Private Sector Intelligence Careers:

Analyzing Job Titles and Professional Trends

Judit Gaspar, Maria Robson-Morrow, and Katherine Tucker

JANUARY 2025

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs
INTELLIGENCE PROJECT

Introduction

If an aspiring intelligence professional were to type "intelligence analyst" into a job search, what might they find? Traditional government intelligence roles are discoverable online through domains such as intelligencecareers.gov with reasonably standardized titles. However, the job search would also produce a wide variety of private sector roles. Some of these closely resemble traditional intelligence positions, while others bear little relation to intelligence.

The corporate world has a vast and growing array of intelligence and security roles that focus on geopolitics, risk, and security threats. These jobs are obscured under a bewildering array of terminology. The young aspiring intelligence professional would find a vast range of disparate jobs whose responsibilities range from analyzing threat actors to managing consumer pricing data. Roles listed as "intelligence" may prove to be purely economic or computer science positions, while other roles may prove to be classic intelligence positions without ever using the word intelligence. This poses challenges for students, young professionals, and former government practitioners looking to transition into corporate intelligence roles. Intelligence is professionalizing and evolving, as are the roles within it, and the array of jobs posted in this field have never before been systematically studied.

At the Belfer Center's Intelligence Project, we undertook a multi-year initiative to systematically track job postings in private sector intelligence, building a dataset of 425 intelligence postings. These positions appear in over 200 different organizations in multiple countries, reflecting the varied, international landscape of private sector intelligence. Our goal is to illuminate this landscape and to provide insight into skills and qualifications that private sector intelligence employers are seeking in their new hires. We also aim to encourage future research on an understudied domain that has implications for corporate security and national security.

Key Takeaways

1. **Private sector intelligence jobs have a terminology problem.** Many positions entitled "Intelligence Analyst" or similar have profoundly different profiles and responsibilities. Meanwhile, many positions do not have intelligence terminology in their titles but are quintessentially intelligence roles.

2. **While studying security or intelligence is valuable, there are many educational backgrounds that are conducive to intelligence employment.** Studying security or intelligence is a useful gateway into these roles, with 58% of job postings citing security as a useful degree, and 47% mentioning intelligence studies. However, there are many other appealing educational backgrounds with relevance in this space, from studying business to a myriad of other areas such as journalism, finance, and computer science, as well as the importance of developing critical thinking and communication skills. Furthermore, language skills can be a gateway to intelligence work, with the most frequently mentioned being Spanish, Arabic, French, and Russian.

3. **Government experience is less of a prerequisite than expected.** While having worked in the intelligence community, the military, or law enforcement is conventionally seen as an asset for corporate intelligence, the jobs data reveal a surprisingly low proportion of positions that actually mention this as helpful. A full 65% of the job postings made no mention of previous government experience, and only 2% specifically required prior government experience. This finding suggests a shift away from what historically had been a de facto job requirement. It continues to be an asset; however, the postings reveal a myriad of other backgrounds that can bring value to corporate intelligence.

Analyzing the Intelligence Jobs Landscape: Methodology

This project involved collecting positions in non-government entities (corporations and non-profit organizations) in which the majority of the role was related to security or geopolitical risk intelligence. Our team collected 425 postings from jobs websites such as LinkedIn and Indeed, the websites of intelligence vendors, intelligence email listservs, and professional contacts, ultimately collecting postings from over 200 organizations over 10 years, with the majority of jobs in the dataset being from the last five years (2020-2024).

Positions included in the dataset had to have intelligence responsibilities, regardless of job title. Settling on parameters for what constitutes an intelligence job is no easy task. The academic literature on intelligence has historically struggled to reach a common definition, both for government intelligence and private sector intelligence (Troy, 1991; Breakspear, 2013; Stout and Warner, 2019; Warner, 2019; Ard, 2022; Robson Morrow, 2022). Attempts are further complicated by the lack of professionalization and standardization in the emerging private sector intelligence field (Duvenage, 2021; Robson Morrow, 2022). For example, a job entitled "intelligence analyst" might have wildly different job responsibilities depending upon the company, some of which might encompass a true intelligence analysis role and others that might in reality be an administrative or data collection role.

Inclusion criteria:

1. To merit inclusion in the dataset, a job needed more than the word intelligence or intel in the title. A full 57% of the included postings did not include any intelligence terminology whatsoever.
2. The focus of this intelligence work had to be on security or geopolitics. Market and competitive intelligence are a distinct profession and not within the scope of this study.
3. The position had to include intelligence duties of some kind, such as analyzing data, cultivating sources, or synthesizing trends. If the responsibilities included intelligence and at least half of the working time was related to intelligence gathering, analysis, or managerial duties, the posting was included in our dataset.

Limitation: One limitation of this project is the exclusion of any job postings not in English. This means that the dataset is representative only of positions in English-speaking countries.

Data Analysis: Once a job posting qualified for the dataset, we mined it for several pieces of information. For each posting, we identified the required qualifications, preferred qualifications, job description, educational requirements, experience requirements, language requirements, and security clearance requirements. Once we had collected all the data, we aggregated the findings across the 425 postings to analyze the trends, with the following results.

Figure 1: Comparing Intelligence Analyst Jobs

The following table shows three verbatim job postings from the dataset.

Enterprise Threat Intelligence and Travel Security Manager	Senior Threat Intelligence Analyst	Intelligence Analyst, Recon
• Monitor OSINT, SOCMINT, and internal intelligence resources for known and potential threats to Team Member safety, company security, business operations, or reputation risks • Research, comprehend, and disseminate intelligence assessments on a variety of topics, ranging from geopolitical events, global terrorism and insecurity, natural disasters and pandemics, and other concerns related to crime and security in places of interest to [company] operations, in collaboration with Regional Security Managers and when activated, Crisis Management Teams. • Support the Executive Protection team's efforts with identifying, assessing, and monitoring POIs and GOIs that do or may pose a threat • Create timely, actionable, and visually compelling intelligence documents that aid leadership's efforts to inform and brief senior executives on critical security events • Develop policies and procedures that improve the overall security of [company] Team Members, whether at [company] sites or traveling domestically or abroad • Collaborate with [company] Global Security & Emergency Command Centers while monitoring and communicating about security or crisis incidents worldwide • Collect from Regional Security Managers and communicate changes in the travel risk profile of destination countries or risks specific to individual travelers • Liaise with [company] Travel and administer third party service providers' tools that support the program • Create and execute on meaningful metrics, KPIs, and OKRs that serve to drive the program and demonstrate value	• Provide input into development of security technologies. • Analyze and understand advanced cyber actors, capabilities, and techniques. • Analyze and understand exploit proliferation in gray markets. • Collaborate with security researchers to contextualize cyber threat intelligence for decision makers and work cooperatively to drive solutions. • Work with security engineers in designing innovative mitigations to cyber threats while preserving privacy, ease-of-use, and user experience. • Work closely with external partners in support of cyber threat intelligence activities. • Remote work, with occasional travel.	• Drive high levels of customer satisfaction, maintaining a strong sense of ownership over many customer relationships. • Work closely with the [company] Intelligence teams in performing reviews and coordinate RFI responses for threat intelligence requests • Understand the dark and deep web ecosystem; be able to properly convey analytical findings to customers • Be a strong voice for customers into the Intelligence and Engineering teams to improve the product and ensure that customer's feedback, feature requests, and overall satisfaction is conveyed and accounted for. • Plan and lead process improvement initiatives tailored to improve overall customer satisfaction with the [company] team.
This threat intelligence job is not a cyber job.	*This threat intelligence role mixes in cyber responsibilities.*	*This intelligence role strongly suggests a cyber role despite not using the term cyber.*

Trends in Private Sector Intelligence Opportunities

Years of experience: how many positions are entry level?

A relatively high percentage of the jobs in our dataset proved to be entry-level jobs, requiring 0-3 years of experience. For postings that did not require a college degree, 26% of postings asked for only 0-3 years of experience. For jobs requiring a bachelor's degree, that percentage rose to 38%. And, for jobs requiring a master's degree, it was 52%. These numbers signal a focus on entry-level roles, indicating opportunities for either new graduates or people looking to switch careers.

Non-government backgrounds: how important is government intelligence experience?

It has been common for decades for private sector intelligence professionals to transition from an intelligence agency, military, or law enforcement, with 57% of private sector professionals having that background. However, recent job postings tell a different story. A promising finding for those looking to break into the private sector intelligence space is the low percentage of jobs requiring a prior government, military, or intelligence community background. 65% of the job postings made no mention of previous government experience. Only 2% of job postings specifically required prior government experience, compared to 23% of job postings that required prior experience of some type (not necessarily government). The other 9% of jobs preferred prior government experience, but did not require it. Moreover, only 4% of the job postings required a security clearance.

Educational background and skills: what fields of study are considered useful?

Education is a critical component for those trying to secure a job in private sector intelligence. 67% of the jobs required a minimum of a bachelor's degree; another 5% required a master's degree. Unsurprisingly, the most popular backgrounds requested included security (58% of job postings), intelligence (47%), and business (35%). However, employers sought a myriad of other backgrounds as well, including international relations (22%), political science (18%), law enforcement (16%), cyber (12%), finance (9%), criminal justice (8%), journalism (7%), information technology (7%), and media (6%). Moreover, employers look for a wide range of skills that can be cultivated through a variety of disciplines, such as communication skills (62%), interpersonal skills (41%), analysis skills (41%), computer proficiency (26%), the ability to work independently (25%), and the ability to multitask (22%). Finally, foreign language skills can be a gateway to intelligence work; Spanish, Arabic, French, and Russian were the most desired languages in our dataset.

Key Implications

For students or young professionals new to the field of private sector intelligence, the trends above suggest a need for educated people with strong communication skills, analysis skills, and foreign language skills, and indicate that this is more significant than prior intelligence and security experience. While it is still immensely challenging to find and obtain these jobs, these findings present some indications of what employers are seeking in intelligence roles.

1. ***Widespread applications of intelligence techniques:*** These findings reflect the widespread application of intelligence tradecraft outside of government roles in the national security and intelligence community, providing tangible examples of how multinational corporations and humanitarian organizations employ legal intelligence collection and analysis techniques to mitigate security and geopolitical risks to their operations.

2. ***Employable hard and soft skills:*** Our findings suggest tangible actions that those interested in an intelligence job can take, including developing geographic or regional expertise, cultivating language skills (particularly in Arabic, Spanish, French, or Russian), and honing soft skills such as critical thinking and communication.

3. ***Varied academic backgrounds:*** The debate over whether intelligence should be offered as a college major is still unsettled. Our research on the private sector parallels Dujmovich's commentary on the public sector and the benefits and challenges of universities teaching intelligence. As Dujmovich argues, government intelligence agencies want analysts to be familiar with intelligence concepts; our dataset similarly shows that 47% of private sector job postings require candidates to have background in intelligence or be familiar with the intelligence process. On the other hand, as he notes, government intelligence agencies favor candidates with subject matter expertise or foreign language skills; we see the same trend in our private sector data, with a preference for political science, international relations, technical and science fields, cybersecurity, finance, criminal justice, and journalism.

4. ***Challenges in private sector intelligence employment:*** Lastly, our data points to some shortcomings in the private sector intelligence jobs market that can lead to challenges in obtaining employment.

    i. *Lack of standardization:* First, the variability in the job responsibilities and qualifications suggest a need for standards and cooperation across complementary professions such as Human Resources. Currently, job descriptions are written by benchmarking across comparable jobs, which, as shown by this research, are challenging to identify. Some jobs are intelligence without saying "intelligence." Furthermore, some use "intelligence" in the job description without it appearing in the title. HR is a key partner for developing more standardized and recognizable terminology, benefitting both employers and applicants.

    ii. *Barriers to entry:* Second, this variability may impose significant barriers to entry for young professionals by fostering confusing or contradictory messaging. The lack of consistency may cultivate information asymmetry between seasoned intelligence professionals and potential newcomers, wherein experienced professionals are able to better navigate the confusing environment and young professionals are deterred from pursuing a career in private sector intelligence.

iii. *Demand over supply:* Third, while, on the one hand, the proliferation of entry-level positions and jobs with general skill requirements (as opposed to niche skills) are positive trends for people looking to break into the field, on the other hand this may produce a prolific number of qualified candidates that makes it difficult for any single person to secure a job.

Figure 2: Comparing intel jobs without the name intelligence

The following table shows two verbatim job postings from the dataset.

Threat Monitoring Specialist	Senior Analyst, Global Security
• Triage global incidents by collecting information, analyzing, and assessing the incident based on Standard Operating Procedures and the Trigger Matrix, and issuing Awareness/Advisory alerts. • Conduct global threat monitoring and research according to defined parameters. • Develop and maintain a deep knowledge base of sources including OSINT, social media, client databases, sources and archives. • Quick to verify real-time news as it happens and be able to write a concise and accurate business reports to be distributed within minutes to key stakeholders. • Work closely with team lead, regional lead and other analysts for additional gathering, vetting, and review of information. • Support crisis communications process as events dictate. • Develop and maintain deep, current subject matter expertise of geopolitical and threat issues in assigned areas of responsibility in alignment with client risks and threat concerns/interests. • Regularly creates data visualizations to convey analytical information and insight relevant to client needs. • Successfully complete any other approved professional development and training relevant to project mission and job duties.	• Analyze and monitor global events and activities using specialist knowledge to determine, with good judgement, impacts on [company] operations with a strong analytical acumen. • Develop and disseminate security risk reports for locations where [company] operates. • Develop and disseminate political/economic/security risk reports on possible future countries of operation and exploration. • Daily monitoring of high-risk countries for security risk and, if necessary, circulate a special advisories. • Support the development and implementation of an open-source intelligence program, including daily monitoring. • Conduct Threat Risk Assessments as required. • Assist with the [company] travel security program. • Apply innovative research techniques and develop sources of information. • Handle search queries from other stakeholders in the business. • Use of [company] specific social media searching technology. • Use of [company] specific incident and investigations database platform. • Assist in the development of new tools for security analysis and reporting. • Provide due diligence of companies and individuals using specific software and traditional methods to flag potential high impact risk, such as sanctions or criminal concerns. • Support [company] unique Global Security Standardization Program through the collection of data and metrics from regional and site security management. • Serve on the GSSP audit team; conduct security audits of [company] locations to support program compliance. • Develop educational material for employees in the area of security risk. • Develop new tools to support site and global security management achieve their goals • Assist with investigations as needed. • Support other Global Security functions such as access control, development of security policies, and procedures.

Future Research

There is much more to learn from studying data on private sector intelligence employment opportunities. Future goals for this research include:

1. Cataloging enough job postings to see time trends and changes over time. We suspect that the state of the economy and the increasing prevalence of private sector intelligence jobs might shift the types of jobs in the field.

2. Comparing job qualifications to the profiles of candidates who were actually hired. We suspect actual hiring practices may not perfectly reflect the wording of job postings. Our team plans to interview hiring managers to assess the characteristics of the candidates that ultimately get hired.

3. Relating these findings to the academic literature on the professionalization of the private sector intelligence field to help build a foundational understanding of how the field is evolving.

The research team welcomes ongoing input from private sector intelligence professionals.

The **Intelligence Project** at the Belfer Center for Science and International Affairs seeks to build a new generation of intelligence practitioners prepared to serve in a rapidly changing world and to help future policymakers and intelligence consumers understand how best to interact with intelligence to gain a decision advantage. Building on multidisciplinary research at the Belfer Center, from history to geopolitics to emerging technologies, the Intelligence Project links intelligence agencies with Harvard Kennedy School researchers, faculty, and students to enrich their education and support public policy decision-making.