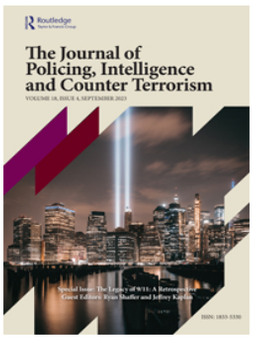

Routledge
Taylor & Francis Group

Journal of Policing, Intelligence and Counter Terrorism

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rpic20

Intelligence warning in the corporate sector: the 2013 In Amenas terrorist attack in retrospect

Michael J. Ard

To cite this article: Michael J. Ard (26 Oct 2023): Intelligence warning in the corporate sector: the 2013 In Amenas terrorist attack in retrospect, Journal of Policing, Intelligence and Counter Terrorism, DOI: 10.1080/18335330.2023.2274614

To link to this article: https://doi.org/10.1080/18335330.2023.2274614

JOURNAL OF POLICING, INTELLIGENCE AND COUNTER TERRORISM
https://doi.org/10.1080/18335330.2023.2274614

Intelligence warning in the corporate sector: the 2013 In Amenas terrorist attack in retrospect

Michael J. Ard

Johns Hopkins University, Washington, D.C., United States

ABSTRACT

The 2013 terrorist attack at the In Amenas, Algeria gas production facility killed 40 innocent people and shook the corporate security industry. Analyzing this event raises important questions about the nature and limitations of intelligence warning for private industry. Corporate security intelligence has been adopted by many companies that desire a 'decision advantage', but in this case, it failed to foresee the attack. A seminal report on the attack produced by Statoil (now Equinor) encouraged numerous changes in how companies should protect themselves against severe security threats. One conclusion was that in uncertain and dangerous environments, intelligence cannot be relied upon to reduce uncertainty and provide adequate warning. The Statoil report acknowledges that the joint venture likely would not have gotten the intelligence necessary to warn of an impending attack. The core business is not necessarily focused on the changing threat environment. In this case, even more accurate 'tactical' intelligence might not have led to a timely evacuation. Moreover, as the Algerian Army's failure to prevent the In Amenas attack reveals, corporations' risk assessments cannot ignore the severe limitations of their host country security institutions. This case study raises some concerns about overvaluing corporate intelligence's effectiveness in high-risk security environments.

ARTICLE HISTORY
Received 16 June 2023
Accepted 18 October 2023

KEYWORDS
Terrorism; warning; intelligence; Algeria; oil and gas industry

On January 16, 2023, near the desert town of In Amenas, Algeria, the People's National Army Chief of Staff and the CEO of the national energy firm Sonatrach commemorated the ten-year anniversary of a terrorist attack that killed 39 foreign oil and gas employees and one local security guard at the Tiguentourine gas plant. Senior executives from BP and the Norwegian state energy company Equinor also attended the solemn event (Algeria Press Service, 2023).

The 2013 In Amenas terrorist attack shook the oil and gas industry. At an industry conference soon afterward, one security professional described it as the industry's 'Deepwater Horizon', referring to the 2010 disastrous offshore blowout of a BP-owned oil rig. This large-scale attack appeared to signal a new jihadist focus on oil and gas infrastructure. It also led to an important report commissioned by the Norwegian state energy company Statoil (now Equinor) on the lessons learned from the attack, which included

CONTACT Michael J. Ard mard@jhu.edu 6014 Coral Springs Court, Katy, TX 77494, USA

the need to develop better risk analysis and a 'culture of security' (Statoil, 2013). Neither Statoil nor its joint venture partner BP, claimed to have any prior warning of the deadly attack.

Ten years later, reviewing what we have learned from this attack seems appropriate. In the years that transpired, how has the attack changed the oil and gas industry's approaches to intelligence-led risk analysis? Would better corporate security intelligence have prevented or mitigated the attack? What does this event tell us about the effectiveness of corporate security intelligence? The candid and thorough Statoil report has rightly earned praise from industry analysts and anyone interested in the challenges of working in high-risk environments. However, it also raises some important questions about corporations' natural blind spots regarding host government, their security institutions, and the efficacy of corporate security intelligence itself. Due to Statoil's commercial arrangement with Algerian government, the report avoids analyzing the performance of the People's National Army before and during the attack, even though, as we will see, it was the crucial variable to understanding this tragic event.

This paper explores how the In Amenas case reveals the ongoing challenges of making such intelligence effective, especially in dealing with hard-to-predict events. For this retrospective on the In Amenas case, the author has reviewed the available literature and interviewed several industry experts with special insight into the impact of this event. Some of these experts also have deep regional experience, including prior service in the U.S. intelligence community. Unfortunately, given the continued legal sensitivity of the In Amenas issue, some security professionals declined to comment for this paper. As one remarked that, even after ten years, the subject is still 'raw'. In a few cases, interviewees requested not to reference their names, although they provided valuable insight, which is included here.

To undertake this retrospective look, this paper will review the context of the attack and its aftermath, how some companies in the oil and gas industry responded to the attack, and how this case study sheds light on the role of intelligence in corporate security. Throughout this paper, 'corporate intelligence' refers to security-focused proprietary information on threats that potentially affect a company's people, assets, operations, and reputation.

The literature on warning intelligence is extensive, but it focuses nearly exclusively on national security threats (See Gentry & Gordon, 2019; Grabo, 2002). Yet the literature can apply to warning issues for corporate entities in difficult environments. The purpose of warning intelligence, as stated by Gentry and Gordon – 'communication to senior national decision-makers of the potential for, or actually impending, events of major significance to national interests and recommendations that leaders consider making policy decisions and/or taking actions to address the situations' – can apply to senior corporate managers with only slight modification (Gentry & Gordon, 2019, p. 12).

However, these managers cannot always expect timely and reliable information. Intelligence failure literature likewise is robust and the emphasis on causation varies; but one influential study, which is relevant to this research, emphasizes that lack of intelligence and policymaker decision-making often are the decisive causes of failure (Dahl, 2013). Dahl notes that even if 'strategic' intelligence of a general warning nature is available, it often fails to move policymakers to action. In contrast, more useful and precise 'tactical' intelligence on an impending threat typically is difficult to acquire. (Dahl, 2013, pp. 21–22).

For example, strategic intelligence warned of an impending terrorist attack before 9/11, but the lack of tactical intelligence arguably prevented an adequate response.

Corporate security must design their warning systems with this lack of information in mind. As Roberta Wohlstetter noted in her classic work on the Pearl Harbor surprise attack, lack of information must be part of the planning (Wohlstetter, 2002, 401). Likewise, in considering the principles of warning systems, Bracken notes plans must account for lack of warning intelligence; prudent organizations cannot bet on getting the right information at the right time (Bracken, 2008, p. 30). As will be demonstrated in the In Amenas case, the security system failed to adequately compensate for a dearth of intelligence, relying too heavily on static defenses and standard risk assessment procedures that failed to account for a changing threat environment.

Background on the security environment before the attack

The oil and gas industry has long experience operating in Algeria's security environment. During the civil war period (1991–2002), the companies took special precautions against terrorism. For instance, during the 1990s, companies led by Bechtel Corporation managed a common security operations center in the energy hub of Hassi Messaoud. Threat reporting was integrated, with the US Embassy in Algiers cooperating, and the companies invested in aerial surveillance and reconnaissance around their facilities. According to former US diplomatic security officer Scott McHugh, although successful, these measures were expensive and not sustained for long after the civil war ended (McHugh personal interview, March 2023). In 2013, the security around the In Amenas gas plant did not include aerial surveillance.

The large Tiguentourine plant outside In Amenas involved a production sharing contract between Sonatrach (51% ownership of the venture) in partnership with BP (24.5%) and Statoil (24.5%). The two junior partners in this joint venture had much different experiences working in North Africa. BP had a long history of operations in the region; Statoil was a newcomer to this difficult security environment. However, Statoil recognized Algeria as a high-risk environment when it entered the production-sharing agreement in 2003 (Statoil, 2013, p. 5).

Even in surprise attack scenarios, the victims have been known to take some precautions before the attack, which also was the case here. Risk assessments by the commercial partners regularly assessed the security situation in Algeria. The facility's security management plan was updated twice a year, scored based on a low, medium, high, and very high threat level, and reviewed weekly. The management plan included the highest risk score on terrorism. But, as the Statoil report notes, security was only one of 12 indicators that made up the overall risk assessment (Statoil, 2013, pp. 48–52).

The In Amenas plant featured layered protection with outer and inner security, designed to deter or defeat a terrorist attack. The People's National Army garrisoned in In Amenas 45 kilometers away, took charge of the wider military exclusionary zone around the facility and monitored a wide desert area. A paramilitary force – the Gendarmes – took control of the immediate surroundings, including transportation, checkpoints, and security patrols. The Gendarmes also operated a station at the facility. The job of both military forces was to deter, detect, and respond to a terrorist attack inside the facility itself. Unarmed guards manned the facility's gates. On paper, the security

appeared adequate for the threat level. As the Statoil report noted, 'There was a profound belief among everyone involved that the military would protect against the threat of a large terrorist attack' (Statoil, 2013, p. 69).

The Algerian People's National Army (PNA) and the intelligence service had successfully protected the nation's oil and gas infrastructure during the civil war against various Islamic extremist groups, earning a reputation for both efficiency and brutality (McHugh personal interview, March 2023). The KGB-trained intelligence service DRS (Département du Renseignement et de la Sécurité) penetrated the Armed Islamic Group (GIA) and other Islamic insurgencies and probably manipulated their behavior (Roberts, 2007). One terrorism analyst even believes the GIA was a false-flag operation created by the DRS (Schindler, 2012). Later, the DRS would ensure the GIA offshoot, the Al Qaeda in the Maghreb (AQIM), were pushed into Mali. Moreover, rumors have persisted that the DRS kept ties with key terrorist leaders in the AQIM and its offshoots (Riedel, 2013). The DRS's murky ties with the Islamic insurgency in Algeria and its failure to anticipate the attack remain significant gaps and points of controversy in the In Amenas story.

The PNA's pressure campaign fragmented the Islamic terrorists and the predominant group that emerged was the Salafist Group for Preaching and Combat. In 2007, it would become AQIM, a small terrorist band whose connection to Al Qaeda, RAND analysts believed, was more aspirational than real (Chivvis & Liepman, 2013). Its most prominent member was the smuggler and kidnapper Mokhtar Belmokhtar, who had long been on the CIA's radar in his base in northern Mali, where an attempt to kill him in 2003 failed. Belmokhtar led a breakaway band from AQIM called Mourabitoun – the Masked Ones.

After Al Qaeda's deadly attack on 9/11, the fear emerged that terrorists would aim to disrupt global oil supplies by attacking oil infrastructure. In 2006, Al Qaeda sent suicide bombers to penetrate the gates at Abqaiq, Saudi Arabia's huge oil processing facility. That same year, the Movement for the Emancipation of the Niger Delta (MEND) launched a 'total war' campaign against Nigeria's oil industry, sabotaging pipelines and kidnapping oil workers, which led to a 20 percent decline in national oil production (Luft and Korin in Fukuyama, 2007, 71). Attacks on pipelines were ubiquitous during the Iraq war (2003–2011).

However, in Algeria, the overall terrorist situation after the civil war became more favorable. Only 11 attacks on oil and gas infrastructure occurred between 2005 and 2011 (GTD), and none in remote locations (Statoil, 2013). Algerian officials overestimated their success against AQIM. In 2011, the interior minister declared that AQIM had lost its ability to cause harm in Algeria, although some attacks continued in the Kabyle mountains, east of Algiers, where AQIM was based (Arieff, 2013). With success against the terrorists, Algeria's counterterrorism efforts and energy companies's response experienced a letdown in attentiveness. Surveillance flights stopped, and the better army units withdrew to their barracks. As McHugh noted, the PNA also never successfully achieved domain awareness over the smuggling routes used by criminals and terrorists in the vast desert areas in southern Algeria and the eastern border with Libya (McHugh personal interview, March 2013).

Nevertheless, Algerian authorities and the In Amenas joint venture were not completely complacent. In 2009, concerned about suicide attacks by AQIM near Algiers, the joint venture decided to improve security. Facilities were upgraded with double

fences, vehicle barriers, CCTV and alarm systems, although implementation was not completed (Statoil, 2013, p. 38). After the 2011 Arab Spring, the PNA strengthened its presence on its borders, which may have led to a false sense of security on the part of the joint venture.

The situation worsened in 2012 when a coup in Mali and the overthrow of the Qaddafi regime in Libya created power vacuums in vast parts of the Sahel region. That year, a splinter group of AQIM conducted suicide attacks on Saharan police bases in Tamanrasset and Ouargla (Lebovich, 2016). In the region, 42 western tourists were targeted by the Belmokhtar group for kidnapping (Lacher, 2012). In November 2012 state-run newspaper claimed Algerian intelligence discovered a terrorist cell that planned to bomb oil facilities (Nield, 2014). According to BP Director of Global Intelligence Paul Kolbe, the company understood the security situation had worsened, with neighboring Libya destabilized and Mali hosting terrorist groups (Kolbe personal interview, Feburary 2023). Despite this growing awareness, the companies made no provisions for improving their access to actionable, tactical intelligence.

Facing a rising threat environment, Algeria's state-owned energy company Sonatrach took over security at the gas plant and acted as the sole intermediary with the Algerian Army. Shortly thereafter, Paul Morgan, the now-replaced security liaison at the gas facility, informed BP and Statoil members of the joint venture that security was slipping badly at the compound and that he could no longer guarantee their safety, according to a UK media report (Gatton & Olden, 2013). According to former CIA operations officer and security expert Charles Goslin, Morgan noted that anyone could walk in and around the perimeter of the facility and residential compound without being challenged by the unarmed guards (Goslin mail correspondence, February 2023). He also warned the joint venture partners of the potential threat of a high-impact terrorist event (Statoil, 2013, p. 57). Meanwhile, a lengthy contractor strike at the gas facility raised tensions between plant management and the local workers. Kolbe noted that his intelligence unit of three analysts tasked with a broad view of risk assessment had no knowledge of the labor issues at the plant (Kolbe personal interview, February 2023).

Apparently unknown to In Amenas security, in late 2012, Belmokhtar announced his intention to strike western interests with his band renamed 'Those Who Sign in Blood' (Statoil, 2013). Another group involved was 'Sons of the Sahara for Islamic Justice', who allegedly involved local drivers in the gas complex (Armstrong, 2014). Libyan groups reportedly joined forces with Belmokhtar (Gilpin, R. et.al., 2013). According to the Statoil report, Belmokhtar probably intended to take hostages and blow up the plant (Statoil, 2013, p. 40). Algerian authorities claimed the attack was planned and launched from Libya with supporters inside Algeria, possibly motivated by a lack of access to energy sector jobs (Lebovich, 2016). Some experts believe that Belmokhtar, who had a falling out with AQIM leadership, sought purely political aims in the attack. Later in May 2013, his forces would stage two bloody attacks in Niger against an army base and a uranium mine, neither of which had an economic rationale (Lacher & Steinberg, 2015). According to former US intelligence operative and security executive Lance Fitzmorris, other reports claimed the jihadists planned to capture 100 foreigners to sell ransom or to kill them (Fitzmorris personal interview, February 2023).

The attack itself

At approximately 5:30 am on January 16, 32 terrorists of Belmokhtar's organization attacked the gas plant. They first attacked a bus loaded with expatriate workers heading back to In Amenas. While some engaged the Algerian gendarme guarding the bus – Paul Morgan was killed in the lead vehicle – the rest assaulted and breached the main gate and entered the workers' quarters, taking hundreds of hostages. The terrorists released the Algerian nationals and, apparently with inside knowledge, began searching for some expatriates by name (Fitzmorris personal interview, February 2023). An alert guard set off the emergency alarm; upon hearing the alarm, the employees sheltered in place, making it difficult for the terrorists to find many of them. The terrorists communicated with BP leadership and appeared to request a ransom for the hostages and safe passage to Mali. The terrorists demanded an end to the Azawad military campaign in Mali by French forces and the release of prominent convicted terrorists from prison (Barak, n.d.). Belmokhtar did not participate in the attack itself, which suggests he doubted it would succeed.

The DRS's special forces spearheaded the response to the crisis. DRS deputy chief Bashir Tartag himself led the assault on the terrorists at the plant and followed the intelligence organization's usual 'eradicationist' strategy (Riedel, 2013). On the second day, special forces engaged the terrorists with helicopter gunships. Demonstrating that Algerian public authorities had little confidence in its garrison near the site, the Army relied on special forces from Algiers and not the troops at the In Amenas barracks, for its main response to the terrorist attack. The terrorists killed some hostages outright and used others as human shields on their vehicles. They retreated to the main operational section of the plant and planted bombs on one of the gas trains. The Army, refusing to negotiate, continued to attack the terrorists. When the siege ended on January 19, three terrorists had been captured, 29 had been killed during the attack, and 40 workers also perished. Statoil lost four employees in the attack, and BP lost seven. The Japanese energy services firm JGC suffered the worst casualties, losing 17 employees, of which 12 were Japanese nationals (Statoil, 2013, i). One of the three main gas trains of the production plant suffered heavy damage from explosives. Algerian authorities undertook some international criticism about its draconian response, but in fact, it was unclear whether the terrorists had any intention of releasing the hostages. Some hostages probably were killed by the army's lethal actions.

How intelligence failed

Was the attack an intelligence and risk analysis failure on the part of the companies involved? The literature on intelligence failure is varied, with many root causes identified. As Dahl emphasizes, intelligence failure tends to result from two main factors: (1) lack of information and (2) policy decisions (Dahl, 2013, pp. 2–3). Both factors appear particularly relevant in the In Amenas case. A band of thirty well-armed terrorists had crossed hundreds of miles of desert and entered the country at the Libyan border, slipping past Algerian army surveillance. The Statoil report squarely puts the blame on the military's shoulders.

> Prevention of and protection against terrorism are the responsibilities of states. Statoil and the In Amenas joint venture trusted that the military would deter or detect and respond to any terrorist threat, and the border security would prevent it from getting close to In Amenas. For this particular attack, this could have happened at the border, in the outer military zone, or in the security zone provided by the gendarmes. (Statoil, 2013, p. 4)

Part of the joint venture's risk assessment failure was its inadequate assessment of the PNA's performance and capabilities. An in-depth analysis of the Army's policies and weaknesses, which were known to close observers, might have led to different conclusions about its ability to respond. There were good reasons to question the companies' optimistic assessment of military protection, especially given the Algerian security services' opaque relationship with terrorist groups and counterterrorism policies. Likewise, the Army's heavy-handed responses to some terrorism incidents, particularly when AQIM kidnapped several French Trappist monks in 2006, foreshadowed its response to the hostage situation at In Amenas (Leveque, 2009). Sensitivities about including a sharp critique of the host country's security forces as part of a risk assessment probably contributed to this.

The surprise attack reminds us of Judge Richard Posner's gloomy conclusion in his critique of the 9/11 Commission report, 'it is almost impossible to take effective action to prevent something that hasn't occurred previously' (Betts, 2007). The Statoil emphasized the 'unprecedented' nature of the attack but also doubted that intelligence would have provided warning. 'Companies cannot expect to receive clear tactical warnings, with specific information about where, when, and how a potential adversary may attack' (Statoil, 2013, p. 4). However, the report acknowledges that none of the partners in the joint venture conceived of a scenario where a large force of armed attackers reached the facility. Echoing the famous conclusion from the 9/11 commission report, the Statoil cited a 'failure of imagination' in that the company had not foreseen a scenario of failure of the outer security as part of its emergency planning. The Statoil authors judged that prior warning signs did not represent a clear tactical warning (Statoil, 2013, p. 4).

In fact, such a destructive attack had never occurred against an oil and gas facility. But terrorists' groups in the region had shown an ability to carry out complex attacks in the past. Analysis by terrorism expert Scott Stewart pointed out that Mokhtar Belmokhtar's group attacked a Mauritanian army base in 2005, killing 15 soldiers. His group also demonstrated impressive range by capturing hostages throughout the Sahel region (Stewart, 2013).

As Bracken notes, literature on intelligence failure rarely mentions management as a key performance indicator for warning, but it was a crucial factor here (Bracken 2008, p. 21). In Amenas was a tactical intelligence failure because there never was an integrated information system that fed timely information either via surveillance or human intelligence from the field to headquarters (McHugh personal interview, March 2023). The Statoil offers no evidence that the joint venture attempted to implement such a system, and former chief of intelligence for BP Paul Kolbe offers that his unit had no visibility on facts on the ground at the plant (Kolbe personal interview). According to industry expert Charles Goslin, the joint venture failed to take advantage of specific tactical intelligence being reported on the ground, and broader and multiple threat reporting from several private sources outside of Algeria (Goslin email correspondence, February 2023). It also is questionable what weight

Sonatrach and the Algerian Army would have given intelligence collected independently by BP and Statoil.

The embarrassing failure of In Amenas attack probably served as a catalyst for upheavals in Algeria's national security apparatus. Algeria's vaunted DRS failed to detect this terrorist attack. Shortly afterward, Algerian President Abdelaziz Bouteflika began retiring key generals in the PNA, and in 2015 removed longtime spymaster Mohamed Mediene as head of the DRS. In 2016, the whole intelligence apparatus was restructured (Chikhi, 2016). Some observers believe the reform of the Algerian intelligence apparatus was encouraged, if not pressed, by the US, UK and France (Goslin email correspondence, February 2023). After the attack, Algerian authorities scrambled to ensure the safety of foreign workers at their facilities, but one year later still refused BP and Statoil permission to hire their own security at the plant. Though the plant would be provided an airstrip to move workers out of the plant, BP didn't return to its Algiers office until late 2013, and Statoil in mid-2014 (Langved, 2014).

Although considered at the time to be the start of a 'new normal' for attacks on extractive industries, In Amenas, in retrospect, looks like an aberration. Belmokhtar's terrorist group failed to scare international companies away from Algeria, although companies probably became less reluctant to pull out personnel temporarily at the sign of danger. In 2016, after an AQIM mortar attack at their facility in In Saleh, Statoil, and BP withdrew personnel from the country, even though the attack caused no damage (Krauss, 2016). The In Amenas attack, as Stewart highlighted, was a disaster for Belmokhtar, who lost 32 men and gained no hostages (Stewart, 2013). After that, the group lost most of its fighting capability.

Results of the attack on the industry

The In Amenas attack caused many companies in the international oil and gas industry to review their security procedures, but according to former counter-terrorism special agent Fred Burton, there is little indication companies decreased their tolerance for working in risky environments because of the attack (Burton email correspondence, March 2023). For its part, Statoil set out to implement all the recommendations in its foundational In Amenas Report to create a genuine 'culture of security'. Its former security information center upgraded to a security threat analysis team, with a dedicated analyst focused on the Maghreb and Sahel region. To emphasize its seriousness, security was separated from safety in its organization and came under a senior vice president. Better security-related information would come from its internal and external networks, including engaging local communities. Equinor (Statoil's name since 2018) did not consider upgrading its security 'intelligence', but improving its security awareness through improved information flows (Industry expert personal interview, February 2023).

The attack raised awareness among Japanese international extractive firms on risk, as they had never before become victims of an attack by Al Qaeda-aligned terrorists. A security adviser of a Japanese-based extraction and production company commented that the attack prompted his company to enhance its security management function immediately because the attack directly impacted one Japanese company (JGC). Shortly after the attack, his firm created a security and crisis management group to conduct high-level security reviews of high-risk countries and to enhance governance and effectiveness of travel security and production site physical security at high-risk areas with terrorism (Industry expert email correspondence, February 2023).

Another change was an improvement in the way in which security information was exchanged across the industry. Former OMV security manager Paul Reither notes that more cooperation and information sharing after the attack by member companies of the International Organization of Oil and Gas Producers, of which BP and Statoil were both members, took place regularly (Reither personal interview, February 2023).

More emphasis on security – creating a 'culture of security' in the Statoil reports phrase – became more important for some firms, with more training offered on travel security and kidnap and ransom response. As former Director of Global Security Operations at Anadarko Petroleum Aidan Hales noted about the attack, 'it allowed us to improve physical protection systems in all high-risk environments' and especially instituting aerial surveillance program in some locations. Demonstrating an improved commitment to security was essential to get expatriate oil workers to locate to high-risk environments (Hales email correspondence, February 2023).

Not all experts suggested the changes were deep or long-lasting. For his part, Hales claimed 'there was the normal after-action review, but most businesses have short memories, so consequently not much happened despite the initial hysteria and media attention' (Hales email correspondence, 2023). Also, it should be noted that most if not all of these steps were already in place in many companies doing business abroad. None of these sensible preparations would have done much to mitigate an attack of In Amenas's scale. However, from a management perspective, these steps are necessary to bolster a company's 'duty of care'.

The In Amenas attack prompted the US government, at least briefly, to attempt a closer partnership with the oil and gas industry on security issues. Some companies also found a greater willingness to engage with US Africa Command. Under its director General Michael Flynn, the Defense Intelligence Agency sought greater capacity to analyze threats to the international oil and gas industry, and in 2014 sponsored a conference on the threat picture in oil-producing states, which the author attended. However, interest in pursuing a closer partnership was lukewarm, and these initiatives soon faded. That year, the Department of Energy hosted an exercise, with several high-level policymakers in attendance, to play out responses to a hypothetical terrorist attack on an offshore oil rig in Southwest Africa. One takeaway from the exercise was how difficult it was to conceive of such an attack rising to the level of a foreign policy crisis on the part of Washington, D.C.

As for intelligence upgrades, BP claimed to have enhanced its intelligence capabilities to better identify hidden threats (Kolbe and Morrow, 2022). Following BP's lead, Statoil upgraded its strategic risk unit after the attack, but it would not refer to this as an 'intelligence' unit (Industry expert personal interview February 2023). In fact, some of the responses cited by industry experts focus on improved security measures and response, rather than intelligence acquisition. According to Hales, more interaction with the host government on intelligence matters remained aspirational than functional. However, companies were prompted to share more risk intelligence with each other (Hales 2023).

The 'Enemies' of corporate intelligence

Intelligence expert Richard Betts has noted numerous 'enemies' of intelligence – analytic, bureaucratic, policy-related, etc. – which led him to conclude that some intelligence failures are by necessity inevitable (Betts, 2007). He advised that accepting occasional failure

might be the only rational stance for policy. The In Amenas case offers an opportunity to consider the unique problems, or 'enemies', of corporate security intelligence as well.

For some years now, many international companies have sought to acquire an intelligence capacity on geopolitical threats (Robson Morrow, 2022, p. 404). As we see in the In Amenas case, these efforts account for nothing if the information flow is lacking between the high-risk assets and headquarters. However, there are other obstacles for intelligence in the corporate environment. As noted above, Equinor does not deal in secret intelligence in making its assessments. Other industry security experts also raise issues about the appropriateness of using the word 'intelligence' in the corporate setting. As security executive Fitzmorris notes, without the ability to collect secret information, what we are doing cannot be considered intelligence, as it is properly understood (Fitzmorris personal interview, February 2023).

Security expert McHugh goes further, referring to intelligence as the 'third rail' in the corporate environment. It has great potential for being discounted or ignored because senior executives know little about that world and are not typical intelligence consumers. Unless 'intelligence' can be associated with clear-cut business decisions, and offers an unambiguous message, it will fail to have any impact. 'Emerging intelligence must be applied to a business issue to be solved', McHugh says (McHugh personal interview, 2023). Persuasion in such circumstances is difficult. As we have seen in the In Amenas case, even the insights of Paul Morgan probably did not rise to that 'tactical intelligence' level of clarity senior managers need to make important 'should we stay or should we go' decisions. Moreover, Bracken notes, 'People in the warning business do not have total control over resources or their organizations. The intelligence warning service cannot tell the secretary of defense or the president what to do' (Bracken, 2008, p. 31). The same holds true for intelligence in the corporate environment. Corporate intelligence will always be limited; it cannot be expected to offer clear tactical warning of an impending attack (Statoil, 2013, p. 4). We cite below some chronic obstacles that suggest corporate security intelligence has limited effectiveness in anticipating serious unexpected threats like at In Amenas.

Lack of information flow. The corporation may be a 'knowledge community', but that does not always work for useful security-related intelligence. The core business is not necessarily focused on the changing threat environment. Those responsible for that in corporate security and intelligence might be out of the normal information flow (Ard., 2022, pp. 131-132). Information on a rising terrorist threat can be diluted with other information on the overall risk picture. The unique organizational culture of Equinor might have a solution for this, but other companies will likely struggle unless similar circumstances force them into drastic changes. In 2013 BP had three analysts looking at the entire geopolitical threat picture (Kolbe personal interview February 2023). They were confident they could identify the trend lines of risk but had little ability to provide tactical intelligence that might make a difference. For a company with far-flung assets, it is difficult to perceive the ground truth in many assets that might have a real-world impact on a dynamic threat environment. The story of Paul Morgan's report raising the issue of a potential terrorist risk underscores the perils of compartmented information.

Tactical Intelligence Is Limited The corporate intelligence function needs to have some capacity to incorporate tactical intelligence to be effective at warning. One outcome of In Amenas was that some international companies spent more time engaging with

corporate social responsibility projects, putting them in touch with a wider spectrum of locals (Reither personal interview February 2023). These measures doubtless are helpful, but national intelligence services with far greater resources have poor track records of predicting terrorist strikes or political unrest. As noted above, a prudent organization must design a warning system that assumes timely intelligence will not be available.

When Intelligence Itself Can Be a Threat Corporate intelligence professionals face bureaucratic challenges in getting their analyses read and accepted by top decision-makers. To be effective, they must engage with and help shape policy as part of their normal duties. But putting emerging threats 'down on paper' – especially something as dramatic as a potential terrorist attack – may expose the company to future liability. The general counsel's office or the asset managers might be reluctant to expose themselves to a potentially bad news story (Kolbe personal interview, February 2023). Assets managers likewise might resent other elements of the enterprise criticizing their assessment of the situation on the ground. As noted above, the company might also recoil from evaluating the host government's security forces as being inadequate to the task or perhaps even contributing to the potential threat picture themselves.

Corporate intelligence has been adopted by many companies that desire a 'decision advantage'. These intelligence programs can contribute to greater environmental awareness and can improve corporations' strategic risk assessments, but these should not be relied upon for successful threat warnings. The Statoil report acknowledges that the joint venture likely would not have gotten the intelligence necessary to warn of an impending attack. Even more accurate intelligence – of the pre-9/11 'system is blinking red' variety – might not have led to a timely evacuation or prevention of the deadly terrorist attack. This case study raises some concerns about rating too highly corporate intelligence's effectiveness in high-risk security environments. Corporations run a great risk of overvaluing intelligence's contribution to their warning systems.

Disclosure statement

No potential conflict of interest was reported by the author.

References

Algeria Press Service. (2023). General said Chanegriha supervises ceremonies commemorating Tiguentourine events (January 16). https://www.aps.dz/en/algeria/46401-general-said-chanegriha-supervises-ceremonies-commemorating-tiguentourine-events

Ard, M. J. (2022). Lessons learned for the private-sector intelligence analyst. In R. Arcos, N. K. Drumhiller, & M. Phythian (Eds.), *The academic-practitioner divide in intelligence studies* (pp. 129–145). Lantham, MD: Rowman and Littlefield.

Arieff, Alexis. (2013). Algeria: Current issues. *Congressional Research Service* RS21532 (January 18).

Armstrong, H. (2014). The In amenas attack in the context of southern Algeria's growing social unrest. *CTC Sentinel*, *7*(2), 14–16.

Barak, M. (N.D.). The In Amenas gas facility attack – An analysis of the Modus Operandi. International Institute for Counter-Terrorism.

Betts, R. K. (2007). *Enemies of intelligence: Knowledge and power in American national security*. New York: Columbia University Press.

Bracken, P. (2008). How to build a warning system. In P. Bracken, I. Bremmer, & D. Gordon (Eds.), *Managing strategic surprise* (pp. 16–42). Cambridge: Cambridge University Press.
Chikhi, L. (2016). Algeria's Bouteflicka dissolves DRS spy unit, creates new agency: Sources. *Reuters* (January 25). https://www.reuters.com/article/us-algeria-security-idUSKCN0V31PU
Chivvis, C. S., & Liepman, A.. (2013). *North Africa's menace AQIM's evolution and the U.S. policy response*. Santa Monica, CA: RAND Corporation.
Dahl, E. J. (2013). *Intelligence and surprise attack: Failure and success from pearl harbor to 9/11 and beyond*. Washington, DC: Georgetown University Press.
Economist Intelligence Unit. (2014). One year on from In Amenas Attack (January 14).
Gatton, A., & Olden, M. (2013). Exclusive: Death in the desert—Did a security man see it coming? *The Independent* (September 12). https://www.independent.co.uk/news/world/africa/exclusive-death-in-the-desert-did-a-security-man-see-it-coming-8812972.html
Gentry, J. A., & Gordon, J. S. (2019). *Strategic warning intelligence: History, challenges, and prospects*. Washington, D.C.: Georgetown University Press.
Gilpin, R., et al. (2013). Regional security lessons from the attack on Algeria's In Amenas Gas Plant. *US Institute for Peace* (January 23).
Grabo, C. M.. (2002). *Anticipating surprise: Analysis for strategic warning*. Washington, D.C: Center for Strategic Intelligence Research.
Kolbe, P. R., & Morrow, M. R. (2022). How corporate intelligence teams help businesses manage risk. *Harvard Business Review* (January). https://hbr.org/2022/01/how-corporate-intelligence-teams-help-businesses-manage-risk
Krauss, C. (2016). BP and Statoil Pull Employees from Algeria Gas Fields After Attack. *New York Times* (March 21) https://www.nytimes.com/2016/03/22/business/energy-environment/bp-and-statoil-pull-employees-from-algeria-gas-fields-after-attack.html
Lacher, W. (2012). *Organized crime and conflict in the Sahel-Sahara region*. Washington, DC: *Carnegie Endowment* (September).
Lacher, W., & Steinberg, G. (2015). Spreading local roots: AQIM and its offshoots in the Sahara. In G. Steinberg, & A. Weber (Eds.), *Jihadism in Africa: Local causes, regional expansion, international alliances* (pp. 69–83). Berlin: SWP Research Paper. (June)
Langved, A. (2014). Statoil is Back in in Amenas. *Dagens Noeringsliv* (July 23). https://www.dn.no/algerie/statoil-tilbake-pa-in-amenas/1-1-5156150
Lebovich, A. (2016). Algeria: The stirrings of change? In *Algeria: Five years on: A new European agenda for North Africa* (pp. 39–50). EU: European Council on Foreign Relations.
Leveque, T. (2009). French monks killed by Algeria, not Islamist-source. *Reuters* (July 6). https://www.reuters.com/article/idUSL6376690
Luft, G., & Korin, A. (2007). Fueled again? In search of energy security. In F. Fukuyama (Ed.), *Blindside: How to anticipate forcing events and wildcards in global politics* (pp. 71–81). Washington, DC: The Brookings Institution.
Nield, R. (2014). Business and terrorism in Algeria. MENASource. *The Atlantic Council* (January 24). https://www.atlanticcouncil.org/blogs/menasource/business-and-terrorism-in-algeria/
Riedel, B. (2013). Algeria a complex ally in war against Al Qaeda. Brookings (February 3). https://www.brookings.edu/opinions/algeria-a-complex-ally-in-war-against-al-qaeda/
Roberts, H. (2007). Demilitarizing Algeria. Carnegie endowment for international peace (May) No. 86.
Robson Morrow, M. A. (2022). Private sector intelligence: On the long path of professionalization. *Intelligence and National Security*, *37*(3), 404–422. doi:10.108002684527.2022.2029099
Schindler, J. R. (2012). The Ugly Truth about Algeria. *The National Interest* (July 10). https://nationalinterest.org/commentary/the-ugly-truth-about-algeria-7146
Statoil. (2013). The In Amenas attack, report of the investigation into the terrorist attack on in Amenas. www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf
Stewart, S. (2013). The unspectacular, unsophisticated Algerian hostage crisis. *Stratfor* (January 24). https://worldview.stratfor.com/article/unspectacular-unsophisticated-algerian-hostage-crisis
Wohlstetter, R. (2002). *Pearl harbor: Warning and decision*. Redwood City, CA: Stanford University Press.