Embedded Agency - Periodico registrato presso il Tribunale di Campobasso il 7/07/2010 n.17/10 - Numero 01/2021

CISINT

Centro Italiano di Strategia e Intelligence

O.S.S.I.S.Na.

Embedded Agency

INTELLIGENCE COLLETTIVA
di Angelo Tofalo

DUE CHIACCHIERE CON LUTTWAK
di Marco Pugliese

O.S.S.I.S.Na. È INIZIATO COSÌ

ANNO 2021

C I S I N T

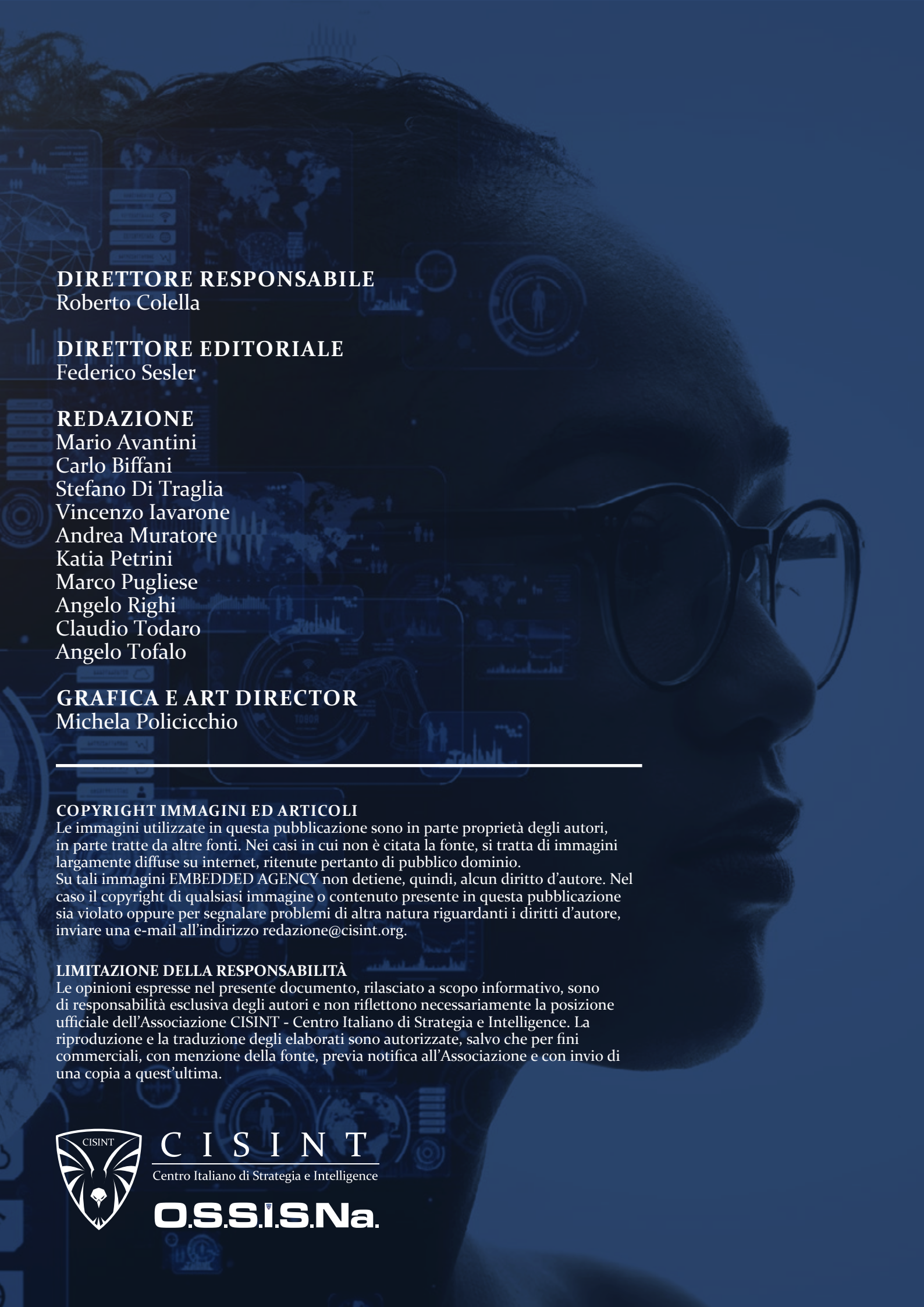
Centro Italiano di Strategia e Intelligence

O.S.S.I.S.Na.

Embedded Agency

Embedded Agency - Periodico online registrato presso il Tribunale di Campobasso il 7/07/2010 n. 17/10

CISINT - Centro Italiano di Strategia e Intelligence
Via Aurelia 424 - 00165 Roma | CF: 97895100580 | info@cisint.org



DIRETTORE RESPONSABILE
Roberto Colella

DIRETTORE EDITORIALE
Federico Sesler

REDAZIONE
Mario Avantini
Carlo Biffani
Stefano Di Traglia
Vincenzo Iavarone
Andrea Muratore
Katia Petrini
Marco Pugliese
Angelo Righi
Claudio Todaro
Angelo Tofalo

GRAFICA E ART DIRECTOR
Michela Policicchio

CISINT
Centro Italiano di Strategia e Intelligence
O.S.S.I.S.Na.

Indice

Editoriale

La pandemia ha messo a dura prova l'economia globale. In un momento così delicato siamo convinti che bisogna proteggere il nostro settore industriale. I miliardi del Recovery Fund serviranno ad una ripresa economica del nostro Paese con l'obiettivo finale di tenerci agganciati all'Eurozona. Si tratta davvero di un'ultima chance vista la situazione precaria in cui versiamo. Per questo è fondamentale proteggere il nostro settore vitale garantendo degli standard di sicurezza. Il mondo della sicurezza industriale sta cambiando in risposta alle crescenti minacce globali. Oggi le aziende hanno urgente bisogno di migliorare le loro pratiche e sistemi di sicurezza generali inerenti sia le risorse intellettuali che fisiche. Il settore industriale deve affrontare sfide concrete poiché la tecnologia è in continuo progresso. Tradizionalmente le aziende industriali si sono concentrate sulla produttività.

Tuttavia, le recenti minacce alle infrastrutture critiche hanno portato a un inasprimento delle misure di sicurezza. Nell'articolo introduttivo si propone un modello organizzativo con cui l'operatore economico (gestore dell'asset industriale strategico) possa implementare un piano integrato di Security Management, Operations Continuity & Crisis Communication da applicare in scenari non convenzionali (emergenze sanitarie, eventi bellici, atti terroristici e crisi socio-economiche), in modo da disporre di un efficace strumento di protezione da minacce ed eventi che possano pregiudicarne la capacità produttiva. La riduzione delle vulnerabilità ai sistemi di automazione degli impianti e ad altre risorse critiche è necessaria per garantire la sicurezza, l'affidabilità, l'integrità e la disponibilità di questi sistemi. Informare è il primo passo. Per questo nasce una nuova collaborazione tra la testata giornalistica Embedded Agency e l'Osservatorio per la Sicurezza del Sistema Industriale Strategico Nazionale (O.S.S.I.S.Na.), costituito all'interno del CISINT (Centro Italiano Strategia ed Intelligence). Un progetto orientato all'approfondimento di tematiche inerenti alla sicurezza degli asset industriali strategici nazionali (imprese e filiere), fondamentali per lo Stato e per il benessere sociale.

Una nuova sfida nazionale è rappresentata dalla necessità di rispondere in modo urgente e capillare al fabbisogno di presìdi farmaceutici e attrezzature biomedicali da impiegare nella lotta al Covid-19. Intere filiere industriali si stanno mobilitando al fine di predisporre i propri sistemi di produzione e distribuzione per una risposta efficace alle urgenze sanitarie del Paese. Nell'approfondimento tematico si offrirà al lettore un'analisi dello scenario operativo (attuale e per i prossimi mesi) e i possibili criteri di pianificazione per le attività di protezione delle filiere logistiche afferenti all'intero ambito industriale biosanitario. Completano il primo numero del periodico una serie di rubriche afferenti a tematiche geopolitiche ed intelligence.

Buona lettura!

Roberto Colella (Direttore Responsabile)

RUBRICA: Un occhio sul mondo

CARLO BIFFANI - Attacco alla Diplomazia

Esistono episodi che hanno la capacità di metter in moto processi fino a quel momento inimmaginabili e che rappresentano dei veri punti di svolta. In questa sede analizzeremo cosa hanno rappresentato in termini di impatto e di conseguenze, le uccisioni di due diplomatici di altissimo rango, avvenute in aree conflittuali distanti fra loro, ma entrambe appartenenti al continente africano, come quella occorsa a Bengasi all'ambasciatore statunitense Chris Stevens l'11 settembre del 2012 e quella molto più recente occorsa il 22 febbraio di questo anno, che ha purtroppo riguardato il nostro ambasciatore in Congo Luca Attanasio assassinato insieme al carabiniere Vittorio Iacovacci.

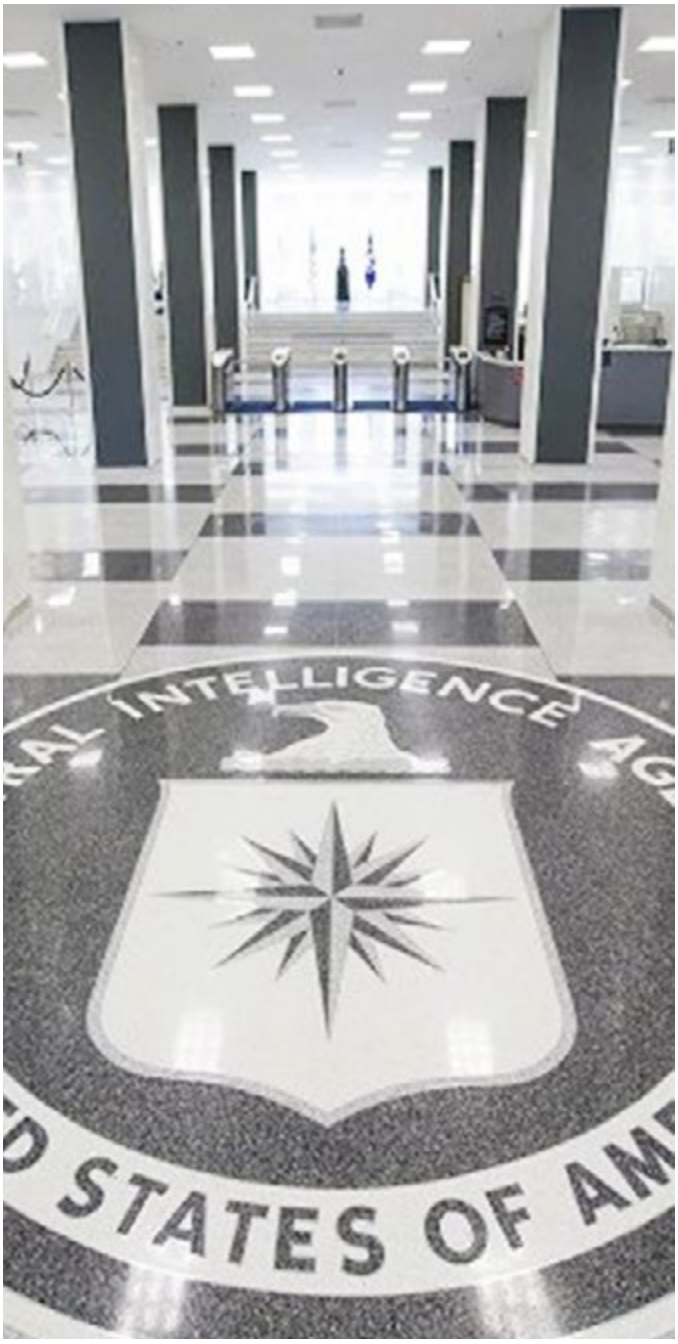
L'attacco che porta alla morte del diplomatico americano avviene all'interno del compound che ospita una "accomodation" consolare statunitense a Bengasi: nella tarda serata dell'11 settembre, un numero consistente di miliziani, probabilmente appartenenti al gruppo terroristico islamista Ansar al Sharia, dotati di armamento individuale, di mitragliatrici e di lancia granate, irrompe proditoriamente all'interno della base nella quale l'ambasciatore è protetto da personale del GRS Global Response Staff della CIA, di fatto un gruppo molto ristretto di operatori che da appaltatori (leggasi security contractors) hanno il compito di proteggere, insieme a militari statunitensi e ad appartenenti alla Brigata 17 febbraio della forza armata libica, la sede diplomatica e la persona dell'ambasciatore. L'attacco si trasforma in una battaglia e le sorti dello scontro subiscono immediatamente una virata estremamente negativa per la compagine statunitense, allorché i soldati libici della 17 febbraio, tranne pochi elementi, fuggono all'arrivo degli attaccanti, che riescono senza alcun impedimento ad entrare rapidamente nel perimetro del compound, costringendo l'ambasciatore ed alcuni uomini che lo proteggevano a chiudersi in un edificio che poco dopo sarà dato alle fiamme dai terroristi. L'ambasciatore ed un ufficiale americano moriranno di lì a breve, probabilmente per soffocamento in conseguenza dell'incendio appiccato dagli insorti e del fumo che invade i locali dello stabile. Per evacuare i caduti ed i feriti dovranno giungere altri elementi del GRS da una sede poco distante, che una volta arrivati ingaggeranno una vera e propria battaglia per riuscire ad aprirsi la strada, per estrarre il personale e portarlo in sicurezza verso una sede sicura, fino all'aeroporto.

L'azione di attacco da parte degli "insurgents" arrivò in maniera totalmente inaspettata e senza che vi fossero state avvisaglie o scaramucce di alcun tipo. Si trattò della prima volta nella quale un diplomatico statunitense di così alta levatura venne fatto oggetto di un'azione terroristica strutturata e le conseguenze di questo drammatico episodio avranno di lì a breve, e nei mesi a seguire, una ricaduta pesantissima sulla politica interna americana, allorché l'allora segretario di stato Hillary Clinton vide, di fatto, precipitare le sue quotazioni nella corsa alla presidenza, dopo la pubblicazione di email, in alcune delle quali si evinceva la sua determinazione a non autorizzare l'intervento dell'aeronautica americana a supporto del personale impegnato nella battaglia a Bengasi, lasciando al loro destino i quattro caduti e rendendo ancor più complesse e drammatiche le fasi dello scampo.

Alcuni passaggi riguardanti lo svolgimento degli eventi in questo specifico, drammatico episodio hanno rappresentato una specie di “unicum”. Proviamo ad evidenziare quali.

In primis si è trattato, come già ripetutamente sottolineato, di un attacco proditorio ad un diplomatico statunitense, culminato con la sua uccisione e con l’assassinio di altri suoi tre connazionali. Mai si era verificato nulla di simile, malgrado i numerosi interventi in teatri nei quali, in situazioni di guerra o di conflitti asimmetrici, il governo degli Stati Uniti si è trovato ad operare negli ultimi decenni, situazioni nelle quali non di rado il personale assegnato ha corso rischi anche gravissimi in termini di incolumità fisica e di minacce.

Appare poi evidente la totale mancanza di concreto supporto in termini di intelligence. Nessuno degli apparati preposti e delle numerose compagini governative, impegnate in quel teatro in tale ambito, aveva raccolto, elaborato e diffuso dati relativi ad una possibile, siffatta minaccia. Non erano stati generati e diffusi “alert” specifici che avrebbero reso più adeguato il sistema di difesa e certamente più performante la risposta in caso, come poi è drammaticamente accaduto, di attacco. Questo “gap informativo” è tanto più grave se si considera la pericolosità del teatro, il momento storico ed il dispiegamento di uomini e tecnologia, tutti aspetti che caratterizzano da sempre l’impiego del dispositivo di difesa americano e che evidenziano una gravissima sottovalutazione della minaccia e dei rischi. Di questo e di molti altri aspetti relativi ad inadempienze ed inadeguatezza, si è fatta ricadere la responsabilità sul Segretario di Stato Hillary Clinton, inficiandone la corsa alla presidenza nella successiva tornata e causando, come già detto, una pesante ricaduta sulla politica interna. Malgrado l’impego di personale altamente specializzato, addestrato ed equipaggiato, come è nel caso degli operatori del GRS, non è stato possibile salvare la vita dell’ambasciatore e degli uomini caduti nell’imboscata fra i quali vi era peraltro un ufficiale di quella Unità. Soltanto le capacità tattiche, il coraggio e la ferrea volontà degli altri appartenenti a quella che si può considerare a tutti gli effetti una unità paramilitare della CIA, hanno permesso lo scampo dei sopravvissuti, scampo che è comunque costato ulteriori feriti ed una difficilissima fuga operata armi in pugno.



Omicidio dell'ambasciatore Luca Attanasio

Nel febbraio di questo anno, l'ambasciatore italiano in Congo, Luca Attanasio, si trovava sulla strada nei pressi di Kibumba nella provincia del Nord Kivu, ai confini del Ruanda, in viaggio insieme a personale del PAM (Programma Alimentare Mondiale) ed al carabiniere Vittorio Iacovacci, assegnato alla sua tutela. Il trasferimento si prospettava come potenzialmente rischioso, vista la necessità di attraversare aree instabili di quella regione, aree nelle quali si muovono gruppi armati che svolgono attività criminali e nel cui territorio agiscono, stando a recenti calcoli, circa cento milizie, alcune delle quali da qualche tempo vanno manifestando le loro simpatie e la loro vicinanza al terrorismo islamista di Daesh. La premessa "tattica", in ordine al coefficiente di sicurezza nel quale il dispositivo si muoveva, è quella di essere sufficientemente protetti dall'ombrello garantito dal Programma Alimentare Mondiale al quale faceva riferimento l'attività in cui erano coinvolti in quella circostanza i nostri Attanasio e Iacovacci e di avere poco lontano la missione Monusco percepita come "strong partnership" in quell'area.

Questi due fattori, ovvero la bandiera del PAM e la vicinanza di Monusco, hanno probabilmente orientato in maniera negativa, visto poi l'epilogo con il quale si è chiusa la vicenda, le scelte relative alle disposizioni da prendere in materia di sicurezza, innescando una serie di accadimenti che sono culminati nella tragedia del 22 febbraio. Una breve ma doverosa premessa: appare evidente come un solo operatore armato di pistola, come era nel caso del carabiniere Iacovacci, non possa in alcun modo essere considerato in grado di difendere la personalità, tanto più se si considera che, in termini di potenziale minaccia, i possibili aggressori che si muovono ed agiscono in quell'area sono in genere dotati di armamento individuale da guerra, spesso consistente in un fucile d'assalto di fabbricazione russa o cinese, di lanciagranate e di pistola.

Ma torniamo alla cronaca dei fatti ed alla ricostruzione degli accadimenti che è possibile fare sulla base delle notizie acquisite e delle testimonianze raccolte. Mentre il convoglio del PAM, privo di qualsiasi ulteriore assetto di sicurezza ad esclusione del solo carabiniere Iacovacci (armato unicamente della pistola di ordinanza poi ritrovata nel cassetto porta oggetti della autovettura, con tutte le munizioni nel serbatoio) ed a bordo di SUV "soft-skin" (ovvero non dotati di protezione balistica) sta attraversando l'area precedentemente descritta, viene improvvisamente fatto oggetto di colpi di arma da fuoco (sparati, parrebbe, da un gruppo di assalitori composto da sei elementi), colpi che uccidono all'istante l'autista congolese della autovettura sulla quale viaggiano Attanasio e Iacovacci. Stando alle informazioni raccolte dai nostri inquirenti che hanno ascoltato i testimoni della vicenda, i due vengono poi costretti a scendere sotto la minaccia delle armi, in quello che sembra configurarsi a tutti gli effetti come un tentativo di sequestro di persona. Il gruppo composto dai rapitori e dai due italiani, non appena addentratosi nella foresta,

viene però immediatamente ingaggiato da una pattuglia di Rangers congolesi che trovandosi casualmente nelle vicinanze del luogo di accadimento dei fatti ed avendo, in pratica, quasi assistito in diretta alle fasi iniziali dell'azione, decidono di intervenire armi in pugno, accendendo un breve ma intenso conflitto a fuoco con i banditi. Nello scambio caotico, breve ma molto intenso di colpi, rimane praticamente ucciso sul colpo il carabiniere Iacovacci e viene più volte colpito l'ambasciatore Attanasio che, pur se soccorso immediatamente, morirà per le ferite riportate, poco più tardi sulla via dell'ospedale. In tema di comprensione di quanto accaduto, gli inquirenti si orientano sin da subito verso la possibilità che si sia trattato di un tentativo di rapina o, peggio ancora, di sequestro, finito in tragedia. Resta il fatto che, in entrambi i casi, il presupposto è quello che gli assalitori fossero stati in qualche modo informati riguardo al transito di un piccolo convoglio del PAM con a bordo personale straniero di rango e che attendessero il passaggio delle due autovetture per sferrare l'attacco. In tal caso, sarà importante cercare di comprendere come sia avvenuta la perdita di informazioni e di riservatezza riguardo alla attività in programma e chi abbia eventualmente trasmesso la notizia agli assalitori.

Vorrei sottolineare come organizzare un trasferimento di molti chilometri, in area non permissiva, senza un adeguato dispositivo di protezione, esponga a rischi che possono purtroppo anche generare esiti drammatici come accaduto in questa situazione. Spesso in circostanze simili, chi scrive ne ha esperienza diretta, malgrado si sia pensato a tutto e non si sia lesinato sulla pianificazione e sulla messa in atto di un dispositivo adeguato, si ha come l'impressione di essere sotto dimensionati rispetto alle possibili minacce ed alle reali esigenze, vista la tipologia di potenziali aggressori, la loro ferocia, le non trascurabili motivazioni di carattere terroristico e la conoscenza che hanno del territorio nel quale si è costretti a muovere. Senza in alcun modo voler puntare il dito contro i due nostri poveri connazionali che hanno pagato con la vita la loro volontà di agire, non si può non partire dalla considerazione che un errore di valutazione riguardo allo scenario nel quale si andrà ad agire, oppure una sottostimata capacità di portare attacchi da parte di chi si muove in quella stessa area, così come un errore nella analisi e valutazione del rischio, possono purtroppo portare a conseguenze drammatiche.

Parallelismi

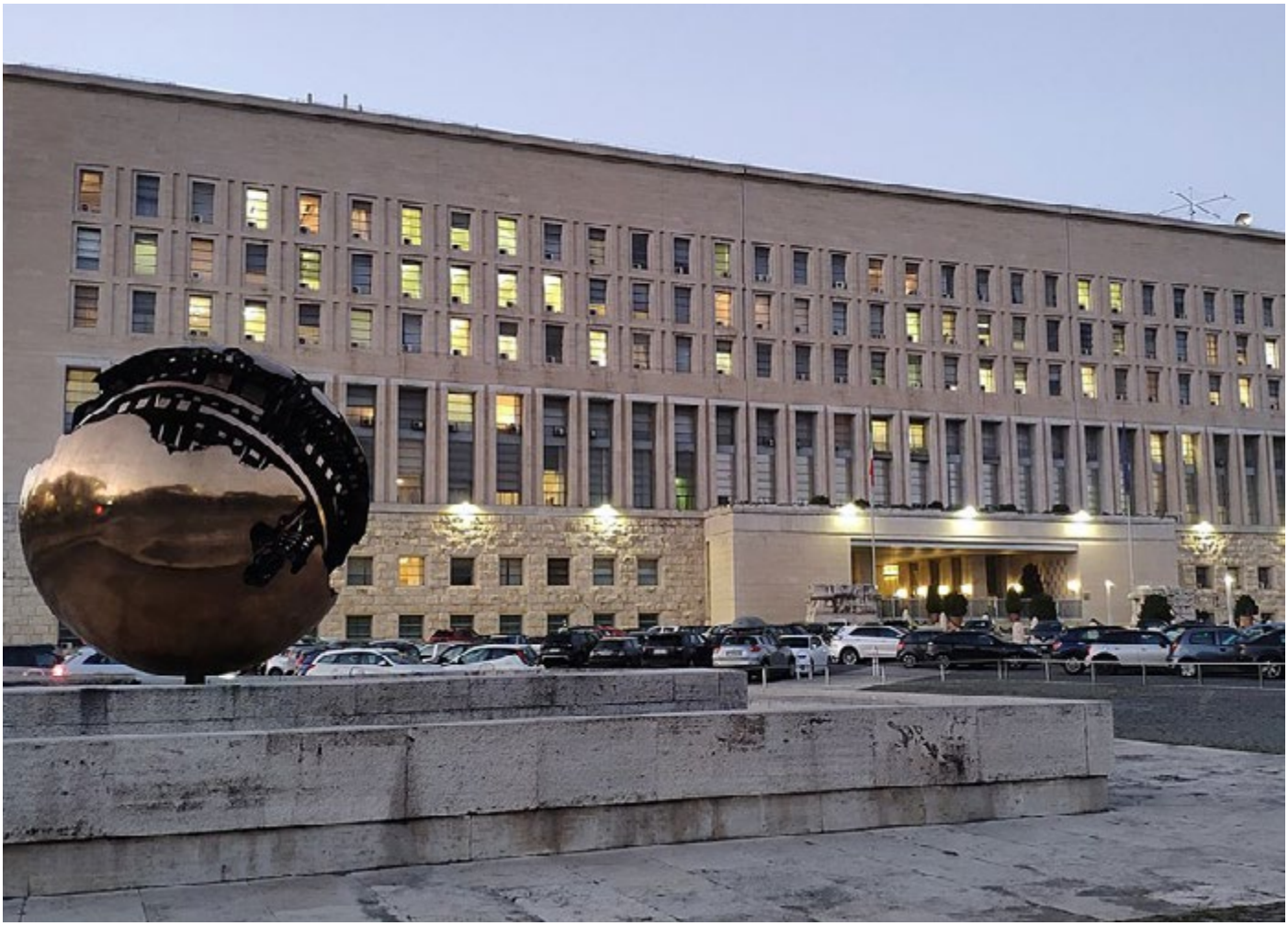
I due episodi presi in esame hanno collocazione temporale e localizzazione diverse, si sono svolti con modalità differenti (nel primo l'attacco è stato portato all'interno di un compound diplomatico, mentre nel secondo l'aggressione armata si è verificata durante un trasferimento) ed hanno entrambi cagionato la morte di due ambasciatori oltre che di alcuni dei componenti del dispositivo di protezione.

Ulteriori differenze rispetto a quanto già ricordato, possono essere individuate nel fatto che nel primo episodio hanno trovato la morte un ambasciatore ed alcuni appartenenti al suo dispositivo di protezione composto da un numero non limitato di operatori di alto profilo, mentre nel secondo sono deceduti un ambasciatore e l'operatore incaricato della sua protezione, ma sarebbe più corretto dire della sua tutela, operatore che pur se addestrato e motivato non apparteneva, per specificare, alla aliquota che per standard e procedura è sempre coinvolta nella protezione di personale diplomatico in locazioni ad alto rischio, ovvero quella composta da operatori del Reggimento Carabinieri Paracadutisti Tuscania (personale questo che, è lecito immaginare, avrebbe ancor più rigidamente adottato procedure ed attuato disposizioni che avrebbero certamente ridotto l'esposizione al rischio nel quale sono incorsi l'ambasciatore Attanasio ed il carabiniere Iacovacci). Va anche specificato che l'impiego o meno di personale del Tuscania in una

determinata ambasciata è decisione che viene presa sulla base di una valutazione del rischio operata da un apposito ufficio del MAE che stabilisce, appunto, quale sia il coefficiente di rischio ed il livello della minaccia, sede per sede.

C'è però un aspetto che va sottolineato e che costituisce a mio avviso un parallelismo fra i due drammatici episodi e si tratta delle mancanze che potrebbero, ed almeno nel primo caso parrebbero assodate, esservi state in termini di raccolta e condivisione di informazioni di intelligence utili a definire i contorni della attività che ci si preparava a compiere, informazioni necessarie ad inquadrare il livello di rischio nel quale si agisce sulla base del tipo di minaccia, permettendo così di essere pienamente consapevoli di quanto potrebbe accadere e di adottare le necessarie contro misure.

Riesce infatti difficile comprendere come in un teatro come era la Libia post rivoluzione il dispositivo pur di alto profilo incaricato di proteggere la più alta carica degli Stati Uniti d'America non fosse informato riguardo all'incremento esponenziale del rischio di attacchi, così come sembra davvero complicato capire come il sistema di intelligence non avesse colto segnali, pur se deboli, che indicassero la volontà di compiere azioni che colpissero l'ambasciatore e la sua scorta addirittura violando una locazione diplomatica.



D'altro canto, nel drammatico caso del nostro ambasciatore e del carabiniere uccisi in Congo, credo vada compreso quanto gli organismi preposti alla raccolta di informazioni in loco ed alla valutazione della minaccia avessero messo in guardia riguardo alla pericolosità dello spostamento e della inadeguatezza degli assetti di protezione relativamente al contesto ed al rischio. Per quanto attiene a questo aspetto, riterrei sia stato possibile che a qualche livello vi sia stata una sottovalutazione del rischio, probabilmente correlata alla falsa convinzione che la sommatoria fra, abitudine a muoversi in quello specifico settore da parte del PAM con la convinzione di agire "dalla parte del bene" (ovvero in un contesto di supporto alle popolazioni locali ed alle fasce più disagiate oltre ad una consolidata esperienza nel lavorare e muoversi in quel paese) rendessero, a parere dell'ambasciatore, esigue le possibilità di incappare in problemi seri e di difficilissima soluzione, come è poi invece drammaticamente accaduto.

Appare comunque evidente il fatto che una non adeguata ed integrata attività di intelligence, una sottovalutazione del rischio e assetti di protezione numericamente sottodimensionati (oppure inadeguati dal punto di vista addestrativo e della performance) possono portare a conseguenze davvero drammatiche.

La sempre più frequente necessità di muoversi in ambienti non permissivi, unita ad una connotazione di tipo terroristico di gruppi e milizie che operano attacchi in molti continenti, oltre ad un incremento di azioni criminali in vaste aree del mondo, rendono sempre più necessaria l'integrazione fra l'intelligence, la raccolta di informazioni dettagliate sugli scenari e la disponibilità di aliquote altamente specializzate sia in termini di supporto di intelligence che di preparazione tattica orientata alla protezione ravvicinata. Appare anche evidente come sia fondamentale, visti gli scenari in divenire e le sfide che attendono il nostro paese, tornare ad un più concreto e serrato impiego di risorse humint ed enfatizzare la raccolta di informazioni attraverso l'impiego degli operatori in teatro. Non è più pensabile, a mio parere, delegare la raccolta al mero strumento tecnologico ed all'utilizzo di apparati che offrono certamente vantaggi, ma che hanno dimostrato di valere davvero poco senza l'irrinunciabile supporto ed apporto degli operatori sul terreno.

RUBRICA: L'intervista

MARCO PUGLIESE - Luttwak: nessuna guerra batteriologica, solo incompetenza e propaganda

In USA ormai hanno le idee chiare e l'analista Edward Luttwak, raggiunto dalla nostra testata, ci illustra nel dettaglio che cosa successe nell'ormai famoso laboratorio di Wuhan, che tanto ha fatto parlare e speculare i media globali.

L'origine del Sars-Cov-2 naturale od artificiale? La risposta a questa domanda aleggia nelle redazioni di mezzo mondo da circa un anno e tutto ruota intorno a Wuhan, sede d'un laboratorio di classe 4.

Anche una trasmissione italiana (TGR Leonardo, Rai 3) s'occupò del laboratorio, in questa puntata del novembre 2015 (Coronavirus e Sars2 - Puntata di TGR Leonardo RAI3 del 16/11/2015 - YouTube), citata anche da Luttwak nel corso dell'intervista. Nel servizio del 2015, firmato da Maurizio Menicucci, si sosteneva che scienziati cinesi avessero creato un "supervirus polmonare da pipistelli e topi" per "motivi di studio", aggiungendo: "Un gruppo di ricercatori cinesi ha innestato una proteina superficiale presa dai pipistrelli su un virus che provoca la Sars ricavato da topi, creando un supervirus che potrebbe colpire l'uomo".

La comunità scientifica s'affrettò a smentire ma il dubbio rimase. Poi s'aggiunge la figura di Shi Zhengli, 55 anni, citata anch'essa da Luttwak. La dottoressa dirigeva il centro di nuove malattie infettive del laboratorio di virologia di Wuhan, un centro sperimentale, legittimo e con all'interno dei progetti ricercatori cinesi, britannici, francesi e perfino americani.

Professor Luttwak, il Covid è artificiale?

Il Covid esce da un laboratorio cinese, un laboratorio di ricerca legittimo ma gestito male. A Wuhan lavoravano ricercatori internazionali.

Gestito male?

Si, un laboratorio di classe 4 che fu aperto alla vostra trasmissione italiana Leonardo come nulla fosse... si tratta d'incompetenza.

Professore, quindi lei smentisce si tratti di un'arma?

Non siamo di fronte ad armi ma ad esperimenti gestiti male. In questi laboratori si hanno massimo due studenti a ricercatore, qui erano dieci. Un viavai continuo, una pubblicità continua. Si tratta di propaganda...

Ma quindi la Cina avrebbe semplicemente gestito male un laboratorio di ricerca?

Assolutamente, con all'interno ricercatori internazionali. Ma dirò di più: la propaganda cinese ha fatto un lavoro ottimo, si è autoaccusata d'aver creato un qualcosa di militare, in questo modo gli altri ricercatori hanno smentito per forza e la comunità internazionale ha abboccato. L'OMS che ha fatto? Nulla.

Ma il virus pare sia in circolo da prima di gennaio?

Stando ad informazioni non classificate e quindi pubbliche sappiamo che tre virologi operanti nel laboratorio nel novembre 2019 furono ricoverati e trattati

come pazienti gravi. Non fu specificato il motivo e nessuno poi può sapere se fossero i primi.

La Cina quindi avrebbe dovuto avvisare il mondo due mesi prima?

Alla Cina interessava solo fare i propri eventi a Wuhan, una vera e propria capitale economica. Quindi chiunque in quel periodo si mettesse di traverso veniva fatto tacere. Come quel medico...

Il dottor Li?

Esatto. Il dottor Li venne fermato dalla polizia cinese, minacciato, screditato prima di essere riabilitato e fatto tornare al suo lavoro in corsia a Wuhan, poi fu ucciso dal virus. Il cordoglio dell'OMS fu inutile, andava protetto prima.

Quei due mesi furono quindi cruciali?

Assolutamente, la Cina e l'OMS non fecero nulla onde evitare questo disastro globale. Ora il resto del mondo deve fare qualcosa, UE ed USA in primis.

Che genere d'iniziative?

Vanno fatte delle indagini, gli USA lo stanno facendo, è stato preso in mano il lavoro di Trump da Biden ed infatti in questi giorni i nostri giornali se ne occupano.

Esiste un rapporto d'intelligence USA dettagliato, cosa contiene?

Non risponde (NdA).

L'ipotetica iniziativa del G7 o del G20 avrebbe un senso?

Va fatta chiarezza e bisogna andare oltre la propaganda cinese. Ci sono paesi che comprano il vaccino cinese ad esempio, aderiscono alla Via della Seta, alleanza militare, non economica come si dice.

Cosa suggerisce professore?

Di essere coesi, di non parlare di guerra biologica ma d'incompetenza.

Ci congediamo dal professor Luttwak proprio con la mente all'ultimo anno di pandemia, agli ossimori che abbiamo vissuto ed all' infodemia che ha dilaniato società e media, fino alla comunità scientifica.

In mezzo tanti piccoli progetti di vita, molte volte devastati dallo tsunami pandemico che ha spezzato vite e sogni. Forse però uno spiraglio arriva dal mondo dell'intelligence USA, si vuol far chiarezza, capire, analizzare ed è un bene, questo è un periodo storico che brama delle fondamenta di certezza.

Marco Pugliese

*Edward Nicolae Luttwak (Arad, 4 novembre 1942) è un economista, politologo e saggista romeno naturalizzato statunitense, conosciuto per le sue pubblicazioni sulla strategia militare e politica estera, esperto di politica internazionale e consulente strategico del Governo degli Stati Uniti d'America.

RUBRICA: La parola all'esperto cyber

ANGELO RIGHI - Ransomware e Infrastrutture Critiche

Il 7 Maggio 2021, la Colonia Pipeline, un'azienda texana con sede nei pressi di Houston, viene colpita da un attacco ransomware. La notizia potrebbe non avere particolare rilevanza (dopotutto, quotidianamente, aziende, privati e agenzie pubbliche vengono colpite da attacchi di questo genere) se non fosse per il fatto che Colonia Pipeline gestisce uno dei più grandi oleodotti statunitensi che rifornisce la costa orientale.

L'attacco ransomware in questione porta, nel giro di poche ore, alla paralisi dell'importante infrastruttura energetica, durata alcuni giorni.

Per la prima volta, un attacco cibernetico, in questo caso un attacco ransomware, blocca un'importante infrastruttura americana.

Criptovirus e Criptovalute

I ransomware sono una particolare famiglia di malware (programmi nocivi e pericolosi), che "sequestrano" i dati cifrandoli, rendendoli così illeggibili e inutilizzabili dal legittimo proprietario. L'utente, per riottenere il controllo dei propri dati, deve pagare un riscatto (dall'inglese "ransom").

Conosciuti anche come "criptovirus", i ransomware non sono una novità. Benché esistano da decenni, hanno avuto una diffusione sempre maggiore negli ultimi anni.

Probabilmente, a facilitare il successo di questo modello criminale sono state la diffusione e la sempre crescente popolarità delle criptovalute. Infatti, generalmente il riscatto è rappresentato da richieste di versamento di criptovalute (in genere Bitcoin) sui "conti correnti" dei pirati.

Dal punto di vista dei cybercriminali, le criptovalute offrono il vantaggio di un alto grado di anonimato.

Ransomware as a Service (RaaS)

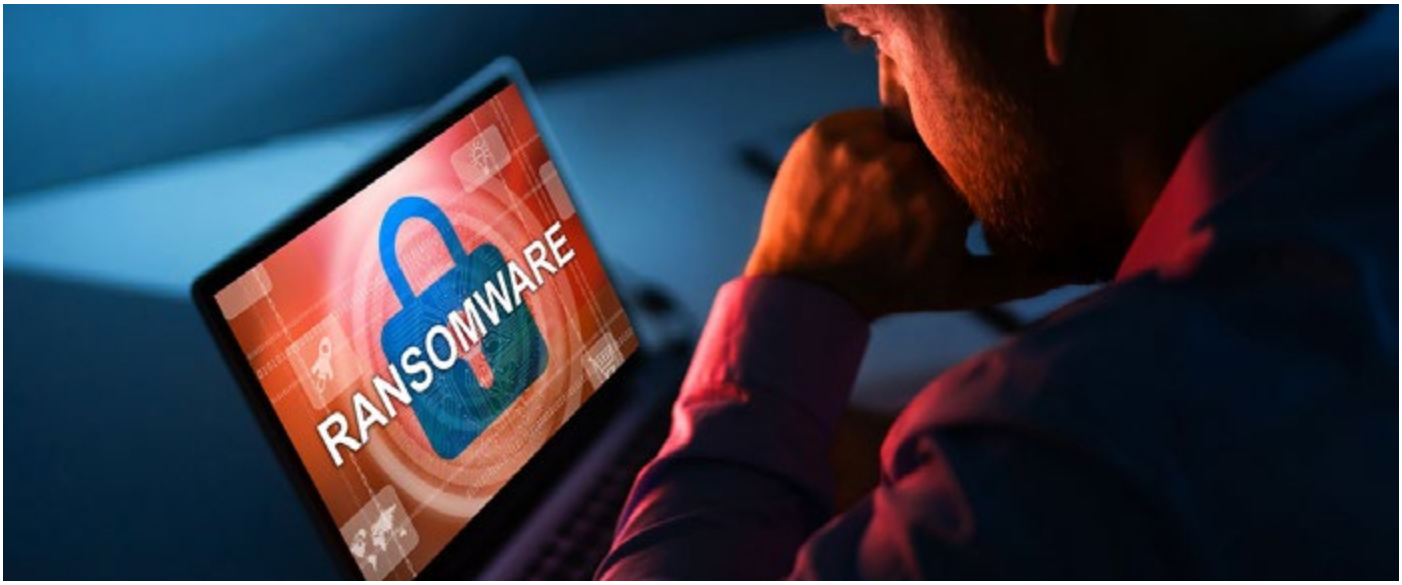
I primi attacchi ransomware erano molto semplici: gli stessi hacker che creavano i malware infettavano le proprie vittime (in genere tramite attacchi phishing), riscuotevano il riscatto e, dopo aver ricevuto i Bitcoin, inviavano alle vittime le chiavi per poter decifrare i dati in "ostaggio".

Oggi il modello si è notevolmente evoluto. In alcuni casi, i gruppi di cybercrime più potenti organizzano dei veri e propri servizi, i cosiddetti RaaS (Ransomware as a Service, Ransomware come servizio).

Le gang che gestiscono questi servizi affittano, tramite portali nel Dark Web, i malware ad altri gruppi o individui: sono poi questi ultimi ad effettuare gli attacchi veri e propri, riconoscendo una percentuale del riscatto ai gestori del servizio (in genere tra il 20% o 30%).

Doppio ricatto

Non solo il modello di business si è evoluto nel tempo, ma anche la tipologia di attacco. Se all'inizio i



ransomware si limitavano a cifrare automaticamente i dati e una volta conclusa l'operazione crittografica presentavano una pagina con la richiesta del riscatto e le modalità di pagamento, negli ultimi anni le operazioni si sono trasformate in vere attività di spionaggio e furto di dati.

Negli attacchi ransomware più sofisticati, i pirati, una volta aggirate le barriere perimetrali, si insinuano furtivamente nel sistema, setacciando la rete alla ricerca di dati sensibili; questi dati vengono quindi esfiltrati e utilizzati come ulteriore ricatto nei confronti della vittima.

Infatti, i cybercriminali non solo cifrano i dati (rendendoli inutilizzabili), ma minacciano di rendere pubblici i dati sensibili sottratti.

Attori principali e Attribuzione

Chi c'è dietro a questi attacchi? A differenza dalle operazioni di spionaggio sponsorizzate da Stati, ed eseguite da gruppi mercenari, più o meno dirette emanazioni di agenzie di intelligence, le attività di Ryuk, REvil, Conti, DarkSide (questi i principali ransomware) sembrerebbero essere generate da gruppi criminali orientati esclusivamente al profitto economico.

Anche la localizzazione geografica, individuata in Russia o comunque nei territori delle ex repubbliche sovietiche, non dovrebbe avere particolari implicazioni geopolitiche.

Non è escluso che il cybercrime e lo spionaggio cibernetico abbiano un sotterraneo legame comune (di natura soprattutto tecnica); non si può neppure escludere che operazioni ransomware siano in realtà sabotaggi mascherati (è già accaduto, per esempio in Ucraina nel 2017, attacco NotPetya).

Di fatto, al di là della propaganda e dal sensazionalismo mediatico, l'attribuzione di questo tipo di attività può essere un vero rompicapo, reso ancor più complicato dalla potenziale presenza di elementi di depistaggio.

Quello che è certo è che non ci libereremo facilmente di queste minacce cibernetiche, anzi probabilmente assisteremo ad un'escalation di attacchi sempre più dannosi.

RUBRICA: Riproponiamo...

O.S.S.I.S.Na. - La protezione degli asset industriali strategici

INTRODUZIONE

La grave emergenza sanitaria dovuta al COVID-19 ha determinato la necessità, da parte del Governo Italiano, di ricorrere alla capacità del Sistema Paese per affrontare la drammatica situazione in corso. L'improvvisa comunicazione della pandemia e la sua rapida diffusione "a progressione geometrica" hanno comportato, in tempi brevissimi, una forte riduzione delle attività economiche, il blocco quasi totale della mobilità privata e l'isolamento sociale (meccanismo di lockdown).

Ci si è trovati di fronte a uno scenario inimmaginabile, che - ancorché ipotizzato nella letteratura accademica - è però risultato non prevedibile nella gestione dei suoi effetti, nei tempi e nei modi. Ciò ha determinato a posteriori, da parte delle istituzioni nazionali e locali, l'assunzione di decisioni urgenti e limitative dei diritti costituzionalmente riconosciuti ai cittadini e con restrizioni nella produzione economica del Paese, con lo scopo assolutamente prioritario di contrastare efficacemente la diffusione incontrollata del virus.

Il rapido accadimento degli eventi è stato accompagnato da una accettabile disciplina nei comportamenti della quasi totalità dei cittadini e da una comunicazione mediatica però non sempre coerente, dapprima rassicurante e poi costretta a toccare - anche attraverso inedite metafore belliche - le corde emotive della paura reale e percepita. La situazione contingente ha determinato pesanti conseguenze sull'intero tessuto socio-economico del Paese, con elevati rischi per la disponibilità di beni e servizi di primario interesse collettivo. L'immediata attivazione di strumenti pubblici (operativi e finanziari) da parte dei ministeri competenti, coordinati dalla Presidenza del Consiglio dei Ministri, ha consentito di far fronte alle necessità più urgenti, evitando la paralisi generale e mantenendo adeguati livelli di tenuta sociale. Nel contempo è stato possibile massimizzare gli sforzi per gli interventi di gestione dell'emergenza, anche attraverso la creazione di alcune task force tematiche.

In tale scenario di crisi è emersa - come fattore di particolare rilevanza per la Sicurezza Nazionale - la necessità di protezione degli asset industriali strategici, definiti come infrastrutture e filiere produttive per le quali il blocco parziale o totale delle proprie capacità operative può arrecare pregiudizio alla sicurezza e al benessere della collettività.

Il presente studio si propone di affrontare tale tematica, proponendo un modello organizzativo con cui l'operatore economico (gestore dell'asset) possa predisporre un piano integrato di security management, operations continuity & crisis communication da applicare in caso di "stato di emergenza".

PROTOCOLLO DI PROTEZIONE

Per la definizione del protocollo di protezione da adottare si è attinto alle best practices di gestione dei rischi già introdotte efficacemente nel settore

della protezione antisabotaggio/antiterrorismo di infrastrutture critiche e siti sensibili, avendo ritenuto particolarmente utile quell'approccio "all hazard", meticoloso e concreto al tempo stesso, orientato all'ottimizzazione organizzativa.

I comparti produttivi prioritariamente interessati sono quelli legati alle utilities (energia elettrica, gas, risorse idriche, gestione rifiuti), all'industria hi-tech (difesa, aerospazio, ecc.), alla sanità (ricerca biomedica, produzione chimico-farmaceutica, ecc.), alle telecomunicazioni (prodotti e servizi IT, emittenti radiotelevisive, ecc.), all'intero sistema dei trasporti (terrestre, aereo e marittimo), alla produzione siderurgica, al settore petrolchimico e alla filiera agroalimentare.

Il modello organizzativo proposto si applica ai cosiddetti scenari di crisi, intesi come situazioni non convenzionali nelle quali fattori esterni - non adeguatamente prevedibili negli effetti - possono recare grave pregiudizio alla capacità operativa dell'organizzazione stessa.

Tipici scenari di crisi sono le emergenze sanitarie, gli eventi bellici, gli atti terroristici e le crisi socio-economiche.

Si distinguono inoltre due tipologie di gestione dell'organizzazione: esercizio ordinario (in situazione di normale operatività) ed esercizio straordinario (in situazione di crisi).

La gestione operativa dell'asset strategico in scenari di crisi deve essere definita, implementata e validata in periodi ordinari.

Il piano di protezione viene definito sulla base di un protocollo specifico, già sviluppato per esigenze di Sicurezza Nazionale nell'ambito delle infrastrutture critiche e ora completato con una sezione dedicata alla gestione della comunicazione, di particolare rilevanza nelle situazioni di crisi, che la pandemia in corso ha fatto emergere sia come ulteriore e significativo elemento di rischio che come strumento di mitigazione dello stesso (utile anche nella condotta esecutiva per i comportamenti di massa).

ANALISI E GESTIONE DEL RISCHIO

L'attività è basata su una rigorosa metodologia di risk management con l'obiettivo primario della tutela del patrimonio tangibile e intangibile dell'organizzazione (risorse umane, beni strumentali, know-how tecnologico) e della relativa struttura finanziaria.

Il protocollo è principalmente rivolto a mitigare i rischi derivanti da minacce di natura fisica, biologica, cibernetica, reputazionale e finanziaria da parte di entità ostili nazionali ed estere, aventi finalità di interdizione e sabotaggio delle attività operative oppure di acquisizione malevola delle capacità tecnologiche.

Le minacce vengono così classificate (in ordine crescente per gravità):

- minacce percepite (minacce possibili, ma senza informazioni precise);
- minacce diffuse (minacce generiche per la presenza sul territorio di gruppi criminali, per situa-

zioni socio-politiche instabili, ecc.);
- minacce indirette (minacce rivolte a infrastrutture esterne ma con possibili ripercussioni sull'asset);
- minacce dirette (minacce rivolte in maniera specifica all'asset).

Ogni possibile evento ostile (per ciascuna delle minacce considerate) viene valutato nel suo impatto e nella sua probabilità di accadimento sulla base delle informazioni acquisite (in cooperazione con gli organismi di pubblica sicurezza e di intelligence nazionali preposti allo scopo), pervenendo alla definizione del cosiddetto "Livello di rischio" (secondo le categorie: accettabile, medio, inaccettabile).

Per ciascun livello di rischio è altresì stabilita la necessità dell'intervento di mitigazione, il quale può comportare opzioni organizzative, operative, tecnologiche e finanziarie che confluiscono nel "Piano di gestione dei rischi", integrato da un "Piano per la continuità operativa" e da un "Piano per la comunicazione in stato di crisi".

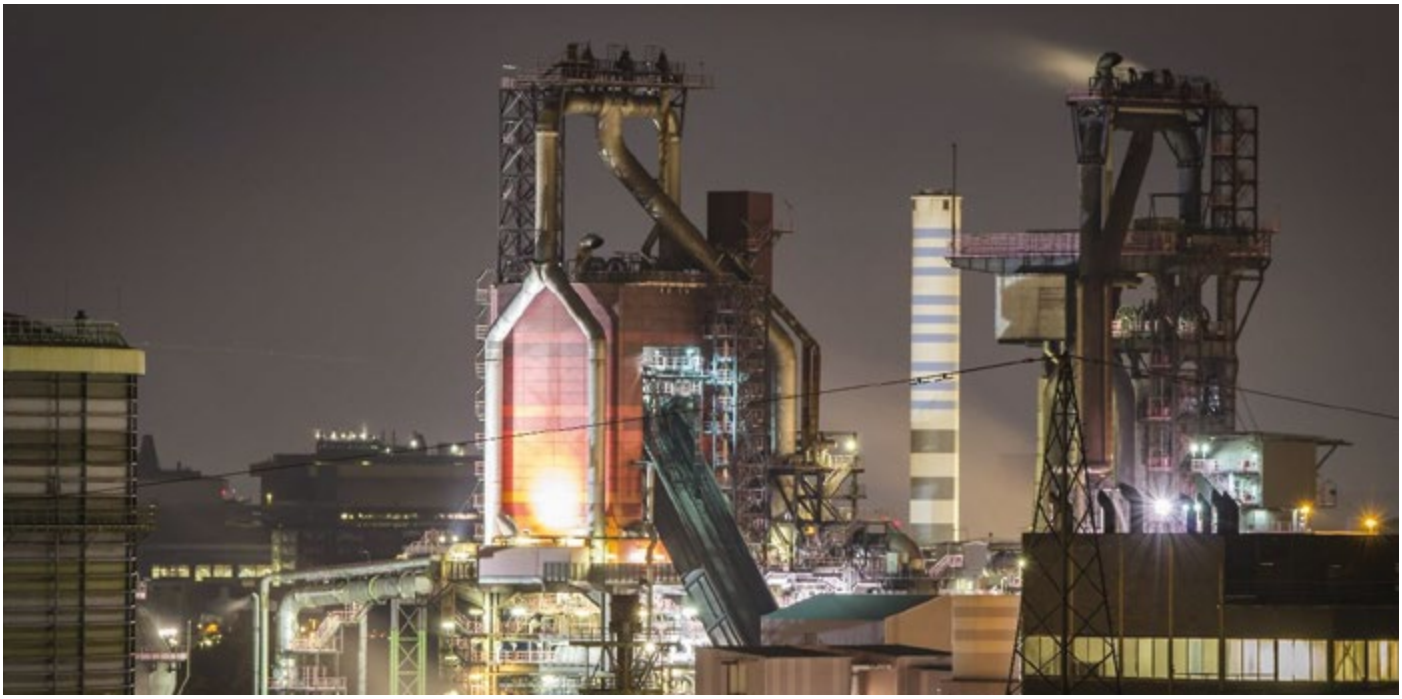
PIANO PER LA CONTINUITÀ OPERATIVA

Il protocollo prevede innanzitutto la definizione del "Piano di Emergenza" che considera per le diverse categorie di eventi:
- immediata attivazione di un'Unità di Crisi con un Responsabile Unico (con eventuale supporto di uno staff specialistico) in possesso di tutti i poteri ordinari e straordinari per un corretto e tempestivo coordinamento delle attività di emergenza e come unico referente verso le Pubbliche Autorità;
- esistenza di un efficace dispositivo di Comando & Controllo (procedure, postazioni e sistemi di comunicazione verso l'interno e verso l'esterno del sito industriale, ecc.);
- esistenza di squadre di Pronto Intervento (protezione antincendio e primo soccorso, gestione dei protocolli sanitari, eventuale protezione armata, ecc.);
- mantenimento in efficienza operativa di tutto il dispositivo previsto (esercitazioni periodiche, piano di formazione per il personale, ecc.);
- piano per la continuità delle attività operative interne ed esterne del sito industriale (svolta a cura dell'organizzazione interna e a cura della filiera di fornitura di beni e servizi o "supply chain");
- piano per il ripristino (parziale e totale) delle attività operative interne ed esterne del sito industriale.

Il "Piano di Continuità Operativa", da attuarsi durante l'intera situazione di crisi, deve quindi integrarsi in modo complementare al "Piano di Emergenza" e deve prevedere la definizione dei seguenti criteri operativi:
- tipologia delle attività operabili presso il sito;
- tipologia delle attività necessarie dalla filiera di fornitura esterna (supply chain) per beni e servizi;
- livelli minimi di "produzione beni" e/o "erogazione servizi" da garantire durante il periodo di crisi (criteri MPL - Mimimum Performance Level), prioritari rispetto ai normali obiettivi definiti dall'organizzazione per l'esercizio ordinario (i quali possono pertanto essere parzialmente o completamente derogati in considerazione delle mutate esigenze);
- risorse umane, strumentali e finanziarie necessarie in accordo ai possibili scenari di crisi;
- assetti di Comando, Controllo & Comunicazione durante la crisi (criteri Crisis-C3).

PIANO PER LA COMUNICAZIONE IN STATO DI CRISI

Il "Piano per la Comunicazione in stato di crisi" (o "Crisis Communication Plan") costituisce un potente strumento di gestione dei rischi operativi dell'asset, migliorando internamente la coesione organizzativa



e mitigando esternamente l'effetto di possibili fattori destabilizzanti anche di natura ostile (campagne di disinformazione, eccessi di informazioni o infodemie, scalate non controllate nei capitali azionari, ecc.).

Da un punto di vista operativo il piano di comunicazione prevede la definizione dei "target interni" (management, dipendenti, ecc.) e dei "target esterni" (stakeholder, soggetti istituzionali, clienti, fornitori, opinione pubblica, ecc.).

La comunicazione deve attuarsi secondo i criteri di completezza, chiarezza, trasparenza, coerenza ed efficacia, ancor più importanti in situazioni di crisi ove le attenzioni dell'intera organizzazione sono maggiormente focalizzate su aspetti operativi e il flusso di informazioni tra interno ed esterno può vedersi collocato in secondo piano (aumentando sensibilmente le vulnerabilità di sistema).

In tal senso il protocollo considera il piano di comunicazione come strumento fondamentale durante tutte le fasi dell'emergenza per minimizzare i rischi di carattere operativo (dovuti a confusione, incertezza e disorientamento) e di carattere reputazionale (dovuti a informazioni false, incomplete o inopportune), i quali possono a loro volta costituire - se non contrastati adeguatamente - un elemento amplificatore degli impatti relativi alle singole minacce.

Il piano di comunicazione deve prevedere:

- identificazione di un Responsabile Unico per la Comunicazione;
- modalità per la comunicazione delle azioni di emergenza verso il personale operante all'interno del sito industriale, inclusa la definizione dei dispositivi idonei per le comunicazioni di emergenza (sistemi informativi, dispositivi telefonici, altoparlanti, display, ecc.);
- esistenza di una lista di organizzazioni esterne da attivare in caso di crisi (agenzie di stampa, agenzie ambientali, ecc.);
- modalità per la comunicazione verso le organizzazioni esterne;
- definizione dei dispositivi idonei per le comunicazioni verso le organizzazioni esterne (sistemi di

telefonia su piattaforma fissa/mobile/satellitare, ponti radio, ecc.).

GESTIONE DEL RISCHIO REPUTAZIONALE

Il protocollo adottato prevede l'esistenza di un dispositivo organizzativo idoneo alla "Gestione del Rischio Reputazionale" durante il periodo di crisi, che ne definisca:

- il Responsabile (che può coincidere con il Responsabile della Comunicazione);
- gli strumenti operativi (quali il documento di "Analisi Preventiva per il Rischio Reputazionale");
- l'insieme degli elementi da considerare per l'analisi del Rischio Reputazionale, assicurando che vengano presi in esame fattori esterni (attacchi mediatici, fake news, eventi di diretta o indiretta potenziale responsabilità dell'organizzazione, ecc.) e fattori interni (eventi di natura sindacale, fake news, eventi di diretta o indiretta potenziale responsabilità dell'organizzazione, ecc.);
- il piano di monitoraggio per il profilo reputazionale dell'organizzazione del sito da attuarsi durante l'intero periodo di crisi (mediante analisi sistematica dei mass-media, raccolta informativa da iniziative di informazione interne/esterne quali volantinaggi e manifestazioni, ecc.);
- le tipologie di intervento (campagne di comunicazione di carattere preventivo e/o reattivo, ecc.)

Il "Piano di Gestione del Rischio Reputazionale" potrà essere incorporato all'interno del piano di comunicazione.

Inoltre, è opportuno che le attività definite per l'organizzazione del sito industriale nei possibili scenari di crisi e sin qui esposte (piano di gestione del rischio sicurezza fisica/cibernetica/reputazionale, piano di comunicazione, piano di continuità operativa) vengano riportate e riesaminate con sistematicità dalla Direzione Aziendale all'interno del "Rapporto di Sostenibilità" come elemento focale di responsabilità sociale e a beneficio di tutti i possibili portatori di interesse (stakeholders, lavoratori, fornitori, clienti, popolazione circostante, ecc.).

LA PROTEZIONE DELLE PMI NELLE FILIERE STRATEGICHE NAZIONALI

Particolare attenzione deve essere posta per gli operatori economici di piccole/medie dimensioni (PMI) operanti all'interno delle filiere strategiche nazionali.

Questa tipologia di impresa costituisce indubbiamente un elemento di forte potenzialità per know-how, capacità di innovazione e contributo al PIL nazionale, ma costituisce nel contempo un fattore di vulnerabilità nella catena produttiva (il cosiddetto "anello debole") per la forte esposizione a rischi di natura operativa e finanziaria.

Uno scenario di questo tipo è altamente probabile in contesti di crisi (come è avvenuto per l'evento pandemico del Covid-19) e in presenza di possibili soggetti ostili - soprattutto esteri - interessati a indebolire la capacità di tenuta del sistema produttivo nazionale (come emerge chiaramente dalle recenti audizioni del COPASIR).

Le PMI italiane - ancorché operanti all'interno di tali filiere strategiche - non appaiono oggi sufficientemente strutturate (nella quasi totalità dei casi) per mantenere livelli di protezione idonei a garantire continuità operativa e stabilità finanziaria durante le situazioni di emergenza nazionale, a differenza delle cosiddette "big corporate" che possiedono invece adeguate capacità organizzative in tal senso.

È quindi un interesse strategico delle grandi imprese (alla testa delle proprie filiere) il riposizionamen-

to dei propri "albi fornitori" su criteri di Crisis Risk Management, privilegiando quelle aziende che diano adeguate garanzie in situazioni degradate di sicurezza (come quelle indotte da una crisi globale) e garantendo pertanto una piena continuità operativa nella produzione/erogazione di beni e servizi a valle dell'intera catena.

Recependo questa necessità, il protocollo proposto nel presente studio intende fornire uno strumento di efficace implementazione nel contesto delle PMI operanti all'interno delle filiere strategiche nazionali, consentendo alle singole organizzazioni di mantenere - al manifestarsi di una improvvisa situazione di emergenza globale - le proprie capacità di protezione e di continuità operativa. Il protocollo è facilmente applicabile all'interno del sistema di governance (già operante nell'impresa) e necessita di essere successivamente validato e mantenuto latente in situazioni ordinarie, pronto ad attivarsi entro un arco temporale di 24 ore dal determinarsi di una situazione di crisi.

Per come già esposto nei paragrafi precedenti e in modo particolarmente significativo per una PMI, il protocollo affronta aspetti di protezione fisica, cibernetica, reputazionale e finanziaria in contesti di accentuata vulnerabilità (come quelli determinati da una crisi globale), basandosi su politiche di sinergia tra settore pubblico e privato in materia di obiettivi e strumenti operativi.

Ciò al fine di mitigare i possibili effetti generati da un'emergenza generale, che per una PMI possono essere identificati principalmente in blocco operativo, crisi finanziaria e acquisizione societaria ostile da parte di entità esterne (con conseguenti rischi di perdita/cessione di know-how, di riposizionamento di mercato e di delocalizzazione).

In un simile scenario, tutt'altro che teorico, le conseguenze sarebbero devastanti per il singolo operatore economico, per l'intera filiera di riferimento e per tutto il Sistema Paese, in un drammatico effetto domino.

Il rafforzamento delle misure di protezione è quindi orientato al conseguimento della massima efficacia in termini di rapporto costi/benefici, in modo da risultare ampliamente sostenibile per un operatore economico di dimensioni medio/piccole.

In questa "mission" si intende anche fornire un contributo metodologico alle politiche nazionali di attuazione della "Agenda 2030 per lo Sviluppo Sostenibile" promossa dalle Nazioni Unite, ove all'obiettivo 9 ("Imprese, innovazione e infrastrutture") e ai relativi sotto-punti è espressa la volontà di promuovere l'innovazione e una industrializzazione equa, responsabile e sostenibile (obiettivo generale), sviluppare infrastrutture di qualità, affidabili, sostenibili e resilienti (punto 9.1), aumentare l'accesso dei piccoli industriali e di altre imprese (punto 9.2), aggiornare le infrastrutture e ammodernare le industrie per renderle sostenibili (punto 9.3), promuovere le capacità tecnologiche dei settori industriali (punto 9.5).

Da questa prospettiva, si ritiene che un tessuto produttivo sostenibile debba essere prima di tutto un "contesto sicuro" come condizione imprescindibile di sviluppo per quella piccola e media impresa che in Italia è - da sempre - volano di innovazione e di forza creativa.

APPLICAZIONE DEL PROTOCOLLO ALLA FILIERA FARMACEUTICA PER LA LOTTA AL COVID-19

L'industria farmaceutica italiana sta assumendo un ruolo di primo piano su scala mondiale per la messa a disposizione del vaccino antiCOVID-19 e per i sistemi di rilevamento del virus (tamponi, reagenti, apparecchiature di analisi, ecc.). La visibilità mediatica di tale attività (di ricerca, sviluppo e avvio industriale) e i relativi valori economici espongono tutte le strutture

operative coinvolte a rischi reali di sicurezza da parte di entità ostili aventi l'obiettivo di acquisire know-how in modo fraudolento (per successiva immissione sul mercato di quantitativi imponenti di dosi, in tempi relativamente veloci) e di sabotare le attività di sperimentazione (esercitando un'azione criminale di "concorrenza sleale").

Non sono da escludere gli interessi geopolitici che i fragili equilibri economici sembrano offrire: alcuni governi infatti hanno la reale necessità di dimostrare la propria superiorità nella ricerca tecnologica e scientifica, la cui utile applicazione nelle strategie di "soft-power" a livello internazionale è facilmente intuibile.

In ambito nazionale, seppur con minore capacità operativa, potrebbero giocare un ruolo di disturbo alcuni movimenti cosiddetti no-vax, anche attraverso campagne mediatiche ad hoc (notizie fake sulle principali piattaforme social e azioni dimostrative di varia natura).

Come è possibile evincere, si tratta di una materia di primario interesse nazionale e in cui il Governo Italiano è pronto a rivestire un ruolo da protagonista. È infatti allo studio la possibilità di ingresso dello Stato nell'assetto societario delle aziende coinvolte, così da garantire nel contempo il necessario sostegno finanziario nelle successive fasi di produzione dei vaccini e un efficace presidio di sicurezza contro potenziali minacce.

La necessità di proteggere tali asset (da considerarsi "strategici" a tutti gli effetti) deve essere esercitata lungo l'intera filiera per evitarne l'interruzione e quindi l'efficacia:

- catena di approvvigionamento (afferente soprattutto al comparto chimico-farmaceutico e al settore del packaging dedicato);
- laboratori di ricerca e sviluppo (in ambito industriale);
- centri di sperimentazione clinica (in ambito ospedaliero);
- stabilimenti di produzione;
- siti di stoccaggio;
- operatori per la distribuzione (trasporti e farmacie);
- presidi per la somministrazione (ospedali, ambulatori, medici di famiglia, ecc.).

L'azione di protezione deve essere approntata in tempi estremamente veloci attraverso un'iniziativa sinergica tra Stato (tramite le sue articolazioni operative di Intelligence, di Pubblica Sicurezza e della Difesa) e i vari "operatori di filiera" coinvolti (industrie, laboratori di ricerca, strutture sanitarie, organizzazioni logistiche).

L'aspetto critico appare essere proprio quello relativo all'estensione della filiera, la quale dovrebbe disporre di specifici protocolli di sicurezza per prevenire azioni ostili (sabotaggi di natura fisica e cyber, furti di materiale e di know-how, attacchi mediatici di natura reputazionale).

Ulteriori minacce saranno costituite dai furti e dalla contraffazione dei suddetti vaccini per opera soprattutto della criminalità organizzata, afferente ai canali della distribuzione logistica, ove le attività di preven-

zione e contrasto saranno sostenute dalle autorità preposte in modo specializzato (in primis, Guardia di Finanza, Carabinieri/NAS e Ministero della Salute) e supportate comunque da sistemi avanzati di tracciabilità (identificazione e localizzazione) da predisporre e rendere accessibili a cura dell'industria.

Tali protocolli dovranno essere adottati in una prospettiva di alta efficacia (sia per le attività interne di filiera che per la sinergia tra settore pubblico e privato in ambito sicurezza) e di massima copertura (per casistica di minaccia e di aree di intervento), presupponendo le capacità operative particolarmente aggressive dei potenziali "soggetti ostili" e nella considerazione degli altissimi interessi economici e di potere in gioco.

Il protocollo presentato in questo studio - già sviluppato per la protezione degli asset strategici nazionali in contesti di crisi - viene pertanto reso ora disponibile per una veloce implementazione nelle filiere sopra descritte e su tutti gli aspetti critici evidenziati, con l'intento di disporre di un efficace strumento per la protezione delle organizzazioni coinvolte (in ambito industriale e sanitario) e affinché queste siano rese in grado di massimizzare i risultati delle proprie attività nella lotta al COVID-19.

ASSET INDUSTRIALI STRATEGICI E GEOPOLITICA

L'Interesse Nazionale rappresenta da sempre un obiettivo di difficile definizione, poiché legato profondamente a quelle che sono le prerogative di un determinato stato. Per questo motivo esso è in continuo mutamento.

Con la ripresa della grave emergenza sanitaria legata al Covid-19 (che sta nuovamente flagellando paesi già duramente colpiti nella prima fase della pandemia) e in un momento caratterizzato da elevata incertezza generalizzata, risulta ancora più complesso individuare gli ambiti rispetto ai quali è opportuno intervenire per aumentare la capacità di resilienza del sistema paese, proprio a tutela dell'Interesse Nazionale stesso.

Volgendo un rapido sguardo al passato, l'evoluzione biologica fornisce un importante insegnamento: solo quelle specie in grado di adattarsi ai cambiamenti riescono a sopravvivere, le altre sono destinate ad estinguersi. I tempi pertanto ci impongono di rivalutare le priorità e riprogrammare lo spettro degli interessi nazionali da proteggere. Tutto ciò tenendo conto del complesso fenomeno della globalizzazione, poiché proprio grazie ad essa è possibile avvicinare qualunque luogo in qualunque momento e questo è un processo irreversibile, dal quale non si può tornare indietro. Proprio in questo scenario di emergenza sanitaria la globalizzazione ha consentito di mantenere vivi sistemi finanziari, industriali e commerciali, garantendo una business continuity durante le fasi di lockdown.

Ma se da un lato la globalizzazione ha favorito le interazioni socio-economiche, dall'altro ha accentuato anche l'esposizione a un rischio di ingerenza maggiore verso l'Italia da parte di altri paesi, soprattutto durante la fase di confinamento.

Ad esempio, la missione cubana della Brigata Henry Reeve (composta da personale medico e infermieristico) presso le strutture ospedaliere di Crema e l'impiego del contingente militare russo di difesa NBC nelle province di Bergamo e Brescia hanno costituito elementi di assoluta novità per l'Italia in uno scenario di cooperazione internazionale (seppur con finalità di supporto sanitario). Gli stessi aiuti umanitari all'Italia provenienti dalla Cina e dagli Stati Uniti possono essere considerati come interventi di solidarietà internazionale o come strumenti di "soft power", a seconda di come se ne vogliano interpretare i motivi ispiratori e gli effetti sull'opinione pubblica in un quadro di complesse relazioni diplomatiche.

CONCLUSIONI

Con il presente studio di approfondimento si è ritenuto opportuno definire e proporre una metodologia applicabile ai cosiddetti asset industriali critici in qualunque circostanza di emergenza che possa degradarne sensibilmente le condizioni di sicurezza fisica (security conditions) con dirette conseguenze sulla capacità operativa. La predisposizione di un piano integrato di security management, operations continuity & crisis communication, secondo i criteri qui esposti, può sicuramente determinare un notevole miglioramento del grado di resilienza dell'organizzazione.

Lo stesso comparto assicurativo dovrà farsi carico con maggiore frequenza dei rischi finanziari derivanti da eventi speciali di natura emergenziale e - anche al fine di limitare una propria eccessiva esposizione a rischi di default parziale o totale delle organizzazioni assicurate (con conseguente forte aumento dei premi delle relative polizze) - promuoverà un'implementazione veloce ed efficace di possibili strumenti di mitigazione nell'interesse di tutte le controparti.

L'emergenza COVID-19 ha quindi evidenziato la drammaticità nelle sue conseguenze sociali, imponendo un nuovo e coerente approccio di analisi delle vulnerabilità nei sistemi organizzativi complessi del tessuto produttivo nazionale. I fatti odierni dimostrano che le emergenze (nei molteplici livelli di criticità) costituiranno in futuro uno scenario operativo ad alta probabilità di accadimento per qualsiasi attività industriale.

Conseguentemente, con riferimento agli operatori economici preposti alla gestione degli asset strategici e in uno scenario di minaccia globale, le singole organizzazioni saranno chiamate a sempre maggiori impegni nella gestione delle crisi (in termini di misure per la sicurezza e la continuità operativa), mentre lo Stato - come rappresentante dell'interesse generale - dovrà continuare a garantire i necessari strumenti di protezione e di sostegno finanziario, realizzando così un meccanismo virtuoso e sinergico per un efficiente "sistema integrato nazionale".

RUBRICA: Riproponiamo...

O.S.S.I.S.Na. - Pianificazione e protezione delle filiere logistiche per il comparto industriale biosanitario nella lotta al Covid-19

INTRODUZIONE

Una nuova sfida nazionale è rappresentata dalla necessità di rispondere in modo urgente e capillare al fabbisogno di presìdi farmaceutici e attrezzature bio-medicali da impiegare nella lotta al Covid-19.

Intere filiere industriali si stanno mobilitando al fine di predisporre i propri sistemi di produzione e distribuzione per una risposta efficace alle urgenze sanitarie del Paese.

Le strutture ospedaliere, già sottoposte giorno dopo giorno a notevoli stress nella loro operatività, iniziano a lamentare difficoltà di approvvigionamento di materiale essenziale nelle cure legate alla pandemia: dispositivi di protezione (mascherine, guanti, camici, tute, visiere), prodotti chimico-farmaceutici per la diagnosi (tamponi, reagenti e relativi dispositivi di test), apparecchiature per terapie intensive (respiratori, sistemi di monitoraggio e controllo), normali strumenti di uso clinico e prodotti vari per l'igienizzazione e la sterilizzazione.

Notevoli appaiono anche le difficoltà riscontrate nelle attività di assistenza domiciliare ai malati Covid-19, legate soprattutto alla scarsità di bombole per il trasporto e la somministrazione dell'ossigeno medicale.

La complessa macchina organizzativa nazionale si sta inoltre preparando all'avvio delle attività di distribuzione dei vaccini, in attesa di capire se e come ne sarà coinvolta anche l'industria farmaceutica (in particolare, per l'eventuale produzione su licenza sul territorio italiano).

Da un punto di vista della Sicurezza Nazionale, orientata alla primaria esigenza di tutela della salute pub-

blica, l'aspetto critico appare essere costituito dall'intera organizzazione dei flussi logistici nelle attività di approvvigionamento e distribuzione dei vari prodotti farmaceutici e biomedicali.

In termini di "protezione", una gestione non adeguata delle eventuali vulnerabilità della catena logistica (costituita soprattutto dai vettori per il trasporto e dai siti di movimentazione e stoccaggio) potrebbe compromettere la tenuta dell'intero sistema sanitario, favorendo l'operato di potenziali soggetti nel compimento - con finalità diverse - di azioni di natura terroristica o criminale.

Si rende pertanto necessario un massiccio dispiegamento - il più possibile coordinato e interagente - di capacità e assetti organizzativi da parte dei comparti industriali interessati, da affiancare, in modo ausiliario nelle attività di prevenzione e contrasto, alle cosiddette "istituzioni preposte" dello Stato (forze dell'ordine, forze armate, apparati informativi di sicurezza).

Con il presente approfondimento tematico si intende pertanto fornire un'analisi dello scenario operativo (attuale e per i prossimi mesi) e i possibili criteri di pianificazione per le attività di protezione delle filiere logistiche afferenti all'intero ambito industriale biosanitario.

ANALISI DELLO SCENARIO

La pandemia di Covid-19 ha richiamato gli Stati, i loro decisori politici, gli apparati di sicurezza e gli operatori economici a valutare a livello sistemico il valore strategico delle filiere sanitarie e biomedicali.

La tutela e la garanzia del corretto funzionamento delle principali filiere legate ai comparti produttivi e logistici connessi alla risposta alla pandemia si sono imposte come primarie necessità politiche e organizzative nel contesto dell'avanzamento di questa battaglia.

Questo vale in particolar modo per l'Italia, tra i Paesi maggiormente colpiti dall'emergenza sanitaria.

La salienza di tali questioni è destinata nei prossimi mesi a essere ulteriormente amplificata dalla prospettiva di arrivo nel Paese di uno o più vaccini contro il Covid-19 che stanno venendo studiati e testati dai principali gruppi farmaceutici del pianeta.

L'arrivo del vaccino, la sua conservazione e la sua somministrazione determineranno non solo nuove sfide d'interesse nazionale ma anche un effetto moltiplicatore di quelle già esistenti.

L'esperienza della prima ondata della pandemia e le nuove problematiche della seconda ondata aiutano a individuare i principali fattori di criticità.

In primo luogo, per il Paese è fondamentale mobilitare un'efficace catena logistica che consenta la corretta gestione dei flussi dei presidi sanitari chiave (mascherine, siringhe, dispositivi di protezione, ossigeno biomedicale, contenitori per preservare la catena del freddo dei vaccini, ventilatori polmonari) e dei farmaci in tutto il territorio nazionale. Possibili ostacoli a tale necessità possono essere incertezze nella catena di comando tra autorità centrali ed enti locali, conflitti di competenze tra strutture deputate alle varie fasi del progetto, mismatch tra domanda e offerta di dispositivi in fasi cruciali per contrastare l'avanzata del contagio. Questo tema appare fondamentale in vista dell'apertura della corsa al vaccino.

In secondo luogo, come accaduto nelle prime settimane di pandemia, è utile un ragionamento strategico volto a individuare quali siano i presidi che possono, nei limiti della capacità del sistema industriale o sulla scia di riconversioni estemporanee, venire realizzati direttamente sul territorio nazionale

e quali invece, specie nel contesto dei prodotti più complessi, siano legati a catene del valore globali. In quest'ultimo caso, la discesa in campo del potenziale strategico dello Stato ha portato diversi Paesi a valutare il reshoring di parte dei processi produttivi legati all'ambito sanitario e biomedicale in quanto definiti di interesse nazionale (è il caso dei programmi "Build Back Better" del Regno Unito e che l'entrante amministrazione Biden negli USA propone con lo stesso slogan). Chiaramente vanno tenute in considerazione le necessarie economie di scala utili ad adattare o creare ex novo impianti deputati a produrre in maniera massiccia tali presidi e la disponibilità di università, centri di ricerca, competenze tecniche volte ad accelerare i processi più urgenti.

In terzo luogo, si pone il tema del coordinamento tra i piani di rilancio del sistema sanitario sotto il profilo della dotazione di risorse, delle infrastrutture e dell'organizzazione territoriale e una coerente strategia di politica industriale che sappia mobilitare le migliori e più produttive risorse del Paese per dare sostanza ad essi.

Quarto punto è il fondamentale aspetto securitario: le filiere in questione vanno poste al riparo da qualsiasi possibilità di perturbazione e la loro protezione è da intendersi a trecentosessanta gradi.

Parliamo in questo caso della possibilità che le aziende di nicchia più importanti finiscano preda di attori stranieri (per la scarsa capitalizzazione o il mancato inserimento, in un discorso sistemico, del tema della cybersecurity e del rischio di furto di proprietà intellettuali e dati sensibili) e delle possibili infiltrazioni della criminalità organizzata a monte o a valle di una catena biomedicale.

Un'analisi di scenario multidimensionale del fenomeno non può che prendere in considerazione questi quattro punti e combinare ogni risposta tenendoli fortemente in considerazione.

Sia sul profilo della produzione dei dispositivi critici che, in prospettiva, della sua sovrapposizione con la partita del vaccino è possibile ipotizzare una strategia articolata e di medio-lungo periodo, nella previsione che gli effetti della pandemia non si esauriscano definitivamente che sull'orizzonte temporale di più anni.

PIANIFICAZIONE DEI FLUSSI LOGISTICI DI APPROVVIGIONAMENTO

Le filiere di approvvigionamento del comparto biosanitario nell'ambito della lotta al Covid-19 appaiono piuttosto eterogenee in relazione alle diverse specificità dei prodotti.

Prendendo come primo caso in esame i prodotti farmaceutici (vaccini, tamponi e medicinali di cura), occorre considerare tra i processi "a monte":

- Preparazioni biochimiche;
- Sistemi di confezionamento (packaging dedicati, come i blister farmaceutici, e i relativi macchinari);
- Attrezzature per lo stoccaggio e il trasporto in ambiente controllato (sistemi refrigeranti per impiego fisso e mobile);
- Siti e vettori per le movimentazioni logistiche (magazzini e società di trasporto dedicati);
- Laboratori per analisi chimico-farmaceutiche.

Per quanto riguarda le attrezzature biomedicali di impiego ospedaliero, particolare importanza appaiono quelle dedicate sia alle terapie intensive che semi-intensive:

- Respiratori (valvole di erogazione, maschere e caschi);
- Sistemi elettronici di monitoraggio dei parametri vitali;
- Impianti di stoccaggio e distribuzione dell'ossigeno medicale (serbatoi, valvole, ecc.).

Per le attività di assistenza domiciliare dei pazienti affetti da Covid-19, una situazione di particolare rilevanza è costituita dalla disponibilità di bombole di ossigeno (con relative valvole di regolazione) per le quali sta emergendo una certa difficoltà da parte dell'industria nel reperire i quantitativi via via crescenti necessari ad assicurarne una capillare distribuzione alla popolazione interessata.

La mappatura dei processi di approvvigionamento si conclude con i vari dispositivi di protezione individuale sia di uso civile che per impiego ospedaliero:

- Mascherine (per i diversi livelli di filtrazione);
- Camici e tute di protezione;
- Guanti;
- Visiere.

L'analisi delle minacce per le tipologie dei prodotti sopra elencati, coerentemente con l'analisi di scenario globale approfondita al paragrafo precedente, porta a considerare come principale elemento di rischio il furto e la contraffazione, operati dalla criminalità organizzata come soggetto potenzialmente in grado di agire in modo capillare sui territori per la successiva immissione della suddetta merce in un "mercato parallelo" (con conseguenti rischi per la salute pubblica). Come ulteriore elemento di minaccia appaiono le possibili azioni di sabotaggio dei prodotti chimico-farmaceutici (all'interno degli impianti di produzione e lungo le filiere di stoccaggio e distribuzione), operabili da soggetti interessati a compromettere capacità produttiva e reputazione con finalità di concorrenza sleale.

Tra le possibilità di sabotaggio degli impianti di produzione occorre considerare anche gli attacchi di natura cibernetica, che possono creare una situazione di default totale o parziale soprattutto nei sistemi automatizzati di comando e controllo.

Tutte le possibili azioni potrebbero essere esercitate anche da soggetti aventi finalità di terrorismo sulla popolazione civile (di matrice religiosa o politica) o più semplicemente per azioni dimostrative (ad esempio, da parte di frange estremiste di matrice "No Vax").

Effettuata la caratterizzazione delle possibili minacce, occorre procedere all'analisi delle vulnerabilità per i siti produttivi interessati.

Le minacce sopra considerate devono essere contestualizzate e analizzate singolarmente per modalità di azione.

Ciascun sito di produzione e di stoccaggio deve essere oggetto di un'attenta valutazione di adeguatezza.

A tale scopo, devono essere considerate in modo prioritario:

- Le condizioni di protezione perimetrale delle aree;
- L'esistenza di aree ad accesso ristretto (zone critiche per tipologia di materiale gestito);
- La dislocazione dei sistemi di comando e controllo (inclusi quadri elettrici e sensoristica di monitoraggio) per gli impianti di produzione e per le infrastrutture tecnologiche dedicate al mantenimento delle condizioni ambientali idonee;
- La gestione delle reti IT per la gestione dei processi del sito;
- I sistemi di tracciabilità per i prodotti gestiti.

Le attività di mitigazione dovranno essere definite con interventi di carattere organizzativo, operativo e tecnologico, come ad esempio:

- Il rafforzamento delle infrastrutture antintrusione (recinzioni, sensoristica, illuminazione, ecc.) e di videosorveglianza, abbinate a sistemi di teleallarme;
- La definizione di opportune gerarchie di accesso (anche tra gli stessi dipendenti del sito) su aree critiche;
- L'implementazione di soluzioni di identificazione e geolocalizzazione per la merce (inclusi i sistemi di gestione IT dedicati);
- L'adozione di soluzioni "anticontraffazione" per la merce gestita (mediante apposite architetture di identificazione e di tracciabilità, da rendere altresì accessibili alle forze dell'ordine per eventuali successive verifiche di autenticità sui prodotti in circolazione).

Con particolare riferimento alle attività di televigilanza sopra menzionate e al fine di ottimizzare le capacità operative e i costi di gestione per le singole organizzazioni, è opportuno considerare la possibilità di interazione all'interno del medesimo comprensorio industriale mediante accordi tra i diversi operatori economici e un'unica società di vigilanza. Ciò affinché quest'ultima possa ivi dislocare un unico presidio avanzato di comando e controllo al servizio dei vari consorziati (con evidenti vantaggi in termini di tempi di intervento e costi di gestione).

PIANIFICAZIONE DEI FLUSSI LOGISTICI DI DISTRIBUZIONE

Procedendo ora all'esame delle catene logistiche della distribuzione per i materiali elencati al paragrafo precedente, l'analisi delle potenziali minacce si concentra sui vettori utilizzati per il trasporto e sui siti di stoccaggio intermedio (prima della consegna finale ai soggetti utilizzatori).

I possibili rischi riguardano il furto e il sabotaggio dei prodotti nelle fasi dinamiche e statiche della distribuzione.

Occorre pertanto prevedere apposite dotazioni di sistemi satellitari di geolocalizzazione per il mezzo di trasporto utilizzato (vettore) e/o per il carico (pallet, container, ecc.), così da permettere un costante monitoraggio da remoto.

È inoltre raccomandata una opportuna pianificazione del viaggio che preveda eventuali soste in aree controllate oppure - nei casi più critici (per tipologia di merce e/o per aree geografiche ad alta densità criminale) - scorte con vigilanza armata.

Per quanto riguarda i siti di stoccaggio e con particolare riguardo al materiale di acquisto da parte delle autorità sanitarie (e quindi di prioritario interesse generale) è opportuno definire siti di concentrazione (Hub) multilivello, ad esempio su "scala sequenziale" sui livelli nazionale, regionale e provinciale. Questo approccio tende a favorire la creazione del minor numero possibile di siti e le loro migliori condizioni di attrezzaggio. Potranno infatti essere ottimizzate le modalità per una corretta conservazione dei prodotti (soprattutto quelli chimico-farmaceutici, come vaccini e reagenti) e si potranno implementare infrastrutture di sicurezza adeguate (sistemi an-

tintrusione, videosorveglianza e allarme), ivi inclusa l'organizzazione a supporto (personale, mezzi per la movimentazione e sistemi di vigilanza). La gestione di tali hub (di interesse strategico nazionale) dovrà essere affidata alle forze armate.

Con particolare riferimento alla distribuzione dei vaccini, un recentissimo approfondimento del World Economic Forum propone la tecnologia "blockchain" per gestire e condividere un database decentralizzato, gestito dai vari operatori pubblici e privati coinvolti nella distribuzione, ove riportare e mantenere in costante tracciabilità - in tempo reale - tutte le informazioni riguardanti la distribuzione (incluse la localizzazione e le condizioni ambientali di corretto stoccaggio). Il principale vantaggio di un tale "luogo virtuale condiviso" è rappresentato dal fatto che le informazioni esistenti non possono essere eliminate, mentre quelle nuove possono essere solo aggiunte, determinando un più alto livello di responsabilità da parte di ogni partecipante alla banca dati. Per la distribuzione dei vaccini l'adozione di banche dati con tecnologia "blockchain" costituisce una soluzione robusta in termini di condivisione delle informazioni di tracciabilità e di anticontraffazione, richiedendo altresì agli operatori economici la più ampia cooperazione a livello gestionale (che dovrà essere prevista sin dal primo momento).

ATTIVITÀ PER LA PROTEZIONE E LA CONTINUITÀ OPERATIVA

Le attività di protezione dei siti (incluse le azioni per garantirne la continuità operativa) devono essere attuate in accordo a specifici protocolli già definiti e validati.

Il modello organizzativo qui proposto (denominato "Protocollo SCUDO ITALIA") è specificamente sviluppato per i cosiddetti "scenari di crisi", come le emergenze sanitarie, gli eventi bellici, gli atti terroristici e le crisi socio-economiche.

L'attività deve porsi l'obiettivo primario della tutela del patrimonio tangibile e intangibile dell'organizzazione dell'operatore economico (risorse umane, beni strumentali, know-how tecnologico) e della sua struttura finanziaria.

Il protocollo è principalmente rivolto a mitigare i rischi derivanti da minacce di natura fisica, biologica, cibernetica, reputazionale e finanziaria da parte di "entità ostili" nazionali ed estere, aventi finalità di interdizione e sabotaggio delle attività operative oppure di acquisizione malevola delle capacità tecnologiche.

Le minacce vengono così classificate (in ordine crescente per gravità):

- Minacce percepite (minacce possibili, ma senza informazioni precise);
- Minacce diffuse (minacce generiche per la presenza sul territorio di gruppi criminali, per situazioni socio-politiche instabili, ecc.);
- Minacce indirette (minacce rivolte a infrastrutture esterne, ma con possibili ripercussioni sull'asset);
- Minacce dirette (minacce rivolte in maniera specifica all'asset).

Ogni possibile evento ostile (per ciascuna delle minacce considerate) viene valutato nel suo impatto e nella sua probabilità di accadimento in base alle informazioni acquisite (in cooperazione con gli organismi nazionali di pubblica sicurezza e di intelligence preposti allo scopo), pervenendo alla definizione del cosiddetto "livello di rischio" (secondo le categorie: accettabile, medio, inaccettabile).

Per ciascun livello di rischio è altresì stabilita la tipologia dell'intervento di mitigazione, il quale può comportare opzioni organizzative, operative, tecno-

logiche e finanziarie e che confluiscono nel "Piano di gestione dei rischi", integrato da un "Piano per la continuità operativa" e da un "Piano per la comunicazione in stato di crisi".

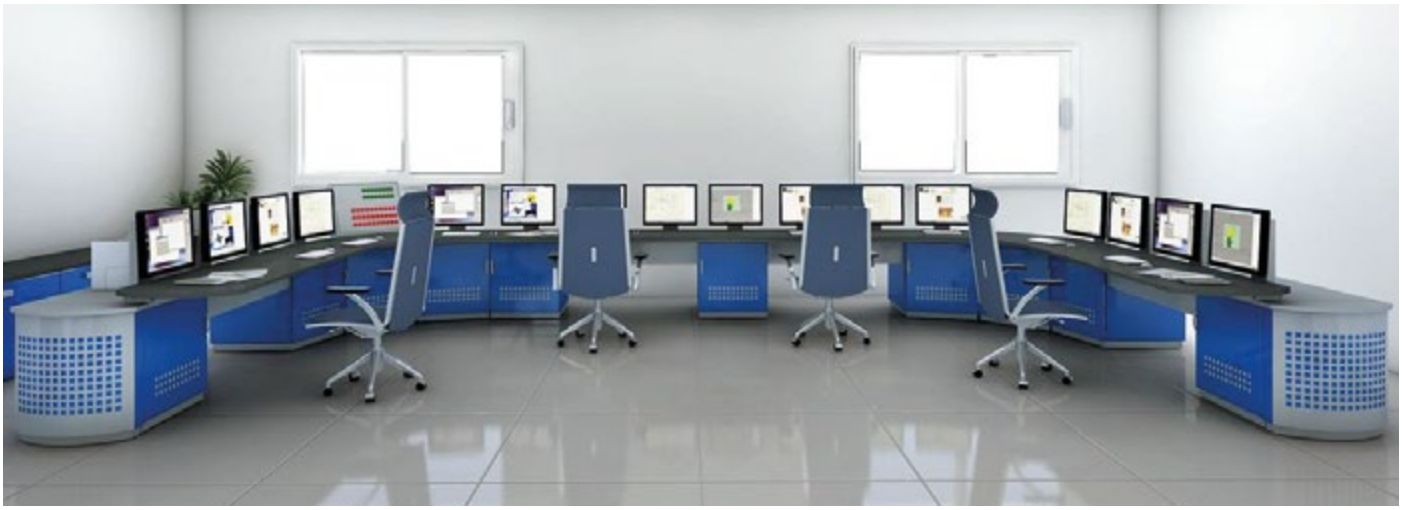
Il "Piano per la continuità operativa" - al verificarsi di un evento di crisi - prevede:

- Immediata attivazione di una Unità di Crisi con un Responsabile Unico (con eventuale supporto di uno staff specialistico) in possesso di tutti i poteri ordinari e straordinari per un corretto e tempestivo coordinamento delle attività di emergenza e come unico referente verso le Pubbliche Autorità;
- Esistenza di un efficace dispositivo di Comando & Controllo (procedure, postazioni e sistemi di comunicazione verso l'interno e verso l'esterno del sito industriale, ecc.);
- Esistenza di squadre di Pronto Intervento (protezione antincendio e primo soccorso, gestione dei protocolli sanitari, eventuale protezione armata, ecc.);
- Mantenimento in efficienza operativa di tutto il dispositivo previsto (esercitazioni periodiche, piano di formazione per il personale, ecc.);
- Piano per la continuità delle attività operative interne ed esterne del sito industriale (svolta a cura dell'organizzazione interna e della filiera di fornitura di beni e servizi o "supply chain");
- Piano per il ripristino (parziale e totale) delle attività operative interne ed esterne del sito industriale.

Il "Piano per la Continuità Operativa", da attuarsi durante l'intera situazione di crisi, deve prevedere la definizione dei seguenti criteri operativi:

- Tipologia delle attività operabili presso il sito;
- Tipologia delle attività necessarie dalla filiera di fornitura esterna (supply chain) per beni e servizi;
- Livelli minimi di "produzione beni" e/o "erogazione servizi" da garantire durante il periodo di crisi (criteri "MPL", Mimimum Performance Level), prioritari rispetto ai normali obiettivi definiti dall'organizzazione per l'esercizio ordinario (i quali possono pertanto essere parzialmente o completamente derogati in considerazione delle mutate esigenze);
- Risorse umane, strumentali e finanziarie necessarie in accordo ai possibili scenari di crisi;
- Assetti di Comando, Controllo & Comunicazione durante la crisi (criteri "Crisis-C3").

Il "Piano per la Comunicazione in stato di crisi" prevede innanzitutto la definizione dei "target interni" (management, dipendenti, ecc.) e dei "target esterni" (stakeholder, soggetti istituzionali, clienti, fornitori, opinione pubblica, ecc.).



Il piano di comunicazione deve inoltre prevedere:

- Identificazione di un Responsabile Unico per la Comunicazione;
- Modalità per la comunicazione delle azioni di emergenza verso il personale operante all'interno del sito industriale, inclusa la definizione dei dispositivi idonei per le comunicazioni di emergenza (sistemi informativi, dispositivi telefonici, altoparlanti, display, ecc.);
- Esistenza di una lista di organizzazioni esterne (agenzie di stampa, agenzie ambientali, ecc.) da attivare in caso di crisi;
- Modalità per la comunicazione verso le organizzazioni esterne;
- Definizione dei dispositivi idonei per le comunicazioni verso le organizzazioni esterne (sistemi di telefonia su piattaforma fissa/mobile/satellitare, ponti radio, ecc.).

Il protocollo adottato prevede l'esistenza di un dispositivo organizzativo idoneo alla "Gestione del Rischio Reputazionale" durante il periodo di crisi e che ne definisce:

- Il Responsabile (che può coincidere con il Responsabile della Comunicazione);
- Gli strumenti operativi (quali il documento di "Analisi Preventiva per il Rischio Reputazionale");
- L'insieme degli elementi da considerare per l'analisi del Rischio Reputazionale, assicurando che vengano presi in esame fattori esterni (attacchi mediatici, fake news, eventi di diretta o indiretta potenziale responsabilità dell'organizzazione, ecc.) e fattori interni (eventi di natura sindacale, fake news, eventi di diretta o indiretta potenziale responsabilità dell'organizzazione, ecc.);
- Il piano di monitoraggio per il profilo reputazionale dell'organizzazione del sito da attuarsi durante l'intero periodo di crisi (mediante analisi sistematica dei mass media, raccolta informativa da iniziative di informazione interne/esterne quali volantinaggi e manifestazioni, ecc.);
- Le tipologie di intervento (campagne di comunicazione di carattere preventivo e/o reattivo, ecc.).

Il "Piano di Gestione del Rischio Reputazionale" potrà essere incorporato all'interno del piano di comunicazione.

CONCLUSIONI

L'emergenza pandemica in corso obbliga a un percorso di totale ridefinizione dei modelli logistici industriali, in particolare per quei beni e servizi identificati come "strategici" per la tutela sanitaria della popolazione.

La sfida, in primo luogo, è quella di valorizzare e mobilitare le eccellenze presenti in Italia a livello di filiera chimico - farmaceutica e biomedicale, che facendo "rete" dietro lo scudo di un progetto nazionale ben articolato possono contribuire al benessere sanitario del sistema-Paese e alla riduzione dei fattori di vulnerabilità, mettendo in campo, al contempo, un indotto tutt'altro che secondario in termini produttivi, occupazionali e tecnologici.

Dal distretto farmaceutico del Lazio a quello biomedicale di Mirandola, passando per imprese strategiche come la Siare (unica azienda italiana a produrre i cruciali ventilatori polmonari all'inizio dell'emergenza Covid-19) e la SIAD (leader nell'ossigeno biomedicale), tutte le eccellenze nazionali in tal senso devono essere messe a sistema perché il loro lavoro possa creare un insieme corale vincente. Ma solo un'accorta strategia capace di promuovere le opportune competenze e prevenire i rischi potrà far sì che i fattori di criticità evidenziati vengano affrontati nel migliore dei modi.

La protezione delle catene di approvvigionamento e distribuzione coinvolte rappresenta quindi una ne-

cessità di assoluta urgenza ove far convergere rapidamente tutte le possibili capacità pubbliche e private.

In una tale prospettiva, l'azione dello Stato (attraverso le sue articolazioni di coordinamento e di intervento diretto non delegabili) potrà esercitarsi con la massima efficacia nei confronti del sistema industriale nazionale solamente in un quadro condiviso di obiettivi e di modalità operative.

ANGELO TOFALO - Intelligence Collettiva

Rapimenti di grandi scienziati, operazioni all'ultimo secondo, spionaggio e controspionaggio internazionale, detonazioni sul filo del rasoio di armi nucleari, servizi segreti deviati e finali ad effetto in compagnia di bellissime donne sono solo alcuni degli scenari ricorrenti nei film e nelle serie tv che si vanno a sovrapporre ad una realtà molto più ampia, complessa e ramificata.

Realtà che ritengo vada fatta conoscere nell'ambito di quella che deve necessariamente essere una costante e continua diffusione della cultura dell'intelligence e della sicurezza, tra l'altro affidata anche al DIS come recita il comma 3 dell'art 4 alla lettera m, della legge 3 agosto 2007, n. 124, "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto".

Proprio per questa necessità, entrato al Copasir nel giugno 2013, capii subito che, seppur nei modi dovuti e soprattutto con un linguaggio adeguato, oltre il 90% delle questioni riguardanti i nostri Servizi potevano e dovevano essere raccontate in primis per "proteggerli" da uno continuo storytelling per lo più inadeguato o disinformato. Dopo anni di impegno e studio, nel dicembre 2015, insieme a ben più autorevoli esperti della materia ho dato vita ad un think thank dal nome "Intelligence Collettiva" con l'obiettivo di diffondere la cultura dell'intelligence e della sicurezza attraverso modalità innovative, usando un linguaggio diretto, concreto, semplice ma allo stesso tempo corretto e istituzionale supportato da info-grafiche frutto di lunghe nottate di lavoro, che costituiscono una facilissima consultazione anche per chi si avvicina per la prima volta alla trattazione di questa materia. Abbiamo quindi portato avanti una serie di eventi alla Camera dei deputati dove autorevoli relatori, protagonisti diretti e indiretti dell'Intelligence di questi anni, hanno raccontato le loro esperienze e il reale funzionamento dei Servizi.

Oggi soprattutto i più giovani hanno la necessità di comprendere che i Servizi informativi di ogni paese, impropriamente chiamati Servizi segreti, si trovano ad affrontare una complessa situazione geopolitica mondiale che sta mutando in maniera sempre più rapida e quindi difficilmente prevedibile. È dovere prima di tutto delle istituzioni raccontare in maniera corretta i molteplici aspetti di questo delicato dossier.

Dopo anni di studio e di attività abbiamo deciso di elaborare un saggio che potesse essere utile agli addetti ai lavori, agli appassionati ed esperti della materia, ma che divenisse allo stesso tempo una guida utile a prendere per mano i più giovani, i neofiti che per la prima volta si avvicinano a questo mondo e che magari sognano in futuro di lavorare per la sicurezza nazionale.

Per analizzare al meglio ogni singola dinamica globale è importante capire prima di tutto cosa sono realmente i Servizi, come opera l'Intelligence ed entrare quindi a fondo nel loro mondo. Nel saggio "Intelligence Collettiva - Appunti di un Ingegnere rapito dai Servizi Segreti", il tema viene affrontato parlando del

percorso storico e dell'evoluzione che hanno avuto e necessariamente subito nei secoli, delle principali categorie e degli strumenti base utili alla raccolta informativa, delle leggi che oggi ne regolano l'operato. Abbiamo in pratica analizzato e reso noti molteplici aspetti del complicato, ma allo stesso tempo affascinante mondo dei Servizi segreti, attraverso l'esperienza e le parole di autorevoli relatori, che per anni hanno avuto ruoli chiave all'interno dell'apparato, o di chi ha ricoperto ruoli istituzionali di controllo e di governo sul comparto Intelligence.

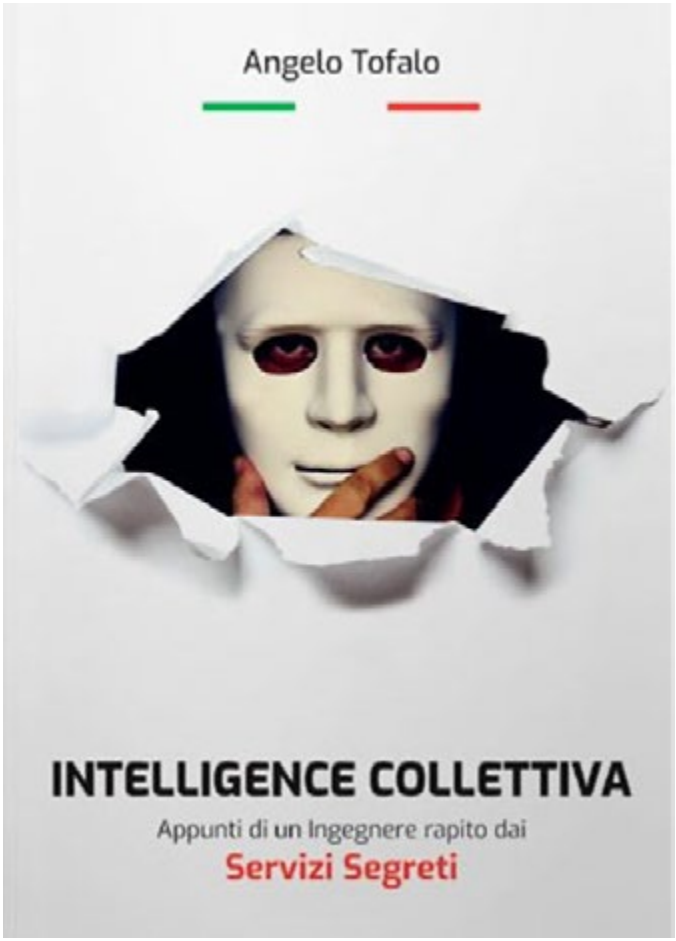
È altresì facilmente riscontrabile, da chi ha prestato attenzione in questi ultimi anni al dibattito tra le diverse forze parlamentari, come i Servizi segreti siano inoltre stati tirati sempre più spesso in ballo nelle dinamiche partitiche determinando, in certi casi, una inequivocabile oscillazione del termometro politico.

Chi si occupa di questa materia così delicata ha il dovere civile e morale di mettere al primo posto sempre e solo le istituzioni democratiche per preservarle da rischi e minacce di ogni matrice. Difendere la nostra democrazia vuol dire avere la consapevolezza che esiste un perimetro di non belligeranza che va tutelato da tutte le forze sociali, una zona franca che chiunque serve pro tempore il Paese deve conoscere e che prende il nome di interesse nazionale.

Sono certo che questa lettura potrà essere utile a comprendere un po' meglio il reale funzionamento del nostro comparto Intelligence per stimolare sempre più persone a non abbandonarsi a fuorvianti semplificazioni e ad evitare di "farsi portare a spasso" da quelle che a volte possono sembrare dichiarazioni estemporanee ma che, al contrario, celano meri interessi di casacca.

È possibile garantire un determinato livello di trasparenza se ciò che sei chiamato a gestire o monitorare è il mondo dei Servizi informativi? Si può preservare la sicurezza nazionale senza dover necessariamente omettere o celare porzioni di verità? La ragion di Stato è sacrificabile sull'altare della conoscenza condivisa? Infondo abbiamo realmente bisogno che i Servizi siano "segreti"?

"Intelligence Collettiva - Appunti di un Ingegnere rapito dai Servizi Segreti", edito dalla Fondazione Margherita Hack, è un lavoro estremamente diretto che raccoglie le schematizzazioni e i ragionamenti di tanti professionisti del settore, che si occupano o si sono occupati di Intelligence a diversi livelli. Tra questi i già direttori del DIS Giampiero Massolo e Gennaro Vecchione, il presidente del COPASIR Raffaele Volpi e il già segretario del comitato Felice Casson. E ancora esperti del settore come il prof. Mario Caligiuri, Aldo Giannuli, Andrea Margelletti, Marco Santarelli e Nicola Bonaccini. L'avvocato Luigi Panella che trat-



ta il delicatissimo strumento giuridico del segreto di Stato. E ancora Umberto Saccone, Adriano Soi, Alfredo Mantici e Nicola Gelao.

L'Onorevole Raffaele Volpi, già Sottosegretario di Stato alla Difesa nel governo Conte I e già presidente del Copasir, ci descrive in modo articolato e capillare come si svolgono i lavori all'interno del Comitato Parlamentare per la Sicurezza della Repubblica. Un ragionamento diretto e sincero senza mai travalicare il confine del segreto di Stato.

Il già magistrato, senatore e segretario del Comitato nella XVII legislatura Felice Casson fa un'attenta riflessione sul complicato rapporto che negli anni hanno avuto e sviluppato i nostri Servizi con il mondo della giustizia, con le procure, e con la magistratura. Casson, nella sua attività di magistrato ha infatti condotto molte inchieste, soprattutto in tema di terrorismo, di lotta alla corruzione, sulle deviazioni dei servizi segreti e degli apparati dello Stato, sull'eversione di estrema destra, sul traffico internazionale di materiale bellico, sull'organizzazione Gladio sulla quale tra l'altro "Intelligence Collettiva" ha portato avanti un'inchiesta sentendo anche il Generale Paolo Inzerilli.

Di rilievo sono gli interventi dei due già direttori dei Servizi, l'Ambasciatore Massolo e il Prefetto Vecchione. Il primo fa una riflessione sul ruolo dell'Intelligence come strumento non convenzionale. Su come il termine "Intelligence collettiva" si sposi con quello di "sicurezza partecipata". Questo termine significa infatti joint venture, collaborazione tra diversi soggetti. Il Presidente Massolo ricorda come la nostra sia forse l'unica Intelligence al mondo ad avere un accordo con il Garante della privacy, non una mera operazione di pubbliche relazioni ma un reale e proficuo rapporto su cui si era ravvisata la necessità coerente con quella logica partecipata di cui prima.

Il prefetto Vecchione fa invece una riflessione sulle prospettive, sui contenuti e sulle metodologie dell'Intelligence economica, riflessione legata inevitabilmente all'esigenza di tener conto dell'impatto che, anche in tale peculiare settore di attività, la pandemia Covid-19 è destinata ad esercitare.

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

MASTER CBRNe
Chemical, Biological, Radiological, Nuclear and explosive
Department of Industrial Engineering and School of Medicine and Surgery

MASTER INTERNAZIONALI DI PRIMO E SECONDO LIVELLO IN PROTEZIONE DA EVENTI CBRNE

PANORAMICA

L'**Università di Roma Tor Vergata** è una giovane Università (fondata nel 1973), con servizi ed infrastrutture moderni ed un profilo internazionale.
Data l'instabilità del contesto socio-politico internazionale, a partire dal 2009 la Facoltà di Medicina e Chirurgia e il Dipartimento di Ingegneria Industriale hanno attivato due Corsi Internazionali post-laurea in Protezione da Eventi CBRNe. **Ufficialmente supportati dall'OPCW, i Master hanno ottenuto lo status di "NATO selected" e sono stati inclusi nell'ETOC (Education and Training Opportunities Catalogue NATO).** Il Master di I Livello (120 ECTS) e di II Livello (60 ECTS) in "Protezione da eventi CBRNE", rappresentano gli **unici corsi di questo tipo**, che consentono di ottenere un **titolo accademico** in questo settore.

L'obiettivo dei Master consiste nel fornire ai partecipanti, delle competenze globali nel campo della **CBRNe Safety and Security**, con particolare attenzione ai bisogni reali, attraverso l'insegnamento e la formazione.

I più importanti **soggetti pubblici e privati** che operano nel settore della sicurezza e protezione CBRNe supportano i corsi di Master con la loro esperienza e sono coinvolti nelle attività didattiche attraverso i loro esperti.

I corsi di master internazionale segnalano alti tassi di **placement**. Il 90% dei laureati ha accettato di posti di lavoro nel settore CBRNe nell'arco di pochi mesi dal conseguimento del titolo.

CORSO AVANZATO

ADVISORS DEI DECISION MAKERS

- **Durata:** 1 anno accademico
- Rilascio di **60 ECTS**
- **Requisiti:** i candidati devono avere acquisito 300-ECTS, equivalenti ad un titolo accademico di II livello.
- **Didattica:** Lezioni frontali ed attività pratiche
- **1 modulo** presso l'Organizzazione per la Proibizione delle Armi Chimiche (**OPAC**).

CORSO BASE

FIRST RESPONDERS

- **Durata:** 2 anni accademici
- Rilascio di **120 ECTS**
- **Requisiti:** i candidati devono avere acquisito 180-ECTS corrispondenti ad una laurea di I livello o equivalente.
- **Didattica:**

Primo anno: Lezioni frontali con esperti che. operano sul campo

Secondo anno: attività di formazione pratica, all'interno di strutture internazionali destinate alla formazione nel campo CBRNe.

Entrambi i corsi sono organizzati in moduli, **ogni modulo può essere frequentato separatamente.**

CONTATTI

Dr.ssa Colomba Russo,
Dr.ssa Alba Iannotti
Email: info@mastercbrn.it
www.cbrngate.com

CBRN GATE
EDUCATION TRAINING RESEARCH

C I S I N T

Centro Italiano di Strategia e Intelligence

O.S.S.I.S.Na.