The Close Protection and Security Journal

Volume 3, Issue 2

Published by the International Protective Security Board

December 2025

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

The CLOSE PROTECTION & SECURITY JOURNAL

Contents

Letter from the Editors

The past year has marked a period of significant expansion and maturation for the close protection and private security profession. In having to respond to major and novel threats, the profession has evolved into a sophisticated, multidisciplinary practice that integrates intelligence analysis, risk management, behavioral assessment, medical preparedness, and strategic decision-making. This expansion reflects not only a changing threat environment, but also a growing recognition that effective protection requires professional judgment, structured methodology, and continuous learning. The studies, research, and analytical contributions in this issue of *The Close Protection and Security Journal* are intended to support practitioners navigating this ambitious moment, offering insights that are both rigorous and directly applicable to real-world security operations.

In response to this growth, the journal has expanded its scope with several new sections designed to better serve practitioners across the private security spectrum. **Interviews with Experts** provides structured conversations with experienced professionals from close protection, intelligence, medicine, law enforcement, and adjacent fields. These interviews will focus less on biography and more on decision-making, lessons learned, and how experienced practitioners think about risk, uncertainty, and professional development. **Tools for Security Professionals** examines emerging technologies, established tools applied in novel ways, and practical techniques that can enhance operational effectiveness. Contributions in this section emphasize not just what tools exist, but how they should be integrated thoughtfully into close protection, intelligence analysis, and risk management workflows. **The Practitioners' Bookshelf** offers analytical book reviews written explicitly for security professionals, focusing on the practical lessons a given work offers rather than academic critique. This section reflects the belief that serious practitioners benefit from maintaining a personal intellectual foundation that supports better judgment in the field.

Several contributions in this issue are intended to advance the profession by strengthening its intellectual, methodological, and operational foundations rather than by offering narrowly situational lessons. Collectively, the research presented here provides generalizable insights that can inform how close protection and private security are trained, how threats are understood and assessed, and how practitioners prepare for uncertainty. The articles engage foundational questions about how intelligence analysis should be conceptualized and applied in private-sector contexts, examine empirical evidence on effective executive protection training, and explore how emerging risk environments, from strike, riot, and civil commotion to evolving threats against hotels should shape protective planning. Other contributions address the philosophical dimensions of the warrior ethos as it applies to close protection, the practical realities of medical emergency preparedness, and the growing impact of automation and regulatory complexity on executive protection operations. These works move beyond prescriptive guidance to offer durable frameworks, conceptual clarity, and practical mechanisms that enhance operational readiness and threat assessment. In doing so, they reinforce the view of close protection as a profession grounded in disciplined thinking, structured preparation, and continuous refinement of both practice and judgment.

The expansion of close protection and private security over the past year has been matched by a quieter but equally important development: the maturation of the field as a knowledge-producing profession. For much of its history, private security has relied primarily on experiential learning, informal mentorship, and

borrowed doctrine from public-sector or military institutions. While operational experience remains indispensable, the profession is now increasingly generating its own research, analytical frameworks, and philosophical debates that are specific to the realities of private-sector risk. This issue reflects that evolution. The articles collected here interrogate assumptions, test approaches, and contribute to a growing body of shared professional knowledge that can be refined, challenged, and built upon over time.

Readers are encouraged to engage with this issue as a collection of tools and perspectives meant to be actively applied. The frameworks, survey findings, and conceptual discussions presented here are most valuable when tested against real operating environments, organizational constraints, and individual experience. Practitioners should approach the material with a critical eye, asking how these insights align with their current practices, where they expose gaps or weaknesses, and how they might be adapted to improve preparedness, decision-making, and threat assessment. Used in this way, the journal becomes a mechanism for professional reflection and continuous improvement.

Finally, the work in this issue reinforces a recurring theme that runs through the profession: operational excellence is inseparable from personal development. Technical proficiency, physical capability, and procedural knowledge are necessary but insufficient on their own. Effective protection depends equally on judgment, intellectual discipline, emotional control, and the ability to think clearly under pressure. The articles presented here indicate that professionalization is about cultivating practitioners who are reflective, adaptable, and committed to lifelong learning. As the field continues to grow in scope and visibility, this integration of professional rigor and personal development will remain essential to maintaining credibility, effectiveness, and trust.

We hope this issue contributes meaningfully to both the practice and the mindset of security professionals operating in an increasingly hostile world. As the profession grows in scope and responsibility, so must its commitment to rigor, professionalism, and personal excellence.

Treston Wheat, PhD
***Editor-in-Chief,* CPSJ**

Charles Randolph
Fred Burton
Charles Tobin
Rachael Frost
Samantha Newbery, PhD
Erin Rowland Carlin, PhD
***Editorial Staff Members*, CPSJ**

Your clients are being watched:

What OSINT can reveal about them

Almost everything we do online leaves behind a digital trace. What many people don't realize is how much of that information is publicly available and how easily it can be pieced together, creating profiles which can lead to a physical threat. This process, known as Open Source Intelligence (OSINT), and involves collecting and analyzing information that's already out there.

Cybercriminals, journalists, or individuals with a grudge can gather data from countless online sources, often without the target ever knowing. The more scattered bits of information that are stitched together, the clearer the picture becomes.

Some of the most common, and revealing, sources of information include:

Social Media Posts: Photos of vacations, kids' soccer games, or even a new car in the driveway can tell someone where your clients are, when they are away from home, and what assets they own.

Old Property Records: Public databases and real estate sites often list previous addresses, purchase prices, mortgage information, or even blueprints.

Data Broker Profiles: Aggregators compile information from public filings, credit headers, marketing databases, and breach data. These can reveal dates of birth, phone numbers, relatives, and sometimes sensitive identifiers like SSNs.

Online Forums & Communities: Long-forgotten posts on hobby forums, Reddit threads, or professional message boards can connect usernames to real identities and provide leverage for social engineering.

News Articles & Obituaries: Media mentions and family obituaries often confirm relatives, children's names, and geographical ties which are useful for impersonation attempts.

Taking Control of Your Clients' Digital Footprint

BlackCloak protects the personal data across every facet of your clients' connected world, securing smart devices, online accounts and home networks. Our award-winning cybersecurity is enhanced by concierge support to reduce the risk of falling victim to cybercrime and prevent physical harm.

Get in touch for more information

Discover how BlackCloak personal cybersecurity can support your physical security program, visit **www.blackcloak.io** or email **info@blackcloak.io**

BLACKCLOAK®

CIA | CENTRAL INSURANCE AGENCY

OVER 1,000 SECURITY FIRMS TRUST CENTRAL INSURANCE AGENCY

25 years of exclusive experience in your industry

Where others miss, we deliver:

- **Audit Counseling:** We uncover overcharges and recover savings.
- **Contract Reviews:** We negotiate terms that protect your business.
- **Cost Efficiency:** We align your premiums with reality.
- **Immediate Response:** No voicemail—always a real person.
- **Stress-Free Renewals:** We start 90 days early to secure the best terms.
- **Fast Certificates:** Issued within the hour.

Book a call with the CEO George Gavaris

www.ciainsures.com
877-242-9600
contactus@ciainsures.com

California license #OH16068 DBA: CIA WEST INSURANCE SERVICES

REDUCE RISK WHERE IT MATTERS MOST™

360PRIVACY.IO

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

Research Articles

Are Executive Protection Agents Prepared? A Study on Training Difficulty and Self-Efficacy

Diego Andreu

Abstract

Limited training time coupled with budget cuts, amplified by lax training requirements, results in executive protection agents often not being able to undergo sufficient recurring-skills training. This frequently leads to under-performance and low skill levels. Utilizing Bandura's concept of self-efficacy as a theoretical foundation, this study aims to understand how specific training modules affect the executive protection agent's own perceptions of their ability to perform effectively while protecting a principal. The study surveyed 48 current practitioners. The bespoke, online survey—utilizing distribution and correlation analysis—incorporates research questions that attempt to understand the relationship between the agents' self-efficacy and the level of difficulty of the following training modules: threat assessment, surveillance and counter surveillance, embus/debus, walking drills, firearms, defensive/evasive driving, personal defense/hand -to-hand combat and medical aid. This study hypothesizes that perceived ease of training would have a negative effect on the executive protection agents' own perceptions of: (H1) their own ability to respond effectively against a threat to their principal, (H2) their own ability to protect the principal, and (H3) of the fact that they have appropriate training.

Mixed results were achieved when attempting to confirm if the level of difficulty was directly correlated to the executive agents' own perceptions of their own ability (H1 and H2). However, the study was able to verify that the training difficulty level has a direct relationship with whether an executive protection agent perceives that he or she has the appropriate level of training (H3). Importantly, it was revealed that the difficulty of firearms training seemed to have a direct correlation to the agents' perception of their own abilities, possibly signifying an overreliance in firearms. Self-efficacy, or people's judgements regarding their own abilities and capabilities, can have significant impact in how executive protection agents perform their job. Understanding how the training they receive either enhances or may even negate this self-efficacy is important to identify which training may have the most benefit. This study can provide policy makers and practitioners with information about which training modules provide more self-efficacy and how that can be translated into actual skills.

Introduction: Statement of Problem

Executive protection agents are paid to protect their principal from physical harm. In order to be proficient at their job, they participate in different levels and numbers of training. The training requirements vary by jurisdiction. In the United Kingdom, the Security Industry Authority mandates a minimum level of training for all individuals seeking to be lawfully employed as executive protection agents.[i] In the United States, executive protection, and its associated training requirements, is regulated at the state level and therefore varies from state to state.

However, most experts argue that the security industry has failed to "promote high level, sophisticated standards of educational requirements."[ii] Often times there is a financial decision to reduce the number

of traning sessions as “training is the first item cut from security budgets.”[iii] Likewise, a mix of low-cost guards and a single executive protection agent is used by clients to save a few dollars. This often leads to poorly trained executive protection agents, either due to lax initial or recurring requiements. In turn, this puts principals in danger as “the difference between the professional and the amateur in the matter of response to these moments of crisis lies in preparation.”[iv]

Although training requirements do vary by jurisdiction and additional training modules do exist, there are certain core modules of training that are generally accepted by the industry as the minimum training curriculum that all executive protection agents must complete.[v] This minimum curriculum includes the following modules:

- Threat assessment
- Surveillance and counter surveillance
- Embus/Debus
- Walking drills
- Firearms
- Defensive/evasive driving
- Personal defense/hand-to-hand combat
- Medical aid

This study seeks to answer the question of how the difficulty of each module of training of executive protection agents affects their perception about their own ability to successfully protect their principals against threats.

Research Questions and Hypothesis

The main goal of this research study was to understand the executive protection agents’ perceptions about their own ability to respond against a threat to their principal and how the difficulty of different training elements may or may not affect that perception. The research questions for this study were:

1. What is the relationship between the perceived easiness of threat assessment training and the executive protection agent’s perceptions of his own ability to respond effectively against threats to the principal?
2. What is the relationship between the perceived easiness of surveillance and counter surveillance training, and the executive protection agent’s perceptions of his own ability to respond effectively against threats to the principal?
3. What is the relationship between the perceived easiness of embus/debus and training, and the executive protection agent’s perceptions of his own ability to respond effectively against threats to the principal?
4. What is the relationship between the perceived easiness of walking drills training and the executive protection agent’s perceptions of his own ability to respond effectively against threats to the principal?
5. What is the relationship between the perceived easiness of firearms training and the executive protection agent’s perceptions of his own ability to respond effectively against threats to the principal?
6. What is the relationship between the perceived easiness of defensive/evasive driving training and the executive protection agent’s perceptions of his own ability to respond effectively against threats to the principal?

7. What is the relationship between the perceived easiness of personal defense/hand to-hand combat training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?
8. What is the relationship between the perceived easiness of medical aid training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

As such, the following hypotheses are put forward for comparison with the results:

H1 The perceived easiness of the training modules will have a negative effect on the executive protection agent's perception of their ability to respond effectively against a threat to their principal.
H2 The perceived easiness of the training modules will have a negative effect on the executive protection agent's perceived ability to protect the principal.
H3 The perceived easiness of the training modules will have a negative effect on the executive protection agent's perception that they have appropriate training.

It is worth noting that the notion of "difficulty level" in this study will be measured in relation to how easy the training was perceived to be.

Delimitations

Participants in this study were limited to employed executive protection agents with at least one year of professional experience. This ensured that the sampled population had a minimum level of experience across the board. Likewise, only a quantitative Likert scale was used in the survey instrument to guarantee manageability. Moreover, given the disparity in training requirements on a state-by-state and country-to-country level, and the fact that this study defined perceived training difficulty in relation to self-efficacy, participants were allowed to be located worldwide. This allowed for a larger pool sample. However, all participants were required to have completed executive protection training and be actively employed in the industry.

Additionally, a custom-made survey instrument was developed by the researcher for this project. Due to the limited time allotted for the implementation of this project, the custom survey instrument had a very limited testing period. However, the survey was checked and approved by the online tool Survey Monkey for accurate logic and answer validation. Lastly, this study was designed to measure the executive protection agents' perceptions about their own ability to handle threats to life to their principal and not necessarily their physical capacity to do so.

Assumptions

It is assumed that all participants in this study provided truthful and free-willed responses without any fear of negative repercussions by their current employer(s). Additionally, it is assumed that all respondents have received commensurate level of training to their minimum-level mandate by their local jurisdiction. It is also assumed that the participants have not participated in executive protection training in the weeks prior to the completion of the survey. This would compromise the ability of the study to discern the degree to which the participants depended on their beliefs about their recent past performance in training events as opposed to their beliefs about the difficulty of the training when completing this study. [vi]

Theoretical Foundations

In order to bridge the gap in academic knowledge about executive protection, this study aims to understand the confidence in their own ability of executive protection agents to manage threats to their principals by measuring how training difficulty is related to self-efficacy; the aim is to, therefore, analyze how individuals learn and gain self-efficacy through training. Social cognitive theory (also known as SCT) and, specifically, the concept of self-efficacy were used in crafting the research questions.

Social cognitive theory is a theory of self-regulation. According to Bandura, people self-regulate internally and adopt standards of behavior that serve them as guides in the completion of future goals or tasks.[vii] As part of this self-regulation, individuals conduct self-diagnosis of their own ability to be successful at certain tasks and assign an internal value. This is called self-efficacy. In essence, self-efficacy is "people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances."[viii] In other words, it is an individual's own belief or perception of their own ability to perform certain tasks and reach certain goals.[ix]

Research does suggest that individuals with higher self-efficacy perform better and are more motivated than individuals with lower self-efficacy. Likewise, if self-efficacy is low, it is likely that an individual will not perform as well as his or her peers.[x] Importantly, self-efficacy has been proven to have a direct, positive relationship with different motivational and behavioral outcomes in clinical, educational, and organizational settings by two decades of empirical research.[xi] Through his research, Bandura found that "the likelihood that people will act on the outcomes they expect prospective performances to produce depends on their beliefs about whether or not they can produce those performances."[xii] It is worth noting that self-efficacy and confidence are similar yet not interchangeable terms.

Confidence (or self-confidence) is a colloquial, nondescript term that refers to strength of belief but lacks certainty.[xiii] Self-confidence can in fact lead to self-efficacy and can be a part of internal sources of information such as performance accomplishments, vicarious experiences, verbal persuasion and physiological states. Self-confidence may be a combination of self-esteem and general self-efficacy. On the other hand, self-efficacy is related to other factors such as difficulty of the task, an individual's ability, etc. and "includes both an affirmation of a capability level and the strength of that belief."[xiv]

Research Design

This study will utilize a distribution analysis and correlations analysis to examine the survey results (quantitative in nature). A distribution analysis is a summary of the frequency of individuals' values or response in both numeric and percentage form. A distribution analysis will be used to understand the demographics and background information of the participants. However, the main portion of the study will be done as a correlation analysis utilizing the Pearson Correlation Coefficient, expressed as *r*. The correlation coefficient is divided into positive and negative correlations between the numerical range of +1.0 and -1.0. In a positive correlation, if the value of variable X increases, then the value of Y increased in a linear form. A positive correlation runs from +1.0 to 0.0.

Opposite to that, if the correlation is deemed to be negative, then the direction is inversed. In a negative correlation, if the value of variable X increases, then the value of variable Y decreases linearly. A negative correlation runs from 0.0 to -1.0. Correlational research was chosen due to the researcher's inability to manipulate variables throughout the study. Correlational research is effective when we are interested in the relationship, associations, trends, or interactions between one or more variables (e.g., training difficulty and perceived self-efficacy).[xv] It is important to note that the main focus of this research is to find

associations or trends between the variables; it does not seek to find causal relationships between the variables such as those found in experimental research designs where cause and effect can be measured.

Population and Sample

A total number of 80 executive protection professionals were targeted as ideal candidates for this study. As part of the requirements to be eligible, the participants had to meet the following requirements:

- Be at least 18 years old at the time the survey was completed.
- Be currently employed as executive protection professionals on a part-time or full-time basis.
- Have at least one year of experience in executive protection.
- Not be employed, directly or indirectly, by the researcher's employer.

All participants were volunteers in the study and gave their consent to participate by completing the survey. Of the 80 potential participants, complete surveys were received from 48 (60% response rate). These 48 participants constitute the study's sample. A total of 19 participants attempted to complete the survey but were discarded during the qualification stage. The other 13 did not respond to the survey request.

Instrumentation

A custom-made online survey tool was used during this research, called the Executive Protection Agent Training and Efficacy Survey (EPATES) which used a Likertt-style scale:

- 5= Strongly agree
- 4 = Agree
- 3 = Neither agree nor disagree
- 2 = Disagree
- 1 = Strongly disagree

Each response was assigned a score ranging from 1 to 5. The score of this scale reflects the strength of an executive protection agent's self-efficacy belief. This means that the higher the score, the greater the level of self-efficacy belief and, likewise, the lower the score, the lesser the level of self-efficacy belief. The categories of data were treated as an ordinal scale of measurements. Although not within the scope of this paper to discuss in detail, it is worth acknowledging that there is academic disagreement as to whether a Likert scale produces ordinal, nominal or interval data.[xvi]

The instrument was divided into five main categories: qualifying questions, demographics, background, executive protection agent's training level and executive protection agent's readiness. The first section contains qualifying questions for the study. There is no measurement of variables in this section as these questions merely ensure that the participants meet the requirements set forth by the researcher, and importantly, allow the researcher to eliminate any potential participants that may pose an ethical issue. The second section addressed demographics and will be analyzed through descriptive statistics in the form of distribution analysis. These questions included years of experience, gender, age range and level of education of the participants. The reason for including these questions in the study is that they might represent factors that could influence a participant's choice of answers.

Similarly, the third section addresses background data and allows the researcher to collect categorical data specific to how executive protections services are delivered. Although the reason for including these questions is the same as with the demographics, they were put in a different group as they pertain

specifically to the tactical elements of executive protection. This section will also be analyzed with descriptive statistics in the form of distribution analysis.

The fourth section of the survey is called executive protection agent's training level and will be analyzed through a correlation analysis. This section provides the first variable and focuses on difficulty of training from the individual's perspective of his own self-efficacy. Bandura noted that "perceived efficacy should be measured s against levels of task demands that represent gradations of challenges or impediments to successful performance."[xvii] The training section allowed the researcher to understand the amount of training sessions that a participant typically completes within a calendar year. It also seeks to understand the perceived level of difficulty, on average, of the training sessions. This involved question related to training at the classroom level and at the practical level.

Lastly, the fifth section of the survey is called readiness of executive protection agents. Acting as the second variable, it seeks to understand the executive protection agent's owns perceptions of his ability to successfully protect the principal against an attack. This last section will also be analyzed through correlation analysis.

Data Collection and Analysis Procedure

Primary data was to be collected directly from the participants via the aforementioned online survey instrument. The survey instrument was sent to the potential participants via two different methods: one was via a single direct email to known potential participants and the second was via a LinkedIn posting specifically targeting potential participants.

Each survey contained an introductory section that stated:

- Name of the researcher
- The goal and purpose of the survey and the study
- A statement that the responses are anonymous and confidential
- Instructions on how to complete the survey
- Relevant instructions that are not explained in the survey questions themselves
- An electronic consent form

The researcher reached out to 80 possible respondents, out of which 48 made up the final sample. Although minimum samples are dependent on the research being conducted, according to statisticians, samples must be greater than 25 or 30 in order to produce an accurate statistical analysis.[xviii] For each of the two research questions, the executive protection agent's self-efficacy was measured using the Executive Protection Agent Training and Efficacy Survey (EPATES). Demographic and background information was also gathered from the executive protection agents in effort to gather additional information that may provide insight into any relevant tendencies. The responses were received directly by the researcher via the SurveyMonkey website and were exported to the software SPSS for analysis.

Ethical Considerations

The pool of potential respondents comes from the researcher's personal network of executive protection professionals. Having this in mind, there were three main ethical considerations that are part of this research mainly in the form of conflict of interest and potential liability implications. First is the researcher's employment. The researcher for this project is currently employed by a private risk management firm that provides executive protection services to its clients. Part of the researcher's area

of responsibility includes the review and potential hiring of executive protection agents. Participants may feel that participation in this study may provide them with an avenue for future employment.

Second is the source of participants and their relation to the researcher's current employer and its clients. Participants may be inclined to respond in favorable terms if they are currently employed or engaged in executive protection tasks through the remit of the researcher. This could also potentially open the researcher's organization to liability if participants partake in the survey while engaged in tasks. Third is any potential, real or perceived, liability that participants may have by participating in this study. Similarly to the potential liability for organizations, individuals may find themselves liable if they respond negatively in the survey.

To ensure full confidentiality, the researcher did not collect identifying information such as names or employer. Additionally, the study purposely excludes individuals that:

- Are currently employed as subcontractors, on behalf of the researcher's employer, for executive protection
- Are currently employed (as direct hire or subcontractors) by the researcher's employer for any other projects not related to his area of responsibility (i.e., investigative work or due diligence, among others)
- Any individuals that are currently working for one of the clients of the researcher's employer

Any individual that has a current relationship with the researcher's employer to provide work, outside or inside the researcher's remit, was disqualified.

Organization of Data Analysis

All participants were asked questions related to their demographic information and their background. As stated during previous chapters, the main purpose for collecting this information is to find any additional variables that might affect how a participant responds to a survey, thus proving ancillary findings. Questions about participant demographics included their age, gender, and experience and education level. Questions about their background included current assignment, use of weapons, training profile and training frequency. These questions were analyzed through the use descriptive statistics, via the software SPSS, in the form of a distribution analysis. Following the demographic and background questions, participants were asked about the difficulty in the different training modules that make up a representative executive protection training based on the SIA standards mentioned in Chapter I. Likewise, participants were also asked about their beliefs about their ability to protect their principal and be effective executive protection officers. These questions were analyzed using a correlation analysis through software SPSS.

The Results

Presentation of Descriptive Characteristics of Respondents

- **Gender** (Figure 1) – Participants were asked to provide their gender. An overwhelming number of participants were male (93.8%) and only three participants reported being female (6.3%).
- **Age** (Figure 2) – Participants were asked to provide their age by ranges. The vast majority of the participants were between 40 and 49 years old (41.7%), followed by the 30-39 range (31.3%). The range between 30-49 years old accounted for 73% of the participants. Only six participants were under the age of 30 (12.5%) and seven over the age of 50 (14.6%). No participants reported being 60 years of age, even though the category was included.

Figure 1: Gender

Statistics

Gender

N	Valid	48
	Missing	0

Gender

		Frequency	Percent
Valid	F	3	6.3
	M	45	93.8
	Total	48	100.0

Figure 2: Age

Statistics

Age

N	Valid	48
	Missing	0

Age

		Frequency	Percent
Valid	21-29	6	12.5
	30-39	15	31.3
	40-49	20	41.7
	50-59	7	14.6
	Total	48	100.0

- **Experience** (Figure 3) – Participants were asked about their work experience in terms of years. Most participants had between six and ten years (35.7%), or 11 and 15 years of experience (35.4%). These two ranges accounted for 70.9% of the total number of participants. Only seven participants had two to five years of experience (14.5%) and six had 16 to 19 years respectively (12.5%). Only one participant had one year of experience (2.1%).
- **Education** (Figure 4) – Participants were asked about their formal academic education. Some college education without a degree and a bachelor's degree were the categories accounting for the most participants, with 14 (29.2%) and 12 (25%) respectively. These two categories were followed by nine participants with an associate degree (18.8%) and eight with graduate degrees (16.7%). Lastly, five participants only had a high school degree or equivalent (10.4%).

Figure 3: Experience

Statistics

Experience

N	Valid	48
	Missing	0

Experience

		Frequency	Percent
Valid	1 year	1	2.1
	2-5 years	7	14.6
	6-10 years	17	35.4
	11-15 years	17	35.4
	16-19 years	6	12.5
	Total	48	100.0

Figure 4: Education

Statistics

Education

N	Valid	48
	Missing	0

Education

		Frequency	Percent
Valid	High school or equivalent	5	10.4
	Some college but no degree	14	29.2
	Associate degree	9	18.8
	Bachelor degree	12	25.0
	Graduate degree	8	16.7
	Total	48	100.0

- **Assignment** (Figure 5) – All participants were asked if they had continuity with the same principal or if they rotated with different ones (different clients). Of the 48 participants, 31 stated that they did not have a fixed principal (64.6%) and 13 of them responded that they did have a single principal on a full-time basis (27.1%). The four remainder participants responded that they have a full-time principal but occasionally do work with other clients (8.3%).
- **Weapons** (Figure 6) – Participants were asked if they carried weapons while on duty or not. There were equal percentages of participants responding that they worked unarmed or both armed and unarmed; there were 18 participants in each category (37.5% each and 75% cumulative). The other 12 participants reported working in an armed capacity (25%).

Figure 5: Assignment

Statistics

Same principal or rotate

N	Valid	48
	Missing	0

Same principal or rotate

		Frequency	Percent
Valid	Full time	13	27.1
	Rotate	31	64.6
	Both	4	8.3
	Total	48	100.0

Figure 6: Weapons

Statistics

Armed or unarmed

N	Valid	48
	Missing	0

Armed or unarmed

		Frequency	Percent
Valid	Armed	12	25.0
	Unarmed	18	37.5
	Both	18	37.5
	Total	48	100.0

- **Training profile** (Figure 7) – Participants were asked if they trained with current teammates or with other executive protection agents that did not work with them on a regular basis. A little more than half, 26 agents, responded to training alone (54.2%) and the other 22 responded that they trained with teammates (45.8%).
- **Training recurrence** (Figure 8) – Participants were asked about their training recurrence in a calendar year. An overwhelming amount of participants, a total of 40, responded that they trained 1-2 times per year (83.3%). The remainder eight participants stated that they trained three or more times per year (16.7%).

Figure 7: Training profile

Statistics

Train with team or alone

N	Valid	48
	Missing	0

Train with team or alone

		Frequency	Percent
Valid	With teammates	22	45.8
	Alone	26	54.2
	Total	48	100.0

Figure 8: Training recurrence

Statistics

Practices per year

N	Valid	48
	Missing	0

Practices per year

		Frequency	Percent
Valid	1-2 times per year	40	83.3
	3 or more times per year	8	16.7
	Total	48	100.0

Analysis of Data

After completing the demographics and background questions, the participants were asked to respond to questions related to their training experiences and their own beliefs on their ability to execute a task. Each of the survey questions sought to answer a specific research question. The following provides a detailed description of the results from the correlation analysis.

Research question # 1

1. What is the relationship between the perceived easiness of threat assessment training and the executive protection agent's perceptions about his own ability to respond effectively against threats to the principal?

Results

Correlations

		Threat assesment easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Threat assesment easiness	Pearson Correlation	1	.005	.145	-.108	.125
	Sig. (2-tailed)		.972	.325	.464	.397
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	.005	1	.844**	.376**	.893**
	Sig. (2-tailed)	.972		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	.145	.844**	1	.217	.910**
	Sig. (2-tailed)	.325	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	-.108	.376**	.217	1	.464**
	Sig. (2-tailed)	.464	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	.125	.893**	.910**	.464**	1
	Sig. (2-tailed)	.397	.000	.000	.001	
	N	48	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of threat assessment training and belief that the executive protection agent can effectively protect the principal shows a weak, positive correlation between variables (r= .125, p < .397) and this relationship is not highly statistically significant.
- The relationship between ease of threat assessment training and the belief in the ability to respond effectively shows a weak, positive correlation between variables (r= .145, p < .325) and this relationship is not highly statistically significant.
- The relationship between ease of threat assessment training and the belief that the individual has the appropriate training shows a weak, negative correlation between variables (r= -.108, p < .464) and this relationship is not highly statistically significant.
- The relationship between ease of threat assessment training and the belief that an attack is probable shows a very weak, positive correlation between variables (r= .005, p < .972) and this relationship is not highly statistically significant.

Research question # 2

2. What is the relationship between the perceived easiness of surveillance and counter surveillance training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Results

Correlations

		Surveillance/ Countersurveillance easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Surveillance/Countersurveillance easiness	Pearson Correlation	1	.317*	.081	-.140	.195
	Sig. (2-tailed)		.028	.583	.341	.185
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	.317*	1	.844**	.376**	.893**
	Sig. (2-tailed)	.028		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	.081	.844**	1	.217	.910**
	Sig. (2-tailed)	.583	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	-.140	.376**	.217	1	.464**
	Sig. (2-tailed)	.341	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	.195	.893**	.910**	.464**	1
	Sig. (2-tailed)	.185	.000	.000	.001	
	N	48	48	48	48	48

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of surveillance/counter surveillance training and belief that the executive protection agent can effectively protect the principal shows a weak, positive correlation between variables (r= .195, p < .185) and this relationship is not highly statistically significant.
- The relationship between ease of surveillance/counter surveillance training and the belief in the ability to respond effectively shows a weak, positive correlation between variables (r= .081, p < .583) and this relationship is not highly statistically significant.
- The relationship between ease of surveillance/counter surveillance training and the belief that the individual has the appropriate training shows a weak, negative correlation between variables (r= -.140, p < .341) and this relationship is not highly statistically significant.

- The relationship between ease of surveillance/counter surveillance training and the belief that an attack is probable shows a moderate, positive correlation between variables (r= .317, p < .028) and this relationship is not highly statistically significant.

Research question # 3

3. What is the relationship between the perceived easiness of embus/debus and training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Results

Correlations

		Embus/Debus easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Embus/Debus easiness	Pearson Correlation	1	.317*	.081	-.140	.195
	Sig. (2-tailed)		.028	.583	.341	.185
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	.317*	1	.844**	.376**	.893**
	Sig. (2-tailed)	.028		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	.081	.844**	1	.217	.910**
	Sig. (2-tailed)	.583	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	-.140	.376**	.217	1	.464**
	Sig. (2-tailed)	.341	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	.195	.893**	.910**	.464**	1
	Sig. (2-tailed)	.185	.000	.000	.001	
	N	48	48	48	48	48

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of embus/debus training and belief that the executive protection agent can effectively protect the principal shows a weak, positive correlation between variables (r= .195, p < .185) and this relationship is not highly statistically significant.
- The relationship between ease of embus/debus training and the belief in the ability to respond effectively shows a weak, positive correlation between variables (r= .081, p < .583) and this relationship is not highly statistically significant.
- The relationship between ease of embus/debus training and the belief that the individual has the appropriate training shows a weak, negative correlation between variables (r= -.140, p < .341) and this relationship is not highly statistically significant.
- The relationship between ease of embus/debus training and the belief that an attack is probable shows a moderate, positive correlation between variables (r= .317, p < .028) and this relationship is not highly statistically significant.

Research question # 4

4. What is the relationship between the perceived easiness of walking drills training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Results

Correlations

		Walking drills easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Walking drills easiness	Pearson Correlation	1	.063	-.159	.276	.055
	Sig. (2-tailed)		.673	.279	.058	.712
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	.063	1	.844**	.376**	.893**
	Sig. (2-tailed)	.673		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	-.159	.844**	1	.217	.910**
	Sig. (2-tailed)	.279	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	.276	.376**	.217	1	.464**
	Sig. (2-tailed)	.058	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	.055	.893**	.910**	.464**	1
	Sig. (2-tailed)	.712	.000	.000	.001	
	N	48	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of walking drills training and belief that the executive protection agent can effectively protect the principal shows a very weak, positive correlation between variables (r= .055, p < .712) and this relationship is not highly statistically significant.
- The relationship between ease of walking drills training and the belief in the ability to respond effectively shows a weak, negative correlation between variables (r= -.159 p < .279) and this relationship is not highly statistically significant.
- The relationship between ease of walking drills training and the belief that the individual has the appropriate training shows a weak, positive correlation between variables (r= .276 p < .058) and this relationship is not highly statistically significant.
- The relationship between ease of walking drills training and the belief that an attack is probable shows a very weak, positive correlation between variables (r= .067, p < .673) and this relationship is not highly statistically significant.

Research question # 5

5. What is the relationship between the perceived easiness of firearms training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Results

Correlations

		Firearms easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Firearms easiness	Pearson Correlation	1	-.543**	-.557**	-.629**	-.694**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	-.543**	1	.844**	.376**	.893**
	Sig. (2-tailed)	.000		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	-.557**	.844**	1	.217	.910**
	Sig. (2-tailed)	.000	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	-.629**	.376**	.217	1	.464**
	Sig. (2-tailed)	.000	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	-.694**	.893**	.910**	.464**	1
	Sig. (2-tailed)	.000	.000	.000	.001	
	N	48	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of firearms training and belief that the executive protection agent can effectively protect the principal shows a strong, positive correlation between variables (r= .694, p < .000) and this relationship is highly statistically significant.
- The relationship between ease of firearms training and the belief in the ability to respond effectively shows a strong, positive correlation between variables (r= .557, p < .000) and this relationship is highly statistically significant.
- The relationship between ease of firearms training and the belief that the individual has the appropriate training shows a strong, positive correlation between variables (r= .629 p < .000) and this relationship is highly statistically significant.
- The relationship between ease of firearms training and the belief that an attack is probable shows a very weak, positive correlation between variables (r= .543, p < .000) and this relationship is highly statistically significant.

Research question # 6

6. What is the relationship between the perceived easiness of defensive/evasive driving training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Results

Correlations

		Defensive/evasive driving easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Defensive/evasive driving easiness	Pearson Correlation	1	.090	-.332*	.394**	-.003
	Sig. (2-tailed)		.541	.021	.006	.985
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	.090	1	.844**	.376**	.893**
	Sig. (2-tailed)	.541		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	-.332*	.844**	1	.217	.910**
	Sig. (2-tailed)	.021	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	.394**	.376**	.217	1	.464**
	Sig. (2-tailed)	.006	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	-.003	.893**	.910**	.464**	1
	Sig. (2-tailed)	.985	.000	.000	.001	
	N	48	48	48	48	48

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of defensive/evasive driving training and belief that the executive protection agent can effectively protect the principal shows a very weak (null), negative correlation between variables (r= -.003, p < .985) and this relationship is not highly statistically significant.
- The relationship between ease of defensive/evasive driving training and the belief in the ability to respond effectively shows a moderate, negative correlation between variables (r= -.332, p < .021) and this relationship is highly statistically significant.
- The relationship between ease of defensive/evasive driving training and the belief that the individual has the appropriate training shows a moderate, positive correlation between variables (r= .394 p < .006) and this relationship is highly statistically significant.
- The relationship between ease of defensive/evasive driving training and the belief that an attack is probable shows a very weak, positive correlation between variables (r= .090, p < .541) and this relationship is not highly statistically significant.

Research question # 7

7. What is the relationship between the perceived easiness of personal defense/hand to-hand combat training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Results

Correlations

		Personal defence/hand to hand combat easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Personal defence/hand to hand combat easiness	Pearson Correlation	1	.227	.194	-.201	.281
	Sig. (2-tailed)		.120	.187	.172	.053
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	.227	1	.844**	.376**	.893**
	Sig. (2-tailed)	.120		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	.194	.844**	1	.217	.910**
	Sig. (2-tailed)	.187	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	-.201	.376**	.217	1	.464**
	Sig. (2-tailed)	.172	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	.281	.893**	.910**	.464**	1
	Sig. (2-tailed)	.053	.000	.000	.001	
	N	48	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of personal defense/hand to-hand combat training and belief that the executive protection agent can effectively protect the principal shows a weak, positive correlation between variables (r= .281, p < .053) and this relationship is not highly statistically significant.
- The relationship between ease of personal defense/hand to-hand combat training and the belief in the ability to respond effectively shows a weak, positive correlation between variables (r= .194, p < .187) and this relationship is not highly statistically significant.
- The relationship between ease of personal defense/hand to-hand combat training and the belief that the individual has the appropriate training shows a moderate, positive correlation between variables (r= -.201 p < .172) and this relationship is not highly statistically significant.
- The relationship between ease of personal defense/hand to-hand combat training and the belief that an attack is probable shows a very weak, positive correlation between variables (r= .227, p < .120) and this relationship is not highly statistically significant.

Research question # 8

8. What is the relationship between the perceived easiness of medical aid training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Results

Correlations

		Medical aid easiness	Belief that an attack is probable	Belief in my ability to respond effectively against threat	Belief that I have the appropiate training	Belief that I can protect my principal
Medical aid easiness	Pearson Correlation	1	.258	.113	.558**	.173
	Sig. (2-tailed)		.077	.443	.000	.238
	N	48	48	48	48	48
Belief that an attack is probable	Pearson Correlation	.258	1	.844**	.376**	.893**
	Sig. (2-tailed)	.077		.000	.008	.000
	N	48	48	48	48	48
Belief in my ability to respond effectively against threat	Pearson Correlation	.113	.844**	1	.217	.910**
	Sig. (2-tailed)	.443	.000		.139	.000
	N	48	48	48	48	48
Belief that I have the appropiate training	Pearson Correlation	.558**	.376**	.217	1	.464**
	Sig. (2-tailed)	.000	.008	.139		.001
	N	48	48	48	48	48
Belief that I can protect my principal	Pearson Correlation	.173	.893**	.910**	.464**	1
	Sig. (2-tailed)	.238	.000	.000	.001	
	N	48	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

- The relationship between ease of personal medical aid training and belief that the executive protection agent can effectively protect the principal shows a weak, positive correlation between variables (r= .173, p < .238) and this relationship is not highly statistically significant.
- The relationship between ease of medical aid training and the belief in the ability to respond effectively shows a weak, positive correlation between variables (r= .113, p < .443) and this relationship is not highly statistically significant.
- The relationship between ease of medical aid training and the belief that the individual has the appropriate training shows a strong, positive correlation between variables (r= .558 p < .000) and this relationship is highly statistically significant.
- The relationship between ease of medical aid training and the belief that an attack is probable shows a very weak, positive correlation between variables (r= .258, p < .077) and this relationship is not highly statistically significant.

Demographics & Background

The vast majority of the respondents reported to be male. This is not surprising given the fact that the security industry and, specifically the subset of executive protection, has been historically a male-dominated industry.[xix] From an age standpoint, participants were mostly in the 30 to 49-year-old range, giving them an average of 11-15 years of experience with some level of college education.

There was a consistent mix of respondents whose principals rotated and some who protected just one. Additionally, respondents indicated they both work both in an armed and unarmed capacity (75% cumulative), with 18 participants reporting that they work solely in an armed capacity (25%).
Next, the training profile and the recurrence of the training were examined. The majority of the respondents (54.2%) responded to training alone while the rest responded to training with colleagues. Additionally, in an overwhelming fashion, 83.3% of respondents stated that they only train one to two times per year. As mentioned before, training is often limited by time and financial constraints.

Neither of these results is strikingly different from what was expected and show no type of potential correlation or effect on how the agents responded in subsequent sections except for one item.

Interestingly, even though some respondents stated that they do not use firearms while on duty, their responses potentially indicate that they all place heavy emphasis in the training and use of firearms; this can be speculated based on the fact that all the responses in the firearms module were statistically significant and validated H3. This provides ancillary support to the argument to be discussed in the following discussion section that an overreliance in the use of weapons possibly exists that may distort the executive protection self-efficacy and real ability to protect a principal.

Threat assessment

Research question # 1

1. What is the relationship between the perceived difficulty of threat assessment training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

The relationship between threat assessment training ease and its perceived effect on self-efficacy provided mixed results. None of the participants reported that threat assessment training ease had a strong direct relation with their own ability to protect the principal or their ability to effectively protect the principal against a threat. The relationship, although positive, was weak at best; possibly indicating that the agents did not place too much importance on this specific training module. This does not effectively support H1 and H2.

Conversely, there seems to be a weak, negative relationship between the threat assessment level of ease and the belief that they have the appropriate level of training. This suggests that the easier the threat assessment training was found to be, the less it affected their belief in their in their level of training. Although the relationship between the variables was negative, as expected, it being a weak relationship was not. This mildly supports H3.

Lastly, the results show that there is almost no relationship between the threat assessment training difficulty and the belief that an attack is possible. This is another interesting finding, given that threat assessments provide the executive protection agent with a baseline understanding of what threat actors might potentially attack the principal. This result could suggest that executive protection agents might already believe that an attack is probable and how difficult or easy that specific training module is does not change that perception.

Threat assessments are the cornerstone for all risk mitigation strategies, including executive protection. Weak relationships between variables, regardless of the direction, might suggest two things: One is that the population sample was not large enough to produce conclusive results or that the executive protection

agents are not placing enough importance on the role that threat assessment has within the executive protection.

Surveillance and counter surveillance

Research question # 2

2. What is the relationship between the perceived difficulty of surveillance and counter surveillance training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Similarly to the threat assessment training module, the surveillance/counter surveillance section offered diverse responses from the participants. In this module, all of the relationships between the difficulty of training and self-efficacy variables were weak.

There was almost a null relationship reported between ease of surveillance/counter surveillance training module and their belief in their own ability to respond effectively against a threat. Additionally, there was only a very weak, positive relationship between the difficulty variable and their belief in their ability to protect the principal against an attack. This does not effectively support H1 and H2.

Lastly, the results suggest that ease in this training module has a very weak, yet negative, effect on their own belief that they have the appropriate training. This is finding is similar to the one in the previous section; this slightly suggests that the easier the surveillance module was perceived to be, the less the individual thought that he or she had appropriate training. This supports H3.

The only exception that showed statistical significance is the relationship between the surveillance/counter surveillance training ease and the belief that an attack is possible. This could possibly be due to how during training executive protection agents recognize how easy it can be to covertly survey a potential target (i.e. their principal) and how difficult it can be to conduct covert counter surveillance on potential aggressors (i.e., the attacker). This would raise their awareness on tactics and therefore reinforce the idea that an attack is possible.

Embus/Debus

Research question # 3

3. What is the relationship between the perceived difficulty of embus/debus and training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

The relationship between the embus/debus training module and its perceived easiness during training was reported to have the same relationship with the agent's perceived ability as the previous module of surveillance and counter surveillance.

There was almost a null relationship reported between perceived difficulty of embus/debus training module and their belief in the agent's ability to respond effectively against a threat. Additionally, there was only a very weak, positive relationship between the difficulty variable and their belief in their ability to protect the principal against an attack. This does not effectively support H1 and H2.

The results suggest that ease in this training module has a very weak yet negative effect on their own belief that they have the appropriate training. This suggests that the easier the embus/debus training module

was perceived to be, the less the individual thought that he or she had appropriate training. This mildly supports H3.

Walking drills

Research question # 4

4. What is the relationship between the perceived difficulty of walking drills training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

The results establish that there is a weak but negative relationship between the walking drills training variable and the agents' belief in their ability to respond effectively to threats. This narrowly suggest the easier the training the less confident they feel in their own ability. This supports H1 on a very limited basis.

Next, the relationship between the variable and the belief that the agent can protect his principal is almost null. This does not support H2. Lastly, the correlation between the walking drills variable and the belief that the agent has the appropriate level of training is weak to moderate and positive. This does not support H3 either.

The reason for the lack of support for any of the hypotheses is not clear. None of the correlations were particularly moderate or strong in any direction, which might suggest that the agents do not perceive this training module to be as critical to their overall training curriculum and the effect it has on their work-related performance is believed to be inconsequential.

Firearms

Research question # 5

5. What is the relationship between the perceived difficulty of firearms training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

One of the most interesting findings of this research is that the firearms module presented strong, negative correlations in all categories. This suggests, in principle, that executive protection agents place great emphasis on the ability to carry firearms during protective assignments.

First, the results may show that executive protection agents do not believe that they can protect their principal appropriately if the firearms training is too easy to pass. The same results are applicable to their belief that they have the ability to respond against a threat. This strongly supports H1 and H2.

Likewise, the relationship between firearms training that is low in difficulty and the belief that the agent has the appropriate training is negative and strong. This strongly supports H3. If the executive protection agent completes a firearms module but finds it to be easy, he or she might feel that they were not able to polish their skills.

These results prove to be valuable not only because of their strong statistical significance, but also because it also provides insight into how much value executive protection agents place in the ability to use firearms during a protection detail.

Defensive/evasive driving

Research question # 6

6. What is the relationship between the perceived difficulty of defensive/evasive driving training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

The results for this answer suggest that the easier the driving training was found to be the greater the belief that the agent does not have the appropriate training. This might suggest that security agents place great importance on the value of defensive/evasive driving. This supports H1.

Next, the relationship with this variable is weak and positive, indicating possibly that the easier the driving training was perceived to be, the more the individual believes that he or she has can protect the principal. This is the exact opposite of the results found in the previous firearms section. This would suggest that agents seem to place limited importance on the effect that the driving training might have on their ability to protect their principal (null relationship). This does not support H2.

Lastly, a moderate, positive relationship between the defensive/evasive driving easiness level and the belief that the individual has the appropriate training was found. This correlation is significant at the 0.01 level, indicating that the likelihood of this being a result of pure accident is calculated at 1%. This does not support H3.

Personal defense/hand to-hand combat

Research question # 7

9. What is the relationship between the perceived difficulty of personal defense/hand-to-hand combat training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

Participants responded in a similar fashion when answering questions to this module than in previous questions. According to their responses, there was a weak but positive relationship between their perceived difficulty of training and their own belief that they have the ability to respond to a threat. This does not support H1.

Next, likewise, the study suggests that the relation between this variable and the agent's belief that they can protect the principal is weak and positive. In other words, the easier the training, the more confident the agent is in his or her ability to protect the principal. This does not support H2.

Lastly, the relationship between the personal defense/hand to hand combat training easiness and their belief that that they have the appropriate training is weak and negative in nature. This mildly suggests that the easier the training was perceived to be, the less prepared they felt. This supports H3.

Medical aid

Research question # 8

8. What is the relationship between the perceived difficulty of medical aid training and the executive protection agent's perceptions of his own ability to respond effectively against threats to the principal?

The medical portion of the results provided another batch of mixed results. According to the survey, there is a very weak, positive relationship between the medical training difficulty level variable and the belief that training participants can protect their principal and their ability to respond effectively against a threat.

Given that the relationships are weak and not statistically significant, it be concluded that the results are inconclusive at best. This does not support H1.

Subsequently, the relationship between medical aid training easiness and the agents' perceptions of their own ability to protect their principal also has a weak, strong relationship. Similarly to the previous results, this does not support H2.

Finally, the relationship between the training difficulty of the module and the belief that the individuals have the appropriate level of training is strong, positive and statistically significant. This suggests, contrary to the findings in relation to firearms trainings, the easier the training is the stronger the belief that they have the appropriate training. This does not support H3.

These results could be partially due to a counterintuitive reason. First aid and the field of medicine are complex topics. Therefore, the individual might have certain expectations about the difficulty of the training. Once the individuals complete training on a difficult topic and perceive it to be easy, they might believe that the training was indeed of high quality given that they were able to easily comprehend it. This might differ from firearms training as that might be seen as a simpler training module, in which case a very easy training might indicate to them that the content was not adequate.

Discussion

The researcher expected that all hypotheses would be confirmed or at the very least partially validated. However, the results of the survey provided mixed results. First, demographics and background variables were examined to see if there was any effect on the respondents' answers. Upon first inspection none of these variables seem to have a direct effect on how the correlation between the difficulty level of training variable and their respondent's own perceptions of their own ability. However, upon further examination, it is clear that even though 37.5% of the respondents stated that they work exclusively without weapons, as it will be discussed below, the firearms training module questions suggests that all respondents believe that the easier the firearms training is, the less prepared they are. This means that even though they might not use them on active duty (based on jurisdiction restrictions or possibly upon the client's request), they still train with them and place great emphasis on their value. More of this will be examined below.

Next, the correlation between the two aforementioned variables was analyzed and examined to see if the results validated or not the presented hypotheses. This exercise was conducted with every single research question. When analyzing the hypotheses, H1 saw very limited validation. The results suggest that perceived easiness of the training modules did not have a negative effect on their perceptions when it comes to responding effectively and protecting the principal. This was true for the threat assessment, surveillance and counter surveillance, embus/debus, personal defense/hand to-hand combat and medical aid training modules. Conversely, on a more limited basis, defensive/evasive driving, firearms and walking drills training modules yielded results that did provide evidence that the easiness of training affected the agents' belief in their own ability in relation to H1 and therefore providing some validity to the hypothesis.

H2 followed very similar results to H1 possibly due the similarity in the wording of the questions being posed. Although the questions are different in nature, the similarity of wording could have meant that respondents answered both questions as if they were similar. For H2, only the firearms training module provided validation.

H3 was the one hypothesis that received more validation with five out of the eight training modules providing either limited or strong correlation. This suggests that perceived easiness of certain training modules can have a negative effect on the executive protection agents' perception that they have appropriate training. The easier the training, the less prepared agents might feel. These modules included threat assessment, surveillance and counter surveillance, embus/debus, firearms and personal defense/hand to-hand combat. Walking drills, defensive/evasive driving and medical aid did not support this hypothesis.

As stated before, it was expected that all hypotheses would be validated by the survey results. However, most of the results were not highly statistically significant and did not clearly validate H1 or H2. Only H3 was truly validated. There are several reasons why this may have happened.

First, it could be argued that the survey instrument was not properly created and that it provided misguided questions. However, the fact that the firearms training module provided highly statistical and consistent answers across the board as expected, suggests that the survey instrument was in fact properly worded.

Second, respondents may have had a certain level of apathy or indifference towards the vast majority of the training modules with the only exception being firearms training. This again is possibly evidenced by the highly statistically significant responses when it came to firearms training. It is possible that respondents did not believe that the training modules' level of difficulty had a real effect on their perceived ability of performance due to an overreliance on firearms and their possible neutralizing effect against a potential attacker.

Third, the lack of statistical support could be a function of possibility vs. ability. The agent may feel that such training is appropriate and that he or she has the ability to partially protect their principal. However, given the numerous potential sources of threats towards a principal (i.e. terrorism, common crime, natural disasters, accidental fires, targeted crime, etc.) and the finite resources to protect it (i.e. resources, personnel, etc.) it is not possible to unequivocally state that any given training can provide the absolute ability to effectively protect a principal from all threats. In other words, agents believe that they can mitigate the risk but cannot eliminate it no matter how high the quality of the training is.

These three notions can possibly explain some of the mixed results and inconsistencies across the surveys in relation to what the researcher expected to be consistent answers that positively validated all three of the hypothesis. Based on the results, it is more likely than not that apathy or indifference may have affected some of the effects of the survey.

This study does indicate that a challenging training curriculum provides the agent with a perception that he or she has completed a commensurate training to counter any possible threat. However, as mentioned above, inconclusive results were unable to verify how this is related to agents' perceived ability to put that training into practice. It is possible that the executive protection agent may feel that the training was appropriate and sufficient but still feels unable to effectively protect the principal.

That being said, there was an interesting finding that validated H3. There was only one training module that validated all three hypotheses and did so with statistically significant results in every category. That is the firearms training module. The use of firearms in executive protection has always been a source of controversy. It can be argued that executive protection agents' perceptions and opinions about the use of

firearms during protection details come from their own personal experiences. Generally speaking, there are two schools of thought.

The first one believes that the use of firearms should be limited and only in locations where is absolutely necessary with some even calling it "the most useless tool in executive protection."[xx] Instances where the use of weapons might be required include those when a principal has been subject to direct threats of harm or high risk locations such as active war zones.

This is justified by the belief that the use of weapons changes the mind-set of even the best executive protection teams (and the principals) from preventative to reactive security and protection. The main focus of preventative security is to train agents so they can identify threats before these affect the principals. For any crisis situation, the agents are trained in conflict resolution and would seek to divert the threat while they evacuate the principal.

Alternatively, the second school of thought believes that firearms are an integral part of the executive protection service. There is a belief that threat assessments, defensive and evasive driving, personal defense and other non-lethal risks mitigation techniques, can only assist to a certain extent and that the firearm serves as the last layer of protection.

Conclusions

The results of this survey provided mixed results to the question of whether the perceived difficulty level of different training modules directly affected executive protection agents' perceptions of their ability to protect their principal or respond effectively against a threat. However, this study has validated that training perceived as easier leaves the security agent with the belief that they may not have the right training and the right skills sets to perform at their job. Conversely, the more difficult the training was perceived to be, the more the security practitioner agent feels that they have received quality training.

Since most of the answers were statistically insignificant in either direction, this may suggest a certain level of apathy on the part of executive protection agents when it comes to placing significance on specific training modules. Simply put, the case could be that there is no real consensus on how certain training modules affect agents' perceived ability in part because they do not regard any of them as particularly more important than the rest, with the apparent exception of firearms training.

The security and protection industry has certainly become more professionalized over time; intelligence-based preventive approaches are being favored versus reactive and tactical methods. This study has unexpectedly shed light on the fact that executive protection agents may continue to place greater emphasis on the apparent value of firearms training over other executive protection skills.

Recommendations for Policymakers and Practitioners

Executive protection agents add great value to the lives and employers of people in need of their services. However, the lack of available research on what an effective training curriculum should include represents a problem for policy makers who seek to regulate and improve the quality of the services rendered, as well as ensure that firearms are used in the appropriate situations and within the scope of the law. As a consequence, training regiments vary wildly across jurisdictions at a national and international level.

New research can assist policy makers in adjusting or creating laws to ensure that minimum training requirements for executive protection agents place the right emphasis on training modules found to be

the most effective through research. Furthermore, this study suggests that executive protection agents may have an overreliance on the use of firearms and do not place the proper emphasis on other preventive risks mitigation techniques taught in other training modules.

Similarly to policy makers, executive protection practitioners and professional organizations that provide certifications, such as ASIS International, should closely examine the training modules for each executive protection course that is attended, recommended or endorsed. The courses should borrow from both preventive and reactive techniques and provide a robust and comprehensive approach to security. Additionally, the practitioners should know the limitations of each approach and understand that overdependence on any single one, such as firearms use, can be counterproductive.

This potential overreliance cannot only put the principal at greater risks, but it can also be argued that a reactive mentality—overly emphasizing the use of weapons versus a preventative mentality that relies on threat assessments, advance work and other preventative techniques—puts the general public at greater risk by virtue of the possibly avoidable use of weapons in public spaces. In jurisdictions such as the United States, the minimum training standards are stricter and the risk of civil or criminal liability due to improper or negligent training offerings is higher than in other jurisdictions. Hence, organizations can reduce liability exposure in these sensitive jurisdictions if they offer or endorse sound and well-rounded training regimes.

Author: Diego Andreu is the Principal for Protective Service for Crisis and Security Consulting at Control Risks. He has two decades of experience in private security, and this research article is based on his previous academic research.

Endnotes

[i] Security Industry Authority, "Training – Close Protection," 2016, accessed November 2, 2016, http://www.sia.homeoffice.gov.uk/Pages/training-cp.aspx.
[ii] Charles P. Nemeth, *Private Security and the Law* (Waltham, MA: Elsevier, 2012), 309.
[iii] ASIS International, *The United States Security Industry: Size and Scope, Insights, Trends, and Data* (Alexandria, VA: ASIS International, 2013), 4.
[iv] H. H. Cooper, PPS, CST, "Trying to Be a Hero and Winding Up a Zero," *Journal of Security Education* 2, no. 2 (2007): 11–25, 17.
[v] Security Industry Authority.
[vi] Brendan Moriarty, "Research Design and the Predictive Power of Measures of Self-Efficacy," *Issues in Educational Research* 24, no. 1 (2014): 55–66.
[vii] Albert Bandura, "Social Cognitive Theory of Self-Regulation," *Organizational Behavior and Human Decision Processes* 50, no. 2 (1991): 248–87.
[viii] Albert Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory* (Englewood Cliffs, NJ: Prentice Hall, 1986), 391.
[ix] Albert Bandura, *Self-Efficacy: The Exercise of Control* (New York: W. H. Freeman, 1997).
[x] Terrence R. Mitchell and Marilyn E. Gist, "Self-Efficacy: A Theoretical Analysis of Its Determinants and Malleability," *Academy of Management Review* 17, no. 2 (1992): 183–211.
[xi] Alexander D. Stajkovic and Fred Luthans, "Self-Efficacy and Work-Related Performance: A Meta-Analysis," *Psychological Bulletin* 124, no. 2 (1998): 240–61.
[xii] Albert Bandura, "Social Cognitive Theory: An Agentic Perspective," *Behaviour Research and Therapy* 42, no. 10 (2004): 1129–48.
[xiii] Bandura, *Self-Efficacy*.

[xiv] Ibid, 382.
[xv] Laerd Dissertation, "Dissertation Essentials," 2012, accessed October 1, 2012, http://dissertation.laerd.com/types-of-quantitative-research-question.php.
[xvi] Gerald Albaum, "The Likert Scale Revisited: An Alternate Version," *Journal of the Market Research Society* 39, no. 2 (1997): 331–49.
[xvii] Albert Bandura, "Guide for Constructing Self-Efficacy Scales," in *Self-Efficacy Beliefs of Adolescents*, ed. Frank Pajares and Timothy Urdan (Greenwich, CT: Information Age Publishing, 2006), 307–37, 311.
[xviii] Robert V. Hogg and Elliot A. Tanis, *Probability and Statistical Inference* (Upper Saddle River, NJ: Pearson Education International, 2009).
[xix] Sarah J. Davies, *Women in the Security Profession: A Practical Guide for Career Development* (Cambridge: Elsevier, 2017).
[xx] Kevin Moyer, producer, *The World Protection Group: The Use of a Gun in Executive Protection* (Beverly Hills, CA: YouTube, 2011).

Additional Resources

1. Academy of Criminal Justice Sciences, "Aims and Scope," *Western Journal of Criminal Justice* (n.d.), accessed November 10, 2016, http://www.tandfonline.com/action/journalInformation?show=aimsScope&journalCode=wasr20.
2. ASIS International, *Workplace Violence Prevention and Intervention* (Alexandria, VA: ASIS International, 2011).
3. Albert Bandura, "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* 84, no. 2 (1977): 191–215.
4. Albert Bandura, "Self-Efficacy," in *Encyclopedia of Human Behavior*, vol. 4 (New York: Academic Press, 1994), 71–81.
5. Albert Bandura, "A Social Cognitive Theory of Personality," in *Handbook of Personality: Theory and Research*, ed. Lawrence A. Pervin and Oliver P. John (New York: Guilford Press, 1999).
6. Albert Bandura, "Guide for Constructing Self-Efficacy Scales," in *Self-Efficacy Beliefs of Adolescents*, ed. Frank Pajares and Timothy Urdan (Greenwich, CT: Information Age Publishing, 2006), 307–37.
7. Theodore Becker, "The Place of Private Police in Society: An Area of Research for the Social Sciences," *Social Problems* 21, no. 3 (1974): 439–53.
8. David Berdnarz, "Quantity and Quality in Evaluation Research: A Divergent View," *Evaluation and Program Planning* 8, no. 4 (1985): 289–306.
9. Richard Brislin, *The Effective Security Officer's Training Manual* (St. Louis, MO: Elsevier Science, 2014).
10. James D. Brown, "Likert Items and Scales of Measurement?," *JALT Testing & Evaluation SIG Newsletter* 15, no. 1 (2011): 10–14.
11. James Cullen and Amanda Gravert, *Crime in 2015: A Final Analysis* (New York: Brennan Center for Justice at New York University School of Law, 2015).
12. Sarah J. Davies, *Women in the Security Profession: A Practical Guide for Career Development* (Cambridge: Elsevier, 2017).
13. Andrew Davis, "In U.S., Concern About Crime Climbs to 15-Year High," *Gallup*, October 26, 2016, accessed November 11, 2016, https://www.gallup.com/poll/190475/americans-concern-crime-climbs-year-high.aspx.
14. Cathy Durham, Don Knight, and Edwin A. Locke, "Effects of Leader Role, Team-Set Goal Difficulty, Efficacy, and Tactics on Team Effectiveness," *Organizational Behavior and Human Decision Processes* 72, no. 2 (1997): 203–31.
15. Federal Bureau of Investigation, *Crime in the United States* (Washington, DC: FBI, 2015).
16. Robert A. Fein, Bryan Vossekuil, and Gwen A. Holden, *Threat Assessment: An Approach to Prevent Targeted Violence* (Washington, DC: National Institute of Justice, 1995).

17. Global Information, Inc., *Private Security Services: Demand and Sales Forecasts, Market Share, Market Size, Market Leaders* (Cleveland, OH: Freedonia Group, 2015).
18. Andrew Hunsicker, *Advanced Skills in Executive Protection* (Boca Raton, FL: Universal Publishers, 2010).
19. Chris Jackson, "Correlation vs. Causation Differences," *Study.com*, 2003, accessed November 17, 2016, http://study.com/academy/lesson/correlation-vs-causation-differences-lesson-quiz.html.
20. Dale L. June, *Introduction to Executive Protection* (Boca Raton, FL: CRC Press, 2015).
21. Thomas Lee, Linda Swanson, and Andrew Hall, "What Is Repeated in a Repetition? Effects of Practice Conditions on Motor Skills Acquisition," *Movement Science Series* 71, no. 2 (1991): 150–56.
22. Abraham H. Maslow, "A Theory of Human Motivation," *Psychological Review* 50, no. 4 (1943): 370–96.
23. Todd J. Maurer and Heather R. Pierce, "A Comparison of Likert Scale and Traditional Measures of Self-Efficacy," *Journal of Applied Psychology* 83, no. 2 (1998): 324–29.
24. Robert Muggah, "Why Personal Security Should Be Part of the Post-2015 Development Agenda," *Global Observatory*, November 2012, accessed November 9, 2016, https://theglobalobservatory.org/2012/11/why-personal-security-should-be-part-of-the-post-2015-development-agenda/.
25. Helen Page-Bucci, *The Value of Likert Scales in Measuring Attitudes of Online Leaders*, 2003, accessed November 9, 2016, http://www.hkadesigns.co.uk/websites/msc/reme/likert.htm.
26. Dale H. Schunk, "Self-Efficacy, Motivation, and Performance," *Journal of Applied Sport Psychology* 7, no. 2 (1995): 112–37.
27. C. Sergeev and A. M. Lipsky, "Training Modalities and Self-Confidence Building in Performance of Life-Saving Procedures," *Military Medicine* 177, no. 8 (2012): 901–6.
28. Somporn Sukamolson, *Fundamentals of Quantitative Research* (Bangkok: Language Institute, Chulalongkorn University, 2010).
29. Jacques Tacq, "Causality in Qualitative and Quantitative Research," *Quality & Quantity* 45, no. 2 (2011): 263–91.
30. United Nations, *Universal Declaration of Human Rights* (Paris: United Nations, 1948).
31. United Nations Office on Drugs and Crime, *Global Study on Homicide 2013* (Geneva: UNODC, 2014).
32. Helmut Waldemar, "The 'Somatophylakes' of Alexander the Great: Some Thoughts," *Zeitschrift für Alte Geschichte* 27, no. 1 (1978): 224–50.

Toward a Philosophy of Intelligence Analysis: Epistemology, Method, and Judgment in the Production of Forecasting

Treston Wheat, PhD

Abstract
Intelligence analysis is routinely described as an applied craft or a quasi-scientific activity, yet it remains under-theorized as a distinct epistemic practice. This essay argues that intelligence analysis warrants a formal philosophical framework analogous to the philosophy of science but grounded in fundamentally different epistemic conditions. Unlike scientific inquiry, intelligence operates under adversarial uncertainty, deliberate deception, institutional constraint, and irreversible decision-making, where verification is often impossible ex ante and outcomes are shaped by reflexive human behavior. Drawing on philosophy of science, cognitive psychology, organizational theory, and intelligence studies, the essay conceptualizes intelligence as a knowledge-producing activity oriented toward uncertainty reduction and decision advantage rather than predictive certainty. It examines the epistemology of intelligence judgment, the pluralistic reasoning models employed in analytic tradecraft, and the institutional dynamics that shape analytic consensus and failure. Through case studies treated as epistemic stress tests, the essay demonstrates that intelligence failures arise less from isolated errors than from systemic vulnerabilities embedded in analytic frameworks and organizational processes. In response, it proposes *pragmatic adversarial epistemology* as a coherent philosophy of intelligence analysis, emphasizing provisional truth claims, epistemic humility, structured skepticism, and the management of uncertainty. The essay concludes by outlining methodological and institutional implications for analytic rigor, professionalization, and reform, positioning this framework as a foundation for advancing both theory and practice in intelligence analysis.

Introduction

Intelligence analysis is a systematic effort to produce knowledge under conditions of radical uncertainty, strategic deception, and time pressure, yet it remains conceptually under-theorized as a distinct epistemic practice. While analysts routinely debate methods, tradecraft, and organizational reform, these discussions often proceed without an explicit philosophical framework comparable to those that guide inquiry in the natural and social sciences. As a result, intelligence analysis is frequently described as an "art," a "craft," or an applied discipline that resists formal theory, rather than as a coherent mode of knowledge production with its own epistemological assumptions, methodological constraints, and standards of justification. This absence of philosophical clarity has contributed to recurring analytic failures, persistent confusion over the relationship between intelligence and policy, and unresolved tensions between accuracy, relevance, and decision utility.[i]

This essay argues that intelligence analysis warrants a formal philosophy analogous to the philosophy of science, not because intelligence aspires to scientific certainty, but precisely because it does not. Intelligence operates in environments where evidence is fragmentary, adversaries actively manipulate

information, causal mechanisms are opaque, and outcomes are shaped by reflexive human behavior rather than stable natural laws.[ii] These conditions distinguish intelligence from experimental science while placing it closer to historically contingent and adversarial fields such as strategy, history, and political judgment. Yet unlike those disciplines, intelligence analysis is institutionalized within bureaucratic systems that demand confidence assessments, predictive judgments, and policy relevance under conditions that preclude verification in advance. Any philosophy of intelligence analysis must therefore account for how analysts justify beliefs, manage uncertainty, and translate probabilistic judgments into actionable assessments without collapsing into either false precision or analytic paralysis.[iii]

The need for such a framework has become more acute in recent decades. Major intelligence failures are often treated as discrete historical episodes rather than as manifestations of deeper epistemic and organizational problems. Postmortems typically emphasize cognitive bias, information silos, or politicization, yet these explanations remain incomplete without a broader theory of how intelligence knowledge is generated, challenged, and revised. Similar debates within the philosophy of science, particularly those concerning falsification, paradigms, and theory-ladenness, offer useful analogies for understanding why intelligence assessments persist even in the face of contradictory evidence and why analytic consensus can harden into dogma.[iv]

At the same time, intelligence analysis cannot simply import the standards of scientific inquiry. Intelligence judgments are rarely falsifiable in a Popperian sense, as adversaries adapt, conceal, and change behavior in response to observation. Outcomes often depend on counterfactuals, what might have happened absent intervention, and on decisions taken by policymakers who may accept, distort, or ignore analytic conclusions.[v] Intelligence analysis is therefore best understood as a form of *pragmatic epistemology*: a disciplined attempt to reduce uncertainty, anticipate risk, and minimize catastrophic error rather than to discover immutable truths. Its success lies not in prediction alone, but in warning, framing, and enabling better decisions under uncertainty.[vi]

This essay proposes the foundations of a philosophy of intelligence analysis grounded in what may be termed pragmatic adversarial epistemology. This framework treats intelligence as a distinct knowledge practice shaped by strategic interaction, institutional constraints, and bounded rationality. It emphasizes provisional truth claims, structured skepticism, and the management of uncertainty rather than the pursuit of definitive explanation. By drawing on philosophy of science, decision theory, cognitive psychology, and intelligence studies, the essay seeks to clarify the epistemic status of intelligence judgments, the methodological logic of analytic tradecraft, and the responsibilities that accompany predictive assessments affecting national and organizational security. In doing so, it aims to contribute to the professionalization of intelligence analysis by making explicit the philosophical assumptions that already, often implicitly, govern analytic practice.

Intelligence as a Knowledge-Producing Activity

To develop a philosophy of intelligence analysis, it is first necessary to clarify what kind of knowledge intelligence analysis produces and how that knowledge differs from other established forms of inquiry. Intelligence is neither a derivative of scientific research nor a variant of journalism or historical scholarship. Rather, it is a distinct knowledge-producing activity oriented toward anticipation, warning, and decision advantage under conditions of uncertainty, secrecy, and strategic opposition. Its purpose is the reduction of uncertainty in contexts where failure carries disproportionate costs.[vii]

Unlike scientific inquiry, intelligence analysis does not operate in controlled environments, nor does it rely on repeatability, experimental isolation, or stable causal relationships. The phenomena intelligence seeks to understand, such as state intentions, non-state actor behavior, technological trajectories, political instability, are reflexive and adaptive. Targets of analysis respond to observation, alter behavior to evade detection, and actively attempt to manipulate the analyst's evidentiary environment through denial, deception, and narrative shaping.[viii] As a result, intelligence knowledge is produced in an adversarial epistemic context, where the absence of evidence may be deliberate, and apparent confirmation may itself be an artifact of manipulation. This adversarial dimension distinguishes intelligence from most social-scientific inquiry and imposes unique constraints on standards of justification.

At the same time, intelligence analysis differs from journalism and historical research in both temporal orientation and evidentiary burden. Journalism privileges immediacy and public accountability, often reporting discrete facts without requiring probabilistic integration into forward-looking judgments. Historical scholarship, by contrast, benefits from retrospective access to fuller records and the ability to assess causation after outcomes are known. Intelligence analysis operates in the inverse condition as it must render judgments before events unfold, often without access to complete information and without the possibility of immediate verification.[ix] Its knowledge claims are therefore provisional by necessity, evaluated not by their correspondence to settled fact, but by their coherence, plausibility, and usefulness to decision-makers at a given moment.

This distinction gives rise to a critical tension at the core of intelligence work: the difference between analytic truth and actionable truth. Analytic truth refers to assessments that most accurately reflect underlying reality, even if those assessments are uncertain, ambiguous, or politically inconvenient. Actionable truth, by contrast, refers to judgments that enable decision-making, prioritization, and risk management, even when confidence is limited. Intelligence analysis must navigate between these poles, translating uncertain knowledge into forms that can inform policy without overstating confidence or obscuring uncertainty.[x] This translation function is central to intelligence as a knowledge-producing activity and underscores why intelligence cannot be evaluated solely on predictive accuracy.

Because intelligence knowledge is produced for use rather than contemplation, it is inherently pragmatic. Analysts are tasked with identifying patterns, trends, and warning indicators that may never culminate in observable events precisely because intervention or deterrence occurs. In such cases, analytic success is epistemically invisible. The absence of crisis may reflect correct assessment and effective response rather than analytic failure.[xi] This feature complicates traditional notions of validation and falsification, as intelligence judgments often concern counterfactual futures rather than testable hypotheses.

Intelligence analysis also relies heavily on synthesis rather than discovery. Analysts rarely uncover entirely new facts; instead, they integrate disparate data streams—human reporting, technical collection, open sources, and contextual knowledge—into structured judgments. This synthetic process resembles what philosophers of science describe as model-building rather than law-seeking. Intelligence assessments construct interpretive models of adversary behavior, political dynamics, or strategic trajectories that organize evidence into coherent explanatory and predictive frameworks. These models are necessarily incomplete and subject to revision, but they serve as cognitive tools for navigating complexity.

Finally, intelligence analysis is irreducibly collective. Unlike individual scientific inquiry, intelligence knowledge is produced within institutional settings shaped by bureaucratic processes, classification regimes, division of labor, and hierarchical review. Analytic judgments emerge through coordination, debate, and compromise across organizational units, each with distinct access to information and analytic

cultures.[xii] As a result, intelligence knowledge reflects not only epistemic reasoning but also organizational cognition. Any philosophy of intelligence analysis must therefore account for the ways institutions shape what can be known, how dissent is managed, and how analytic confidence is constructed.

Together, these characteristics suggest that intelligence analysis constitutes a distinct epistemic practice defined by adversarial conditions, temporal urgency, pragmatic orientation, and institutional mediation. Recognizing intelligence as a knowledge-producing activity in its own right is a prerequisite for developing a coherent philosophy of intelligence analysis capable of explaining both its strengths and its recurring failures.

Epistemology of Intelligence Analysis

Any philosophy of intelligence analysis must begin with the epistemic question that underlies all analytic activity: how do intelligence analysts know what they know, and with what degree of justification can those beliefs be held? Unlike scientific inquiry, where epistemic authority is grounded in repeatable observation and experimental control, intelligence analysis operates in an environment characterized by incomplete information, deliberate deception, and strategic interaction. Knowledge claims in intelligence are therefore neither deductively certain nor empirically stable; they are probabilistic judgments formed under adversarial conditions that actively undermine epistemic reliability.[xiii]

A defining feature of intelligence epistemology is the problem of *structured ignorance*. Analysts rarely confront mere absence of information; rather, they must contend with the possibility that missing data are the result of intentional concealment. Denial and deception efforts are designed precisely to distort the analyst's evidentiary field, creating false confirmations, suppressing disconfirming signals, or shaping analytic expectations over time.[xiv] This condition parallels longstanding debates in the philosophy of science regarding theory-ladenness and underdetermination, in which evidence alone cannot uniquely determine which hypothesis is correct. In intelligence, however, this problem is intensified by the presence of an adaptive adversary whose objective is not truth-seeking but misdirection.

The epistemic challenge is further compounded by the limited applicability of falsification. Karl Popper's criterion of falsifiability has influenced intelligence tradecraft through an emphasis on hypothesis testing and structured skepticism, yet intelligence judgments are rarely falsifiable in a strict sense. Predictions often concern future actions that may be altered by deterrence, policy intervention, or changes in adversary intent. When a predicted event does not occur, analysts cannot easily determine whether the assessment was incorrect or whether it was rendered obsolete by external action.[xv] This mirrors critiques in the philosophy of science that highlight the difficulty of falsifying complex theories embedded within broader research programs, as articulated by Imre Lakatos. Intelligence assessments function similarly as components of evolving analytic frameworks rather than isolated hypotheses subject to decisive refutation.[xvi]

In practice, intelligence epistemology relies on disciplined judgment rather than formal proof. Probability language, confidence levels, and estimative terms serve as epistemic tools for expressing degrees of belief rather than claims of certainty. Sherman Kent's insistence on explicit probability statements reflected an early attempt to impose epistemic transparency and analytic accountability within an inherently uncertain domain.[xvii] Modern structured analytic techniques (SATs) extend this effort by forcing analysts to surface assumptions, consider alternatives, and examine disconfirming evidence. These techniques do not eliminate bias or uncertainty; instead, they function as epistemic scaffolding designed to make reasoning processes more explicit and therefore more contestable.[xviii]

The use of such techniques aligns intelligence analysis with Bayesian approaches to reasoning, particularly in the emphasis on updating beliefs in light of new information. However, intelligence rarely conforms to ideal Bayesian conditions. Analysts must often assign priors without reliable base rates, update on ambiguous or contradictory evidence, and operate under severe time constraints. As a result, intelligence epistemology is best understood as Bayesian-inspired rather than Bayesian in a strict mathematical sense. Heuristics and qualitative judgment remain indispensable, echoing findings from cognitive science that human reasoning under uncertainty cannot be fully formalized without sacrificing responsiveness and contextual awareness.[xix]

Another core epistemic feature of intelligence analysis is its dependence on abductive reasoning. Analysts frequently infer the most plausible explanation for observed behavior rather than deriving conclusions deductively or statistically. This form of reasoning, described by Charles Sanders Peirce as abduction, is particularly well-suited to environments where data are sparse, causality is opaque, and multiple explanations remain viable.[xx] In intelligence practice, abductive reasoning underlies pattern analysis, anomaly detection, and early warning, allowing analysts to generate hypotheses that can guide further collection and analysis. The epistemic risk of abduction lies in its susceptibility to narrative coherence and confirmation bias, reinforcing the need for structured challenge mechanisms.

Importantly, intelligence epistemology is not purely individual; it is collective and institutional. Analytic judgments are shaped by organizational cultures, classification barriers, review processes, and incentive structures. What counts as "known" within an intelligence organization often reflects consensus-building processes rather than purely evidentiary thresholds. This institutional mediation parallels sociological critiques of scientific knowledge that emphasize the role of communities, norms, and power in shaping epistemic authority.[xxi] In intelligence, however, the stakes of such mediation are higher, as distorted consensus can persist unchallenged until failure occurs.

All of this suggests that intelligence analysis rests on an epistemology of provisional belief, adversarial uncertainty, and pragmatic justification. Knowledge claims are evaluated not solely by their correspondence to reality, but by their coherence, transparency, and capacity to support sound decision-making under uncertainty. A philosophy of intelligence analysis must therefore treat epistemic humility, revisability, and structured skepticism not as optional virtues, but as foundational requirements for analytic credibility.

Institutional and Organizational Epistemology of Intelligence

Intelligence analysis is not produced by isolated analysts but by institutions that structure how information is collected, interpreted, validated, and communicated. Any philosophy of intelligence analysis must therefore move beyond individual cognition to examine the organizational epistemology of intelligence: the ways institutions shape what can be known, what is treated as credible, and how analytic consensus is formed. Intelligence organizations and agencies function as epistemic communities whose norms, hierarchies, and incentives profoundly influence analytic judgment, often in ways that are invisible to practitioners themselves.[xxii]

Organizational epistemology begins with the division of labor. Intelligence institutions fragment knowledge across collection disciplines, regional desks, functional specialties, and classification compartments. This fragmentation is operationally necessary, yet epistemically costly. Analysts rarely possess a complete evidentiary picture. Instead, they work with partial, mediated representations of

reality shaped by collection priorities, access constraints, and reporting chains.[xxiii] This mirrors classic problems in the philosophy of science regarding distributed cognition, where no single actor fully grasps the totality of evidence supporting a theory. In intelligence, however, the problem is compounded by secrecy and bureaucratic gatekeeping, which can prevent critical information from reaching those best positioned to interpret it.

Consensus formation within intelligence organizations further shapes epistemic outcomes. Analytic products typically pass through multiple layers of review, coordination, and editing, each intended to improve rigor and clarity. Yet these processes also introduce pressures toward convergence, smoothing over dissent and uncertainty in favor of institutional coherence. Dissenting views may be formally recorded, but they are often marginalized unless they align with senior expectations or prevailing analytic frames. This dynamic resembles Thomas Kuhn's account of "normal science," in which paradigms guide inquiry and anomalies are managed rather than immediately embraced. In intelligence, dominant analytic paradigms, such as assumptions about adversary rationality, regime stability, or technological feasibility, can persist long after evidence begins to erode them.

Bureaucratic incentives further condition analytic knowledge. Intelligence organizations are embedded within decision environments that reward timeliness, relevance, and decisiveness. Analysts are therefore incentivized to produce clear judgments even when underlying uncertainty is substantial. Over time, this can generate what might be termed *institutional confidence inflation*, where repeated exposure to ambiguous outcomes leads organizations to express assessments with greater certainty than the evidence warrants. The epistemic risk is not deliberate politicization, but gradual normalization of overconfidence driven by organizational demand signals.

The relationship between intelligence and policy represents a particularly fraught epistemic boundary. Sherman Kent famously argued for analytic objectivity and separation from policy advocacy, warning that proximity to decision-makers could distort judgment.[xxiv] Subsequent scholarship has shown that complete separation is neither possible nor desirable, as intelligence that is insufficiently attuned to policy needs risks irrelevance. The epistemic challenge lies in maintaining analytic autonomy while ensuring relevance. From an organizational epistemology perspective, this tension reflects competing standards of validity: truth-tracking versus utility-tracking. When policy preferences implicitly shape what questions are asked, what assumptions are challenged, or which uncertainties are emphasized, institutional knowledge production becomes vulnerable to subtle forms of bias without overt political interference.[xxv]

Classification and secrecy further complicate organizational epistemology. While secrecy protects sources and methods, it also constrains peer review, limits external challenge, and isolates analytic communities from broader epistemic correction. Unlike scientific knowledge, which benefits from replication and open criticism, intelligence knowledge circulates within closed systems where error detection depends on internal dissent mechanisms. Red teams, alternative analysis units, and structured dissent channels represent institutional attempts to compensate for this epistemic closure, yet their effectiveness varies widely depending on organizational culture and leadership support.

Institutional memory also plays a critical role in intelligence epistemology. Past assessments, estimative language, and analytic judgments create cognitive and bureaucratic path dependencies. Once an assessment becomes embedded in doctrine, planning assumptions, or interagency consensus, it acquires epistemic inertia. Reversing such judgments requires not only new evidence but organizational willingness to reinterpret prior commitments. This phenomenon parallels Lakatos's concept of "research programmes,"

in which core assumptions are protected while auxiliary hypotheses absorb anomalies.[xxvi] In intelligence, this can lead to prolonged misjudgment even in the presence of accumulating contrary indicators.

Finally, intelligence institutions must manage the epistemology of warning. Warning analysis involves identifying low-probability, high-impact events and persuading decision-makers to take them seriously without inducing alarm fatigue. Organizationally, this requires balancing sensitivity and specificity, an epistemic tradeoff analogous to error management debates in philosophy of science and statistics.[xxvii] Institutions that over warn risk losing credibility; those that under-warn risk catastrophic failure. How organizations calibrate this balance reflects not only analytic judgment but institutional tolerance for risk and failure. Intelligence analysis is best understood as an institutional epistemic practice shaped by organizational structures, incentive systems, and cultural norms. Knowledge production in intelligence is neither purely rational nor purely political; it is mediated through bureaucratic processes that privilege certain forms of reasoning while constraining others. A philosophy of intelligence analysis that ignores these institutional dynamics risks attributing failure to individual bias alone, while overlooking the deeper epistemic conditions that shape analytic judgment at scale.

Methodology and Reasoning Models in Intelligence Analysis

If epistemology addresses what can be known and with what justification, methodology concerns how intelligence analysts reason from evidence to judgment under conditions of uncertainty and opposition. Intelligence analysis employs no single method. Rather, it relies on a pluralistic set of reasoning models adapted to different analytic problems, time horizons, and evidentiary environments. This methodological eclecticism reflects the reality that intelligence problems rarely conform to the assumptions required by any one formal approach. Rather than aspiring to methodological purity, intelligence analysis prioritizes adaptability, coherence, and decision relevance.[xxviii]

One of the most influential methodological frameworks in intelligence analysis is Bayesian reasoning. Bayesian logic provides a formal structure for updating beliefs as new information becomes available, offering a principled way to incorporate uncertainty and revise judgments incrementally. In theory, Bayesian inference aligns closely with intelligence needs, particularly in estimative analysis and forecasting. In practice, however, intelligence analysis rarely meets the conditions required for rigorous Bayesian application. Analysts often lack reliable base rates, face ambiguous or contradictory evidence, and must contend with reporting of uneven quality. As a result, Bayesian reasoning in intelligence functions more as an organizing heuristic than as a mathematically precise tool. Analysts update confidence qualitatively rather than computationally, relying on professional judgment to approximate probabilistic reasoning.[xxix]

This limitation has led to persistent reliance on heuristics. Cognitive science demonstrates that heuristics are not merely sources of bias but adaptive tools that allow humans to function under conditions of limited information and time pressure.[xxx] Intelligence analysis reflects this reality. Pattern recognition, analogical reasoning, and rule-of-thumb judgments remain central to analytic practice, particularly in tactical and operational contexts. The methodological challenge is not eliminating heuristics but disciplining their use. SATs attempt to do precisely this by forcing analysts to externalize assumptions, compare competing hypotheses, and evaluate evidence systematically. These techniques represent a methodological compromise between formal reasoning and human cognition, designed to reduce error rather than guarantee correctness.[xxxi]

Abductive reasoning occupies a particularly important place in intelligence methodology. Unlike deduction, which derives conclusions from known premises, or induction, which generalizes from repeated

observations, abduction infers the most plausible explanation for observed phenomena. Intelligence analysts frequently rely on abduction when confronting incomplete or ambiguous data, such as unexplained military movements, anomalous financial transactions, or shifts in political rhetoric. Abduction allows analysts to generate hypotheses that can guide collection priorities and analytic focus. Its epistemic strength lies in creativity and responsiveness; its weakness lies in susceptibility to narrative coherence and premature closure. Consequently, abductive reasoning must be paired with systematic challenge and revision mechanisms to prevent analytic drift.

Quantitative methods increasingly supplement traditional qualitative analysis, particularly in areas such as signals intelligence, cyber threat analysis, and economic assessments. Statistical modeling, trend analysis, and forecasting tournaments have demonstrated value in improving probabilistic judgment and highlighting systematic biases. However, quantitative approaches face limitations in intelligence contexts where data are sparse, manipulated, or strategically generated. Moreover, quantitative outputs often obscure underlying assumptions, creating an illusion of precision that may mislead decision-makers. Intelligence methodology therefore requires careful integration of quantitative tools with qualitative judgment, ensuring that numerical outputs are interpreted within appropriate contextual and strategic frameworks.

Narrative reasoning represents another essential methodological component. Intelligence assessments frequently take the form of structured narratives that link actors, motivations, capabilities, and constraints over time. Such narratives help decision-makers understand not only what might happen, but why. From a philosophy of science perspective, this resembles historical explanation rather than law-based prediction.[xxxii] Narrative reasoning enables analysts to synthesize complex information into intelligible models, but it also introduces epistemic risks. Coherent stories can become resistant to disconfirmation, especially when they align with institutional expectations or prior assessments. Methodological rigor therefore requires continual interrogation of narratives, testing whether alternative explanations can account for the same evidence.

Methodological pluralism also reflects the diverse temporal horizons of intelligence analysis. Tactical intelligence emphasizes speed and responsiveness, often privileging heuristic and pattern-based reasoning. Strategic intelligence prioritizes long-term trends and structural drivers, lending itself to scenario analysis, comparative case studies, and model-based reasoning. Warning intelligence occupies an intermediate space, demanding sensitivity to weak signals and nonlinear dynamics. Each of these analytic functions requires different methodological emphases, underscoring the inadequacy of one-size-fits-all approaches.

Ultimately, intelligence methodology is best understood as a repertoire of reasoning models rather than a unified method. Analysts must select, combine, and adapt methods based on the problem at hand, the quality of available information, and the consequences of errors. This methodological flexibility distinguishes intelligence analysis from disciplines governed by stable methodological hierarchies. It also reinforces the need for philosophical clarity. Without explicit understanding of why certain methods are used and what their limitations are, intelligence organizations risk mistaking procedural compliance for analytic rigor. A philosophy of intelligence analysis must therefore treat methodology as a dynamic practice grounded in uncertainty management rather than methodological orthodoxy.

Case Studies as Epistemic Stress Tests

Case studies play a distinctive role in the philosophy of intelligence analysis because they operate as epistemic stress tests rather than as simple historical narratives. In intelligence, failures and surprises

expose not only incorrect conclusions but also the underlying assumptions, reasoning models, and institutional dynamics that shaped those conclusions. Much as anomalies in scientific inquiry reveal the limits of prevailing theories, intelligence case studies illuminate where analytic frameworks, organizational epistemologies, and methodological practices break down under real-world pressure. When treated philosophically, case studies allow analysts to examine how intelligence knowledge is produced, stabilized, challenged, and revised.

The U.S. intelligence assessment of Iraqi weapons of mass destruction between 2001 and 2003 represents a paradigmatic epistemic failure rooted in interpretive closure rather than in the absence of information. Analysts worked within a dominant analytic framework that assumed Iraqi intent to reconstitute WMD programs, an assumption shaped by prior behavior, regime incentives, and post–Gulf War experience. Ambiguous indicators were interpreted through this lens, while disconfirming evidence was discounted or reinterpreted as deception.[xxxiii] The epistemic failure was not simply confirmation bias at the individual level, but the institutional entrenchment of a core analytic commitment. From a philosophy of science perspective, this resembles a Lakatosian research programme in which a protected "hard core" assumption is preserved while auxiliary hypotheses absorb anomalies. Once this framework achieved bureaucratic consensus, analytic challenge became procedurally difficult, even when uncertainty was acknowledged in footnotes and confidence language.

The September 11 attacks present a contrasting epistemic failure centered on aggregation rather than interpretation. In this case, intelligence agencies possessed numerous fragments of relevant information, including warnings about al-Qaeda's intent, suspicious travel patterns, and indicators of operational preparation. The epistemic failure lay in the inability to synthesize these fragments into a compelling warning narrative that overcame organizational compartmentalization.[xxxiv] Analysts did not lack imagination so much as institutional mechanisms that allowed abductive reasoning to connect disparate signals across agencies and disciplines. This failure parallels problems identified in distributed cognition and systems theory, where complex organizations fail to generate system-level knowledge despite adequate local inputs. The 9/11 case demonstrates that epistemic failure can occur even when individual analytic judgments are reasonable in isolation.

The Arab Spring constitutes a different category of epistemic stress test, one that reveals the limits of prediction in complex social systems. Prior to 2011, intelligence assessments accurately identified many structural conditions associated with instability, including economic stagnation, demographic pressure, and regime fragility. What analysts failed to anticipate was not the existence of unrest but its timing, velocity, and regional diffusion.[xxxv] This failure highlights a critical epistemic distinction between identifying permissive conditions and predicting catalytic events. From the perspective of philosophy of science, this aligns with critiques of deterministic forecasting in nonlinear systems, where small perturbations can trigger disproportionate outcomes. The Arab Spring case illustrates that intelligence analysis can succeed descriptively while failing predictively, a distinction often obscured in post hoc evaluations.

Western intelligence assessments preceding Russia's 2022 invasion of Ukraine provide a revealing counterexample that complicates standard narratives of intelligence failure. In this case, intelligence agencies accurately assessed Russian intent and warned of imminent military action. The epistemic challenge arose not within analysis but in the reception of intelligence by policymakers, allies, and publics conditioned by earlier false alarms and skepticism toward worst-case assessments.[xxxvi] Intelligence knowledge, although well-grounded, struggled to achieve credibility outside the analytic community. This case highlights an often-neglected epistemic dimension of intelligence in which knowledge is socially

situated, and its influence depends on institutional trust, historical memory, and political context. Even correct assessments may fail to shape outcomes if epistemic authority has been eroded.

Across these cases, several recurring epistemic vulnerabilities become visible. First, dominant analytic frameworks can stabilize prematurely, transforming probabilistic judgments into quasi-certainties. Second, organizational fragmentation can prevent meaningful synthesis, especially when warning requires abductive inference across disparate data streams. Third, complex adaptive systems limit the predictive reach of intelligence, even when structural analysis is sound. Fourth, analytic accuracy alone is insufficient if intelligence institutions lack the credibility or communicative capacity to persuade decision-makers. These vulnerabilities do not represent isolated pathologies but structural features of intelligence as a knowledge-producing activity.

Importantly, these case studies also reveal the limits of reform strategies that focus narrowly on cognitive bias or collection gaps. While such factors matter, they do not fully explain why epistemic failures occur across different agencies, eras, and problem sets. A philosophical approach suggests that intelligence failures are often the result of misaligned epistemic expectations, such as treating intelligence judgments as predictive truths rather than as conditional assessments designed to inform decision-making under uncertainty. When intelligence is evaluated against inappropriate epistemic standards, failure becomes inevitable.

Treating case studies as epistemic stress tests therefore reframe their analytical value. Rather than serving as cautionary tales or instruments of blame, they become empirical probes into the conditions under which intelligence knowledge is most fragile. This approach allows intelligence professionals and scholars to move beyond reactive reform toward a more systematic understanding of how analytic systems can be designed to tolerate uncertainty, manage disagreement, and adapt to adversarial complexity.

Toward a Coherent Philosophy of Intelligence Analysis

The preceding sections suggest that intelligence analysis cannot be adequately understood as a derivative of scientific inquiry, policy analysis, or journalism. Nor can its recurring failures be explained solely through cognitive bias, collection gaps, or politicization. What emerges instead is the need for a coherent philosophical framework that treats intelligence analysis as a distinct epistemic practice, governed by its own standards of justification, reasoning, and institutional constraint. A philosophy of intelligence analysis must explain how analysts generate warranted beliefs under adversarial conditions, how institutions stabilize or distort those beliefs, and how judgments are translated into decision-relevant knowledge without collapsing into either false certainty or analytic nihilism.

At the core of such a framework is the recognition that intelligence operates under adversarial epistemic conditions. Unlike scientific inquiry, where nature does not intentionally deceive the observer, intelligence targets actively seek to manipulate what analysts can know. Deception, denial, and strategic ambiguity are features of the system. Any philosophy of intelligence analysis will need to reject epistemological models that assume passive subjects and transparent evidence. Instead, intelligence knowledge must be understood as contingent, contested, and strategically shaped. This places intelligence closer to disciplines concerned with conflict, strategy, and political judgment than to the natural sciences, even as it borrows methodological tools from both.

Building on this foundation, intelligence analysis can be conceptualized through what may be termed *pragmatic adversarial epistemology*. This framework rests on several interlocking propositions. First,

intelligence judgments are inherently provisional. They are claims about evolving intentions, capabilities, and contexts rather than statements of settled fact. Second, uncertainty is not a flaw to be eliminated but a condition to be managed. Intelligence analysis succeeds not by eradicating uncertainty, but by bounding it, clarifying its sources, and communicating its implications for decision-making. Third, the value of intelligence lies primarily in decision advantage, not in predictive accuracy alone. Assessments that shape posture, preparedness, or risk mitigation may be epistemically successful even when specific predicted outcomes do not occur.

This framework also clarifies the role of methodology within intelligence analysis. Bayesian reasoning, abductive inference, structured analytic techniques, and narrative synthesis are not competing paradigms, but complementary tools suited to different epistemic tasks. A coherent philosophy of intelligence analysis does not privilege one method as universally superior. Instead, it evaluates methods based on their capacity to surface assumptions, manage bias, and adapt to changing evidentiary conditions. Methodological rigor, in this sense, is defined by transparency and revisability rather than formal precision.

Institutional considerations are equally central. Intelligence knowledge is produced collectively within bureaucratic systems that shape what questions are asked, what evidence is accessible, and what conclusions are institutionally acceptable. A coherent philosophy of intelligence analysis must therefore treat organizations as epistemic actors in their own right. Institutional incentives, review processes, and cultural norms influence analytic confidence and dissent as much as individual reasoning does. The persistence of flawed assessments across time and agencies, as demonstrated in multiple case studies, reflects not individual failure but systemic epistemic inertia. Recognizing this shifts reform efforts away from blaming analysts and toward redesigning institutional processes that govern analytic judgment.

The case studies examined earlier function as empirical validation of this philosophical approach. The Iraq WMD failure illustrates how adversarial uncertainty and institutional consensus can harden provisional judgments into dogma. The 9/11 failure demonstrates the epistemic fragility of fragmented organizational cognition. The Arab Spring highlights the limits of prediction in complex systems, reinforcing the need for epistemic humility. The Ukraine invasion case shows that even accurate intelligence may fail to influence outcomes when epistemic authority is contested. Together, these cases affirm that intelligence analysis must be evaluated not against unrealistic standards of certainty, but against its ability to inform decisions under uncertainty.

A coherent philosophy of intelligence analysis therefore rejects both scientism and cynicism. It does not pretend that intelligence can achieve the predictive precision of the natural sciences, nor does it concede that intelligence judgments are merely subjective or political. Instead, it situates intelligence analysis as a disciplined practice of probabilistic reasoning, institutional coordination, and strategic interpretation. Its normative commitment is not to truth in the abstract, but to responsible judgment in contexts where error carries asymmetric and sometimes catastrophic consequences.

Such a framework has practical implications for training, professionalization, and reform. Analysts must be educated not only in tradecraft but in the epistemic logic that underpins it. Institutions must design processes that reward analytic transparency, tolerate uncertainty, and preserve dissent without paralyzing decision-making. Above all, intelligence organizations must align their epistemic standards with the realities of adversarial complexity rather than with retrospective ideals of certainty. A philosophy of intelligence analysis does not eliminate failure, but it offers a systematic way to understand why failure occurs and how its consequences can be mitigated.

Conclusion

This essay argued that intelligence analysis constitutes a distinct form of knowledge production that warrants its own philosophical framework, comparable in ambition to the philosophy of science but grounded in fundamentally different epistemic conditions. Intelligence does not operate in a domain of stable phenomena, transparent evidence, or repeatable experimentation. It functions in environments shaped by strategic deception, institutional constraint, and irreversible decision-making under uncertainty. Treating intelligence analysis as either an applied science or an intuitive craft obscures these realities and contributes to recurring analytic and organizational failures.

By examining intelligence as a knowledge-producing activity, this essay has shown that intelligence judgments are inherently provisional, probabilistic, and purpose-driven. Their value lies not in predictive certainty but in their capacity to reduce uncertainty, frame risk, and inform decisions under conditions where error is unavoidable and often asymmetric. The epistemology of intelligence is therefore best understood as adversarial and pragmatic, shaped by denial and deception, incomplete information, and reflexive human behavior. Methodologically, intelligence analysis relies on a pluralistic repertoire of reasoning models, including Bayesian-inspired updating, abductive inference, structured analytic techniques, and narrative synthesis. No single method is sufficient in isolation; analytic rigor emerges from disciplined combination rather than methodological orthodoxy.

The institutional and organizational dimensions of intelligence analysis further complicate its epistemic character. Intelligence knowledge is produced collectively within bureaucratic systems that shape what is seen, what is prioritized, and what is judged credible. Organizational incentives, review processes, and classification regimes influence analytic confidence and dissent in ways that individual-focused explanations cannot fully capture. The case studies examined in this essay demonstrate that intelligence failures are rarely the result of singular errors or inadequate collection. Instead, they arise from systemic epistemic vulnerabilities, including premature consensus, fragmented cognition, misplaced expectations of prediction, and contested epistemic authority.

In response to these conditions, this essay has proposed *pragmatic adversarial epistemology* as a coherent philosophical framework for intelligence analysis. This approach situates intelligence analysis as a disciplined practice of judgment oriented toward minimizing catastrophic error and maximizing decision advantage under adversarial uncertainty. This philosophical orientation carries important methodological implications. Analytic rigor should be assessed less by adherence to specific techniques than by the transparency and revisability of analytic judgment. Methods are valuable insofar as they surface assumptions, clarify uncertainty, and facilitate structured challenge, not because they conform to a prescribed analytic canon. Quantitative precision should not be treated as a substitute for epistemic confidence; numerical estimates and models must be explicitly contextualized, with their assumptions and limitations made clear to decision-makers. Analytic training should place greater emphasis on abductive reasoning, hypothesis generation, and uncertainty management alongside bias mitigation and probabilistic thinking. Finally, institutional processes should be designed to preserve epistemic pluralism, ensuring that alternative explanations and dissenting judgments remain visible even as consensus forms.

The contribution of this essay lies in making explicit the philosophical assumptions that already, often implicitly, govern intelligence practice. By integrating insights from philosophy of science, cognitive psychology, organizational theory, and intelligence studies, it offers a systematic account of how intelligence knowledge is generated, justified, challenged, and revised. This perspective reframes intelligence reform efforts away from reactive fixes and toward deeper epistemic alignment between

analytic expectations and operational realities. For the field of intelligence studies, this approach provides a foundation for more rigorous theory-building and professionalization. For practitioners, it offers a conceptual vocabulary for understanding why analytic rigor cannot be reduced to procedural compliance or data accumulation. For institutions, it highlights the need to design epistemic environments that tolerate uncertainty, preserve dissent, and align analytic standards with the realities of adversarial competition. A philosophy of intelligence analysis does not eliminate failure, but it clarifies its causes and constrains its consequences.

Author: Dr. Treston Wheat is the Chief Geopolitical Officer at Insight Forward and adjunct professor at Georgetown University. Dr. Wheat is a researcher on private sector intelligence and the intersection of geopolitics and corporate security. In addition, he is the editor-in-chief of *The Close Protection and Security Journal.*

Endnotes

[i] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949); Stephen Marrin, "Is Intelligence Analysis an Art or a Science?," *International Journal of Intelligence and CounterIntelligence* 25, no. 3 (2012): 529–45, https://doi.org/10.1080/08850607.2012.678690.

[ii] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010).

[iii] Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2014), 1–18.

[iv] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1962); Imre Lakatos, "Falsification and the Methodology of Scientific Research Programmes," in *Criticism and the Growth of Knowledge*, ed. Imre Lakatos and Alan Musgrave (Cambridge: Cambridge University Press, 1970).

[v] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (1978): 61–89.

[vi] Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Crown, 2015); Deborah G. Mayo, *Error and the Growth of Experimental Knowledge* (Chicago: University of Chicago Press, 1996).

[vii] Kent, *Strategic Intelligence for American world Policy*

[viii] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Washington, DC: Potomac Books, 2002), 15–38.

[ix] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. (Washington, DC: CQ Press, 2023), 87–110.

[x] Stephen Marrin, "Evaluating the Quality of Intelligence Analysis: By What (Mis)Measure?" *Intelligence and National Security* 27, no. 6 (2012): 896–912.

[xi] Richard K. Betts, "Intelligence Warning: Old Problems, New Agendas," *Parameters* 28, no. 1 (1998): 26–35.

[xii] Amy B. Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999), 7–34.

[xiii] Jervis, *why Intelligence Fails*, 13-28.

[xiv] Shulsky and Schmitt, *Silent Warfare*, 39-62.

[xv] Betts, "Analysis, War, and Decision."

[xvi] Lakatos, "Falsification and the Methodology of Scientific Research Programmes."

[xvii] Kent, *Strategic Intelligence for American World Policy*, 54-83.
[xviii] Heur and Pherson, *Structure Analytic Techniques for Intelligence Analysis*, 31-58.
[xix] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011); Gerd Gigerenzer, *Adaptive Thinking: Rationality in the Real World* (New York: Oxford University Press, 2002).
[xx] Charles S. Peirce, "Abduction and Induction," in *Philosophical Writings of Peirce*, ed. Justus Buchler (New York: Dover, 1955), 150–156.
[xxi] Kuhn, *The Structure of Scientific Revolutions*; Barry Barnes, *Scientific Knowledge and Sociological Theory* (London: Routledge, 1974).
[xxii] Stephen Marrin, "Intelligence Analysis and Decisionmaking: Methodological Challenges," in *Intelligence Theory: Key Questions and Debates*, ed. Peter Gill, Stephen Marrin, and Mark Phythian (Abingdon, UK: Routledge, 2008), 131–50.
[xxiii] Zegart, *Flawed by Design*, 35-67.
[xxiv] Kent, *Strategic Intelligence for American World Policy*, 178-201.
[xxv] Richard K. Betts, "Politicization of Intelligence: Costs and Benefits," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, ed. Richard K. Betts and Thomas Mahnken (London: Frank Cass, 2003).
[xxvi] Lakatos, "Falsification and the Methodology of Scientific Research Programmes."
[xxvii] Richard K. Betts, "Surprise Despite Warning: Why Sudden Attacks Succeed," *Political Science Quarterly* 95, no. 4 (Winter 1980–81).
[xxviii] Marrin, "Evaluating the Quality of Intelligence Analysis,"
[xxix] Morgan, M. Granger, and Max Henrion, *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis* (Cambridge: Cambridge University Press, 1990), 43–78.
[xxx] Gigerenzer, *Adaptive Thinking*, 19-41.
[xxxi] Heuer and Pherson, *Structured Analytic Techniques for Intelligence Analysis*.
[xxxii] R. G. Collingwood, *The Idea of History* (Oxford: Oxford University Press, 1946), 214–236.
[xxxiii] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President* (Washington, DC: Government Printing Office, 2005), 74–109, https://georgewbush-whitehouse.archives.gov/wmd/report.html.
[xxxiv] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington, DC: U.S. Government Printing Office, 2004), https://www.9-11commission.gov/report/.
[xxxv] Marc Lynch, *The Arab Uprising: The Unfinished Revolutions of the New Middle East* (New York: PublicAffairs, 2012), 21–44.
[xxxvi] Massimo Calabresi, "Inside the White House Program to Share America's Secrets," *Time*, February 29, 2024, https://www.time.com/6835724/americas-intelligence-secrets/.

Strike, Riot, and Civil Commotion (SRCC): A Growing, Global Threat Targeting Hotels

Jeff M Moore, PhD

Note: This article is part of a chapter for an up-and-coming book the author is writing on hotel violence.

Introduction

Violent protests, crowd harassment, riots, and group violence is on the rise, globally. The insurance sector has a unique but fitting term for this kind of action, "SRCC" or Strike, Riot, Civil Commotion. Whether it is wedding brawls, gang-motivated beatdowns, or agitated protests where crowds in the tens, hundreds, or thousands perpetrate wanton violence and calamitous damages, SRCC is now a fixture of society that security managers, protection teams, and insurance companies must deal with. Nowhere is this more evident than in the hotel sector, which has experienced copious SRCC violence. Threat intelligence, or *risk intelligence* to the insurance sector—which it also calls "data and insights"—is key to understanding and then mitigating the problem.

When did SRCC take off, and why did this happen?

The following section dives into the recent history of SRCC, but first it is important to define the issue. Lloyd's of London defines SRCC (along with "malicious act"), which is distinct from peaceful protest, as follows:

> "*Strike means a lockout or total or partial work stoppage to enforce demands made on an employer or to protest against an act or condition. Riot means a violent disturbance by a group of persons assembled together for a common purpose which threatens the public peace. Civil Commotion means a substantial violent disturbance by a large number of persons assembled together and acting with common purpose or intent. Malicious Act means deliberate act(s) causing loss of or damage to property during and/or following Strike, Riot or Civil Commotion, including but not limited to vandalism, looting, theft of or the taking of goods by force.*"[i]

With that definition in mind, a discussion on the rise of SRCC over the previous few decades is salient. Insurer Swiss Re reports a more than 3,000% increase in SRCC globally from 2000–2020. Heightened SRCC has continued into 2025 and is expected to persist well into 2026. Property losses from major global SRCC events, excluding small and medium events, well exceed $10 billion.[ii] Casualty rates are difficult to calculate, but estimates range into the thousands killed and tens of thousands injured.

Why is this happening? Populations are more politically active, and technology—smartphones, the Internet, 24-hour news, and especially social media—has made them more aware, more easily agitated, and more quickly mobilized.[iii] Activists can now nimbly propagandize for a cause and generate supportive crowds with relative ease. Additionally, nefarious politicians who are not directly linked to SRCC street violence often use unrest as a tool to politically tar and feather their opponents. They passively justify the violence, giving perpetrators implicit support while deceptively blaming a sitting government's "chaos-causing policies." This tactic encourages SRCC actors to escalate, benefiting those politicians.

Essentially, it is now easier to get masses of people angry about issues, then organized, and then deployed onto the streets. Once engaged in riotous behavior, highly incensed individuals often cease taking responsibility for their own actions, and frenzied group violence can take over. In many cases, nefarious activists apply psychological operations to manipulate people into violence. In other instances, militants infiltrate peaceful protests and turn crowds violent for their own ends. In still other cases, it is simply criminal, anti-social behavior, such as a street-gang beating. Regardless, it is a "social violence" phenomenon, and it is not subsiding.

As for the ideological drivers of SRCC, the list is endless. There are far-left and far-right motivations, though historically, the far left has been more prone to mass protest.[iv] There is anger at government corruption or incompetence, religious tensions, ethnic and tribal disputes, immigration stressors, economic grievances, and many other catalysts.

SRCC Insurance Issues

Insurance is a vital part of mitigating the impact of SRCC. Insurers under Lloyd's of London (aka, the London Market) began systematically removing SRCC from standard property policies and shifting it toward standalone coverage around 2019–2020, with significant acceleration in 2020. In other words, SRCC had previously been offered by insurers as a rider to general liability (GL) policies. But with the global onslaught of SRCC, the London Market repositioned it as its own dedicated line of insurance, separate from GL—much like terrorism and war insurance, which similarly address violence-related perils.

This shift was primarily triggered by major loss events: The 2019 riots in Chile, Bolivia, and Colombia, which caused more than $7 billion in damages, killed hundreds, injured thousands, and resulted in insurers excluding SRCC from all-risk policies at renewal after experiencing significant losses. The trend intensified dramatically during the summer of 2020 following the George Floyd protests and Black Lives Matter (BLM) demonstrations, when SRCC coverage was increasingly pulled from property policies and standalone SRCC coverage became necessary.[v]

Hotel SRCC Data: Geography, TTPs, and Cases

General SRCC violence, including hotel SRCC, occurs in nearly every region of the world. Data from 2022 in Muir Analytics' *SecureHotel Threat Portal*, the world's largest, most sophisticated hotel violence database, shows that 27 countries experienced 75 hotel SRCC incidents. They were:

1. Australia	15. Peru
2. Botswana	16. Serbia
3. Canada	17. South Africa
4. Cyprus	18. South Korea
5. Ethiopia	19. Spain
6. France	20. Sri Lanka
7. Haiti	21. Thailand
8. India	22. UAE
9. Israel	23. UK, England
10. Jamaica	24. UK, Northern Ireland
11. Mexico	25. UK, Scotland
12. New Zealand	26. UK, Wales
13. Nigeria	27. USA
14. Pakistan	

Common tactics, techniques, and procedures (TTPs) applied during these actions included:

1. Arson
2. Violent and/or harassing protest-riots
3. Chemical attacks
4. Physical-personal attacks
5. Raids
6. Vandalism
7. Vehicular assaults
8. Shootings/attacks with firearms w/no discharge
9. Sexual assaults

Crowd sizes in these incidents ranged from a handful of individuals to more than 10,000. Some events involved harassment that disrupted hotel operations or conferences. For instance, in April 2022, two radical environmentalists glued and chained themselves to the doors of the five-star JW Marriott Parq Vancouver, disrupting the Canadian Council of Forest Industries conference.[vi] Violent? No. Harassing and security-resource-draining? Absolutely. The hotel manager, hotel security, police, and emergency services all had to expend resources to resolve the situation. The event was disrupted, undermining the conference's messaging. Additionally, covert event infiltration by political antagonists can remain just a nuisance, or they can turn violent in a millisecond.

In another case, in December 2012 in Mexico City, protesters on the losing side of the national election gathered in the thousands, many of them violent anarchists and Black Bloc agitators, and rioted, attacking scores of businesses with sticks and clubs, hand-thrown missiles, and arson. They targeted banks, coffee shops, retail stores, and at least two hotels: The Hilton Mexico City Reforma and a Fiesta Inn, both of which sustained façade and window damage. Fox News Latino described the scene, "Broken glass littered Avenida Juárez where protesters destroyed the façade of the Hilton and Fiesta Inn hotels. The plush purple chairs of a corner Starbucks sat in the open air, covered in shards of glass."[vii] These two examples represent common SRCC hotel scenarios, but there are also cases in which riotous actions include assaults on hotel staff, severe damage, and mass arson, events that can lead to total-loss outcomes, as the following cases demonstrate.

George Floyd/BLM riots, 2020, Charleston, SC—Hotel Bennett

The George Floyd/BLM riots caused an estimated $2 billion in property damage in the U.S., killed roughly 20 people, and wounded 2,000 law enforcement officers.[viii] A decisive count of wounded civilians remains elusive, save for a handful of medical reports documenting injuries from police riot-control weaponry.

Muir Analytics registered more than 15 hotels that suffered damage from these riots, including, but not limited to:

1. The Hay-Adams, Washington, DC
2. The Sofitel, Washington, DC
3. The Omni Atlanta, GA
4. Sheraton Grand Sacramento Hotel, CA
5. The Langham, Chicago, IL

Most damage fell into the light-to-medium category. For example, the Omni Atlanta suffered smashed-out lobby windows ($10,000–$30,000 estimated) and an overturned grand piano ($60,000–$120,000

estimated). However, rioters also attempted to set the Hay-Adams on fire, a dangerous arson attack that luckily was extinguished before tragedy occurred.

One of the most concerning situations occurred at the five-star Hotel Bennett in Charleston, SC, which appeared to be on the verge of turning ultra-violent but ultimately avoided catastrophic outcomes. On 30 May 2020, George Floyd/BLM protesters gathered peacefully in Charleston, but by late afternoon the demonstrations became violent, and a group attacked the Hotel Bennett. Desperate 911 calls from hotel staff, as recounted by *The Post and Courier*, captured the escalating danger:

- "They've got bricks. They've got weapons. I need help! I need help!"
- "We just had a bunch of people enter through our garage…they just assaulted our general manager; they hit him in the face!"
- "We have people who entered the building, and we don't know where they are."[ix]

The Post and Courier reported that guests and staff sought "relative safety" in a makeshift safe room in the sixth-floor Presidential Suite and Terrace, but were still "huddled together in unspeakable dread." [x] Rioters threw rocks into the lobby, smashed windows and doors, attempted—but failed—to breach the hotel en masse, and spray-painted graffiti on the exterior walls. Tear gas from the intense street fighting outside, which included assaults and vehicle arson, drifted into the hotel. Interestingly, the nearby Courtyard by Marriott and Francis Marion Hotel were neither attacked nor damaged. Although both are reputable hotels, they do not share the "southern, monied elite" aesthetic of the Bennett, suggesting the rioters specifically targeted the latter.

Ethiopia, Oromo Riots,[xi] June-July 2020

In June–July 2020, following the assassination of prominent Oromo singer and activist Hachalu Hundessa and allegations of long-running anti-Oromo government policies, large-scale SRCC violence erupted across Ethiopia's Oromia region. Oromo mobs attacked non-Oromo businesses and residents, leaving at least 239 people dead, more than 200 injured, and over 3,500 arrested, according to police figures. In the towns of Shashemene and Ziway, rioters burned or severely damaged at least a dozen hotels, including properties in famed Ethiopian Olympian Haile Gebrselassie's Haile Resorts portfolio. The Haile Shashemene Hotel, a three-star property, was sacked and torched in a total-loss event. Haile told the press, "Our three-star hotel in Shashemene has been totally burned down. We had worked hard to get it finished."[xii] The property reopened in August 2025.

The Haile Resort Ziway, also a three-star property, was partially burned, and the remainder of the hotel was trashed by marauding crowds. Haile explained, "Our resort in Ziway is also badly damaged. Only the structure is left. Its windows are smashed. The resort's spa, gym, store, laundry, and kitchen are entirely damaged."[xiii] The hotel reopened in December 2020. Combined, the destruction of these two properties put roughly 400 employees out of work and caused an estimated $8–$11 million USD in damage at 2020 conversion rates. (In 2025 currency, this would equate to approximately $10-13 million).[xiv]

Bangladesh, July Revolution, June–August 2024

Bangladesh's 2024 unrest began in June when nationwide student protests erupted over a controversial quota system that reserved 30% of government jobs for descendants of veterans of the 1971 War of Independence.[xv] Anger over this policy quickly merged with broader political grievances, drawing in citizens frustrated with the ruling Awami League (AL). As demonstrations spread, the government deployed military and police units, mobilized AL activists as counter-demonstrators, shut down the Internet, closed universities, and imposed curfews in an attempt to contain the movement.[xvi] Despite

these measures, violence escalated sharply. By early August, widespread clashes, arson, and property destruction had left hundreds dead, and Prime Minister Sheikh Hasina resigned and fled the country.[xvii] Celebrations over her departure soon devolved into mass looting and vandalism targeting government buildings, AL-linked businesses, and even minority Hindu and Buddhist homes.

Amid this chaos, a large mob attacked the five-star Zabeer Jessore (Zabeer International Hotel) on August 5, 2024 in Jessore, a property known for hosting business travelers and VIPs.[xviii] Protesters singled out the hotel because it was owned by AL leader Shahin Chakladar. At 3:45 p.m., rioters surged inside, looting and vandalizing the property.[xix] By 4:15 PM, they had set the ground floor ablaze, and flames quickly engulfed the 14-story structure. Photographs show the hotel fully on fire by late afternoon.[xx] Fire crews initially struggled to reach the site due to the mob blocking access, and once they arrived, they battled the blaze for several hours.[xxi] A Bangladeshi Air Force helicopter managed to extract one—or a small number—of trapped guests from the roof (reporting differs) as the fire intensified.[xxii] At least 25 people were killed and more than 150 injured, many suffering severe burns and smoke inhalation.[xxiii] Survivors described the scene as a nightmare as fire consumed the building, while emergency personnel reported being overwhelmed by the intensity of the flames.[xxiv] Military and police forces eventually restored order and arrested several rioters, but the hotel was left catastrophically damaged—"cooked," as one news outlet described it.[xxv]

Nepal, Gen Z Riots, September 2025

Nepal's Gen Z Riots of September 2025 erupted from deep frustration with government corruption, widening wealth inequality, and anger toward perceived elite privilege; grievances intensified by youth unemployment and long-standing political stagnation.[xxvi] Seemingly leaderless (investigations might eventually reveal otherwise), the movement began as mass anti-government demonstrations but rapidly escalated into violent attacks on parliament, ministries, transportation hubs, and private businesses across Kathmandu, Pokhara, and other cities.[xxvii] As the unrest spread, protesters and infiltrators—whom movement leaders later blamed for the most destructive acts—torched government buildings, stormed prisons and freed thousands of inmates, and clashed with police in running street battles.[xxviii] By the time security forces restored control, 72 people had been killed, hundreds injured, and major tourist districts had sustained catastrophic damages.[xxix] Insurance claims surged, while tourism, a critical pillar of Nepal's economy, collapsed almost overnight.[xxx]

Among the most severely affected properties were Kathmandu's luxury hotels, which became symbolic targets of anti-elite anger. ABC News reported that more than 20 hotels were looted, burned, or destroyed, with overall sector losses exceeding NPR 25 billion (USD $175–187 million).[xxxi] Total losses for all Gen Z Riot destruction are estimated at $25 billion USD. The Hyatt Regency Kathmandu suffered one of the worst attacks. Rioters set parts of the property ablaze, causing structural fire damage and killing a visiting Indian woman trapped during the chaos.[xxxii] The Hilton Kathmandu was overrun by crowds who vandalized and burned portions of the lobby and guest areas, forcing the hotel to close indefinitely. Photos of the Hilton show a burned-out hulk, and current reporting says the property appears to be a total loss.[xxxiii] The Barnabas Museum Hotel, a high-end cultural boutique property, was set on fire by rioters, resulting in major physical losses and forcing its credit rating into emergency surveillance due to the scale of destruction.[xxxiv] Industry associations later estimated that dozens of luxury and mid-tier hotels across the capital and tourist regions faced long-term closures, massive rebuilding costs, and uncertain recovery timelines—marking one of the most severe, intentional and malicious-driven hotel-sector loss events in modern history.[xxxv]

Threat/risk analysis takeaways

Across multiple regions, SRCC violence continues to impose substantial and sometimes catastrophic impacts on hotels. While each of the reviewed cases differs in cause, political context, and intensity, several broad observations emerge.

United States—opportunistic hotel impacts during unrest

The more than 15 hotels struck by SRCC violence during the 2020 BLM-related unrest fortunately did not experience the extreme destruction seen in Ethiopia, Bangladesh, or Nepal. Reported hotel damages ranged from shattered glass to vandalism and limited arson attempts. Several luxury hotels were impacted simply because crowds were moving through major downtown corridors. Targeting appeared largely opportunistic, and although nationwide property losses were exceptionally high, the unrest did not escalate into systematic hotel destruction or large-scale lethal violence. Compared with other countries' SRCC events, the US unrest exhibited more restraint in both intent and tactical execution, though the underlying reasons for this are multi-factor and beyond the scope of this article.

Ethiopia—identity-driven violence and heavier structural damage

In Ethiopia, the Oromo-related unrest produced more deliberate attacks on businesses perceived as belonging to opposing groups. At least one hotel was burned so severely that reconstruction required roughly five years. Another hotel, heavily vandalized by crowds, reopened only after several months. It is nothing short of a miracle that no one at these two resorts was killed. These losses demonstrate how SRCC can escalate from spontaneous damage to prolonged economic impairment of hospitality infrastructure.

Bangladesh—extreme violence and mass casualties

Bangladesh's 2024 "July Revolution" unrest marked a sharp increase in severity and deadly intent. A major five-star hotel was attacked in conjunction with political violence, looted, and set on fire. The casualty toll, approximately 25 people killed and about 150 injured, is shocking. This was murder on a mass scale. This event underscores the grim reality that SRCC can rapidly cross into mass-casualty territory, particularly when political anger, crowd momentum, and symbolic targets converge.

Nepal—widespread, systematic targeting of hotels

Nepal's Gen Z riots of September 2025 demonstrated that hotels can become primary targets during large-scale political unrest. More than 20 hotels in Kathmandu and Pokhara were systematically attacked, vandalized, looted, or burned. None of this was opportunistic. Several iconic properties, including a Hilton that appears to be a total-loss event, sustained severe destruction. Nationwide, 72 people were killed, hundreds injured, and overall economic losses reached staggering levels. This case illustrates the upper end of modern SRCC's destructive potential for hospitality sectors.

Security Takeaways

VIP/executive protection teams

VIP and corporate protection teams must acknowledge that SRCC poses unique challenges in hotel environments:

- Situational awareness is critical — teams must monitor unrest indicators before arrival and continuously during operations.
- Understanding casualty and destruction trends helps teams gauge the realism of worst-case scenarios, including building fires, mob surges, blockades, and trapped-occupant situations.
- "Get off the X" principles still apply; routes out of the hotel and city must be pre-identified and adaptable.

- Safe rooms may or may not be relevant depending on building integrity, fire risk, and crowd penetration patterns. Mobility often outweighs static sheltering options during SRCC.
- Protection teams benefit from reviewing real case studies of hotel violence so they understand the operational pressures and environmental failures that have occurred elsewhere.

Hotel operators

Hotels in SRCC-prone environments should consider:

- Basic lockdown procedures for front-of-house and guest areas.
- Anti-arson measures, including rapid removal of flammable lobby materials during unrest periods.
- Staff training on when to shelter guests vs. when to evacuate areas.
- Coordination with local authorities ahead of known protest cycles.

Insurance implications

SRCC's impact on hotels has repeatedly produced:

- Complete building loss events.
- Multi-year closures.
- High cleanup and demolition costs.
- Costly temporary boarding and reconstruction.
- Brand damage requiring expensive re-positioning campaigns.

Premiums and coverage structures in many regions may need reassessment as SRCC incidents worldwide continue to generate claims well beyond traditional vandalism thresholds.

Conclusion

SRCC is now a structural fact of life in global politics, not an anomaly. It is relatively easy for opportunistic activists and cynical political actors to mobilize anger, push people into the streets, and tip protests into violence that produces serious property damage, injuries, and deaths. The boundary between SRCC and terrorism is often gray, but when destruction and casualty levels climb, the convergence becomes obvious. SRCC can also be weaponized, used deliberately by nefarious movements against governments, rival communities, and "elite" targets such as luxury hotels.

Compounding the risk, SRCC can ignite with little or no warning, and once unrest breaks out, the momentum and "frenzy factor" can attract a wide array of hostile actors who escalate violence beyond what organizers originally imagined. It is exceedingly difficult to predict in advance whether a given crowd, whether spontaneous, infiltrated, or purpose-built, will limit itself to broken windows or drive toward total-loss fires and mass-casualty outcomes. For VIP protection teams, hotels, and insurers, this means planning must be anchored on worst-case scenarios, whether those scenarios emerge organically or are baked into the event from the outset.

The first step in managing this threat is disciplined intelligence analysis of SRCC statistical trends, AI analyses with a human in the loop, and case studies, understanding who was targeted, how the violence unfolded tactically, and why casualty and damage levels escalated in some cases but not in others. Without this kind of protective intelligence, security measures and insurance structures are little more than educated guesses, which is unacceptable when lives and hundreds of millions (or billions) in physical assets are at stake. As global political and cultural tensions intensify, there is no indication that SRCC will diminish. Hotels, VIP protection providers, and insurance companies must therefore treat SRCC as a recurring

strategic hazard, invest in real threat intelligence, and harden their operations now—before the next wave of unrest arrives at the lobby doors.

Author: Dr. Jeff Moore is the CEO of Muir Analytics, which conducts threat assessments for corporations. Dr. Moore created the company's flagship product, the SecureHotel Threat Portal, which is the largest hotel violence database. Dr. Moore earned his PhD in counterinsurgency/counterterrorism from the University of Exeter in the UK, and he is the author of *Spies for Nimitz* and *The Thai Way of Counterinsurgency*.

Endnotes

[i] Lloyd's Market Association, "Recently Issued Wordings: LMA5553 – Strike, Riot, Civil Commotion & Malicious Acts," Lloyd's of London, August 5, 2021.
[ii] Monti Pande, "Strikes, Riots and Civil Commotion: Exploring Solutions to Proactively Manage Heightening Risk," *Swiss Re Institute*, March 12, 2024.; and "Swiss Re: Frequency and Severity of Strikes, Riots and Civil Commotion Losses on the Rise," *Claims Journal*, June 6, 2024.
[iii] Ibid.
[iv] John A. Johnson, *"Do Liberals Protest More Than Conservatives? The Personality Traits of Liberals May Make Them More Likely to Protest Publicly," Psychology Today* (blog), June 23, 2025, accessed December 18, 2025, https://www.psychologytoday.com/nz/blog/cui-bono/202506/do-liberals-protest-more-than-conservatives.
[v] Lockton, "Insurers' Response to Riots in Chile Reflects a Broader Trend," October 26, 2021.
[vi] "Save Old Growth Logging Protest Shuts Down Vancouver Hotel Entrance," *Global News*, May 4, 2022.
[vii] "Random Detentions of Protesters as Mexico Swore in President Peña Nieto, Commission Says," *Fox News Latino*, December 7, 2012.
[viii] Major Cities Chiefs Association, Intelligence Commanders Group, *Report on 202 Protests & Civil Unrest*, October 2020.
[ix] Glenn Smith, "911 Calls: Charleston Restaurant Workers Hid in Coolers, Courtyards in Horror amid Riots," *The Post and Courier*, June 10, 2020.
[x] Ibid.
[xi] The Oromo are a major ethnic group indigenous to Ethiopia and neighboring regions of East Africa.
[xii] "Haile Gebreselassie's Properties in Oromia Region Sustained 290 Million Birr in Damage," *Mereja.com*, July 26, 2020; and "Athlete Haile Gebresilassie Demands Justice for Destroyed Hotels," *Ezega.com*, July 28, 2020.
[xiii] Ibid.
[xiv] "Ethnically Motivated Attacks in Shashemene and Elsewhere," *Ethiopia Observer*, July 6, 2020.
[xv] "Bangladesh Student Protests Swell into Mass Movement against Dictator," *The Guardian*, July 26, 2024.
[xvi] Ibid.
[xvii] "At Least 135 Killed in Monday Unrest in Bangladesh; Situation Remains Tense," *The Economic Times*, August 5, 2024.; and "What Sparked the Protests That Toppled Bangladesh's PM?," *BBC News*, August 6, 2024.
[xviii] "18 Die at Zabeer International Hotel in Jashore," *Daily Messenger*, August 7, 2024.
[xix] "Bangladesh Riots: 24 People Burnt Alive as Mob Set Fire to Hotel," *Pragativadi*, August 6, 2024.
[xx] Ibid.
[xxi] "Dozens Killed after Hotel Torched in Bangladesh," *United Press International*, August 6, 2024.
[xxii] "18 Die at Zabeer International Hotel in Jashore," *Daily Messenger*, August 7, 2024.

[xxiii] "Bangladesh Riots: 25 Burnt Alive as Mob Sets Hotel on Fire," *CNBCTV18*, August 6, 2024.
[xxiv] Ibid., and "Dozens killed," August 6, 2024.
[xxv] "Bangladesh Riots: 24 Burnt Alive as Mob Sets Hotel Owned by Awami League Leader on Fire," *Moneycontrol*, August 6, 2024.
[xxvi] "Nepal's Leaderless Gen Z Revolution Has Changed the Rules of Power," *Al Jazeera*, October 3, 2025.
[xxvii] "What We Know about Nepal Anti-Corruption Protests as PM Resigns," *BBC News*, September 9, 2025.
[xxviii] "What we know about," 9 September 2025, and "Nepal's protests estimated to have caused hundreds of millions of dollars in damage as families farewell those killed," ABC News Australia, September 16, 2025.
[xxix] "Nepal's protests estimated," 16 September 2025.
[xxx] "Nepal's leaderless Gen Z revolution has changed the rules of power," Al Jazeera, October 3, 2025.
[xxxi] "Hotel Association estimates Rs 25 billion loss to hotels in GenZ protest," *Bizness News,* September 12, 2025*,* and "'I Just Want To Go Home': Indian presenter who went to host volleyball event in Nepal, pleads for embassy's help after hotel set on fire amid unrest - VIDEO," *Free Press Journal*, September 10, 2025.
[xxxii] "'We jumped off 4th floor of hotel…my wife died…': Ghaziabad woman killed after Nepal protestors set fire to Hyatt in Kathmandu," *The Indian Express*, September 15, 2025.
[xxxiii] "Five-star Hilton Kathmandu hotel damaged amid Nepal anti-corruption protests," *Travel Market Report*, 10 September 2025, and "Protesters storm Hilton Hotel in Kathmandu," Khabarhub, September 9, 2025, and "Rajendra Bajgain reports arson at hotel during GenZ protest," Khabarhub, September 13, 2025, and "Protesters target Hilton Kathmandu over elite wealth ties," *Chosun Ilbo*, September 12, 2025.
[xxxiv] "Barnabas Museum Hotels' credit rating under surveillance after arson," *Insurance Khabar,* October 7, 2025*.*
[xxxv] "Hotel Association estimates," September 12, 2025.

Professional Articles

Warrior Leader:

Moral Courage, Self-Mastery, and Character in Executive Protection

Chuck Randolph

Abstract

Executive protection now operates across physical, digital, and reputational domains, creating a level of complexity that demands strong leadership. One of the profession's emerging challenges is cultural confusion about what strength and influence truly look like. Online personalities promote aggression, dominance, and performance, but these models contradict the authentic warrior traditions that shaped effective leadership in the past. Drawing from Stoic philosophy, samurai teachings, and classical thinkers such as Plutarch, this article argues that modern protectors are best served by an ethos rooted in moral courage, self-mastery, and service. These pillars provide a practical framework for making sound decisions, navigating uncertainty, and shaping healthy team culture. By rejecting performative models of masculinity and embracing an ethic grounded in humility, character, and responsibility, protectors elevate their leadership and reinforce the professionalism of the field. Real-world scenarios illustrate how this approach strengthens trust, stabilizes operations, and supports mission success.

Introduction: The Warrior Ethos Misunderstood

The landscape of executive protection has evolved. Today's protector must navigate a dangerous intersection of physical, digital, psychological, and reputational threats. Yet amid this growing complexity, another risk has emerged of a different kind. It does not stem from extremist ideology, geopolitical tension, or personal grievance. Rather, it originates from a cultural confusion surrounding strength, masculinity, and leadership. A wave of online personalities who promote dominance, volatility, and performative aggression has created a counterfeit image of the modern warrior. These voices are loud, packaged, and easy to digest. Their influence has crept into the protective profession, particularly among newer practitioners searching for identity and belonging.

This distortion stands in stark contrast to the authentic warrior traditions that shaped centuries of leadership. For the Greeks, Romans, samurai, and medieval knights, warrior identity was rooted in humility, restraint, and moral discipline. A warrior's strength came not from domination but from self-governance. The Stoics taught that mastery of one's mind was the highest form of power.[i] Samurai codes demanded loyalty, honor, and the subordination of ego. Classical leadership texts, including Plutarch's writings, insisted that leaders begin with inward moral cultivation before assuming any external authority.[ii]

The true warrior leader in the executive protection arena is defined by three interconnected attributes: *moral courage, self-mastery,* and *character-driven service*. These principles form an ethical framework for protectors operating within a high-consequence environment. They serve as a counterweight to the ego-driven narratives influencing today's culture and anchor the protector's identity in virtues that are

enduring, stable, and grounded in a long lineage of philosophical and professional tradition. Importantly, the protector's profession does not need more intensity. It needs more integrity. It does not need louder personalities. It requires quieter strength. It does not need posturing. It demands character. By reclaiming an authentic warrior ethos and merging it with the protector's mission, practitioners develop a more disciplined, effective, and principled leadership identity for the challenges ahead.

Warrior Codes Through History: Virtue Before Violence

The popular imagination often equates the warrior with violence or dominance, but throughout history, warrior cultures emphasized something entirely different. The true warrior was defined not primarily by strength but by virtue. Combat skill mattered, but moral formation mattered far more. For example, Greek hoplites embodied this philosophy. They fought not as individual champions but as citizens responsible for one another. Courage was not the absence of fear but the willingness to act for the community despite fear. Roman warriors embraced a similar mindset. Marcus Aurelius, remembered primarily as a Stoic philosopher but also a wartime emperor, wrote that the most difficult battles are internal and that the disciplined mind is the foundation of leadership.[iii] The samurai elevated this idea further. Bushido stressed that martial skill without virtue was dangerous. A samurai was expected to cultivate self-restraint, humility, and calmness under pressure. Recklessness and emotional impulsiveness were signs of immaturity. A warrior without discipline was unfit for service.

Shannon E. French, a leading scholar on warrior ethics, argues that warrior codes exist primarily to protect the moral core of the warrior.[iv] These ethical boundaries preserve integrity when individuals face pressure, violence, or the temptations of power. Warrior codes therefore serve as a form of moral armor, shaping behavior in ways that preserve humanity even in chaos. Plutarch reinforces this truth. In *How to Be a Leader*, he teaches that leadership begins with the cultivation of virtue. A leader who cannot govern himself cannot govern others. [v] He warns against vanity, pride, and emotional volatility, arguing that these traits lead to instability and failure. Across these traditions, common virtues emerge: courage, temperance, honesty, loyalty, justice, and self-restraint. Warrior identity is not about posture. It is about character. It is mastery of the self, long before mastery of the environment. When viewed through this historical lens, modern online interpretations of "warrior masculinity" bear little resemblance to actual warrior philosophy.

Why Warrior Ethos Now

The modern protector operates in an environment defined by complexity, ambiguity, and rapid threat escalation. Risks originate from digital stalking, reputational attacks, disinformation, political volatility, and unpredictable public behavior. Decisions often must be made with incomplete data and under significant time pressure. The protector must project calm and credibility while navigating complex human dynamics.

The U.S. Army's *ADP 6-22: Army Leadership and the Profession* states clearly that character forms the foundation of leadership.[vi] Presence and intellect strengthen leadership, but without character they cannot generate trust or influence. This principle applies directly to executive protection. A protector's authority does not come from force of personality or tactical prowess. It flows from moral consistency, emotional maturity, and the ability to make sound decisions under pressure. Those entrusted to the protector's care respond to character—not to aggression or performative bravado.

In this environment, the warrior ethos provides a stable ethical frame. It reinforces that leadership is a responsibility, not a status symbol. It demands humility over dominance, restraint over impulsiveness,

and service over self-promotion. These principles counter the ego-driven narratives prevalent online and offer protectors a grounded professional identity. By reclaiming classical virtues, protectors gain a compass to guide difficult decisions and stabilize teams. The warrior ethos, properly understood, elevates the protector from technician to guardian. However, before exploring the pillars of this ethos, it is necessary to understand what the warrior path does not include.

What the Warrior Ethos Is Not

To grasp the authentic warrior ethos, it is necessary to clarify what it rejects. Much of what circulates online under the banner of warrior masculinity would have been dismissed by ancient philosophers as weakness disguised as strength. Stoic writers such as Seneca warned that anger reflects a lack of self-control.[vii] Marcus Aurelius wrote that responding to insult with rage reveals instability of the mind.[viii] In every warrior code, the disciplined individual is strong; the reactive one is fragile. Plutarch cautioned that leaders who display vanity or inconsistency are unfit for responsibility.[ix] Warrior traditions consistently condemned ego, self-promotion, and unnecessary displays of dominance.

Many modern influencers invert these principles. They equate intensity with power, volatility with authenticity, and domination with leadership. They present anger as passion, insecurity as confidence, and aggression as strength. These distortions mislead newer protectors into believing that volume equals presence or that authority is achieved through dominance. They undermine credibility and increase operational risk. The warrior ethos is not about projecting power. It is about cultivating inner discipline. It is a philosophy of governance, not performance. It rejects the emotional volatility normalized in contemporary online culture and guides protectors toward steadiness, clarity, and moral conviction.

Having separated contemporary distortions from the authentic warrior ethos, we can now turn to the principles that sustain an effective protector ethos. At its core, this ethos rests on inward discipline, ethical clarity, and a commitment to service. These qualities do not appear in crisis by accident. They are cultivated over time and become the internal framework that guides conduct when conditions are uncertain and the stakes are high. The following pillars outline the essential elements of this ethos and how they shape the protector's daily leadership practice.

Pillar One: Moral Courage

Moral courage is the backbone of protector leadership. It is the willingness to act in accordance with principle rather than convenience. Physical courage can be situational. Moral courage is required every day. In executive protection, moral courage appears in many forms. It is the refusal to cut corners during an advance even when time is short. It is the honesty required when a principal proposes an unsafe course of action. It is the willingness to present unwelcome assessments to senior leaders. It is the accountability that comes with owning mistakes and learning from them. Plutarch insisted that leaders first cultivate the virtues they wish to see in others.[x] Leadership without moral grounding becomes unstable or self-serving. As French argues, warrior codes function to guard the warrior against moral erosion.[xi] They remind individuals that power must be governed by responsibility. For protectors, moral courage is a form of stability. It reassures the principal, reinforces trust within the team, and promotes integrity across the program. It positions the protector not as a mere operator but as a principled leader willing to bear the burdens of truth and responsibility.

Pillar Two: Self-Mastery

Self-mastery is essential for modern protectors. Marcus Aurelius wrote that individuals have power only over their reactions, not external events.[xii] This insight resonates deeply with the demands of protective

work. Public interactions are unpredictable. Emotional provocations are common. Fatigue and stress can accumulate. In these environments, self-governance is a professional requirement.

Seneca described anger as temporary madness and argued that leaders must regulate emotion in the same way they regulate physical discipline.[xiii] Modern Stoic authors such as Ryan Holiday reinforce this concept, describing routines that promote clarity, reflection, and emotional stability.[xiv] For protectors, self-mastery manifests through composure in chaos. It is the ability to remain calm when a stranger confronts a principal. It is the discipline to de-escalate rather than react. It is the maturity to accept criticism without defensiveness. It is the self-awareness needed to recognize when fatigue or personal stress may influence judgment.

The online narratives that glorify impulsive or aggressive behavior undermine this principle. They encourage protectors to celebrate emotion rather than control it. Yet the protector who cannot master himself cannot lead a moment of consequence. Self-mastery strengthens the protector's influence, presence, and effectiveness. It builds confidence not through noise but through steadiness.

Pillar Three: Service and Responsibility

Service lies at the very center of a protector's identity. Warrior traditions across cultures elevated duty to others as the highest expression of strength. Samurai codes demanded loyalty to community and to the ideals of the warrior's path. As Daidoji Yuzan indicates in *The Budo Shoshinsu*, the Way of the Samurai is found in service.[xv] This is a reminder that service is not subordination but purpose. Greek philosophy likewise stressed civic responsibility as the foundation of a meaningful life. Plutarch taught that leaders must serve others rather than seek personal elevation, arguing that self-interest corrodes judgment and weakens the moral authority required for leadership.

Executive protection reflects these values with clarity. Protectors safeguard not only life but also dignity, privacy, and trust. They serve principals, teams, and organizations, often without recognition, often without visibility, and always with an eye toward the well-being of others. This form of service demands humility. It requires avoiding self-promotion, respecting confidentiality, and placing mission above personal pride. It also involves modeling ethical behavior, so the team understands what doing the right thing looks like under pressure.

The influence of a protector extends far beyond physical security. It shapes team culture, reinforces professional boundaries, and builds trust with principals and stakeholders. This stands in sharp contrast to the self-centered narratives that dominate much of modern online culture, where leadership is framed as dominance rather than stewardship. The protector must reject these distortions and embrace a leadership identity grounded in responsibility and service. Doing so strengthens teams, stabilizes operations, and delivers a form of leadership that tactical skill alone can never achieve.

Pillar Four: Discipline and Continuous Development

Discipline is the structural foundation of the warrior ethos. It is what transforms intention into action and potential into competence. Marcus Aurelius and Plutarch both viewed leadership as a lifelong journey of self-improvement. Ryan Holiday's modern interpretations reinforce this perspective, emphasizing daily practices that cultivate clarity, resilience, and growth.

The disciplined protector trains consistently. This includes physical readiness but also intellectual development, communication skills, and ethical reflection. It involves studying threat patterns, learning

emerging technologies, and refining operational procedures. It also requires routine self-assessment to identify areas for improvement. Discipline distinguishes the protector from those who rely on intensity or image. It builds credibility with principals and peers. It strengthens decision-making under pressure. It cultivates the mindset of a leader-scholar who seeks continuous improvement. This disciplined identity stands in contrast to the counterfeit warrior who relies on theatrics or intensity rather than patient mastery. The disciplined protector demonstrates strength through consistency, not bravado.

The Counterfeit Warrior

The influence of online personalities who promote dominance, aggression, or ego-driven action poses a real challenge for the protective profession. These figures present a facade of strength that contradicts the timeless principles of warrior philosophy and the core values of executive protection. They portray leadership as domination rather than responsibility. They prize emotional reactivity over calm judgment. They teach that power flows from volume rather than character. This counterfeit model is seductive for individuals seeking identity, validation, or belonging, but it leads protectors toward behaviors that undermine trust, increase risk, and damage reputations. Classical wisdom offers a remedy. French warns that without moral boundaries, the warrior becomes a danger to himself and others.[xvi] Seneca and Aurelius condemn volatility and ego.[xvii] Plutarch criticizes leaders who seek applause rather than integrity.[xviii]

The protector must therefore resist these distorted models and instead embrace the authentic warrior ethos. The true warrior leader does not perform strength, he practices it. He does not dominate but governs himself. He does not seek attention and humbly accepts responsibility. By rejecting counterfeit narratives, protectors strengthen the profession and elevate their own leadership potential.

Real-World Applications: Leadership in Action

These principles come alive in the daily work of protection. The following scenarios illustrate how these principles manifest under real operational pressure.

1. **The Public Confrontation**: A principal faces a verbal confrontation during a public walk. The counterfeit warrior responds with aggression and escalation. The protector-warrior leader remains calm, creates distance, manages the principal's movement, and controls the emotional temperature of the space. The protector's demeanor prevents escalation and reinforces trust.
2. **The High-Risk Event**: Corporate leadership pressures the team to support an event despite incomplete intelligence. The morally courageous protector presents the risk clearly, offers alternatives, and influences decision-makers toward a safer choice. This is leadership through integrity rather than submission or aggression.
3. **The Team Culture Moment**: A junior protector displays ego-driven behavior. Rather than ignoring or ridiculing it, the protector leader uses the moment to teach. He explains why restraint and humility matter. He reinforces the protector identity and helps the younger team member grow.

These scenarios highlight that warrior leadership is practical and stabilizing. It shapes actions that foster safety, trust, and ethical clarity.

Reclaiming the Warrior Ethos for the Protector Profession

The modern protector is not defined by aggression or dominance. They are defined by moral courage, self-mastery, and character. These virtues shape leadership in ways that preserve trust, stabilize teams, and strengthen operational effectiveness. Warrior leadership, understood through classical philosophy and

modern doctrine, offers a model of strength that counters the distortions of online culture. Reclaiming this authentic ethos is essential for the modern protector. It provides a professional identity grounded in responsibility rather than ego. It ensures that protectors lead with clarity rather than volatility. It elevates the profession and speaks to the aspirational nature of the work.

The protector is a warrior not because he seeks conflict but because he accepts responsibility. He governs himself before he governs the moment. He stands for principles when convenience would be easier. He builds trust through character rather than performance. By embodying these values, the protector not only enhances his own leadership but helps safeguard the profession for the challenges of tomorrow.

Author: Charles "Chuck" Randolph is a Senior Vice President at 360 Privacy who has held extensive security positions at technology companies and protection firms. He is a retired Lieutenant Colonel from the Army National Guard and does extensive volunteer work for the security community, including being on the editorial board of *The Close Protection and Security Journal.*

Endnotes

[i] Marcus Aurelius, *Meditations*, trans. Hays (Modern Library, 2002).
[ii] Plutarch, *How to Be a Leader*, trans. Beneker (Penguin Classics, 2020).
[iii] Aurelius, *Meditations.*
[iv] Shannon E. French, *The Code of the Warrior* (Rowman & Littlefield, 2003).
[v] Plutarch, *How to Be a Leader.*
[vi] U.S. Army, *ADP 6-22: Army Leadership and the Profession* (2019).
[vii] Seneca, *Anger, Mercy, Revenge*. trans. Kaster (University of Chicago Press, 2010).
[viii] Aurelius, *Meditations*, various passages referencing emotional restraint.
[ix] Plutarch, *How to Be a Leader*, passages on vanity and inconsistency.
[x] Plutarch, *How to Be a Leader*.
[xi] French, *Code of the Warrior*, chapters on ethical boundaries.
[xii] Aurelius, *Meditations*, passages on internal control.
[xiii] Seneca, *Anger, Mercy, Revenge*.
[xiv] Ryan Holiday and Stephen Hanselman, *The Daily Stoic: 366 Meditations on Wisdom, Perseverance, and the Art of Living* (New York: Portfolio, 2016).
[xv] Daidoji Yuzan, *Budo Shoshinsu- The Code of the Samurai*, trans. Alasdair Sadler (Tokyo: Charles E. Tuttle, 1988).
[xvi] French, *Code of the Warrior*, warnings on moral injury.
[xvii] Seneca, *Anger, Mercy, Revenge*.
[xviii] Plutarch, *How to Be a Leader*, passages on vanity and inconsistency.

Medical Planning for Close Protection Operations: Bridging the Gap Between Tactical Excellence and Clinical Capability

Huck Finne, MD and Luke Banks, MBBS

Abstract

Close protection operations increasingly demand sophisticated medical planning that extends far beyond basic first aid certification and hospital identification via internet searches. This paper examines the critical gaps in current medical planning practices within the close protection sector and provides a comprehensive framework for integrating medical threat assessment, capability development, pre-deployment intelligence, and emergency response protocols into protective operations. Through analysis of medical planning requirements across domestic and overseas operations, this study identifies three fundamental areas where close protection teams remain vulnerable: inadequate assessment of medical threats beyond trauma scenarios, insufficient medical capability within protective teams to manage identified risks, and limited understanding of local healthcare infrastructure capabilities.

The research demonstrates that comprehensive medical planning requires clinical expertise, regional intelligence, and operational experience—a combination rarely found within individual organizations. Drawing on military medical planning doctrine and contemporary close protection operations, this paper establishes that medical events statistically occur more frequently than kinetic threats yet receive disproportionately less planning attention. Experienced teams understand the importance of detailed medical operational risk assessments, often through first-hand experience of medical events. The study concludes with actionable recommendations for elevating medical planning standards across the close protection industry. This work addresses a critical deficiency in protective services literature and practice, providing both the rationale and methodology for implementing effective medical planning as a core component of comprehensive protection strategies.

Introduction

Medical planning for close protection operations is fundamental to mission success. The contemporary close protection industry operates within an increasingly complex risk environment where the probability of medical emergencies frequently exceeds that of kinetic threats. Despite this reality, most close protection operations maintain medical plans that consist primarily of ensuring operators possess first aid certification and identifying the nearest trauma center through internet searches. While adequate when incidents do not occur, this approach reveals multiple critical vulnerabilities upon any actual medical event.

Common practice during logistical medical planning is to make assumptions using open-source intelligence (OSINT). This may be adequate, but clearly OSINT can only take you so far. These gaps manifest across several dimensions, including operator skill sufficiency for the specific medical scenario, anticipation and preparation for predictable non-trauma medical risks, appropriate facility identification for the clinical

problem at hand, and verification of local healthcare capability to manage the presenting condition. The questions confronting close protection planners extend beyond simple facility identification to encompass fundamental issues of medical capability. Does the identified "trauma center" possess the resources and readiness to manage a bleeding patient requiring emergency surgery? Can the local hospital provide the necessary clinical intervention for the principal's known medical conditions? These questions demand answers before deployment, not during a crisis. Medical planning fundamentally reduces risk and enables optimal decision-making when situations deteriorate. Although this analysis primarily addresses overseas operations, the same principles apply to domestic operations where local healthcare quality, capability, and accessibility vary significantly even within developed nations.

The integration of systematic medical planning into close protection operations represents not merely an enhancement of existing practices but a fundamental shift in how the industry conceptualizes risk. The recently published ASIS International Executive Protection Standard recognizes this reality, establishing comprehensive frameworks that integrate medical planning into core protective operations.[i] Medical threats operate independently of threat profiles that drive physical security planning, yet they occur with greater frequency and can prove equally catastrophic to both the principal and the protective mission. A principal that dies from delayed cardiac intervention because the interventional cardiologist was on holiday, or whose child experiences anaphylaxis without access to appropriate pediatric critical care, represents preventable tragedies that proper planning eliminates. This paper establishes the framework for comprehensive medical planning within close protection operations, drawing from military medical planning doctrine while addressing the unique requirements and constraints of the private sector.

Medical Threat Assessment

Comprehensive medical planning begins with understanding the specific risks inherent to both the operational environment and the individuals being protected. Systematic medical threat assessment in tactical operations provides a framework for identifying potential medical risks and implementing proactive mitigation strategies.[ii] This assessment forms the foundation upon which all subsequent planning decisions rest.

Mission Start State and Individual Risk Factors

How much medical risk is the plan looking to mitigate? What is the mission start state? These fundamental questions must be answered before any operation commences. Traditional close protection threat assessments appropriately focus on physical security threats, yet medical emergencies statistically occur more frequently than kinetic engagements.[iii] Does the principal have significant past medical history and is this controlled? Is the activity likely to provoke a deterioration in a known medical condition—for example, unaccustomed exercise in someone with cardiovascular disease? Who else is traveling with the principal and what is their medical background? Are there children involved?

Knowledge of specific health risks enables targeted facility identification and capability verification. For example, a 76-year-old principal with known coronary artery disease and Parkinson's disease presents fundamentally different medical planning requirements than a healthy 35-year-old executive. Family members may possess medical conditions that, while easily manageable within the robust healthcare environment of a major metropolitan area, require detailed local understanding to optimally obtain emergency and inpatient care when traveling. Medical planning must also account for the possibility that the principal may invite friends or associates into their protective bubble, each potentially carrying their own medical history that could impact operational requirements.

Environmental and Endemic Disease Considerations

Before commencing any operation, planners must systematically evaluate endemic environmental hazards and infectious disease risks present in the operational environment. What are the environmental risks—road traffic collision prevalence or local infectious disease patterns such as dengue or malaria? A methodical review of authoritative sources, including the United States Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO), typically provides sufficient baseline intelligence for most locations. This assessment must extend beyond exotic diseases to include region-specific health risks such as altitude-related illness, extreme temperature considerations, water and food safety concerns, and vector-borne disease prevalence.

Every close protection operation must plan for trauma that could result from kinetic engagement or, more commonly, road traffic accidents resulting in multiple casualties. Transportation-related incidents represent the most frequent cause of serious injury and death among both principals and protective personnel across all operational environments. The medical planning process must therefore include comprehensive consideration of trauma mechanisms specific to the operational environment, ranging from penetrating trauma in high-threat environments to blunt force trauma from vehicular incidents in low-threat settings.

Host Nation Medical Infrastructure

What is the host nation medical infrastructure and how accessible is it to the team? What are the medical facility options? Are there designated receiving trauma centers, and do you have the ability to pre-alert the receiving team? Is the facility capable of emergency surgery 24/7? What is the host nation's typical ambulance response time?

Even in the UK and U.S., an individual hospital's capabilities can vary widely. A principal with ischemic heart disease who develops sudden chest pain needs their team to take them to the right hospital the first time. The ideal hospital will be able to perform a coronary angiogram, unblock an artery, or potentially provide advanced support such as extracorporeal membrane oxygenation (ECMO). With centralization of resources, many hospitals must transfer patients to other centers, meaning potential delays to life-saving treatment. An unconscious child with an obvious head injury may need a neurosurgeon—where is the nearest neurosurgical facility? One might think the optimal plan is to proceed to the nearest hospital with a sick child. However, reality is often more nuanced. A team informed by experts can make life-changing decisions in times of crisis to reach genuine definitive care.

Building Medical Capability Within the Team

Regulatory Requirements and Training Standards

In the United Kingdom, all close protection operatives are required to achieve First Response Emergency Care (FREC) Level 3 qualification by Security Industry Authority regulation. Australia has a similar advanced first aid requirement, but most other countries do not stipulate a minimum medical standard for close protection operatives. In the United States, many operatives possess Tactical Combat Casualty Care (TCCC) training from previous military or law enforcement service.

Clearly, a basic course does not mean medical proficiency. This training may easily be outdated, and operators likely have not maintained significant proficiency absent continued clinical practice or regular refresher training. Given this reality, planners bear responsibility for ensuring adequate operatives possess more than basic first aid capability.

What is the medical training standard within the team? Considering that one medically qualified operative could become the casualty, operational planning should incorporate at least two operatives with medical training to TCCC/FREC 3 or above, with at least one possessing more advanced training. Where specific certification is not legally required, formal training could be substituted with significant operational clinical experience, such as multiple combat deployments as a special operations medic. Even this credential requires careful evaluation, as some medics complete multiple deployments without extensive medical practice, while others accumulate more prehospital experience than all but elite prehospital physicians. No simple methodology exists to evaluate an individual's skills and experience; expert review by a trusted medical authority represents the optimal validation approach.

Proficiency Maintenance and Clinical Currency

Medical planning must account for appropriate skill mix and currency across the close protection team whilst recognizing many close protection operatives will have significant previous medical experience in either civilian or military settings. Acquired skills will fade with a lack of clinical exposure and a program of deliberate skill retention. Research demonstrates that even immediately following training, operator skills begin degrading.[iv] This degradation accelerates over months or years since initial training, particularly when refresher training occurs only with low periodicity.

Detailed threat assessment and training that challenges existing assumptions is crucial to ensure the medical plan is robust and fit for purpose. Planners confront three options to address skill currency challenges:

1. Refresher training demands significant resources in time and money yet still produces sub-optimal clinical skills. While advanced life support (ALS) courses formally teach advanced airway skills, multiple peer-reviewed studies demonstrate that proficiency requires hundreds, if not thousands, of intubations—an impossibility within one or two-day refresher courses.[v] This highlights a critical distinction often overlooked in emergency medical preparedness: training does not equal competence, and competence does not equal proficiency. Prehospital airway interventions are merely the most well-studied example of this phenomenon, but the gap between course completion and clinical readiness exists across the full spectrum of emergency medical procedures. Recognition of this gap is essential for realistic capability planning in remote and austere environments.
2. Active clinical practitioners: Identify operatives who regularly engage in clinical work, such as paramedics maintaining active practice. While no formal criteria define adequate proficiency, approximately 20-40% of time spent in clinical practice provides reasonable assurance of maintained skills.
3. Team augmentation: With an eye on specific risk mitigation, medical team capability can be enhanced in both clinical and non-clinical domains. This ranges from bespoke training packages to individual team augmentees such as critical care paramedics or pre-hospital care doctors, as well as supporting teams with live reach-back medical advice to retained subject matter experts, delivering unsurpassed operational decision advantage. This option proves expensive, easily costing thousands of dollars per day. However, if significant concern exists regarding the principal's risk factors, such an additional team member—providing no tactical benefit—may prove prudent despite cost considerations.

Advanced Life Support Considerations

While TCCC/FREC 3 or equivalent certifications offer solid foundations for both trauma and non-trauma management, they lack Advanced Life Support (ALS) training including fundamental skills such as intravenous cannulation and advanced pharmacological interventions. If the principal is older, cardiac risk, for which ALS offers substantial advantages over basic life support (BLS), likely represents the primary

clinical threat. Thus, strong consideration for incorporating at least one ALS-trained person becomes essential for comprehensive risk mitigation.

Equipment and Logistics

Medical Equipment Scaling

Medical equipment scaling for close protection operations will be aligned to operator scope of practice, likely medical scenarios, and the operational and environmental context. This can range from a basic FREC 3 kit to full physician-delivered pre-hospital critical care equipment enabling advanced time-critical interventions such as emergency anesthesia and blood product administration.

Medication and Cold Chain Requirements

Certain blood products and medications such as insulin have cold chain requirements that impose potential limits of exploitation that must be considered in prior logistical planning. Teams must either transport medications internationally or acquire them in-country, each approach presenting distinct challenges. International transport of medicines requires proper documentation to clear customs. Medication carriage overseas requires documented evidence of authority aligned to a prescription for a named individual. In-country acquisition demands trusted suppliers to ensure medications are not counterfeit—a significant concern in many jurisdictions. If planning for field blood transfusion, three options exist: fresh whole blood transfusion from team members (requires significant operator training and screening), imported blood products (requires substantial administrative burden but ensures quality), or in-country blood product acquisition (demands significant pre-mission due diligence).

Equipment Management and Contingency Planning

The team must understand what the limitations of their equipment and supplies are along with plans for re-supply. They must have considered pragmatic alternative solutions when faced with an unexpected, prolonged field care scenario. What is the team's organic evacuation plan? How many patients can you move in your vehicles, and can you treat on the move? What is your major incident plan? Global operations with often prolonged evacuation timelines mean such scenarios are not unrealistic, and teams should spend time considering vital equipment mitigations such as portable oxygen concentrators and battery cold chain storage. All equipment and supplies must maintain full charge, demonstrate appropriate capability for anticipated scenarios, include spare batteries, and remain within expiration dates. Critically, field equipment must match training equipment—training providers who utilize their own equipment rather than student-owned equipment fail to prepare operatives for actual field conditions.

Pre-Deployment Medical Intelligence

The Medical Assistance Provider Gap

Close protection operations often assume their travel insurance or medical assistance provider will provide rapid and seamless direction to assured medical facilities in location. Evidence suggests this assumption is unfounded. The reality is often disappointing. No medical assistance provider or travel insurer appears to have constructed a comprehensive database of global hospitals detailing their capabilities. Even the largest global assistance companies that service governments and military contracts have incomplete data on global medical facilities. The data they hold is often historical and not subject to periodic appraisal and validation and is largely based on OSINT rather than first-person ground truth. Additionally, information found through internet research requires significant medical sophistication to interpret accurately, remains low-fidelity, and demands hours of review to evaluate properly.

Calls for assistance are routed into call centers which are then triaged according to acuity by nurses and paramedics. When contacted, these providers typically direct clients to reputable hospitals in major or capital cities. Directional facility data is provided from their databases often with no awareness of the environmental, logistical, or individual medical context the team faces. Their primary focus is on call volumes, policy validity, customer eligibility, and cost containment rather than timely and expert medical advice. They excel at authorizing payment for care and arranging evacuation but lack detailed understanding regarding the nuance of medical options.

This reality underlies the importance of a close protection team having its own stress-tested organic plan informed by current highly reliable healthcare infrastructure data. Furthermore, due to fiduciary duties, medical assistance providers require certain administrative steps prior to authorizing care. First, they must ensure the patient did not materially fail to disclose risk factors that would have affected coverage. For the former, the insurer requires the patient's most recent general practitioner or primary care physician's complete history and physical examination documentation prior to authorizing care.
The reality in many parts of the world is that emergency care is often delayed because these guarantees of payment are not in place. Establishing a formal guarantee of payment requires multiple emails and scanned documents with wet signatures. Commonly this is due to the assistance company having no existing relationship with the hospital and the need to engage a local area agent to facilitate the process. Such delays are clearly unacceptable and usually only rectified with a credit card payment of funds on account to the hospital.

Comprehensive medical planning for a single two-week overseas operation typically requires tens to hundreds of hours of research by someone with clinical training. This will include identifying and verifying facility capabilities, establishing payment mechanisms, confirming physician credentials, and understanding local treatment protocols. Most organizations lack both the time and the medical expertise to conduct this due diligence effectively.

Trauma Capabilities Evaluation
Globally, trauma care provision is highly inconsistent even within individual countries. When evaluating trauma capabilities in any location, several critical factors demand assessment. First, establish the presence and proximity of trauma centers, with clarification regarding whether "trauma center" carries the same meaning locally as in UK or U.S. contexts. Trauma center designation varies significantly across jurisdictions, with some regions applying the term to any facility with surgical capability regardless of actual trauma systems integration.

Good surrogate markers of capability that demonstrate institutional commitment to quality of trauma care include:

- Emergency general surgery provision 24/7
- Neurosurgery provision 24/7
- Blood products on site
- Interventional radiology on site
- Intensive care on site
- Pediatric intensive care on site
- Minimum staff training standards such

Local facility capabilities require detailed evaluation, including operational standards and protocols. Payment mechanisms can delay or prevent life-saving care. In many jurisdictions, facilities will not initiate surgery without guarantee of payment—a process consuming hours while the patient deteriorates. It is

always worth remembering local public facilities may actually provide superior initial trauma care compared to the more externally appealing private hospitals. For facilities claiming trauma center status, verification is needed concerning immediate surgical intervention capabilities. The training credentials of physicians who will be present upon patient arrival should be confirmed, with ALS and ATLS (Advanced Trauma Life Support) certifications serving as excellent minimum standards demonstrating institutional commitment to quality emergency medicine.

Specialized Medical Needs

Beyond trauma capabilities, facilities must be identified that possess necessary resources to manage specific, identified medical risks. For instance, when a child with known history of severe anaphylaxis is present, preparation extends beyond simply ensuring multiple doses of epinephrine are available. This consideration matters for trauma as well, as pediatric and adult trauma are often managed by different facilities. Critical infrastructure must include identification of facilities capable of managing intubated and sedated pediatric patients requiring continuous epinephrine infusion support.

Consider the 76-year-old principal with coronary artery disease traveling to a regional capital. The medical assistance company will direct you to the best private hospital. What they won't tell you is that the facility's single interventional cardiologist is on holiday during your operational window. The government-funded catheterization laboratory operates on a 24/3 schedule, meaning it's closed on the nights you'll be in country. This is discoverable information, but it requires a level of medical sophistication and extensive local research per location to ascertain.

Payment and Insurance Navigation

From this analysis, several action steps emerge. For anyone who may require care abroad paid for by an insurer, likely via the insurer's medical assistance partner, maintain a complete primary care physician or general practitioner's history and physical examination ready for immediate transmission. When contacted, these records prove necessary to confirm proper risk was insured. If it emerges the patient underrepresented risks, the medical assistance provider will offer advice only, declining financial coverage. If planners desire maximal risk reduction, establish personnel contacts for each step that may require payment. Once human-to-human relationships are established, arrange payment mechanisms. If private helicopter evacuation becomes necessary, these services cannot afford to fly without fuel money in their bank account. Pre-arranging transfer mechanisms significantly reduces time to becoming airborne.

Emergency Response Protocols

Integration of Tactics and Medicine

This article does not comprehensively address the interplay between tactical operations and medical response. While traditional TCCC offers excellent clinical guidance on appropriate patient treatment, its precept that the first step of care under fire is to return fire may not apply in the close protection mission set.[vi] The translation of military tactical medicine to civilian close protection environments requires adaptation of combat casualty care principles to scenarios where threat neutralization and principal protection must be balanced.[vii] Planners should develop specific protocols regarding the inherent tension between returning fire/neutralizing threats and protecting/evacuating the principal. While Good Samaritan laws may protect non-licensed first responders, teams should consider medicolegal risks they may be assuming.[viii]

Definitive Treatment Versus Evacuation

A similar decision framework must address definitive treatment in-country versus immediate evacuation. If the plan prioritizes evacuation, the team will need either organic or locally vetted clinicians who can be rapidly procured with appropriate training. If the plan prepares the team to treat any contingency, the team will require an anesthesiologist and trauma surgeon. While these professionals can be sourced from the U.S. and UK, they are expensive. Furthermore, beyond clinical skills, planners must assess their ability to work in the challenging environment of close protection operations. Some clinicians prove completely ineffective without perfect equipment provided by technicians. Ensure definitive treatment and evacuation plans for both team members and principals are determined beforehand. These plans may reasonably differ. For example, an injured team member may remain in-country for definitive treatment and later evacuation. This individual may require a non-medical escort, so plan for being down two team members or arranging backup escort availability. All plans require rehearsal at minimum via tabletop exercise.

Medical Evacuation Planning

Embassy and Medical Assistance Company Capabilities

Expect zero support from any embassy; close protection teams must plan their own evacuation. Medical assistance companies use trusted third-party evacuation companies, but their notice-to-effect period is measured in days. Medical assistance companies, whether contracted directly or through insurance companies, demonstrate skill at arranging evacuation, although expect minimum 24-hour timelines. Most larger assistance companies maintain triage phone systems to reduce costs. These systems are not designed to minimize time to treatment. Rarely, if ever, does the customer communicate with the medical director.

Local evacuation to a place of relative medical safety is always the responsibility of the local team. Getting this initial care right can mean the difference to both initial survival but also the risk of onward repatriation once a third-party provider arrives in location. Medical assistance companies rarely interrogate cases with any specialist medical oversight and simply function as medical information messengers. Early treatment decisions are always deferred to local physicians until third-party providers arrive. Thus, if the plan involves efficient local treatment, it will require coordination by the team. If the team desires live medical direction, it must be arranged separately from any retail insurance. Close protection teams should consider expert medical oversight for overseas operations.

Alternative Evacuation Options

If arrival occurred via private fixed-wing aircraft, a backup option involves pre-arranging appropriate local medical personnel who could travel with the team aboard the arrival aircraft. This arrangement requires advance coordination but can significantly reduce evacuation timelines when compared to commercial medical evacuation services.

Conclusion

Medical planning represents a critical yet frequently overlooked component of close protection operations. While tactical aspects rightfully receive significant attention, the ability to effectively manage medical emergencies and onward logistics is crucial. Indeed, medical events remain statistically more likely than kinetic engagements across most operational profiles. Contemporary analysis of close protection methodology demonstrates the evolution toward proactive, intelligence-driven approaches that integrate medical preparedness as a core component rather than an afterthought.[ix] The industry gap between current practices and optimal medical preparedness is substantial, with many close protection operators relying on basic trauma training and internet searches for nearby hospitals. This is an approach that leaves

teams vulnerable when hospital capabilities vary dramatically even within developed capitals, trauma center designations carry different meanings across jurisdictions, and payment mechanisms can delay critical care when seconds matter.

Medical planning requires three types of expertise rarely found in a single organization: clinical knowledge to assess risks and evaluate facility capabilities, regional intelligence to navigate local healthcare systems and payment structures, and operational experience to integrate medical planning with close protection realities. The principal who survives the kinetic event but dies from a delayed cardiac intervention because no one confirmed the catheterization laboratory was operational represents a preventable tragedy that proper planning eliminates. The question for close protection operators and corporate travel managers is not whether comprehensive medical planning matters, but whether they possess the specialized resources to execute it properly. This paper has established the framework for systematic medical planning within close protection operations, providing actionable guidance across threat assessment, capability building, pre-deployment intelligence, and emergency response protocols. Implementation of these frameworks will elevate industry standards and reduce preventable adverse outcomes across both domestic and international protective operations.

Authors:
Dr. Huck Finne is CEO and Co-founder of Aksanio, a medical information company. He is a recently retired US Navy anesthesiologist with extensive experience supporting special operations across multiple theaters and conducting medical planning with NATO. He currently practices clinically at Harefield Hospital and Vanderbilt University Medical Center.

Dr. Luke Banks is Medical Director and Co-founder of Aksanio, a medical information company. He is a Consultant in Anesthesia, Critical Care and Pre-hospital Emergency Medicine with extensive experience in global aeromedical retrieval. He practices clinically at Queen Victoria Hospital East Grinstead, Kent Surrey Sussex Air Ambulance and Lincs and Notts Air Ambulance.

Endnotes

[i] ASIS International. *Executive Protection Standard*. Alexandria, VA: ASIS International, 2025.
[ii] Jeff Thurman and Timothy Price, "EMS Tactical Medical Threat Assessment and Protection," in *StatPearls* [Internet] (Treasure Island, FL: StatPearls Publishing, 2025), https://www.ncbi.nlm.nih.gov/books/NBK546700/.
[iii] Orlando Wilson, *Threat Assessments: For Close Protection & Security Management* (Independently published, 2019).
[iv] A. S. Linde, J. Caridha, and K. J. Kunkler, "Skills Decay in Military Medical Training: A Meta-synthesis of Research Outcomes," *Military Medicine* 183, nos. 1–2 (January–February 2018): e40–e44; N. Pattyn, A. Malfait, M. V. Puyvelde, et al., "A13 Skill Acquisition and Skill Decay in Medical First Response Skills: When More Is More," *BMJ Military Health* 171 (2025): A15–A16.
[v] Sin Young Kim, Sang O. Park, Jong Won Kim, Juno Sung, Kyeong Ryong Lee, Young Hwan Lee, Dae Young Hong, and Kwang Je Baek, "How Much Experience Do Rescuers Require to Achieve Successful Tracheal Intubation During Cardiopulmonary Resuscitation?" *Resuscitation* 133 (December 2018): 187–92; Charles D. Deakin, Peter King, and Fiona Thompson, "Prehospital Advanced Airway Management by Ambulance Technicians and Paramedics: Is Clinical Practice Sufficient to Maintain Skills?" *Emergency Medicine Journal* 26, no. 12 (December 2009): 888–91; Kate Crewdson, David J. Lockey, Jo Røislien, Hans

Morten Lossius, and Marius Rehn, "The Success of Pre-hospital Tracheal Intubation by Different Pre-hospital Providers: A Systematic Literature Review and Meta-analysis," *Critical Care* 21, no. 1 (February 14, 2017): 31, https://ccforum.biomedcentral.com/articles/10.1186/s13054-017-1603-7; Keir J. Warner, David Carlbom, Colin R. Cooke, Eileen M. Bulger, Michael K. Copass, and Sam R. Sharar, "Paramedic Training for Proficient Prehospital Endotracheal Intubation," *Prehospital Emergency Care* 14, no. 1 (January–March 2010): 103–8.

[vi] Frank K. Butler, John Hagmann, and E. George Butler, "Tactical Combat Casualty Care in Special Operations," *Military Medicine* 161, suppl. (August 1996): 3–16.

[vii] David W. Callaway, "Translating Tactical Combat Casualty Care Lessons Learned to the High-Threat Civilian Setting: Tactical Emergency Casualty Care and the Hartford Consensus," *Wilderness & Environmental Medicine* 28, no. 2S (June 2017): S140–S145.

[viii] Good Samaritan Laws offer legal protection for people who voluntarily intervene in emergencies and prevents lawsuits based on that intervention.

[ix] David W. Callaway, "Translating Tactical Combat Casualty Care Lessons Learned to the High-Threat Civilian Setting: Tactical Emergency Casualty Care and the Hartford Consensus," *Wilderness & Environmental Medicine* 28, no. 2S (June 2017): S140–S145.

Closing the Automation Gap: Evidence-Ready Compliance for Protective Operations

Jeff Robbins

"Compliance oversight is the last gap that is usually never filled adequately in any security program, due to a range of variables, such as complexity, resources, time, and a lack of understanding, but it's the one thing that can bring your entire program down."
–Fred Burton, former special agent, CSO and New York Times best-selling author

Introduction

U.S. security licensing and training requirements vary widely across states, creating a high-entropy environment for protective operations organizations that manage compliance manually or in silos. The Clarity Factory 2025 Annual Chief Security Officer (CSO) Survey shows that security leaders have broadly embraced artificial intelligence (AI) for threat assessment, monitoring, intelligence gathering, and physical security systems, while adoption levels of AI for automated compliance checks and reporting remain in the low single digits.[i] This is a clear automation gap, where the most rules-based, repeatable work in many security programs is the least automated, and this gap exists even when security leaders are becoming aware of the risks. ASIS Security Trends shows that fines or citations for non-compliance were among the most important factors for security professionals when conducting risk assessments and were rated as a high-importance factor by 52% of respondents.[ii] When we analyze our modern operating environment, it is easy to see why.

Today, regulators are signaling stricter enforcement as laws simultaneously grow more complex and the demand for security continues to rise, largely driven by activism and recent high-profile attacks on public figures. This backdrop puts security leaders into a precarious situation, where their programs must deliver more security, in more jurisdictions, while navigating a more complicated regulatory environment with less tolerance for error. To meet this challenge, security leaders have a tremendous opportunity to shift the stigma on compliance, from an administrative burden to an operational enabler that allows their organizations to remain mission focused. But to truly understand this opportunity, we need to understand how most organizations manage compliance today.

Standard Compliance Methods in the Security Industry

In most organizations, the process for a standard license renewal looks like this: a supervisor opens a spreadsheet that tracks license expirations and notices several officers due to renew their license in the next 30-60 days. The supervisor fires off texts or emails reminding them to renew. Some officers respond, some ignore the first message, and several return with basic questions (“Which training course do I complete?” “Do I need fingerprints again?” “How long is the application process?”), adding to the manual workload for the supervisor. What should be a simple, rules-based workflow becomes a multi-touch, multi-day exchange that competes with the supervisor’s higher-level responsibilities.

While not ideal, this process can be workable at a small scale. However, when the organization grows, this process is unverifiable and risk is greatly increased. Managers are often forced to accept whatever license an employee has because they simply lack the time to confirm validity with every credential against the state verification website. This means that a forged, altered, or otherwise invalid license can sneak into the system and stay there, never to be revealed until there is an audit or an incident on post.

This is the reality facing most security organizations. Operating in one state is difficult enough, but expansion into more jurisdictions ensures that the problem compounds across different firearm qualification requirements, written tests, psychological examinations, and wildly variable training, insurance, and audit requirements. A manual model cannot keep pace with today's environment. Operationally, it is unsustainable; strategically, it is risky. And we must ask ourselves what this model means for our time, money, and reputation.

Why This Model Is Misaligned in Today's Environment:

Manual Effort and Capacity Drag

Even in more mature compliance domains like information security and GRC, a study conducted by Hyper proof found that compliance professionals spend 38% of their time on manual tasks that could be automated.[iii] Because compliance is less standardized in the physical security industry, and AI adoption is under 5% for compliance checks,[iv] the manual burden is likely to be far higher for physical security compliance managers. Hours spent manually adhering to countless regulatory requirements that change with each state are hours not spent on SOP development, event readiness, intelligence gathering, or after-action reviews, which is the true work that fulfills any security organization's core mission of protecting others.

Regulatory, Financial, and Productivity Exposure

Globalscape and the Ponemon Institute conducted a multi-industry study and found that the average cost of non-compliance was 2.7x greater than the cost of maintaining compliance, and that the average cost of non-compliance has risen 45% over the past decade.[v] In protective operations, an initial fine from a state regulator puts an organization on their radar. This sustained and increased scrutiny has the potential to trigger more fines and even a suspension that halts revenue generation in an entire state. Many states even have automatic suspension clauses for easy-to-miss expirations like certificates of insurance.

Operationally, missed credential expirations lead to last-minute staffing shortages. SHRM found that overtime and replacement workers used to cover absences directly cost organizations 7.3% of their entire payroll.[vi] Furthermore, SHRM found that a replacement worker covering an unplanned absence was 36.6% less productive and also amplified other pressures among employees like morale, stress, and workload due to additional training needs.[vii]

Stakeholder Alignment, Trust, and Reputation

ASIS survey data shows that 77% of security professionals view organizational reputation or image damage as a high-importance factor when conducting security risk assessments – the highest-rated category in their study.[viii] This number aligns with real-world experiences, as security leaders must constantly advocate for budget and headcount as an internal team or for new contracts and revenue as a security services company, both of which are extremely competitive environments where a reputation of professionalism matters.

One of the easiest ways to damage reputation and image is through compliance errors. They are not only easy to make but they are also uniquely damaging because stakeholders assume they should be easy to avoid. In the stakeholder's view, a challenge as difficult as protecting executives from assassins won't be managed well if something as seemingly simple as a license renewal goes awry. Regardless of how skilled an organization is at protection, any compliance lapse or unprofessional operations causes stakeholders to lose trust. These challenges magnify as organizations grow and expand across state lines, where leaders can't realistically verify every license or follow each state's specific training, application, renewal, insurance, or audit requirements. This model is not only labor-heavy; it is structurally fragile.

The Opportunity: Automating the Lowest-Value Work:

"We still have a lot of opportunities to reduce low-grade jobs that would be better done by a machine. One of the things holding us back is the lack of skillset within middle management to identify these opportunities." – 2025 Clarity Factory CSO Survey Respondent

This is a very common theme in today's security industry, where leaders understand there is a problem and an opportunity, but they don't know how to get there. The positive news is that compliance processes are unusually good candidates for automation because most are standardized by regulation or policy. Whether it is determining a renewal window, license term, or required training, there is a set process established by a third party that doesn't allow much room for deviation. This makes the work repeatable and bound by constraints and rules, which is precisely where machines and software excel and where humans add the least value. To take advantage of this automation opportunity, organizations should follow a four-pillar framework to ease and streamline their compliance burdens.

Standardize and Centralize Evidence

All organizations, large and small, should create a living single source of truth that maps each team member to the requirements of their roles and locations. All organizational leaders should be able to easily view a complete status of their organization, from personnel to facilities, vendors, and internal business documents, and quickly determine which areas are compliant with government regulations and internal policies, nearing non-compliance, or non-compliant.

Verification Layer

Trust but verify is a common theme in the security world, but many organizations are unable to verify the licenses their team members bring on shift, and many states will not alert a business if one of their employees' security licenses has been suspended or revoked. Once evidence is centralized, security leaders should automate and log the verification of state licenses on a monthly, weekly, or daily cadence, ensuring that every credential is valid before deployment.

Rules-Based Automation

Establish longevity of the compliance management initiative by automating renewal alerting on 90/60/30-day schedules with automatic escalation to supervisors if no action has taken place. Organizations should also use document intelligence and optical character recognition (OCR) to extract expiration dates and license numbers for future tracking while performing quick validation checks, such as confirming the name on the license matches the employee's name in HR systems. The goal is not to eliminate human oversight, but to ensure human intervention is only used when required, saving time, energy, and money.

Show Your Work: Reporting that Builds Trust, Speed, and Alignment

A reputation of trust and credibility is one of the greatest assets a security program has. The ability to show professional reports to executive leadership or prospective clients proving the compliance, licensing, and training levels of your organization is an unsung hero in generating new revenue or increasing budget. Additionally, when data is reportable, teams can now answer staffing questions in seconds and route the right people to the right assignments with confidence. If an organization needs to fill a shift quickly due to an unexpected absence, a security leader should have the ability to quickly query for a list of all TX Level 4 officers within 100 miles of Austin that are also EMT certified. Having the ability to report quickly and professionally on organizational data allows security organizations to turn compliance into readiness.

Once an organization's data and evidence are centralized, verified, automated, and reportable, they become operational enablers, rather than merely an accumulation of files that need to be stored and managed to avoid a fine. When this transition takes place, the business impact shows up fast. With a visible and defensible posture, regulatory risk is reduced, revenue and budget can be increased, incidents remain focused on facts rather than operational shortcomings, and organizations can scale headcount or expand to new states with greater ease. The organization looks and operates like it is always ready, because it is.

Conclusion

The security industry has embraced AI in many sectors, but not for one of the most rules-based, repeatable, and high-consequence processes that every organization must manage. Shifting organizational mindset to treat compliance management as an operational capability that is standardized, centralized, verified, automated, and reportable unlocks resilience, capacity, and credibility when it matters most. In a climate that consistently demands more from security organizations, through rising threat levels and regulatory scrutiny, the organizations that can show and prove their work on demand will win trust, budget, and business while keeping the focus where it belongs in this high-threat environment – protection.

Author: Jeff Robbins is the Vice President of Operations at CenterSeat.ai**,** a company specializing in providing compliance management software for physical security organizations. He is a licensed California Qualified Manager, a former Field Operations Director at Gavin De Becker and Associates, and a former U.S. Army special forces green beret.

Endnotes

[i] The Clarity Factory, *2025 Annual CSO Survey* (report, 2025), p. 49, 53, https://uploads.strikinglycdn.com/files/1c1ccfc6-0127-4181-b956-6cec67532856/ClarityFactory_2025CSOSurvey.pdf.

[ii] ASIS International, *Security Trends Research Report 2025* (report, 2025), p. 8, https://www.asisonline.org/globalassets/publications-and-resources/asis-2025-security-trends-research-report.pdf.

[iii] Kayne McGladrey, *What Are Your Current Compliance Operations Really Costing You?* (white paper, Hyperproof, 2024–2025), https://hyperproof.io/resource/what-are-your-current-compliance-operations-really-costing-you/.

[iv] Clarity Factory, *2025 Annual CSO Survey*

[v] Globalscape (Fortra), *The True Cost of Compliance with Data Protection Regulations* (report, 2018), p. 2–3, https://static.fortra.com/globalscape/pdfs/guides/gs-true-cost-of-compliance-data-protection-regulations-gd.pdf.
[vi] Society for Human Resource Management (SHRM), *The Total Financial Impact of Employee Absences* (report, 2014), p. 10, 63, https://www.shrm.org/content/dam/en/shrm/topics-tools/news/employee-relations/Total-Financial-Impact-of-Employee-Absences-Report.pdf.
[vii] Ibid.
[viii] ASIS, *Security Trends Research Report 2025*

EVENT RISK
SECURITY SERVICES®

PREMIUM SERVICES + GLOBAL FOOTPRINT

- Exceptionally Trained Associates
- Risk Assessments
- Static Post & Event Support
- Workplace Violence Training
- Protective Transportation
- Armed or Unarmed

WHAT KEEPS YOU UP AT NIGHT?®

CRISIS24 | PRIVATE STRATEGIC GROUP

TOTAL PROTECTION
WITH NO COMPROMISE

TRUE PEACE OF MIND AWAITS.
UNPACK OUR FULL PROTECTIVE
AND MEDICAL CAPABILITIES.

CRISIS24.COM/PSG

Interview with Experts

A Conversation with Ivan Ivanovich

Ivan Ivanovich is the President of WSO Worldwide Security Operations. He is a naturalized Mexican of Serbian origin, trained in security during the Balkan wars. Ivan has more than 30 years of experience in high-risk international environments. He was the first civilian to train Spain's Marine Infantry and other elite Spanish military and police units in executive protection, as well as the first civilian to train Costa Rica's Presidential Protection Unit. Ivan is the author of the Spanish bestselling book *Executive Protection in the 21st Century.*

Introduction

In this wide-ranging conversation, Ivan Ivanovich, President of WSO Worldwide Security Operations and author of *Executive Protection in the 21st Century*, offers a rare, candid look into the evolution of close protection across Latin America. Drawing on more than 25 years of experience operating in one of the world's most complex security environments, Ivan discusses the region's unique threat landscape, the development of professional standards, the role of IPSB in shaping the future of the field, and the lessons Latin American practitioners can offer the global protection community. The interview captures both the operational realities and the strategic challenges facing modern executive protection, delivered in Ivan's distinctly direct and insightful style.

Q&A Interview

Q: What motivated you to help develop the IPSB community in Latin America, and what have you learned from that experience?

Ivan: This really began because, after 25 years in Mexico, I realized around 2016 that we didn't have a proper executive protection certification; not here, and not really anywhere. A few of us started developing a basic body of knowledge that every protector should have. We focused on best practices and built a certification model from scratch. Pablo [Ortiz Monasterio] then suggested hosting a dedicated EP event because the field had been abandoned for years.

So, in 2018 we launched the EP Summit to bring practitioners across Latin America and the world together to build that knowledge base. Over time, IPSB leaders began attending, and we saw an opportunity to expand the global network. This year we even hosted the event in Colombia, which matters because Latin America is the most dangerous non-war region in the world. Many executives truly need well-trained protection, which is why IPSB's presence here is so important.

Q: How would you describe the state of executive protection and private security in Latin America today?

Ivan: I'd divide it into three parts. First, core EP, which grew out of the kidnapping boom of the 1990s in Mexico. That's when corporations and banks started investing real money in professional protection. Corporate EP in Mexico can be among the best in the world because teams operate quietly in genuinely dangerous places while maintaining high standards. Second, government EP, which involves protecting politicians and officials. This sector is deeply inconsistent and has produced some tragic outcomes, like the assassination of the Ecuadorian politician. Political shifts in Mexico have also removed key units, creating capability gaps. Third, private contractors for entrepreneurs, many of whom are armed but not trained in EP. There's almost no regulation, so you see everything from highly skilled professionals to completely unprepared operators.

Operating here also requires understanding three levels of danger: everyday crime, cartel-controlled areas,

and zones where cartels are actively fighting. That range of threat environments is why professionals with experience in Mexico are so highly valued.

Q: How is the Latin American protection community working to advance standards, and what role can IPSB play?
Ivan: IPSB can do a lot by connecting professionals and elevating those with less training. When someone poorly trained makes a catastrophic mistake, the whole industry suffers. Here in Mexico, many protectors simply cannot afford extensive training, so IPSB's challenges and opportunities are expanding free or affordable resources that raise the baseline of professional competence.

Q: What are the biggest barriers to training and certification for protectors in the region?
Ivan: The biggest barrier isn't cost; it's time. Protectors here work 70 hours a week, six days straight. They don't have the flexibility to take long courses, even if they want to. That's why we've shifted to online modules that can be watched during travel or downtime. Another issue is that there is still no standardized certification. IPSB is uniquely positioned to create a legitimate global EP credential, and eventually we need one. Poor training can be deadly. Over the last three years, Mexico has lost 31 protectees, and 42 protectors, most coming from poorly trained sectors.[i]

Q: How do culture, trust, and relationships shape protection work in Latin America?
Ivan: Latin America runs on personal relationships. Trust and local networks are essential, much more than in the U.S. or Europe. When you're a foreign company working here, you cannot operate effectively without strong local support.

Q: What emerging threats should protectors in the region be preparing for?
Ivan: Threats have evolved quickly. Kidnapping dominated in the 1990s. Then assassination became more common, and many teams weren't prepared for that shift. The next big threat is drones. Cartels already use them, including explosive drones and fiber-optic-triggered devices. I think 80 percent of future assassination attempts could involve drones, especially once drone-trained veterans from the Ukraine war enter the global market. Another challenge is communication with principals. Protectors are rarely trained to explain risks effectively. Modern EP is about protecting in time, not just space. You can't rely solely on proximity. Prevention must come first.

Q: How important is language and cultural fluency for cross-border protection work?
Ivan: When I work abroad, I rely on local support; when others work here, I'm their local support. Even basic Spanish helps foreign protectors earn trust and overcome national biases. When you come into Mexico, you're essentially trusting your life to your local counterparts. That's built through respect and communication.

Q: What distinguishes EP work in Latin America from work in the U.S. or Europe?
Ivan: In the U.S. or Europe, you can work thirty years in a suit with a firearm and never face a real threat. In Latin America, threats are constant, including robberies, carjackings, cartel violence. Another important difference is how teams respond to violence. In many countries, the standard policy is straightforward: if gunfire erupts anywhere in the city where a corporate visit is taking place, the immediate protocol is to evacuate the protectee to the hotel—no matter where they are.

In Mexico, however, evacuation is not always practical. Gunfights that are unrelated to the protectee occur frequently, which means that a blanket "evacuate immediately" policy is neither realistic nor effective. This is why protectors must assess each incident dynamically—considering distance, nature of the conflict,

operational context, and available routes—to determine whether to evacuate or to continue the operation with heightened caution. That level of judgment is complex, and it requires training, experience, and a deep understanding of the local threat landscape.

When working in environments with constant and evolving risks, the weaknesses of certain protective methods become evident—firearms being a prime example. Many protectees [in Latin America] have been killed by their own protectors when those protectors attempted to defend them against petty theft or carjacking while operating in soft vehicles.

Another common misconception is that operating in cartel-controlled areas requires a heavy weapons arsenal. This is simply not true. You cannot outgun a cartel. If you are unarmed, they will usually let you pass; if you are armed, they may assume you are a rival and respond accordingly.

Q: What lessons from the Latin American experience are most valuable for the global EP community?
Ivan: One major lesson is the importance of process: intelligence, counter-surveillance, early detection, pattern awareness. Protectors here operate in an environment where failure is punished immediately. That pressure forces constant improvement. Latin American practitioners sometimes underestimate how valuable their experience is. When I trained Spanish military and police units, they saw how our methods built in real-world, high-threat environments applied directly to their work. IPSB can help ensure the global community learns from what Latin America has had to master out of necessity.

Endnotes

[i] For those interested in Ivan's data, please see: Ivan Ivanovich and Carlos Beuvrin. "Historical Analysis of the Effectiveness of Executive Protection Measures: A Study of 141 Assassination Attempts Against Public Figures, 1900–2025 (Abstract)." Last modified December 18, 2025. https://ivanivanovich.com/es/historical-analysis-of-the-effectiveness-of-executive-protection-measures-a-study-of-141-assassination-attempts-against-public-figures-1900-2025-abstract/.

Tools for Security Professionals

Tools for Security Professionals is a practical, application-focused section of *The Close Protection and Security Journal* dedicated to how tools are actually used in the field, not how they are marketed or theoretically described. This section examines emerging technologies, established platforms, and legacy tools through an operational lens, emphasizing how security professionals can integrate them effectively into close protection, intelligence analysis, and risk management under real-world constraints. Rather than showcasing novelty for its own sake, the focus is on utility, limitations, and the conditions under which a tool meaningfully improves decision-making, detection, response, or resilience. Contributions to Tools for Security Professionals are written by experienced practitioners and subject-matter experts who understand that tools do not replace judgment, tradecraft, or leadership. Each piece explores how a specific tool or capability can be adapted, combined, or repurposed to solve practical problems, whether that involves leveraging new emergency communications technology, applying analytical software to protective intelligence, or using long-standing methods in unconventional ways.

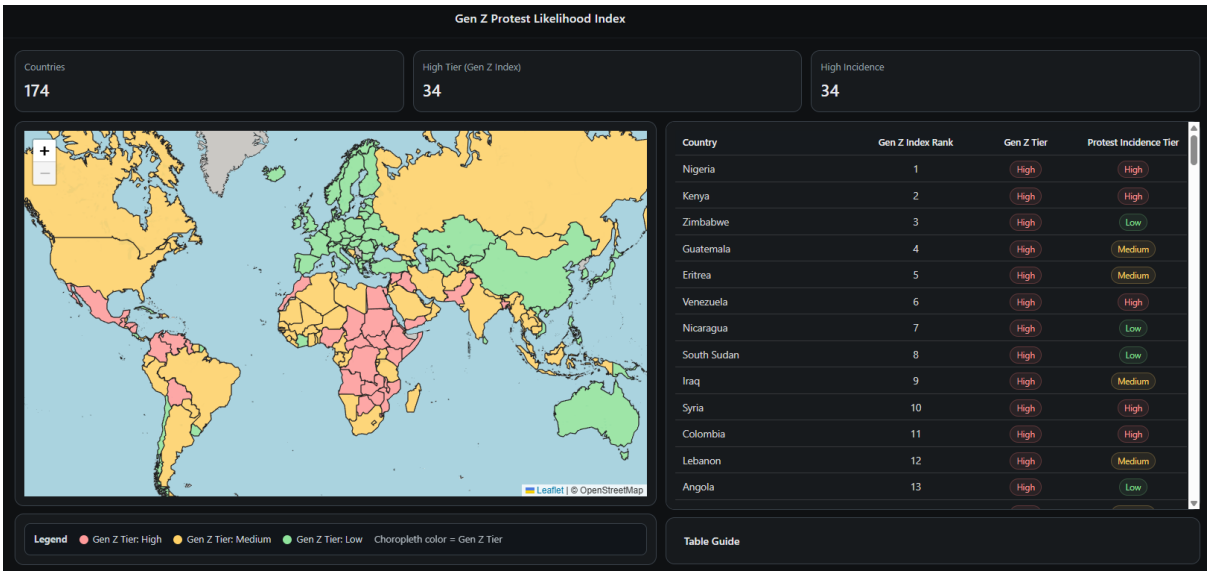
Building a Risk Dashboard With AI: A Practical Guide From the Gen Z Protest Likelihood Index

Ross Hill

Introduction

Dashboards have become a common output in security and risk work. They look authoritative and give the impression of control. Too often, however, they are built backwards. Data is collected first. Visuals are designed next. The decision they are meant to support comes last, if it comes at all. When my company Insight Forward built the Gen Z Protest Likelihood Index, the objective was not to produce a visually impressive product or demonstrate technical sophistication.[i] The aim was much simpler. We wanted a structured way to assess where youth driven protest activity was more likely to emerge and escalate, in a form that could support planning and judgement rather than replace it.

What follows is not an academic methodology and not a technical manual. It is a practical account of the process we used, written so that others can replicate it for different risk questions using their own data, tools, and constraints.



Country	Gen Z Index Rank	Gen Z Tier	Protest Incidence Tier
Nigeria	1	High	High
Kenya	2	High	High
Zimbabwe	3	High	Low
Guatemala	4	High	Medium
Eritrea	5	High	Medium
Venezuela	6	High	High
Nicaragua	7	High	Low
South Sudan	8	High	Low
Iraq	9	High	Medium
Syria	10	High	High
Colombia	11	High	High
Lebanon	12	High	Medium
Angola	13	High	Low

Screenshot of the dashboard in which users could choose a country to receive analysis about the risk from Gen-Z Protests.

Start With a Defined Requirement

The first step was to define the requirement clearly and narrowly. The index was not designed to predict the timing of protests or forecast specific events. It was built to assess likelihood and relative risk across countries in a way that could support comparative judgement. This distinction matters. A clear requirement sets boundaries. It determines what success looks like and what the dashboard should not attempt to do. In practical terms, this step can be replicated by writing a single sentence that answers three questions: What decision is this meant to support? Who will use it? What would make it useful rather than interesting? If that sentence cannot be written clearly, the dashboard should not be built yet.

Define What You Are Measuring

Before any indicators were discussed, time was spent defining what "Gen Z" meant in this context. This was not treated as a simple age bracket but approached as a behavioral cohort shaped by shared conditions: high digital fluency, economic precarity, low trust in institutions, and a tendency toward rapid online-to-offline mobilization. This distinction matters for repeatability. Dashboards fail when they rely on vague or assumed definitions that quietly shift over time. For anyone attempting a similar build, the lesson is straightforward. Define the population or risk actor in behavioral terms where possible and use demographics as context rather than explanation.

Look at Real Events First

Before imposing any analytical structure, recent cases of youth-driven protest activity across regions were examined. The purpose was not to catalogue every protest, but to understand patterns, such as what tended to trigger mobilization, how quickly activity escalated, what role digital platforms played, how states responded, and when disruption spilled into violence or broader instability. This step grounded the model in reality. Indicators that are not rooted in observed behavior tend to drift toward abstraction. Practically, this does not require exhaustive research; a focused set of recent cases is usually sufficient, provided the same questions are asked of each one.

Build Buckets and Indicators

Only after this groundwork was completed did the model begin to take structure. Observed patterns were grouped into a small number of logical risk buckets reflecting pressure, mobilization capacity, and constraint, including economic stress, political legitimacy and repression, social trust and grievance, and digital access and coordination. The aim was to sufficient capture the core dynamics influencing likelihood. Restraint mattered. Too many buckets create noise, while too few obscure meaning. Each bucket needed to be explainable in plain language. Within each bucket, indicators were designed to reflect likelihood rather than general dissatisfaction or instability. Many indices fail here by measuring grievance well but struggling to assess whether grievance translates into action. Indicators were therefore framed to capture pressure, capacity, and permissiveness, such as youth unemployment rather than general unemployment, protest policing thresholds rather than regime type alone, and digital platform usage rather than internet access in isolation. Each indicator had to meet a simple test: could a plausible case be made for why a change in this measure would affect protest likelihood.

Identify Data That Actually Exists

Once indicators were defined, the next step was identifying data sources that could realistically support them. This is where many dashboard projects quietly fail, designing indicators that cannot be measured consistently or updated over time. AI proved particularly effective at this stage by mapping indicators to existing datasets, suggesting viable proxies where direct measures did not exist, and highlighting trade-offs between coverage and quality. This reduced the risk of building a model that appeared coherent but could not be sustained. Source selection still required judgement. AI could surface options, but it could not assess political incentives, underreporting, or reliability in closed environments. The practical lesson was to design indicators and data together; if an indicator cannot be populated with reasonable effort, it should be reconsidered early.

Accept Gaps and Manage Bias

No dataset was treated as complete or neutral. Gaps were expected, proxy measures were accepted, and inconsistent reporting across regions was acknowledged rather than ignored. Rather than excluding imperfect data, the model was designed to absorb uncertainty. AI helped flag potential weaknesses by

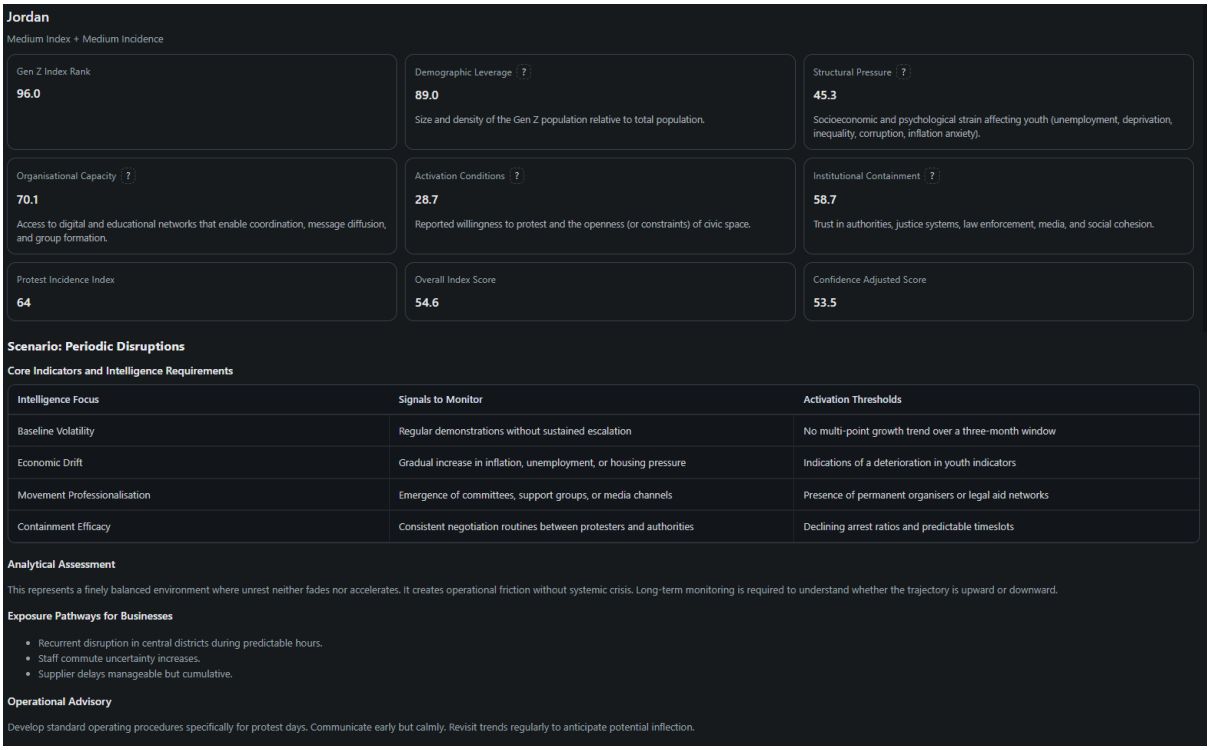
highlighting indicators with thin coverage and regions where data scarcity could distort results, after which adjustments were made manually. This step is essential for repeatability. A dashboard that relies on perfect data will not survive contact with reality.

Structure the Model Carefully

Only after indicators and data were settled did structuring and calculation begin. This involved normalizing indicators, testing different weightings, and ensuring that no single variable dominated the output. AI was highly effective in accelerating iteration and handling mechanical tasks with speed and consistency. It did not decide what mattered most. Weightings were reviewed manually, and outputs were sense-checked against known cases. AI supported the work, but it did not replace judgement.

Design for Use, Not Display

The dashboard itself was designed as a static decision-support tool, and this was deliberate. Static dashboards reduce complexity and force clarity, discouraging the illusion of real-time precision where none exists. Design principles were simple: one-screen comprehension, clear risk banding, minimal explanatory text, and visuals that support judgement rather than replace it. More interactivity does not automatically create more value. Dashboards should reduce cognitive load, not increase it.



Example of the information provided by the dashboard. In this example, Jordan is used.

Validate Against Reality

Before treating the index as usable, it was tested against recent protest activity. The question was straightforward: would this have helped flag elevated risk earlier or more clearly? Where the answer was no, the model was adjusted. This validation step is often skipped due to time pressure, yet it is one of the most important. A dashboard that has not been tested against reality is a presentation tool, not an analytical one.

Be Clear About What the Dashboard Can Do

Finally, boundaries were explicitly defined. The index was not designed to predict dates or trigger decisions on its own. It was meant to inform planning conversations, posture decisions, and comparative assessments. Dashboards without clear usage guidance tend to be overinterpreted or misused. Clear boundaries protect both the tool and the user.

Where AI Helped and Where It Did Not

AI proved most useful at the edges of the process. It accelerated definition and discovery, supported pattern exploration, handled technical execution, helped identify data sources, and surfaced blind spots early. Where judgement, context, and accountability mattered, it was deliberately constrained. AI did not build the index; it supported the people who did**.**

Conclusion

Building a useful dashboard is less about technology than discipline. Clear requirements, explicit assumptions, real-world grounding, controlled use of AI, and an honest treatment of uncertainty were what made the Gen Z Protest Likelihood Index work. Its effectiveness came from a structured and repeatable process, not technical complexity. That lesson applies well beyond this case. Dashboards should support thinking, not replace it.

Author: Ross Hill is the founder and CEO of Insight Forward, a geopolitical risk and strategic intelligence firm. He has two decades of experience in corporate and private security across multiple intelligence disciplines.

Endnotes

[i] Dashboard is available here: https://www.insightforward.co.uk/gen-z-index/

Practitioners’ Bookshelf

The Practitioner's Bookshelf is a dedicated section of *The Close Protection and Security Journal* designed to bridge the gap between theory, history, and real-world security practice. Rather than offering traditional academic book reviews focused on literature placement or scholarly debate, this section evaluates books through the lens that matters most to working professionals: what a practitioner can learn, apply, and internalize to become more effective in the field. Each review treats a book as a tool, case study, or framework, examining how its insights translate into decision-making, risk assessment, protective intelligence, leadership, and operational judgment across close protection, corporate security, and intelligence disciplines.

The guiding premise of The Practitioner's Bookshelf is that professional excellence is cumulative and cultivated over time. A serious security professional should maintain a personal bookshelf not as a display of credentials, but as an evolving archive of hard-won lessons drawn from history, strategy, failure, and adaptation. The books reviewed here may come from security studies, geopolitics, psychology, military history, true crime, or even literature, but each is assessed for its practical relevance to protecting people, organizations, and systems under real constraints. This section encourages readers to think critically, learn continuously, and build intellectual depth as deliberately as they build technical skill, reinforcing the idea that judgment, perspective, and disciplined thinking are as essential to protection as any tactic or tool.

Book Review: *Taking Mr. Exxon* by Philip Jett

Philip Jett's *Taking Mr. Exxon* is best read as an analytical case study in executive targeting rather than as a conventional true-crime narrative. The kidnapping of Sidney Reso, then an executive of Exxon, is historically notable because it involved a senior figure at a globally recognized corporation and prompted what contemporary summaries describe as one of the largest FBI kidnapping investigations in the United States since Patty Hearst. But the more operationally important point is that the incident's enabling conditions were not exotic. They were drawn from the routine architecture of executive life: predictable patterns, residential exposure, and institutional assumptions about what "high risk" looks like. In that sense, the book's relevance for security professionals lies less in the dramatic arc of the case and more in its implicit model of how motivated adversaries convert normalcy into access.

At the level of threat logic, the Reso kidnapping illustrates a recurring dynamic in targeted violence and abductions in which attackers win by controlling the "micro-terrain" where the protectee must be exposed, and by choosing environments where anomaly is socially camouflaged. Residential neighborhoods confer precisely that advantage. Many people move through them with plausible reasons to be present, and the behavioral baseline is diffuse enough that surveillance and rehearsal can occur without immediately triggering suspicion. A driveway or curbside transition also compresses time and distance. The protectee has limited options for evasion, the attacker's approach is short, and the engagement can be completed before help arrives or before bystanders interpret what they are seeing. As a result, the decisive operational contest is not between hardened perimeter and brute force. It is between predictability and preemption, whether the adversary can anticipate the executive's movements with high confidence, and whether the executive's protective system detects or disrupts hostile preparation before the moment of contact.

That observation leads to a larger critique that the book reinforces indirectly in its narrative. Many executive protection programs implicitly model risk as episodic and location-based, concentrating posture on travel, major events, and the corporate campus. The Reso case suggests that risk is often continuous and transition based. The highest-probability exposure surface is not the boardroom or the airport lounge. It is the repeatable seam between private life and movement, such as the walk to a car, the predictable morning habit, the short interval outside the house, the familiar route taken because it is convenient. A security program that is excellent at episodic posture but weak at transition control is structurally misaligned with the adversary's easiest path to success.

The book also functions as a practical demonstration of how hostile reconnaissance can be decisive even when it leaves few obvious traces. While publicly available descriptions and subsequent practitioner commentary on the case emphasize long-term planning by the perpetrators, the deeper point is methodological. Reconnaissance succeeds when organizations lack a disciplined way to translate ambiguous signals into action. Most real-world surveillance indicators are not cinematic. They are weak signals, such as a vehicle that appears twice, an unfamiliar person lingering, a service-provider pretext, a small irregularity in the environment that can be rationalized away. What distinguishes resilient protective systems is not omniscience. It is decision discipline. Effective executive protection treats surveillance detection as an intelligence problem with collection requirements, baseline mapping, indicator libraries, and escalation thresholds that are agreed in advance. Without those elements, observations degrade into anecdotes and warnings become "concerns," which become background noise, which become post-incident hindsight.

A further analytic contribution of *Taking Mr. Exxon* is the way it implicitly separates residential security into two interacting systems: the engineered environment and the behavioral environment. Many organizations understand the first system and underappreciate the second. Cameras, alarms, lighting, and access control are necessary, but they do not resolve the risk created by predictable behavior and solo exposure. An executive can live behind substantial physical measures and still remain operationally permissive if they keep rigid routines, perform predictable tasks alone, and treat the home-to-vehicle transition as inherently safe because it is familiar. Conversely, modest physical measures can be disproportionately effective if paired with behavior change and trained response actions. The book's underlying lesson is that residential security is a protective design problem that integrates deterrence, detection, delay, and response with human habit as the primary variable.

The narrative also provides a sharp window into crisis governance, which is where many corporate security programs fail even if their fieldcraft is strong. A senior executive kidnapping instantly creates a multi-stakeholder decision environment in which the victim's life, the family's welfare, corporate reputation, investor confidence, and public legitimacy collide under extreme uncertainty. In such conditions, the highest risk is not simply a bad tactical choice. It is organizational friction. Unclear authority, parallel communication channels, undocumented decisions, competing incentives, and a drift toward improvisation. Jett's reconstruction of investigative and organizational pressures highlighted that "response" is an architecture, not a reaction. Organizations that perform well in these scenarios have pre-defined roles, a single command structure, a disciplined interface with law enforcement, a family liaison function that is trauma-informed and operationally competent, and pre-arranged access to specialized expertise such as kidnap-and-ransom advisory support. When those elements are not designed ahead of time, the organization spends its most valuable hours building the airplane while flying it.

The book's relevance for executive protection professionals becomes even clearer when viewed through a "gray zone" lens of corporate risk, even though the incident predates contemporary hybrid-threat discourse. High-profile kidnappings are strategic events as much as they are crimes, because they can exert coercive pressure on institutions, not only on individuals. They force companies to make consequential decisions under public scrutiny, create internal psychological shock, and can generate second-order security effects such as copycat interest, threat inflation, and employee anxiety. In modern contexts, where digital ecosystems amplify narratives and where adversaries can harvest open-source data at scale, the link between executive vulnerability and corporate stability is stronger than it was in 1992. The Reso case thus reads as an early illustration of a durable pattern in which executives are symbolic nodes in corporate systems, and attacks on them can be designed to produce institutional disruption even when the immediate objective is ransom or leverage.

One of the most analytically important implications concerns how corporations model adversaries. Executive protection in many firms is still framed primarily around opportunistic criminality or localized threats. *Taking Mr. Exxon* supports a broader adversary model that includes organized, patient, project-managed targeting. The operational distinction matters because it changes what "good" looks like. Against opportunistic threats, visible deterrence and basic countermeasures may suffice. Against project-managed targeting, the defensive requirement shifts toward protective intelligence, adversary interdiction, and the reduction of routine-based predictability. The book's central event is a reminder that a capable adversary can treat the executive's lifestyle as a dataset and the residence as an operating environment to be engineered.

A more subtle but critical point is that executive protection depends on executive psychology and buy-in. The protective measures that matter most in residential environments often impose friction. They

challenge convenience, privacy norms, and self-conceptions of independence. The pressure to "live normally" is powerful, and many corporate cultures implicitly reinforce it by treating protection as an exceptional condition rather than a continuous practice. The book's power, for security leaders, is that it provides a narrative basis to reframe that conversation with leadership and boards. It demonstrates that vulnerability does not require recklessness; it can arise from normal, reasonable patterns that become legible to a hostile observer. That reframing is essential for building consent for the kinds of measures that are effective but culturally uncomfortable, including routine variation, two-person rules for exposed tasks, formalized residential assessments, trained household staff protocols, and sustained protective intelligence support.

For corporations, the strategic takeaway is that executive protection should be treated as an enterprise risk discipline that connects physical security, cyber exposure, communications, legal decision-making, and crisis management. The executive is an access point into the organization's reputation, continuity, and governance. *Taking Mr. Exxon* is a reminder that when the threat is focused and the victim is prominent, "security" becomes organizational performance under stress. The question a modern EP program must be able to answer is not simply whether it can provide close-in coverage at events. It is whether it can reduce predictability across daily life, detect hostile preparation early enough to matter, and shift the organization from normal operations into a disciplined crisis architecture without fragmentation. Read that way, Jett's book is less a story about a single crime and more a durable diagnostic tool for assessing whether an executive protection program is built for the threats it is most likely to face.

Book Review: *Inside Terrorism* by Bruce Hoffman

Bruce Hoffman is a leading scholar and practitioner in the study of terrorism and political violence, widely regarded as one of the most influential figures in modern terrorism studies. He is a professor at Georgetown University's Walsh School of Foreign Service, and he has long been affiliated with the RAND Corporation. Hoffman has advised numerous governments and security organizations, including U.S. intelligence and defense agencies, and has been deeply involved in policy-relevant research on counterterrorism strategy, insurgency, and asymmetric warfare. He is best known for his book *Inside Terrorism*, first published in 1998 and subsequently updated, which is considered a foundational text for understanding the evolution, motivations, and strategic logic of terrorist movements. Hoffman's work is characterized by its historical depth, analytic rigor, and practical relevance, bridging academic scholarship and real-world security decision-making, which is why he should be on every practitioner's bookshelf.

Hoffman's *Inside Terrorism* is best understood by corporate security professionals as a book about how violence is used to shape decision-making under conditions of uncertainty. Read through a private-sector lens, it functions as a strategic framework for understanding how terrorism operates as a form of coercive influence that often targets institutions indirectly, through perception, fear, symbolism, and organizational stress. Its enduring value for corporate security, intelligence analysis, and executive protection lies in how it disciplines threat perception and clarifies why companies, executives, and commercial systems are increasingly implicated in conflicts they do not control and did not choose.

One of the book's most practically important contributions is its insistence on distinguishing terrorism from ordinary crime, insurgency, or random violence.[i] Hoffman's argument that terrorism is inherently political and audience-driven has direct implications for how corporations assess risk. In private-sector environments, terrorism is frequently misclassified in two opposite ways: either overstated as an omnipresent existential danger that justifies indiscriminate security responses, or understated as a government-only problem irrelevant to business continuity. Hoffman's framework rejects both errors. Terrorism, as he presents it, is a method, not a fixed threat category. It becomes relevant to corporations when their people, assets, brands, or infrastructure can serve as leverage points in a broader influence campaign. Misclassification occurs when security teams focus narrowly on whether a company is the "target," rather than whether it is part of the adversary's signaling environment.

This misperception often leads to reactive security postures driven by probability rather than effect. Corporate leaders frequently ask whether an attack is likely, when the more relevant question is what consequences an adversary seeks to generate. Hoffman's emphasis on psychological impact over physical damage reframes this calculus.[ii] A credible threat, a disrupted executive itinerary, or an attack on an adjacent sector can produce coercive outcomes without direct contact. For corporate security leaders, the lesson is that terrorism risk must be assessed in terms of second- and third-order effects on operations, workforce confidence, regulatory scrutiny, and investor sentiment, not solely in terms of casualties or facility damage.

A central theme that translates cleanly into corporate security practice is Hoffman's treatment of terrorism as communication. Violence is not the message; it is the medium. The real objective is influence over multiple audiences, often simultaneously. As he writes, "One of the enduring axioms of terrorism is that it is designed to generate publicity and attract attention to the terrorists and their cause."[iii] For corporations, this insight is operationally decisive. Executives, employees, customers, governments, and the media all function as audiences whose reactions can be anticipated and shaped. When a commercial entity becomes

adjacent to a terrorist incident, the organization's response becomes part of the event's communicative arc. Overreaction can amplify fear and validate the adversary's narrative, while underreaction can erode trust and invite regulatory or reputational consequences. Hoffman's framework implicitly argues for disciplined response design that is coordinated across security, communications, legal, and leadership, with explicit attention to what behaviors the adversary is attempting to induce.

This audience-centric model is particularly relevant to executive protection. Senior leaders are not targeted solely because of personal vulnerability or wealth, but because they embody institutions. Hoffman's analysis helps explain why executives in energy, transportation, finance, technology, and media face persistent exposure even in jurisdictions with low baseline violence. The executive functions as a symbolic node through which coercion can be applied to a larger system. For EP practitioners, this reinforces the necessity of integrating protective intelligence with corporate risk analysis. Protection cannot be reduced to close-in security or travel logistics. It must account for narrative context, geopolitical signaling, and how an executive's visibility or movement patterns intersect with broader ideological or political conflicts.

Another area where *Inside Terrorism* is highly applicable, and often misunderstood, is Hoffman's portrayal of terrorist organizations as adaptive and strategic rather than chaotic or purely ideological. Corporate security teams sometimes treat terrorism as static, a known set of actors using known tactics in known regions. Hoffman's historical treatment undermines that assumption. Terrorist groups learn, imitate, and innovate, often faster than bureaucratic institutions adapt. His chapter "The Modern Terrorist Mind-Set: Tactic, Targets, Tradecraft, and Technologies" is especially apropos for this issue. For private-sector intelligence functions, this reinforces the need for continuous reassessment rather than fixed threat matrices. Indicators of change, such as shifts in targeting rhetoric, new operational partnerships, experimentation with delivery methods, or changes in propaganda tone, are often more valuable than lists of past attacks.

This adaptive quality also links terrorism to what is now commonly described as gray-zone competition. While Hoffman does not use that terminology, his analysis anticipates it. Terrorism operates below the threshold of conventional war, exploits ambiguity, and leverages deniability and asymmetry. In modern operating environments, terrorist activity increasingly intersects with criminal facilitation networks, online radicalization ecosystems, state tolerance or sponsorship, and broader campaigns of destabilization. For corporations, this means terrorism cannot be isolated from other risk domains such as cyber disruption, supply chain interference, disinformation, and political coercion. Hoffman's framework supports an integrated risk model in which terrorism is one tool within a spectrum of hostile influence, rather than a standalone phenomenon.

Where corporate security teams could misapply Hoffman's insights is by treating them as justification for maximalist security responses rather than strategic restraint. Recognizing terrorism as communicative does not mean every threat demands escalation. On the contrary, Hoffman's work implies that indiscriminate visibility, heavy-handed security theater, or poorly coordinated messaging can inadvertently serve adversary objectives. Another potential misapplication is overgeneralization: assuming that all ideologically framed threats follow the same logic or pose the same level of risk. Hoffman's historical analysis argues against this, showing that motivations, constraints, and capabilities vary widely even within ostensibly similar movements. Effective corporate security depends on discrimination, not generalization.

A final potential misunderstanding arises when private-sector teams extract tactical lessons without absorbing the strategic logic that underpins them. Hoffman does not offer playbooks, and attempts to turn

his work into checklists would miss the point. The book's utility lies in shaping how security professionals think about uncertainty, influence, and adaptation. It equips leaders to ask better questions: Who is the audience of the terrorist attack? What behavior is being coerced? How does this incident fit into a longer trajectory? Where might our response create unintended incentives? These questions are central to executive decision-making under risk and are directly applicable to corporate governance, crisis management, and protective strategy.

Viewed as a strategic framework, *Inside Terrorism* remains highly relevant to corporate security precisely because terrorism continues to function as a background condition rather than a discrete event. Corporations operate in environments where political violence, ideological polarization, and asymmetric threats are persistent features. Hoffman's work helps security professionals understand why resilience, judgment, and coherence across the organization matter more than any single defensive measure. For corporate intelligence analysts and executive protection practitioners, the book's lasting contribution is what it reveals about how organizations perceive, misperceive, and respond to coercive threats in contested political environments.

Endnotes

[i] Bruce Hoffman, *Inside Terrorism*, 3rd ed. (New York: Columbia University Press, 2017), 43-44.
[ii] Ibid, 206-207.
[iii] Ibid, 202.

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 or members of the editorial board with any questions that you might have regarding journal submission or content.