KCS Group International

We look at the world differently...

Hybrid Warfare II – the forgotten social engineers

February 2025

The over-emphasis on cyber threats in modern warfare and corporate espionage has created a false sense of security, often sidelining traditional methods like human intelligence (HUMINT). While cyber tactics, such as hacking and malware deployment, remain effective, social engineering techniques are still very much in use by both state and commercial actors to gather intelligence. From human agents exploiting the vulnerabilities within an organisation's IT department to gain access to confidential systems, to orchestrating elaborate pretexts where agents assume false identities or fictitious companies, the human element remains a key driver of successful espionage.

The continued relevance of social engineering is underscored by its ability to bypass technical defences. Social engineering is less about cracking firewalls and more about manipulating human behaviour, whether through phishing schemes or carefully executed psychological tactics. Recent cases highlight this, such as foreign agents recruiting individuals from social media platforms to gain access to sensitive information, or corporations using undercover agents to infiltrate rival companies under false pretences. These methods remain highly effective because they exploit inherent human weaknesses - trust, naivety and the pressure of everyday responsibilities.

The risks posed by HUMINT are significant, especially in corporate and geopolitical espionage. The potential for sensitive business information to be compromised through a well-placed human agent could lead to substantial financial losses or a loss of competitive advantage. On the geopolitical scale, the risks are even more pronounced, with espionage efforts leading to shifts in political influence or national security vulnerabilities.

As such, companies must recognise that while digital defence mechanisms are essential, human intelligence still poses a critical threat that demands vigilance and proactive countermeasures.

The commercialisation of espionage: a historical perspective

State intelligence services have long been used for political, military and economic advantage. Initially, espionage was a state-controlled endeavour, designed to protect national interests and gather information on adversaries. However, during the Cold War, as the nature of global conflict evolved, the boundaries between state intelligence operations and private sector activities began to blur. The rise of corporate espionage in the late 20th century marked a pivotal shift, with businesses increasingly relying on intelligence services to safeguard proprietary information and gain a competitive edge.

In this period, private intelligence firms emerged, such as Argen, The Merchant International Group, Control Risks, Kroll, Hakluyt, and sector newcomers Black Cube and Psy-Group - all offering their services to corporations, engaging in activities ranging from commercial intelligence gathering, to industrial influencing and reputational repositioning. These entities deployed methods traditionally associated with state surveillance, such as infiltration and social engineering, to extract confidential information, often fogging legal and ethical lines. Corporate espionage became an extension of market competition, where intelligence gathering was no longer limited to government interests but was actively pursued by corporations vying for dominance.

These developments highlight the growing commercialisation of espionage, where private companies now play an influential role in intelligence operations. As businesses face increasing pressure to protect intellectual property, trade secrets and market positions, they are often willing to engage in covert actions that mimic state-driven espionage tactics. This fusion of corporate and state intelligence strategies raises significant concerns regarding accountability, and the impact of these practices on global business environments, especially as multinational companies navigate the complex intersection of legality, ethics and strategic advantage.

The evolution of private intelligence firms

The rise of private intelligence firms marks a shift in the way espionage is conducted. Initially focused on governmental interests, espionage evolved as companies saw the potential benefits of leveraging intelligence services to secure a competitive edge. These firms, often staffed with former intelligence officers and experts, have pioneered the fusion of corporate strategies with state-level tactics.

Notable firms, such as Psy-Group and Black Cube, have made headlines for their controversial operations. Black Cube, an Israeli firm founded in 2010 by former Israeli intelligence officers, Dan Zorella and Avi Yanus, has been involved in several high-profile cases, including shadowy corporate investigations and political influence operations. Psy-Group, also based in Israel, was founded around 2014 by Israeli-Australian Joel Zamel and CEO Royi Burstein, a former lieutenant colonel in the Israel Defence Forces. Psy-Group gained attention for its engagement in social media manipulation and covert online operations, before its closure following legal investigations. Companies like the Merchant International Group, Kroll, Hakluyt, Control Risks, Pinkerton and Stratfor (RANE) focus on high-level investigations and geopolitical risk analysis.

The global market for intelligence-for-hire services is expanding, with major players based in the United States, Israel and the UK, where the demand for such services grows across industries. These firms offer tailored solutions that include everything from corporate due diligence to covert operations, designed to influence competitors, or in extreme cases, sway political opinions. As these firms grow in influence, they raise important questions regarding the ethical implications of their work, especially as businesses turn to them for increasingly aggressive tactics to protect intellectual property, trade secrets and political leverage.

The rise of such firms has huge implications for both corporate strategy and global geopolitics. As private intelligence operations become more pervasive, multinational companies must recognise the risks associated with their actions, particularly when legal boundaries are tested in the pursuit of strategic advantage.

Common espionage tactics and social engineering techniques

Espionage, both in corporate and geopolitical spheres, often hinges on the effective use of social engineering techniques, which exploit the vulnerabilities of human behaviour rather than relying solely on technical device hacking or surveillance. One of the most commonly employed methods is pretexting, where agents fabricate false identities or backstories to manipulate targets into divulging sensitive information. This tactic allows operatives to infiltrate organisations, gain access to secure environments or extract confidential data, all under the guise of a legitimate request.

In more aggressive cases, coercion, honey traps and blackmail (often leveraging kompromat - compromising material), come into play. This technique exploits personal weaknesses, like financial distress or past indiscretions, to force individuals to co-operate with espionage efforts. Such tactics are not limited to government intelligence services but are increasingly used by private firms seeking competitive advantage or to settle business rivalries.

Psychological manipulation is another powerful tool, where espionage agents employ a deep understanding of human behaviour to influence decisions. Whether by exploiting trust, fear or greed, the objective remains the same: to manipulate the target into providing access to valuable information or resources.

The growing use of ideology and financial incentives in recruiting insiders is particularly concerning. Offering financial rewards or appealing to an individual's personal beliefs can be a highly effective way to secure internal sources of intelligence. As such, these methods pose severe risks to businesses and governments alike, as the costs of a compromised insider can far exceed the immediate benefits gained by espionage.

Who uses these services and why?

Private intelligence firms have become increasingly popular across a range of industries, each with distinct motivations for leveraging these services. Financial and investment firms, for example, rely heavily on competitive intelligence to identify emerging market trends, anticipate strategic moves by competitors, and evaluate the risks associated with new ventures. By gaining access to insider knowledge or understanding key political and economic shifts, these firms gain a significant edge in their decision-making processes.

Technology companies, often operating in highly competitive and innovation-driven environments, use intelligence firms to protect their intellectual property from espionage or unauthorised access. With patents and proprietary technology at stake, ensuring that competitors or malicious actors do not gain access to sensitive data has become paramount.

In the energy sector, where large-scale investments and strategic infrastructure are involved, intelligence is used to secure critical assets from sabotage, corporate espionage or geopolitical risks. Whether through monitoring rival developments or assessing the stability of foreign energy markets, companies must stay ahead of both technological and political challenges.

In the legal sector, private intelligence firms are also utilised to gain critical insights into opponents and source evidence that can be pivotal in winning cases. Law firms, particularly those involved in high-stakes litigation or complex mergers and acquisitions, often hire these firms to conduct background investigations, identify hidden connections, and uncover potentially damaging information about adversaries. This research may involve uncovering financial discrepancies, tracking the movements of key individuals or even gathering intelligence on an opposing party's strategy.

In addition, to providing support in legal disputes, these firms are increasingly used for due diligence in corporate transactions, ensuring that all relevant facts are considered before major decisions are made. The legal sector's reliance on such intelligence highlights the broader role that private intelligence plays in shaping competitive strategies and influencing the outcome of critical business and legal decisions. Government contractors, operating in sensitive political or security domains, frequently turn to private intelligence firms to manage high-stakes negotiations, conduct influence operations or ensure the integrity of due diligence processes, especially during mergers and acquisitions.

In each case, the use of private intelligence services is motivated by the desire for competitive advantage and strategic positioning, reiterating the growing reliance on covert operations in the modern business world.

Controversies and notorious case studies

Private intelligence firms Black Cube and Psy-Group made headlines for their controversial and often ethically questionable operations.

Black Cube became widely known for its involvement in high-profile corporate and political manipulations. Two of the firm's most notorious cases involved sending its employees to secretly find damaging information on two former Obama White House aides involved in negotiating the Iran nuclear deal, and its attempt to discredit journalists and activists who were critical of the former Hollywood mogul, Harvey Weinstein. Black Cube's operations included surveillance and deceptive tactics to undermine victims of sexual abuse and reporters investigating Weinstein's actions.

The firm's tactics raised serious questions about the legal and ethical boundaries of intelligence-gathering, blurring the line between legitimate corporate security and illegal espionage.

The firm's involvement in the Belgian Health Ministry's audit of Medista further exemplifies how intelligence services are increasingly used for political and corporate influence. Black Cube also was involved in a lawsuit between Canadian investment firms West Face and Catalyst Capital. In 2014, a Toronto-based investment firm, West Face Capital Inc., alleged that a rival company called Catalyst Capital Group Inc. directly or indirectly hired both Black Cube and Psy-group to help sway a business dispute over a bid for a telecommunications company. Black Cube were accused of using an undercover agent to meet with the judge in the case and secretly record him in an attempt to discredit him by provoking anti-Semitic remarks. Psy-Group was used to conduct online disinformation campaigns against West Face Capital Inc.

Likewise, Psy-Group, is infamous for its involvement in social media manipulation, including its attempts to influence political outcomes through covert online operations. The firm came under scrutiny for its work with social media trolls and its role in the 2016 US presidential election, where it allegedly aided in spreading disinformation through targeted campaigns working alongside Cambridge Analytica. Psy-Group's methods highlighted the growing role of private intelligence agencies in shaping public discourse and influencing elections.

These case studies reveal an increasing reliance on private intelligence firms in both corporate and geopolitical spheres, often pushing legal and ethical boundaries. The use of such firms for covert influence operations raises critical concerns regarding transparency, accountability and the potential for misuse in highly sensitive areas such as politics, corporate espionage and legal disputes.

Countering the threat: mitigation strategies for business

To protect against the growing threat of human intelligence (HUMINT) and social engineering agents, business must apply mitigation strategies that address both the internal and external espionage risks.

Internal security policies play an important role in protecting sensitive information. Vetting both employees and third-party contractors is vital in ensuring that individuals with access to critical systems or data are trustworthy. Additionally, implementing strict access controls, such as role-based permissions and data encryption, helps limit exposure to sensitive information and reduces the likelihood of internal breaches.

Awareness training is another essential strategy. Educating employees on the risks of social engineering threats - such as impersonation attempts, and pretexting - can reduce the chances of falling victim. Simulated attack exercises, including phishing tests and role-playing scenarios, allow employees to practice identifying and responding to such threats, reinforcing security awareness across the organisation.

Enhanced due diligence is necessary when engaging in high-value deals or partnerships. Companies must conduct thorough background checks and assess the security protocols of potential partners or collaborators to identify any vulnerabilities that could be exploited for espionage. In addition, monitoring transactions and interactions closely can help detect unusual activities early.

Finally, ***legal protections*** are essential in responding to corporate espionage. Strengthening corporate espionage laws and regulations can help deter malicious activities and provide a legal framework for pursuing action against unethical intelligence firms. Businesses should be prepared to take legal action against firms that engage in illegal or unethical practices, ensuring that they are held accountable for any harm caused to the organisation.

Conclusion and strategic recommendations

In today's fluid business environment, it is critical that organisations understand that cyber threats are only one part of the broader risk landscape. While cyberattacks remain prevalent, HUMINT operations - including social engineering and espionage tactics - continue to be powerful tools for both state and commercial players. These operations are often underappreciated, which can leave businesses vulnerable to internal and external threats.

Intelligence operations are not just a government concern, they have become a strategic weapon in global commercial competition. Whether through corporate espionage, industrial sabotage, or political influence campaigns, private intelligence firms are playing an increasingly prominent role in the corporate world. Organisations must recognise that these tactics can be used against them, and they should take proactive steps to defend against them.

Business leaders must integrate their cybersecurity frameworks with human intelligence defences. This means not only securing digital assets but also ensuring that employees, contractors and business partners are equipped with the tools and knowledge to recognise and respond to social engineering threats.

A combined approach that addresses both the human and technical aspects of security is considered essential to minimising risks.

The final takeaway is clear: a proactive, intelligence-driven risk management strategy is necessary to win in today's hybrid warfare landscape. By recognising and countering both cyber and human intelligence threats, businesses can better protect their assets and maintain their reputation in a world where intelligence is key in corporate success.

KCS Group International – Strategic Intelligence & Corporate Security

KCS Group International is a leading provider of security and intelligence services, operating in some of the world's most difficult environments on complex cases of fraud, theft, corruption or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients identify and deal with any risks, weaknesses and threats which could impact on their business, financially or reputationally.

Our key areas of expertise include: Corporate Intelligence Services – New market or sector entry research – Know your customer screening.

In addition, we offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits – providing unparalleled analysis, contingency planning and implementation.

To find out more or to arrange a meeting to discuss your business needs, please email the team at info@kcsgroup.com or call (00 44) 20 7245 1191 – www.kcsgroup.com