propaganda – which invariably meant death,^{vi} life-changing injuries and long-lasting psychological trauma. In the “early years” there was a near complete lack of knowledge about who was responsible, and measures were used that on reflection later were harmful to public safety and a political settlement,^{vii} notably the mass searching of homes^{viii} – often in West Belfast – and the use of internment without trial (August 1971 till December 1975).

A significant part of the British response to The Troubles was the deployment of the Army in August 1969, initially to ‘keep the peace’ after rioting overwhelmed the Royal Ulster Constabulary (RUC, Northern Ireland’s police force) and the decision soon after that the Army would have primacy till 1976 or 1977 in leading the response. The Army, under Operation Banner, continued to provide support till 2007^{ix} especially in some rural counties that were the main state presence for many years.

Over the years the RUC were reformed, strengthened, and enabled to reassert “police primacy.” Other intelligence agencies assisted in various ways: the Security Service (MI5), Secret Intelligence Service (MI6), and Government Communications Headquarters (GCHQ). It was the RUC Special Branch that handled most informants, MI5 had very few and the Army via the Force Research Unit (FRU) had the remainder.^x

One author, William Matchett, ex-RUC and Police Service of Northern Ireland (PSNI, the RUC’s successors as Northern Ireland’s police force), in his book, assessed that approximately 60 percent of the intelligence Special Branch collected during ‘The Troubles’ came from informers.^{xi} Intelligence can be about the terrorists’ tactics, strategy and politics; the author describes this as: “hard information concerning the terrorists’ structure, their commanders’ meeting places, their [arms] dumps, and above all their intentions.”

I agree that as the author states: “intelligence is not evidence.” It can and does provide a starting point for further development,^{xii} which can become evidence and without it state resources cannot be targeted.^{xiii} The development of ‘technical means’, notably the surveillance of communications, CCTV and data analysis does help, but informants are still needed. There is a value in gathering intelligence when terrorist suspects are imprisoned,^{xiv} whether it uses informants or other methods, such as befriending their partners or relatives to gain assistance.

The thirteen chapters of the book cover the use of terrorist informers, often with well-known individuals used as examples, notably the ‘golden egg’ of British intelligence Agent Stakeknife (now deceased) in Chapter One, describing the extreme challenges posed when handling informers.

One of those challenges was the history of a reluctance by civil servants and politicians to not legislate on informant handling (See Ch. 6). This has been recently alluded to elsewhere,^{xv} it was a *revelation* to read that Raymond White (RUC Head of Special Branch) asked Prime Minister Margaret Thatcher directly in 1986 what his handlers should do when running informers within terrorist groups. In response, he was instructed to *carry on, but not to get caught*.



I note that Sir David Omand is cited:^{xvi} “ministers should have provided sufficient strategic and legal guidance to the generals running the campaign.” When the FRU informant at issue, Brian Nelson, who was the Loyalist paramilitary Ulster Defence Association’s intelligence officer, was being considered for prosecution there was a debate in the British cabinet, particularly between the Attorney General and Tom King, Defence Secretary, who is cited as saying: “We are dealing with terrorists, thugs and hooligans and our agents must be drawn from such people...Cabinet discussions focused first on how many lives he saved and then on the dangers of disclosing sensitive information during a trial.”

Brian Nelson was investigated by the Stevens Inquiry in 1992, which led to his prosecution. He made a plea bargain, was jailed, and later died in exile. Note two cited authors,^{xvii} one being Peter Taylor, have written that once Nelson was removed the Loyalists began out-killing the IRA for the first time in decades. One should ask was this possibility considered? Was this politically sanctioned as some ask?

Sir John Chilcot, at one point Permanent Secretary, Northern Ireland Office, commented in 1993: “The existing law appears to leave agents, handlers, and others involved in the intelligence process—including Ministers—unduly exposed.’

In the build-up to the Regulation of Investigatory Powers Bill (known as RIPA, 2000) being presented efforts were made by the RUC to get a section on how to authorize a Covert Human Intelligence Sources’ (CHIS, this Bill’s name for informers) criminality included. In the words of a former senior RUC officer Sam Kinkaid, ‘the Government absolutely refused.’

RIPA was the first legislation passed on informants; it covered the regulation of informers, the circumstances in which they could be used, how their use was to be authorized, and which public authorities could use them. It was *only* the passing in 2021 of the CHIS (Criminal Conduct) Bill, that there was statutory regulation of informers’ criminality. This legislation is fully covered in Ch.7. as to whether immunity from prosecution should be granted for all offences or only the less serious ones, and which post-holder or organization is best placed to provide effective but independent oversight of authorizations for informers to commit offences.

Clearly in Northern Ireland, which was a small society where everyone was known to someone (even more so in the rural counties) and with a real threat of death particular attention was needed to ensure an informant remained anonymous.^{xviii} Incredibly the author refers to a joint republican–loyalist operation when the poison strychnine was smuggled into the supergrass annex of Belfast’s Crumlin Road prison, it did fail though!

The author has several examples where informants survived for long periods,^{xix} far longer than those commonly found in the UK. What was of note was the use of exile,^{xx} invariably to elsewhere within the UK. How many informants were there? Following a security breach in March 2002, so after the end of The Troubles, when the Provisional IRA stole RUC documents, government and republican sources told the BBC that this break-in exposed so many informers ‘that it posed an impossible question: how could they kill them all?’ Some claim that roughly one in thirty or one in forty of the IRA’s “frontline membership’



was an informer in 1976–87, and that one of the eight Loughgall attackers was an informant. Add in that ‘the constant revelations after 1998 imply that the figure was probably higher.’ Another former police Criminal Investigation Department (CID) officer claimed ‘every fifth or sixth’ member of the Ulster Volunteer Force (UVF), a loyalist terrorist group, around the year 1990 was an informer.

It is worth noting that in 2003 the PSNI’s CHIS Review led to 12% of the PSNI’s informers having their relationship terminated because they ‘had been too deeply involved in criminal activity for their continued employment to meet the legal and ethical standards’ of RIPA 2000 and another 12% were terminated as they no longer had access to relevant intelligence. Over one hundred informers were dismissed as a result of this review.

Allegations of state collusion with terrorists regularly appeared and have led to investigations by the British and Irish governments (Chs.8-12). Collusion – which is not legally defined – could be the passing of information, activity to direct attacks, or the supply of expertise and weapons.

The author refers to Robin ‘the Jackal’ Jackson who was a UVF leader, a member of the British Army’s Ulster Defence Regiment, only in 1972-1974, described as the most prolific murderer in the history of Northern Ireland, personally involved in the murders of up to fifty, if not more people.^{xxi} There is evidence to suggest he was an informer. Then adds a remarkable comment by a retired CID officer – note it is unclear if the officer was with the RUC or another body: it was “inconceivable that the Special Branch and/or the British Army would not try to recruit someone as influential as Jackson for intelligence purposes. . . . it would have amounted to a dereliction of their duty if they did not attempt to do so.”

The Robert Hamill murder in April 1997 is used as an example (Ch. 9) and I stress the passage of time and that the report is still not published. The Inquiry was set up in 2004, with an interim report published in March 2010, the full report being held back since due to criminal prosecutions.^{xxii} The one person prosecuted, in June 2024, was ex-RUC Reserve officer Robert Cecil Atkinson who was sentenced to 12 months in prison for conspiring to pervert the course of justice in relation to police investigations into the killing of Robert Hamill in 1997.^{xxiii} Trial judge Patrick Lynch remarked to Atkinson that he had been “a disgrace to [his] uniform and have continued to serve as a police officer for years afterwards as a criminal - for there is no other description for you.” The inquiry’s website shows no sign of an update or publication. In October 2024 a new inquiry chair was appointed: Sir John Evans, ex-Chief Constable Devon and Cornwall Police (1998-2002) and a previous member of the inquiry.^{xxiv}

The murder (Ch. 11) in February 1989 of solicitor Patrick Finucane, is by the government’s own admission in the 2010 De Silva Review’s report, released in 2018 as part of a court action, “the big one” in terms of allegations of state ‘collusion’ with loyalist terrorists. “Paid state agents were directly involved in the killing....Some of the evidence available only internally could be read to suggest that within Government at a high level, this systemic problem with loyalist agents was known, but nothing was done about it.”

After analyzing a considerable amount of evidence showing what intelligence Brian Nelson provided, De Silva concludes that both agencies (the Army’s FRU and police Special Branch) were responsible for sharing



intelligence and ensuring it was exploited. It makes sense that responsibility should be jointly held when potentially lifesaving, time-sensitive intelligence is at hand. Incredibly consideration was given briefly given to petrol bombing his home in order to force him to move out, keeping him away from the threat. This was seen as an option to act on the intelligence received!

Three externally led British criminal investigations (Ch. 12) are reviewed. Each had very different responses. The first was led by Deputy Chief Constable of Greater Manchester Police (GMP) John Stalker (1984–5). Not only was his request for access to a key piece of intelligence denied, but his report never saw the light of day. The second was a group of inquiries led by Commissioner of the Metropolitan Police Sir John Stevens (1989–2003). These were met with some obstruction from the FRU and from parts of the wider army, who withheld information about the existence of informers. His team’s work led to two hundred plus arrests and at least ninety-four convictions. Third, is Operation Kenova which started in 2016 under Chief Constable of Bedfordshire Police Jon Boutcher. This is an investigation into whether there was evidence of any criminal offences having been committed by Agent Stakeknife, with an interim report published and now being reviewed, and three others underway in connection with Agent Stakeknife’s activities.^{xxv}

Author: David Page was a career criminal intelligence officer with West Midlands Police, UK, who joined their Special Branch in July 2005 for six years. He has been a regular participant in academic and professional discussions on intelligence and policing.

Endnotes

ⁱ Initial press reporting: <https://www.theguardian.com/uk-news/2020/oct/12/scottish-mi5-spy-crown-key-witness-new-ira-terror-trial>. Refers to Operation Arbacia, a joint MI5-PSNI operation. The prosecutions are yet to be fully heard, maybe in 2025 and some of the accused are now on bail. The author refers to Dennis McFadden as an informer before becoming an assisting offender. For more than twenty years he worked for MI5, first within Sinn Féin, then—on his handler’s orders—becoming involved with the New IRA shortly after that group was formed in 2012.

ⁱⁱ See: <https://www.theguardian.com/uk-news/2024/nov/17/pat-finucane-family-hope-finally-learn-truth-murder>

ⁱⁱⁱ See: Initial Report <https://www.kenova.co.uk/video-interim-report-publication-press-conference>. Later updates: <https://www.kenova.co.uk/august-2024-fresh-mi5-material-fags> and <https://www.kenova.co.uk/concerns-raised-after-fresh-material-disclosed-by-mi5>

^{iv} See: <https://www.irishnews.com/news/northern-ireland/new-documents-reveal-mi5-instructed-freddie-scappaticci-via-british-army-handlers-VTEFKNVBBHTVED6CI7SJUVUNU/> and <https://www.bbc.co.uk/news/articles/cg7982lpdyo>

^v The author cites the Northern Ireland Retired Police Officers’ Association (NIRPOA): the overriding priority set by HMG at the time was to save life through the effective gathering, assessment, analysis and exploitation of intelligence as opposed to obtaining arrests and perhaps convictions after the offence.

^{vi} Republican paramilitaries killed 2,139 people, followed by Loyalist paramilitaries who killed 1,050. See pgs. 115-116 in: <https://kenova.co.uk/5.%20D13483%20Op%20Banner%20Final%20Report.pdf>. The



author's research shows that between 1966 and 1994, the UDA was responsible for 406 murders, and the much smaller UVF and the violent loyalist group Red Hand Commando were jointly responsible for 534.

^{vii} The late Michael Herman, ex-GCHQ and senior civil servant, at an academic conference.

^{viii} Between 1971-1973 17,000 to 75,000. From:

<https://kenova.co.uk/5.%20D13483%20Op%20Banner%20Final%20Report.pdf>

^{ix} See: <https://kenova.co.uk/5.%20D13483%20Op%20Banner%20Final%20Report.pdf>. A Kings College London Centre of Defence Studies 'primer' report for Operation Kenova (2022).

^x There were during Operation Banner 'some twenty units', citing Mark Urban's book.

^{xi} *Secret Victory: The Intelligence War that Beat the IRA* (2016).

^{xii} A point made when talking to one of the Army authors of the 'Operation Banner' report on the army's deployment (2006) in reference to the value of vehicle stop checks to identify associations, something they had missed. The original report was officially withdrawn, it is now available online.

^{xiii} In England and Wales the absence of an informant within 'serious crime' can be a hinderance. At one point twenty plus years ago specialist units would not be deployed until after a 'scoring' exercise was completed.

^{xiv} A point made by an Israeli observer pre-9/11 on the development of intelligence in Israeli prisons. In the UK and elsewhere interception of telephone calls etc is a reported option.

^{xv} See: <https://sagedespatches.wordpress.com/2024/03/16/op-kenova-the-moral-maze/>

^{xvi} For a 'slim' bio see: <https://www.kcl.ac.uk/people/professor-sir-david-omand>; This is in reference to the Army-run informant Brian Nelson.

^{xvii} See references in: [https://en.wikipedia.org/wiki/Brian_Nelson_\(Northern_Irish_loyalist\)](https://en.wikipedia.org/wiki/Brian_Nelson_(Northern_Irish_loyalist))

^{xviii} The author refers to three sources: Matchett suggests the IRA killed eighty-three people as suspected informers between 1971 and 2006. Sam Kinkaid, RUC and PSNI, said over forty were killed during 'the troubles'. The IRA's focus on looking for potential informers leads Hewitt to suggest they killed more of their own members in 1979–81 than the police and the armed forces did in the same time period.

^{xix} For example, in December 2005, Denis Donaldson (Sinn Féin's Head of Administration) admitted to having been an informer for the British since the mid-1980s. He was murdered in Ireland in April 2006.

^{xx} Being exiled was encountered three times in my career, two from Northern Ireland, one explained it was due to her husband taking down a paramilitary flag from a telegraph pole, even though it was replaced. The exile for a local criminal was still in place twenty plus years later, he was accused of being a 'grass'.

^{xxi} See a well referenced: https://en.wikipedia.org/wiki/Robin_Jackson. He died from cancer in 1998.

^{xxii} See: <https://www.roberthamillinqury.org/>, which has had no updates since 2013.

^{xxiii} See: <https://www.bbc.co.uk/news/articles/c8995q8x2njo>.

^{xxiv} See a detailed parliamentary statement by the Northern Ireland Secretary Hilary Benn, <https://www.parallelparliament.co.uk/debate/2024-10-07/commons/written-statements/legacy-of-the-troubles>.

^{xxv} <https://www.kenova.co.uk/investigations>



Book Review - *Beyond States and Spies: The Security Intelligence Services of the Private Sector* by Lewis Sage-Passant, Edinburgh University Press

Ross Hill and Treston Wheat

Introduction

Intelligence studies generally is a niche field within security studies, and private-sector intelligence studies is even more inchoate by comparison. To help remedy that problem, Lewis Sage-Passant's *Beyond States and Spies: The Security Intelligence Services of the Private Sector* seeks to fill major gaps in the literature, which this book does on several levels. There are a myriad of books on intelligence that help analysts improve their craft or to understand the broad history of intelligence used by governments. However, there is a strong difference between technical analysis of intelligence, e.g., the art or craft of doing intelligence, and the needed research for theory building of private sector intelligence studies. Sage-Passant's book most assuredly does the latter.

In typical scholarly fashion, Sage-Passant rigorously demonstrates the lack of academic literature on the subject, citing a number of doctoral dissertations that have contributed practical or theoretical insights. Yet that is rather unusual in academic disciplines, which reinforces both the inchoate nature of private sector intelligence studies and the important contribution of the book. As he notes, "Few sweeping statements can ring true about such a diverse and fragmented field, something that the literature fails to acknowledge."ⁱ Scholars like Samantha Newberry and Amy Zegart are cited as well, but it is clear through his extensive literature review that such a book as this was necessary as no text truly delved into what *is* private-sector intelligence, its history, and how it operates. There are authors, like Justin Crump, that do offer important insights on this topic, but that is still more practitioner focused on. Sage-Passant offers a book that is equally useful to scholars and practitioners, which is what *The Close Protection and Security Journal* specifically seeks to further the professionalization of the field. As such, this book fills a much-needed lacunae in the writings on private-sector intelligence.

One of the reasons this book will contribute a significant amount to the literature is that the perception of private-sector intelligence is distorted, leading to unnecessary misunderstandings. Sage-Passant clearly states that, "While public perception of the private intelligence industry is certainly prone to inaccuracies and open to misinterpretation, most corporations – at least internally – now appear relatively comfortable with the need for intelligence, at least if managed discreetly."ⁱⁱ He further acknowledges that intelligence is "inherently wrapped in secrecy for the public sector, and in the private sector, the corporate reluctance to divulge potentially controversial or misunderstood practices is an ever-present barrier to studying it."ⁱⁱⁱ Through a literature review and historical documentation combined with interviews and survey, Sage-Passant is giving a much better understanding of private-sector intelligence—what it is and how it works.



Best Contribution to Theory

Briefly mentioned in the introduction and woven throughout the book, Sage-Passant's innovative approach may represent the study's most significant contribution to the field of intelligence studies. In a discipline where theoretical frameworks are often underdeveloped, Sage-Passant presents a compelling theory distinguishing public and private intelligence through the lens of "Audience Centricity." This concept, which posits that the primary audience for intelligence work determines its classification, opens new avenues for scholarly inquiry and practical application. While further research and debate are necessary to refine and expand this theory, its potential to address the current theoretical gaps in intelligence studies cannot be understated. As Sage-Passant wrote, "Where the term 'private-sector intelligence' conjures up images of contractors working for government intelligence agencies, this book argues that we must re-define intelligence work carried out for state audiences – with 'audience' here referring to those ultimate consumers of the finished intelligence product – as 'public-sector intelligence.'"^{iv} By challenging conventional definitions and encouraging a re-evaluation of intelligence roles, this theory is likely to stand as a foundational element for future scholarship in the field.

Is Private Sector Intelligence New?

Sage-Passant spends an entire chapter on the history of private-sector intelligence, which is a needed tonic to the gap in the literature. He takes the position that private-sector intelligence is "much older" than normally seen in the profession, which is typically viewed as a post-9/11 development. Interestingly, part of his survey with practitioners found that 27.9% believed it started with 9/11 while 11.6% in each group viewed it as emerging in the 1990s, in the 1970s, and with Pinkerton. However, 16.3% of interviewees thought that private-sector intelligence has always existed.^v

Sage-Passant goes through an impressive history that notes the collaboration between private and public sectors. For example, he cites the Aztec Pochteca guild employing *Naualoztomeca* (merchant spies) for reconnaissance, and Renaissance Venice's use of "merchant spies" under the direction of the Council of Ten. The book continues to go through an impressive array of historical events, including the British East India Company, Lloyd's of London, and the Rothschilds. Of course, one could not tell the history of private security and intelligence without mentioning Allan Pinkerton, the namesake to the company that still exists today. While Sage-Passant covered a myriad of historical episodes, events, and people that are not typically covered in the history of intelligence, there are specific interesting sections that give a more complete picture of the role corporations played in intelligence. One such example is how corporations helped the Office of Naval Intelligence during the 1910s.^{vi}

Most interestingly is how often anti-socialism and anti-communism played a role in getting corporations to take on an intelligence function, whether it was the Economic League or the United Fruit Company. Furthermore, many of the major intelligence and consulting companies around today originated in the twentieth century, such as Control Risks and Booz Allen Hamilton. Sage-Passant utilizes this sweeping history to show that "the literature does not appear to successfully identify the origins of the field. In part, this is due to the lack of a consolidated effort to assemble a history of the field."^{vii} (52) He demonstrates that private intelligence has essentially coexisted with state/government intelligence throughout the field's history.



Although this impressive history shows the long existence of private intelligence, it does not completely make the case that private-sector intelligence is a pre-9/11 profession, primarily because there is a critical distinction between the mere existence of a field and its professionalization in the Huntingtonian sense. Professionalization requires the establishment of standards, formalized practices, ethical guidelines, credentialing processes, and a body of academic research that legitimizes the field as a distinct and organized discipline. While Sage-Passant effectively demonstrates that private intelligence has existed in various forms and played significant roles throughout history, this does not equate to a cohesive or mature profession.

Private-sector intelligence prior to 9/11 was often fragmented, ad hoc, and largely shaped by the needs of specific corporations or industries rather than governed by universal standards or frameworks. For example, the examples of merchant spies in Aztec and Venetian contexts or the activities of the British East India Company reflect intelligence practices tailored to particular economic or political objectives, rather than the systematic development of a field. Similarly, the intelligence work conducted by Allan Pinkerton or the Economic League served specific, often anti-socialist or anti-communist purposes, but these efforts lacked the broader institutionalization that characterizes a profession.

While Sage-Passant's historical survey is valuable for demonstrating the long-standing relationship between private entities and intelligence activities, his argument that private-sector intelligence is a pre-9/11 profession does not sufficiently address the criteria of professionalization. However, its contribution is to show that private-sector intelligence has existed much longer than many have acknowledged.

Help for Practitioners

While the above highlights Sage-Passant's significant contributions to the theory and history of private-sector intelligence, the strength of his work lies in its ability to move beyond theoretical constructs and into the practical realities of intelligence work. By examining the similarities and differences between public and private applications of the intelligence cycle, Sage-Passant provides actionable insights that can directly influence the development and professionalization of corporate intelligence teams. His nuanced exploration bridges the gap between academic theory and the everyday challenges faced by private-sector intelligence practitioners.

One of the most valuable aspects of his work is the emphasis on the unique demands placed on private-sector intelligence analysts, who must often be proficient in all aspects of the intelligence cycle, from collection to dissemination. This stands in contrast to the more specialized roles typically found in public-sector intelligence, where analysts may focus on narrower tasks within a larger team. Sage-Passant's acknowledgment of this distinction underscores the need for private-sector analysts to cultivate a broader skill set, as well as the organizational flexibility required to manage diverse and complex intelligence challenges.

Particularly thought-provoking is Sage-Passant's discussion on whether private-sector intelligence analysts should maintain the same level of distance from policymaking as public-sector analysts. The



traditional norm in intelligence studies—where analysts refrain from providing explicit recommendations—has long been upheld in government settings to ensure objectivity and prevent undue influence. However, as Sage-Passant notes, the private sector operates under different constraints: “Unlike government decision-makers, corporate decision-makers generally have less experience, training, and expectations of involvement in the handling of security and crisis situations, and as such are more likely to demand policy recommendations from their security services.”^{viii} This divergence raises important questions about the evolving role of intelligence in corporate environments and the ethical and professional considerations it entails.

Sage-Passant’s examination of collection and analysis practices is another area of particular interest, as it highlights the resource disparities between the public and private sectors. Private-sector intelligence analysts are significantly less likely to employ structured analytic techniques—methods commonly used in government intelligence—due to limitations in resources, bandwidth, and budget.^{ix} (181). This practical reality has significant implications for the accuracy and reliability of private intelligence products and points to the need for greater investment in training and resources to bridge this gap. Additionally, Sage-Passant dedicates considerable attention to the recruitment and organizational structure of private-sector intelligence teams. He emphasizes the importance of building multidisciplinary teams capable of addressing the diverse challenges faced by corporations, from geopolitical risks to cybersecurity threats. His insights into recruitment strategies and team dynamics are especially relevant for organizations looking to enhance their intelligence capabilities in a competitive and rapidly evolving landscape.

By addressing these practical dimensions, Sage-Passant offers a roadmap for how private-sector intelligence can mature as a profession. His work not only identifies the challenges but also provides a foundation for developing the standards, training, and practices that will define the field’s future. This blend of theoretical and practical insights makes his book an essential resource for both scholars and practitioners, ensuring its relevance across the spectrum of intelligence studies.

Ethics

Though a smaller section, the ethical discussion is likely to be a controversial aspect of the discussion on the professionalization of the industry. Sage-Passant’s survey found that the majority of practitioners thought physical infiltration activities by covert operatives was unethical.^x Covert human intelligence operations are often seen as posing reputational concerns. Generally, the profession has engaged in what he called “aretaic self-policing” rather than being regulated by government entities, and every practitioner, organization, and corporation will have to decide what they consider to be appropriate ethical standards for them. The issue comes to the extreme limitations these kinds of ethical standards impose. Certain professional organizations, for example, oppose imitating people online and communicating with persons. However, this could be an extraordinarily useful mechanism to gather intelligence on people who intend the corporation harm with protests or even violence. As such, organizations will have to decide the ethical principles that matter most and remains an extremely useful discussion that Sage-Passant brings to the book.



Conclusion

Essentially, all security professionals should read this book even if they agree with its theses or not because it is clearly a strong and enduring contribution to the literature. *Beyond States and Spies* is a groundbreaking text, and Lewis Sage-Passant has crafted a book that fills critical gaps in the literature, bridging theoretical frameworks, historical insights, and practical guidance in a way that advances both the academic study and professional practice of private-sector intelligence.

The book's rigorous scholarship, including its historical analysis and theory of "Audience Centricity," provides a robust foundation for future research and debate. Its exploration of private-sector intelligence's evolution, challenges, and ethical dilemmas sheds light on a complex field often misunderstood or overlooked. Moreover, its practical discussions on the intelligence cycle, recruitment, and organizational structures offer invaluable guidance to practitioners seeking to professionalize and improve their teams.

Whether one accepts Sage-Passant's arguments or views them critically, the book's contribution to the discourse is undeniable. Its insights will remain relevant and influential for years to come, making it an essential read for anyone engaged in intelligence, security, or corporate risk management. To ignore it would be to miss out on one of the strongest contributions to the evolving literature on private-sector intelligence.

Authors: Ross Hill is the founder and CEO of Insight Forward, a geopolitical risk intelligence firm. He has two decades of experience in intelligence analysis in the public and private sectors. Dr. Treston Wheat is the Chief Geopolitical Officer for Insight Forward, Special Advisor for Geopolitics and Security at Riley Risk Inc., and an adjunct professor at Georgetown University.

Endnotes

ⁱ Lewis Sage-Passant, *Beyond States and Spies: The Security Intelligence Services of the Private Sector* (Edinburgh University Press, 2024), 38.

ⁱⁱ Ibid, 53.

ⁱⁱⁱ Ibid, 63.

^{iv} Ibid, 5.

^v Ibid, 85.

^{vi} Ibid, 101.

^{vii} Ibid, 52.

^{viii} Ibid, 152.

^{ix} Ibid, 181.

^x Ibid, 263.



Submitting to the Journal

The Close Protection and Security Journal is a bi-annual publication, and we welcome submissions from scholars, researchers, and practitioners on a number of topics. The scope of the Journal is intentionally broad as there are currently no scholarly publications dedicated only to corporate security. Importantly, the intention of the Journal is to be a scholarly publication led by practitioners, offering their in-depth insights into historic cases, current issues, and emerging threats. The Journal aims to publish articles by authors who have professional or academic research experience with the subjects of their writing to better give insight into corporate security. Professional experience from prior military or government service is also acceptable as a means to bring important ideas from related fields to corporate security.

Topics for the Journal include but are not limited to:

- Close Protection
- Red Teaming
- Security Failures
- Intelligence Analysis
- OSINT
- Emerging Technology
- Due Diligence
- Event Risk Management
- Enterprise Risk Management
- Security Operations Centers
- Political Risk
- Skill Development for Security
- Surveillance/Counter-Surveillance
- Private Security History

Submission Instructions

Please submit your articles to the Editor-in-Chief Dr. Treston Wheat at treston.wheat@ips-board.org as a .doc or .docx attachment by the deadline. Include a short biography about yourself to describe your qualifications to write on the subject of your article.

Please contact Dr. Wheat with any questions that you might have.

