Risk Intelligence

Tutelare le Organizzazioni Italiane Attive in Ambienti Ostili

FRANCESCO CALZONI

Abstract

Questo articolo ambisce a diffondere la consapevolezza che esistono soluzioni per soddisfare i requisiti informativi delle aziende attive in scenari ostili. Pertanto, si rivolge soprattutto a Security Manager, analisti e dirigenti di organizzazioni con una presenza in tali scenari, specialmente nei settori energia, sicurezza privata, infrastrutture, costruzioni, onlus e multilaterale.

Il sistema di sicurezza globale punta a una fase di instabilità a causa di alcuni assestamenti negli equilibri di potenza che sono già in atto.[1] Questa instabilità si manifesterà inevitabilmente lungo le faglie geopolitiche del 21° secolo attraverso nuovi o rinnovati conflitti militari, instabilità politica, disordini sociali ed altri fenomeni destabilizzanti. Le organizzazioni con una presenza sul terreno in tali aree necessitano strumenti adeguati per tutelare la propria continuità operativa, la sicurezza del proprio personale ed i propri margini di profitto.

Nello specifico, queste organizzazioni hanno un crescente bisogno di flussi continui, tempestivi ed affidabili di informazioni ed analisi sull'"ecosistema della sicurezza" nelle aree in cui operano, per tutelare propria sostenibilità identificando ed anticipando minacce ed opportunità. Le organizzazioni che non possiedono queste capacità dovrebbero affidarsi ad un servizio di Risk Intelligence.

Contesto: I movimenti tettonici del sistema di sicurezza globale

Ad oggi l'ecosistema globale della sicurezza è caratterizzato da due macro-trend: la crescente competizione geopolitica fra attori statali e l'emergere di potenti attori non-statali.[2,3] Queste dinamiche risultano in crescenti frizioni geopolitiche e sociopolitiche che pongono serie minacce alla sicurezza fisica ed alla continuità operativa di organizzazioni commerciali e non governative. Si elencano alcuni esempi di seguito:

- L'erosione della supremazia politica e militare americana in contesti dalla rilevanza strategica come l'area MENA, l'Europa orientale, il Caucaso e l'Asia orientale facilita l'emergere di tensioni fra potenze regionali.[4]
- Il progresso economico e tecnologico permette a nuovi attori statali di sviluppare le capacità per proiettare potenza militare al di fuori dei propri confini, al fine di perseguire i propri interessi nazionali.
- La globalizzazione della finanza, della logistica e delle comunicazioni favoriscono la nascita di potenti attori non-statali che spesso hanno delle proprie agende politiche.[5] Sempre grazie al progresso tecnologico, queste organizzazioni hanno oggi accesso a tecnologie *dual-use* a basso costo e

[1] Waltz K. N. (1979). Theory of International Politics. McGraw-Hill, pp. 132-33
[2] Markowitz J. N., Fariss C. J. (2017). Power, proximity, and democracy. Geopolitical Competition in the International System. Journal of Peace Research, 55(1), 78-93.
[3] Bieler A., Higgott R. A., Underhill G. R. (2005). Non-state actors and authority in the global system. Routledge, pp. 1-2
[4] Markowitz J. N., Fariss C. J. (2017). Power, proximity, and democracy. Geopolitical Competition in the International System. Journal of Peace Research, 55(1), 78-93.
[5] Bieler A., Higgott R. A., Underhill G. R. (2005). Non-state actors and authority in the global system. Routledge, pp. 1-2

facilmente accessibili che possono essere usate come moltiplicatori di forza militare. Alcuni esempi sono la tecnologia GPS, i droni commerciali, le stampanti 3-D ed internet.

Che cos'è la Risk Intelligence

Al giorno d'oggi e sempre più nel futuro a medio-lungo termine, le organizzazioni con operazioni in scenari ad alto rischio (come ad esempio Libia, Yemen, Iraq, Afghanistan, Somalia) devono affrontare un ampio spettro di minacce che si estende dal livello tattico (criminalità, attacchi terroristici, disordini sociali nella vicinanza dei propri uffici e siti produttivi), a quello operativo (conflitti armati o fenomeni di insorgenza con implicazioni per la rete logistica dell'azienda), a quello strategico (dispute territoriali inter-statali su territori contesi in cui opera l'azienda). Questi sono solo alcuni esempi della miriade di eventi destabilizzanti che possono significativamente influenzare le operazioni di un'azienda o una organizzazione non governativa.

Risulta quindi evidente la necessità di identificare, anticipare e gestire in maniera ottimale questi ed altri rischi per assicurarsi la propria continuità commerciale. Ciò può essere possibile solo attraverso una profonda ed esaustiva consapevolezza delle dinamiche in atto nell'ambiente in cui si opera. Ecosistemi sicurezza sempre più fluidi e multidimensionali richiedono la capacità di identificare, comprendere e connettere sviluppi tattici e strategici al di là di quello che una formazione puramente accademica permette. Specifici profili professionali permettono alle aziende di cogliere opportunità commerciali altrimenti troppo rischiose.

In generale, il termine Risk Intelligence indica un'applicazione delle attività di intelligence volta all'individuazione ed alla prevenzione di potenziali eventi che potrebbero compromettere la continuità operativa di un'azienda o la sicurezza del suo personale. Tali eventi potrebbero essere pianificati ed implementati a diretto discapito dell'azienda, come nel caso del rapimento di un dirigente o di un attacco ad un sito produttivo, o coinvolgere l'azienda per caso o indirettamente. Nel presente articolo il termine Risk Intelligence esclude il dominio cyber e l'eventualità di fenomeni naturali quali terremoti ed eruzioni vulcaniche, e si riferisce solamente a minacce fisiche che includono ma non si limitano a terrorismo, conflitti armati, fenomeni di insorgenza, disordini sociali, instabilità politica, criminalità. Va notato che la letteratura esistente su questo tema concepisce il concetto di Risk Intelligence in modi diversi, a seconda dei background professionali degli autori.[6]

In questo articolo ci si riferisce al concetto di Risk Intelligence per descrivere le attività ed i sistemi relativi alla raccolta, la valutazione, l'analisi e la disseminazione di informazioni volte all'identificazione preventiva di potenziali rischi, per supportare la sicurezza e la continuità operativa di organizzazioni sul terreno in uno specifico territorio. L'obiettivo di questo prodotto informativo è di fornire all'utilizzatore finale situational awareness ed analisi predittiva del rischio, permettendo di bilanciare il

[6] Evans, D. (2015). Risk intelligence: How to live with uncertainty. Simon and Schuster.

perseguimento di opportunità commerciali in ambienti ostili con la propria tolleranza al rischio.

In base alla definizione fornita sopra, si capisce come la Risk Intelligence si distingua chiaramente da altri prodotti informativi disponibili nel settore privato come quelli focalizzati su stabilità politica o geopolitica, rischi di mercato e finanziari e rischi reputazionali. Questi prodotti informativi hanno scopi diversi da quelli della Risk Intelligence. Il settore Risk Intelligence si differenzia inoltre dalle operazioni di intelligence che alcune entità statali subappaltano a fornitori privati per supplire alle insufficienti risorse del settore pubblico in teatri particolarmente complessi come Afghanistan ed Iraq.[7] Essendo condotte per conto di un governo, tali operazioni sono soggette a vincoli di segretezza. Un servizio di Risk Intelligence invece fornisce ai suoi clienti solo ed esclusivamente informazioni non classificate. Allo stesso tempo, nulla vieta ad entità statali di usufruire di un servizio commerciale di Risk Intelligence per integrare e confrontare i propri flussi informativi, come già accade.

È anche importante rilevare la duplice utilità commerciale della Risk Intelligence: all'anticipazione delle minacce si aggiunge infatti la conoscenza della reale situazione sul terreno che permette una continuità operativa a spese di una meno informata concorrenza. Ad esempio, durante i 14 mesi di ostilità a sud di Tripoli, Libia, fra l'aprile 2019 ed il giugno 2020, sono state registrate attività di combattimento di considerevole intensità, con l'utilizzo di artiglieria pesante e supporto aereo da parte di entrambi gli schieramenti. Nonostante le ostilità abbiano avuto luogo a non più di qualche kilometro dal centro di Tripoli, causando un esodo dello staff internazionale e le conseguenti perdite economiche, reali minacce all'incolumità dello staff stanziato a Tripoli sono state registrate solo in prossimità di luoghi prevedibili e pertanto evitabili come l'aeroporto di Mitiga, il porto commerciale e l'Ambasciata turca. La città vecchia ed il compound di Palm City, dove la maggior parte della comunità internazionale risiede, non sono mai stati coinvolti nelle ostilità. Prendendo un rischio calcolato, alcune organizzazioni hanno deciso di rimanere sul terreno, trasformando poi la propria presenza in loco in nuovi contratti e profitti.

Intuitivamente, dovendo quotidianamente supportare operazioni sul terreno in ambienti ostili, la Risk Intelligence richiede un livello di profondità informativa ed analitica superiore a quello di altri prodotti informativi. Le skills richieste a livello intellettuale, umano e tecnologico sono diverse. Un servizio efficacie di Risk Intelligence impone la raccolta e l'analisi di informazioni in contesti grandemente influenzati da attori locali ed in cui è fondamentale un approccio analitico multi-dominio. Spesso infatti i domini politico, militare, economico, sociale, informativo ed infrastrutturale (PMESII) si intersecano e si influenzano a vicenda, ed alcuni sviluppi risultano contraddittori o fuorvianti per osservatori non sufficientemente informati.[8]

[7] Michaels, J. D. (2008). All the President's spies: Private-public intelligence partnerships in the War on Terror. Calif. L. Rev., 96, 901.

[8] Cagnazzo, M., & Zinzone, F. (2020). THE ART OF WAR IN THE POST-MODERN ERA. The Battle of Perceptions. Youcanprint.

Nello specifico, essendo talvolta focalizzati su contesti interessati da guerre civili o competizione geopolitica, come ad esempio Libia e Yemen, i fornitori di questo tipo di servizi devono saper gestire un dominio informativo fortemente polarizzato e soggetto a disinformazione, la cui incertezza si riflette sugli altri domini di analisi. Questo sottolinea l'importanza fondamentale dell'elemento umano nella valutazione e nell'analisi delle informazioni disponibili. La capacità dell'analista umano di interpretare linguaggio, contesto e bias di alcune fonti è ancora impareggiata da qualsiasi sistema di intelligenza artificiale a conoscenza dell'autore. Ciò non toglie che vi siano strumenti tecnologici che possono apportare benefici notevoli in termini di raccolta ed analisi delle informazioni.

Perché il settore della Risk Intelligence è separato e complementare al settore della sicurezza privata?

Qualsiasi professionista del settore saprà quanto i servizi di Risk Intelligence e di sicurezza privata siano complementari ed imprescindibili gli uni dagli altri. Spesso i primi acquirenti di un buon servizio di Risk Intelligence sono infatti i fornitori di sicurezza privata. Se la Risk Intelligence identifica ad anticipa potenziali rischi, la sicurezza privata si occupa del lato operativo e della pianificazione per far fronte a tali rischi, come ad esempio l'utilizzo di scorte armate, veicoli antiproiettile B-6 eccetera.

Queste due facce della stessa medaglia richiedono figure professionali diverse, e per motivi commerciali e di budget spesso i fornitori di sicurezza privata stentano a devolvere le necessarie risorse al lato informativo ed analitico, più o meno consapevolmente. Si appoggiano (o dovrebbero appoggiarsi) quindi ai fornitori privati di intelligence. Chiunque si avvalga dei servizi di un fornitore di sicurezza privata dovrebbe tenere conto di questa fondamentale distinzione ed evitare di operare in ambienti ostili o non permissivi senza un adeguato supporto informativo.

Ciò sottolinea l'importanza per le aziende di saper distinguere prodotti informativi ed analitici di qualità dalla reportistica fornita solamente per barrare la casella della cosiddetta "duty of care" e proteggersi dal punto di vista legale in caso qualcosa vada storto.

Conclusione

Il sistema di sicurezza globale diventerà più instabile negli anni a venire, e le organizzazioni attive in ambienti ostili devono essere in grado di anticipare rischi e minacce prima che mettano a repentaglio le loro operazioni sul terreno. Ciò richiede un profondo livello di conoscenza specifica delle dinamiche sociali, politiche, economiche e militari nell'ambiente di interesse, ed uno specifico *skill set* a livello tecnologico, umano ed intellettuale. I professionisti del settore della Risk Intelligence forniscono queste capacità, ed ogni organizzazione dovrebbe fornire ai propri Security Manager accesso ad informazioni ed analisi accurate e tempestive, per proteggere il proprio personale, i propri asset, ed i propri margini di profitto.

Nel contesto di crescente instabilità internazionale, le organizzazioni italiane che operano o vorrebbero operare in scenari ad alto rischio dovrebbero essere incoraggiate a non sottovalutare le risorse necessarie. Questo contribuirebbe a sviluppare la cultura della sicurezza fra i nostri attori economici e non-governativi, e ridurrebbe il rischio di dover il coinvolgere fondamentali risorse statali per rimediare a situazioni causate da eccessiva leggerezza nella valutazione dei rischi.

BIBLIOGRAFIA

- Bieler A., Higgott R. A., Underhill G. R. (2005). Non-state actors and authority in the global system. Routledge, pp. 1-2.
- Cagnazzo, M., & Zinzone, F. (2020). THE ART OF WAR IN THE POST-MODERN ERA. The Battle of Perceptions. Youcanprint.
- Evans, D. (2015). Risk intelligence: How to live with uncertainty. Simon and Schuster.
- Glassman M., Kang M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, 28(2), 673-682.
- Markowitz J. N., Fariss C. J. (2017). Power, proximity, and democracy. Geopolitical Competition in the International System. Journal of Peace Research, 55(1), 78-93.
- Michaels, J. D. (2008). All the President's spies: Private-public intelligence partnerships in the War on Terror. Calif. L. Rev., 96, 901.
- Voelz, G. J. (2009). Contractors and intelligence: The private sector in the intelligence community. International Journal of Intelligence and Counterintelligence, 22(4), 586-613.
- Waltz K. N. (1979). Theory of International Politics. McGraw-Hill, pp. 132-33