Ab intra: How Is the Private Sector Changing the Traditional Intelligence Tradecraft and Its View of It ?

Matthias Wilson

Intelligence Analyst & Intelligence Trainer at Corporate Trust Business Risk & Crisis Management GmbH, Munich, Germany.

In order to understand current and future trends in the European Private Intelligence Community (PIC), we must first compare the existing Intelligence Community (IC) in Europe with the IC in the United States. The PIC in the United States has a long history, mainly due to the large governmental intelligence body from which personnel is recruited and, most important, the willingness of the US government to outsource core intelligence tasks to private contractors. The United States Intelligence Community (USIC) has an estimated 854,000 personnel holding top-secret clearances and an undisclosed total amount of personnel. In Germany, for example, outsourcing core intelligence tasks to private contractors is rarely performed and the number of personnel in the governmental IC is approximately 20,000; thus, leading to a much smaller pool to recruit from. Furthermore, most German intelligence personnel are careerists in the German governmental IC, unlike the many short-term contracts in the USIC. The same applies to most other European countries as well. Therefore, intelligence personnel in the private sector in Europe, unlike in the United States, mainly consists of university graduates with no prior governmental experience.

Their range of different educational backgrounds creates a more diverse PIC in Europe, especially because those working in it are willing to share their knowledge and experience with a broader IC. This IC is defined as the community in which no matter what their professional background is, everyone with an interest in intelligence can participate. In the broader European IC context, members of governmental intelligence services are rarely found. Someone working for a government is restricted or less likely to join a public discourse on his or her tradecraft than someone working in the private sector or with no prior governmental experience.

The collaboration within the broader IC is one of the main reasons for the current evolution of intelligence tradecraft. In the past years, we have seen a large community of intelligence experts getting together on social media platforms such as Twitter. Tradecraft is discussed, new methods and techniques are shared, and this overall effort greatly enhances the possibilities of those participating in this virtual intelligence community. The crowdsourcing and community learning approach on social media is one of the keys to success and a process that will continue in the future. Discussions that started out on social media platforms are already moving to dedicated channels, e.g. on Slack or Rocket.Chat. Mostly open to public, these channels enable intelligence experts to specifically discuss and share their knowledge. Many of the contributors in this virtual IC perform intelligence work as a hobby and not as a profession, for example in the case of the recent uncovering of Donald Trump's flight to Iraq, coming from a plane spotter. Another good example depicting current trends in the broader IC[i] is the online platform Bellingcat, which relies on a crowdsourced approach to generate spot on intelligence analysis on recent events. Although Bellingcat does not conduct corporate intelligence, the methods they use are spreading to the PIC as well. It is needless to say that these developments are closely followed by the governmental IC, and new methods and techniques originally coming from the broader IC are also incorporated into their daily work as well.

Another trend in Europe is the fact that major corporations heavily rely on large professional services, such as the Big Four, to perform core intelligence tasks. As an alternative to the Big Four, corporations have also begun to establish their own intelligence analysis teams in Europe, rather than outsourcing tasks to small and medium-sized private intelligence actors. As mentioned previously, Europe does not have the same PIC history as seen in the United States, thus this explains the lack of reliable small and medium-sized private intelligence contractors. Rather than providing direct and actionable intelligence services, many European intelligence contractors are tasked with consulting and training these new corporate intelligence teams. While lacking the amount of hands-down actual intelligence work and investigation cases to sharpen their skills, private intelligence contractors in Europe themselves lean upon and actively participate in the broader IC activity on social media to keep on track regarding new developments in intelligence tradecraft.

In conclusion, not having its roots in the governmental IC has led to a PIC in

[i] The broader IC here refers to PIC, the virtual IC and the government IC

Europe, in which the center of gravity will not be found in small or medium-sized private contractors, but in the growth of intelligence teams in the larger corporations or the Big Four professional services. Additionally, cross-company and cross-platform communications, especially on social media, have led to a broader Intelligence Community that is willing to share and sometimes even collaborate virtually, noticeably providing a great benefit to everyone working in the PIC in Europe. This broader IC will continue to grow as well, and its crowdsourced intelligence will set standards for the future of the intelligence tradecraft.

Andy Lalinde, PMP

Sr. Strategic Intelligence Analyst | AS Solution North America, Inc.

What I have seen is a de-mystification and a convergence. When non-intelligence folks think of intelligence, Jason Bourne and Carrie Mathison are often top of mind. People assume that is just what I do because of the allure associated with intelligence, and often I find myself educating them on the fact that there is much more beyond covert field operations and classified information. I am not alone in educating others, and to our benefit the speed of change driven by the internet and related technology is facilitating this shift in perception. The amount of open-source information ranging from various news outlets, social media, mapping platforms, etc., has created a private sector need for individuals who understand how to collect, organize, and analyze information in order to present it to key business leaders. As a result, the prevalence of academic programs centered on intelligence has grown over the last 20 years.

Does this mean academia is cheapening traditional intelligence? No. If anything, the gap is converging the private sector need with government expertise, and traditional intelligence professionals are of growing value to the private sector for several reasons. One, traditional intelligence professionals are resilient problem solvers and understand how to sift through large amounts of disparate information to present a much clearer outlook for executive teams. Additionally, they are able to supplement various corporate security functions outside of intelligence due to their adaptability and versatility. Two, they understand risk and only need to adjust to a company's risk profile and appetite to become key contributors. Three, seasoned professionals who join a team often take on leadership roles developing junior intelligence professionals coming from academia. Real world problems are often the best education a junior analyst can have. Four, some multinationals require security professionals to obtain, possess, and maintain government clearances to work on certain projects. Lastly, networks are gold in the private sector, and the ability to build and maintain relationships are critical when addressing company problems.

Jason Moran, CFE, CPP

Jason Moran, CFE, CPP, has over 20-year experience leading intelligence programs in both the US public and private sectors, with a special focus on Asia.

Intelligence analysis in the private sector is not so much "changing" traditional intelligence tradecraft as much as it fosters an emerging subclass of intelligence analyst. In my view, after two decades engaged in both public and private sector intelligence, the "corporate intelligence analyst" is now a distinct, viable career option for those, generally speaking, wanting to apply research and analysis skills – typically on a global scale – in support of missions that keep people safe and operations secure and competitive.

While public sector intelligence analysts come in many flavors, at the core of the discipline we find a typical set of drivers and competencies: 1) a need to collect information (requirements, explicit or understood); 2) an ability to analyze that information (be it a threat, a problem, a dynamic, etc.); 3) a determination of the relevancy or impact of that analysis; and 4) the influence to spur change or response through reporting and stakeholder notification. We can now certainly apply that same "intelligence cycle" framework to the private sector intelligence analyst corps, though slightly different (though not necessarily mutually exclusive) underlying motivations might be at play. As a government intelligence analyst, I was often driven by patriotism, some "higher purpose" that ideally secured or even promulgated our way of life. In the corporate arena, which is frequently multinational and ultimately profit-driven, we turn to less ideological, more bottom-line focused -- but equally ambitious -- motivating concepts such as "Duty of Care" and risk mitigation.

Moreover, although costly satellites, complex human source networks, and other highly sensitive and technical methods remain key to the intelligence collection missions of governments and militaries, the exploitation of open-source information, spurred by the relatively rapid and ongoing evolution, availability, and sheer power of information technologies – to include social media platforms, big data link-analysis, and the near-instantaneous awareness of global events – is indispensable to both the public and private sector. For a corporation, open-source collection and analysis, done either internally or through third parties, is typically the most viable option to maintain situational awareness, or the path of least resistance in the rare instances where other collection methods might be available.

Done properly and comprehensively, private sector intelligence analysis is also potentially costly, time-consuming, requires specialized skills, and involves strategic planning. Up until now, incorporating an intelligence analysis capability in the private sector was an initiative mostly seen at large multinational corporations (MNCs). This started when physical security's Global Security Operations Centers (GSOCs) began dabbling in the monitoring of news sites, scouring for threat information relevant to office locations. Or maybe employee travel became seen as a risky and chaotic activity, which lead to basic traveler tracking. These MNCs saw the unique value the intelligence-heavy initiatives brought to their security programs.

Given that firms run smaller teams than government agencies, it is my view that the private sector is creating a more rounded and modern expression of the intelligence analyst, by necessity. The average corporate intelligence analyst in the role for, say, two years, is expected to know their company's operations and stakeholders, where employees operate and travel globally, the potential threats to those employees, where to find and how to exploit threat information, internal and external collection and reporting platforms and technologies, relevancy of intelligence to other security functions (executive protection, investigations, etc.), and how to communicate analysis and recommendations. In some cases, they also manage relationships with vendors, research and understand strategic geopolitical dynamics, and serve as the *de facto* innovator for the intelligence program. Private sector intelligence analysts need to carry out these duties often under stressful, volatile conditions and, more or less, maintain 24/7 availability. Public sector analysts tend be much more focused in the scope of their responsibilities and areas of expertise.

Yet, the private sector needs to mature more in its fostering of this new class of analyst. Intelligence analysts in any setting tend to be knowledge hungry - lifelong learning must be a common goal. Where government analysts often receive formal periodic classroom instruction, sometimes months at a time, training opportunities for intelligence analysts in the private sector are still seen as a luxury, an optional line item in a base intelligence budget that probably did not exist 10 years ago. "On the job" training is the norm. The desire for international travel is another professional goal for the typical intelligence analyst, and a tall order for a corporate security department budget, despite the potential added value of having the boots of an intelligence professional - often with regional expertise or language capabilities -- on the ground to carry out assessments and to consult with local stakeholders. An additional challenge is a paucity of advancement opportunities. Public sector analysts are able to rise through the ranks while remaining within the intelligence discipline. Most corporate intelligence analysts reach their firms zenith in five to ten years, and currently need to expand into other security functions such as investigations or physical security to rise further.

All of these dynamics are leading to the emergence of an impactful new class of corporate security professional, bringing both a unique set of skills and a unique set of professional needs. Firms that are fostering intelligence programs are reaping the benefits of a more robust security program: broader and deeper situational awareness, safer work environments, and increased competitive advantage. It is now up to the private sector to erect a more comprehensive career track for intelligence analysts, which has historically been seen only in the public sector.

Lawrence L. DeSouza

Retired USAF non-commissioned intelligence officer with 20 years' experience in Ground, air and space intelligence operations. Former DOD, DOS, DOJ liaison for counter-narcotics and counter-terrorism for joint and international operations at the US embassies in Colombia, Brazil and Angola. Former security operations and intelligence associate director for Merck & Co. Inc. Former Cybersecurity information systems security manager at USSTRATCOM. Currently SATCOM analyst for international satellite operations coordination for USSTRATCOM and SPACECOM.

The first hurdle to modern security is without a doubt the silos present in Physical Security, IT, and Cyber Security organizations. Security convergence is a subject of debate and in some cases a deeply dividing internal issue for organizations across industry and government. The failed defense against the terrorist attacks on 9/11 were the direct result of silos and divisions between law enforcement and intelligence agencies of the US government. Intelligence is a perishable commodity that is cultivated over long periods but is only actionable at the tactical level and in brief windows of opportunity. Long-term intelligence analysis makes tactical intelligence more agile and actionable. The resulting product from the long-term and short-term intelligence analysis is the catalyst for security convergence, and the missing element between industry and government combined security operations.

Allan Stoddard, Vice President and General Manager for Situational Intelligence Solutions at Verint, said: "Modern enterprises must focus on preventing risk to ensure long-term business continuity. And in today's environment, it is critical to combine physical security, IT functionality, operational technology, and cybersecurity efforts to help gain greater insight and drive actionable intelligence."[ii] But without the intelligence analyst craft, organizations in security and cybersecurity are inept to conceive actionable and unbiased intelligence, making all of the efforts of IT, security, and cybersecurity ineffective. While industry and government keep referring to "collaboration" and "information sharing" as being the solution to holistically defense, without the intelligence professional focusing effort, identifying threats, developing trends, and quickly accessing and distributing relevant data - all of this data gathering is nothing more than raw information without true power or immediate impact on operations.

But how to implement intelligence to the corporate environment? Leadership must understand how to direct and consume information gathering and analysis for solving business issues. Businesses must attribute financial reasoning to risk

[ii] Alan Stoddard, "Intelligence propels evolution within the global enterprise," February 21st, 2018. Available at https://www.securityinfowatch.com/access-identity/access-control/article/12399198/intelligence-propels-evolution-within-the-global-enterprise.

management, in other words, what is the Return of Investment to building an intelligence capability to a company? The challenge of intelligence operations in business is the same as in government. If an intelligence apparatus is working properly, very little attention is given to events that were stopped before they caused damage. So, the measurement of effectiveness is always that of potential cost to the organization. In the same token, if intelligence fails, the value of intelligence operations come to question, and intelligence is almost never measured against previous success. The value of intelligence and the subsequent security convergence must be appreciated as a constant need and as an investment in risk management. A business strategy must include security, cybersecurity, and IT considerations for a company to be successful in the age of information.[iii] Risk is an element of any good strategic plan; therefore, risk strategy must align elements of ownership and governance that clearly brings together the converged security and intelligence by assigning funds, appointing roles, prescribing responsibilities, and describing accountabilities to the business model. This is where the business model ends, and the intelligence life-cycle begins.

Intelligence in the corporate world does not differ from government; what differs are the methods of collection. Government uses collection overtly and covertly, while businesses are limited by methods that are within the boundaries of fair business. Not that corporate espionage does not exist. Corporate espionage does exist, but it comes with serious penalties and it is not the subject of this discussion. Business managers must be trained to identify intelligence requirements and to direct the collection to satisfy those questions. Business managers fail to recognize that the intelligence cycle requires constant guidance and direction and that once the information is processed and disseminated, few business managers actually know what to do with the product. This is why the involvement of business managers is so critical to the planning and direction of intelligence at the first step of the cycle.

Once collaboration and information sharing become possible, the intelligence life-cycle works appropriately - that is, the internal functions of a company benefit first from intelligence and converged operations. Investigative services immediately benefit from intelligence as executive and product protection become much more effective. But other elements such as cyber security and physical security also benefit from long-term threat analysis. As Daniil Davydoff, the manager of global security intelligence at AT-RISK, said: "By the nature of their work, intelligence analysts frequently look at strategic risks while investigative analysts (and so-called 'protective intelligence' analysts) are dealing with past or present operational risks. When these individuals

[iii] Diane Ritchey, "The Unstoppable Convergence Between Physical and Cybersecurity ," April 1st, 2018. Available at https://www.securitymagazine.com/articles/88847-the-unstoppable-convergence-between-physical-and-cybersecurity.

or teams are one and the same or working closely together, the lifecycle of a threat is more apparent. In other words, an organization can more easily see how a broader risk turns into a concrete physical or reputational threat."[iv] An example of the impact of intelligence analysis on security operations was that of my intelligence team's efforts to identify coordinated social engineering and fishing efforts by criminal elements attempting to attack both financial and IT stakeholders of a pharmaceutical company. At the time, we understood that we had multiple attempts worldwide to gather information on company structure and network disposition, but we could not bring together physical and cyber security divisions of the company to address this issue before the company suffered a debilitating attack from the NotPetya ransomware that cost the company $310 million dollars. If not for the silos, the first stage of the cyber-attack (which is information gathering) could have been deterred.

In the private sector, external collaboration and information sharing become empowered by intelligence. The greatest fears for intelligence communities is that information is misused. Methods and sources are critical for the continued success of government intelligence operations. That is not the case for businesses, open-source or shared information is the lifeline for combating criminal activity. Understanding and sharing the critical elements of information about a threat empowers the business community to resist and discourage further attacks. But most importantly, if the information is being processed and distributed by intelligence professionals, the chances of critical information being missed or information that should not be shared leaking is greatly minimized. The collaboration between the Department of Homeland Security (DHS), the Department of State (DOS), the Department of Justice (DOJ), and private security communities is the backbone for domestic and foreign protection of commercial interests of the Unite States, and if more organizations achieve a professional level of intelligence gathering, processing, and distribution, global security can be significantly, and positively, impacted.

The bottom line for security convergence and intelligence is the same bottom line for business: less risk equals more profitability. About 85% of businesses rated as "highly converged" in a study conducted by the Aberdeen Group[v] reported a reduction in physical security incidents over the prior year, 48% reporting a reduction in IT-related incidents, and 55% a reduction in non-compliance incidents. Intelligence professionals have an important place in the future of security because of the nature of the threats that are present in a connected world. The Internet of Things (IoT) is not an IT issue exclusively, it affects

[iv] Daniil Davydoff, "The Benefits of Integrating Intelligence and Investigative Analysis," January 8th, 2018. Available at https://www.securitymagazine.com/articles/88618-the-benefits-of-integrating-intelligence-and-investigative-analysis.

[v] "Logical / Physical Security Convergence. Is it in the Cards?," December, 2007. Available at http://www.neweraassociates.com/downloads/logic1.pdf.

industrial controls and facilities, Physical security is dependent of IT functions and automation, telecommunications and networks are vulnerable to physical security and social media exploitation. Criminal organizations are evolving with the speed of the internet and organized crime can hire organizations specialized in misinformation, hacking, social engineering, and malware attacks to deliver the full gamut of security nightmares to business. Security convergence is inevitable, and the private sector intelligence analyst is the glue that makes the breaking of silos and security convergence possible.

Anat Agron

Anat Agron works as a global security analyst for a major financial firm.

As my career progresses and my horizons expand, I more fully appreciate how far-reaching and all-encompassing the intelligence field is. Coming from the counter-terrorism (CT) world, my working knowledge of the field in retrospect was fairly limited in its scope. I was mostly familiar with threats of a physical and cyber nature; however, after starting a role in the corporate intelligence world my depth of understanding has grown exponentially and has been enriched by my exposure to tools and to other individuals in the field, and within the business.

I worked in CT for four years before assuming a role in the intelligence field as a global security analyst at a major financial firm. In CT, there is a certain rush one gets from decoding jargon and discovering new techniques that extremists use to circumvent restrictions implemented by social media platforms; something at which keyboard jihadists are rather adept. I enjoy the challenge and thrill of finding bad actors. This requires exercising my knowledge and research base alongside predictive techniques and intuition. While I was working exclusively in the CT field, I assisted multiple governmental authorities with my findings, which I have subsequently learned on several occasions has aided in foiling terror attacks and led to several arrests. I have found this work to be immensely rewarding. While my predominant interest remains in CT, I have learned that doing research for background checks, and conducting due diligence analysis on individuals and on companies can be similarly exciting should something incriminating turn up. Internal investigations, and background searches are skills, which I have recently acquired while working in the corporate world.

As my own technical skill-set grew, I could effectively keep tabs on the new platforms and methods jihadists used to disseminate propaganda and radicalize others. I recall the colorful Facebook and Twitter posts from five years ago, which flooded my feeds; jihadist fighters from around the world flocked to Syria as the conflict slowly spiraled out of control. Militants eagerly shared photos of their war booty, and the supposed fancy digs they inhabited or rather captured. After the so-called Islamic State was officially proclaimed in June 2014, militants and their supporters publicly went into overdrive, and unabashedly espoused their beliefs. At first, online supporters tested the waters, and over time, their postings evinced increasingly more radical views. Tracking the progression of radicalization, and extremist ideology's metastasization was important in predicting the challenges that lay ahead and was useful in understanding counter-strategies to combat jihadist rhetoric. In addition to grasping this trajectory, I maintain that understanding the minutiae of a topic, no matter how seemingly arcane, is helpful in gaining insight into a larger topic.

For example, during my CT work, I contributed to a report which was cited in The Washington Post, in which Al-Qaeda and the Islamic State's theological schism regarding the enslavement of women was a divisive topic in the jihadisphere. Such ideological rifts between Islamist extremist camps enhanced my overall understanding of the major jihadi players. I use this example to illustrate how possessing strong analytical skills can assist in understanding a broader topic.

My research in identifying radical elements and content has been of great value to major social media platforms, who admit that relying on algorithms to weed out radical content, is not fool-proof. At the end of the day, people cannot currently be replaced by sophisticated technology, and their role in monitoring platforms is still invaluable. Some of my discoveries have led to arrests, and fanning out a person of interest's network is useful to both authorities and to social media companies. On both encrypted applications, and on widely known social media platforms, I have tracked threats to private companies, military personnel, politicians, and to specific ethnicities. Many hours were spent in my office listening to various radical Western clerics around the globe preach their sermons, in order to grasp their worldview, and their grievances.

Discoveries I have made have appeared in The New York Times, The Washington Post, The Boston Globe, and the ABC television network news. After one particular find, I was asked to testify in court abroad, since my report had a crucial bit of evidence in a case against a terrorist. In addition to briefing social media companies, reporters, and academics, I have had the opportunity to brief members of the FBI, and current Secretary of State Mike Pompeo while he was a Congressmen on Capitol Hill.

I enjoy my current role, which has afforded me a fresh appreciation of the vastness of the threat landscape in the corporate world. My previous role has trained me to be swift and diligent in my work. I previously relied heavily on OSINT, which prepared me well for my current job. I currently draw data from a wider array of intelligence tools and publications to assist me with monitoring and analysis, since I am tasked with tracking a much broader area. Honing anticipatory skills is crucial in the counter-terrorism field, as it is in the corporate world. For example, severe weather and natural disasters can impact assets, personnel, and offices, but being sufficiently prepared, and having a resiliency plan to help a business continue under difficult circumstances relates to techniques I developed in my initial skill-set. In corporate security challenges of various natures are inevitable; my job involves both mitigating risks, and also working to find solutions to problems once they occur.

Having a sound understanding of geopolitics is quite useful in threat forecasting and in assessing risk to the corporate world. Previously, for instance, I was well versed in understanding what various rebel groups and factions desired as their end goal in the Syrian conflict. It is very important to possess a multi-dimensional and nuanced comprehension of a topic, which is something I strive to do in my current role. Discerning bias and developing an understanding of both fiscal and political motives of governments, or groups of people, is critical to assessing an investment, or decision for a business or client. In addition to geo-political savvy, understanding the risk of cyber threats, and conducting due diligence are skills that transfer and prominently apply to maintaining a safe business environment. A well-rounded skillset can pave the way to success for a private sector analyst.

The common denominator in both my previous role and my current role is safety and security. In addition to physical structural damage, it is key for the corporate world to focus on potential economic damage, which often goes hand-in-hand and overlaps. Safety is a multi-faceted undertaking and understanding the wants, needs, and capacities of a business, as well as its physical and organizational structure is vital in maintaining its security.

Moreover, I would be remiss if I failed to underscore the importance of sharing intelligence tools and platforms which can facilitate our roles. Previously, my work would first be shipped off swiftly to clients, or the relevant governmental authorities, and later to the media, so that the public could benefit from this shared knowledge. I have found that attending conferences, and consulting with peers in my industry, and trading notes on the best tools, or security vendors has been of great help For example, I just recently attended my first OSAC conference in Washington DC, and the presentations put on by panelists from the corporate world were extremely engaging and informative. Devoting time to learn from others in this niche field in the corporate world is invaluable; our commitment to safety is what bonds us.

Additionally, I have found that identifying a lacuna of knowledge in an area, and recognizing one's weakness, is a strength if an analyst is pro-active and is eager to consult the appropriate professionals in the relevant fields. For example, seeking advice from medical experts regarding a health pandemic or possible health risks associated with travel, is essential in safeguarding the well-being of a company's employees. I have learned the utility of conferring with colleagues and other professionals both inside and outside of my field leads to success. During my time working in the intelligence field, I have learned that the scope of the field is quite broad, and I appreciate that my initial skill-set outside of the corporate world can complement the one needed for this field. Working in this sector can be like piecing a puzzle together. There are many niche areas in intelligence, and successful professionals strive sort through this wealth of information, and discern how to best utilize the sources, and tools available at their fingertips with the end goal of protecting a business. Understanding the wants, and needs of a business, however, can arguably be just as vital as mitigating risks.

I see the intelligence tradecraft becoming increasingly important and indispensable in the private sector. Firstly, more established brands with a large global presence appear to be relying on specialists who can utilize intelligence and analytic tools to mitigate risks in an increasingly complex world. Threats from the physical and cyber realms are constantly mutating, and success is largely reliant on understanding these threats, and being able to prevent them. Secondly, the corporate world does not exist in a vacuum, and having someone on-hand to understand geo-political developments and their potential impact to a business is vital.