LUISS Guido Carli

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI IMPRESA E MANAGEMENT

CATTEDRA DI ECONOMIA E GESTIONE DELLE IMPRESE

OSINT (Open Source Intelligence):

uno strumento necessario per l'efficienza e la sicurezza del sistema aziendale

Prof.ssa Federica Brunetta

RELATRICE

Gisella Maria Trentin 257711

CANDIDATA

ANNO ACCADEMICO 2022/2023

1. PREMESSA

Quali sono le opportunità ed i rischi in una economia post globale che la pandemia di Covid 19 e la recente guerra in Ucraina hanno reso più insicura?

Ecco la questione: rischio, oppure opportunità? In questo scenario, il web si configura come uno degli strumenti più potenti e rappresentativi di questo dilemma.

Di questo strumento cercheremo, quindi, di cogliere gli aspetti associati all'opportunità, senza però tralasciare i rischi connessi che comunque dovranno essere sempre presi in seria considerazione e di conseguenza gestiti.

Oggi giorno le aziende investono una importante quota parte dei loro profitti nelle infrastrutture di ICT (*Information & Communication Technology*), adeguando sempre di più la propria infrastruttura informatica all'ultima tecnologia disponibile sul mercato, tralasciando uno degli aspetti che invece dovrebbe andare di pari passo, proprio al fine di poter creare sinergie e riduzione degli sprechi.

Si tratta dell'attività di *ricerca*, intesa non come un semplice screening, ma come quell'attività che viene identificata con l'*analisi preventiva finalizzata ad evitare comprovate situazione di rischio per le aziende modernamente organizzate*.

Questo lavoro si pone l'obiettivo di illustrare, in una modalità strutturata e comprensibile, l'*attività di ricerca delle informazioni provenienti da quelle che sono considerate fonti aperte (OSINT - Open Source Intelligence),* ossia da aree informative che possono essere condivise da tutti gli utenti.

L'esplorazione del web, contestualizzato in questa modalità, diviene così una attività che fonda sulla metodologia e strumentazione OSINT un importante valore aggiunto per le aziende. Vedremo infatti che un buon *analista di fonti aperte* è in grado di poter raccogliere e strutturare informazioni che, se portate all'attenzione dei vertici di una organizzazione aziendale, possono rappresentare un contributo decisivo per supportare il processo decisionale del management.

Altresì cercheremo di spiegare come l'attività di analisi delle fonti aperte risulti essere ad oggi indispensabile se si vuole dominare una situazione piuttosto che subirla, e proprio per questo andremo ad approfondire delle tematiche di estrema attualità e di interesse senza mai distogliere l'attenzione sul fatto che l'informazione è *potere*, purché la si possa trasformare in *azione*.

2. INTRODUZIONE

Nella maggior parte dei capitoli presentati verrà trattato il tema dell'OSINT, cioè dell'*Open Source Intelligence*, tematica ad oggi strategica per la maggioranza delle aziende, in particolare per lo sviluppo di due attività di analisi considerate fondamentali, quella dei cosiddetti *critical events* e quella della *market intelligence*.

All'interno del recipiente dei *critical events* si vanno a collocare tutta una serie di situazioni/fenomeni di attualità e di estremo interesse, come ad esempio il mondo – ancora tutto da esplorare – della *Cyber Security*, con tutte le sue sfaccettature estremamente variegate, e quello delle *Infrastrutture Critiche*, che rappresentano oggi giorno due cardini fondamentali sui quali ogni Ente Statuale, ancor prima delle aziende, basa il concetto di Sicurezza Nazionale.

Di seguito illustreremo alcuni casi di studio all'interno dei quali non sarà difficile scorgere il valore aggiunto che può dare un'*attività di analisi tratta da fonti aperte*, sempre se fatta con criterio ed equilibrio, e senza mai perdere di vista l'obiettivo primario che essa deve avere in una organizzazione aziendale: quello di *fungere da supporto al processo decisionale del vertice manageriale*.

Ecco quindi che l'OSINT assume una connotazione di *strategicità*, poiché considerato strumento fondamentale che ci indirizza stabilmente verso una direzione piuttosto che verso un'altra, rilevando eventuali rischi, ma anche opportunità e sinergie.

Di conseguenza l'attività di analisi delle fonti aperte è da considerarsi non solo in funzione della *prevenzione dei rischi*, ma anche come fattore che può alimentare il *vantaggio competitivo* di una azienda e che, quindi, può essere determinante per il suo successo.

Tramite la metodologia OSINT una azienda può, infatti, prevedere scenari futuri e analizzarne i rischi, efficientare i processi che riguardano clienti e fornitori, sviluppare campagne di marketing mirate, analizzare la concorrenza esterna, elevare i livelli di sicurezza interna ed esterna, e non solo: possiamo dire che le sue applicazioni in una azienda moderna sono pressochè illimitate.

In sintesi: le aziende che sfrutteranno in futuro l'OSINT, e le potenzialità ad essa collegate date dallo sviluppo della Intelligenza Artificiale (AI), avranno una arma segreta a loro disposizione formidabile.

3. OSINT: IL GRANDE ALLEATO

3.1 IL MONITORAGGIO DELLE FONTI APERTE: VANTAGGI & OPPORTUNITA'

L'acronimo OSINT sta per *Open Source Intelligence* ed è la branca dell'*Intelligence* che si occupa di raccogliere ed analizzare informazioni ed i dati di pubblico dominio, senza violare le leggi sul c*opyright* o sulla *privacy*, estraendoli quindi da **"**fonti aperte**"** a tutti gli utenti.

L'attività di raccolta informazioni da fonti aperte, quindi la ricerca OSINT solitamente avviene procedendo secondo uno schema ben preciso. Si tratta di un ciclo suddiviso in quattro fasi in cui l'analista deve reperire informazioni e produrre un documento (che comunemente viene definito *report*)[1].

Le fasi del ciclo sono:

1. Ricerca (*Discovery*): è la fase iniziale in cui vengono reperite e raccolte tutte le informazioni relative all'oggetto della ricerca.
2. Selezione (*Discrimination*): in questa seconda fase si fa una scrematura eliminando i dati che non sono inerenti allo scopo della ricerca o che siano rilevanti per lo stesso.
3. Analisi (*Distillation*): dopo la fase di scrematura, i dati rimanenti vengono analizzati e collegati tra loro creando delle connessioni.
4. Diffusione (*Dissemination*): in fase finale viene redatto un documento riportanti le risultanze della raccolta informazioni.

In caso di ricerca sul *web*, quella considerata più diffusa, ci sono degli strumenti che possono essere estremamente utili per le attività di ricerca. Si tratta di strumenti o *tools,* disponibili sul mercato; fra i più conosciuti possiamo citare:

- *Maltego*: è un tool molto utile per indagare negli archivi pubblici inoltre è di facile comprensione riproducendo i risultati della ricerca sotto forma di grafico.
- *Spiderfoot*: è un motore di ricerca di informazioni pubbliche, lavora inviando la richiesta a più di 100 fonti di informazione ed elaborando tutti i dati.
- *Shodan*: con questo motore di ricerca è possibile rintracciare tutti i dispositivi collegati alla rete internet e gestibili da remoto.

Il progresso tecnologico e la società dell'informazione hanno messo a disposizione di chiunque terabyte e terabyte di dati pubblicamente accessibili: è la "democratizzazione"

[1] Vedi: https://www.difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/42175_Minniti_0pdf.pdf

dell'*intelligence* attraverso la quale ciascuno di noi può controllare e verificare le informazioni in origine disseminate in via esclusiva da parte di autorità statuali e non.

Attraverso questa **"**democratizzazione**"**, il mondo dell'OSINT non è più appannaggio delle sole agenzie di intelligence nazionali: anche organizzazioni private, semplici amatori e normali utenti del web hanno oggi a disposizione strumenti formidabili a cui attingere anche per i più svariati fini.

La mole dei dati disponibili attraverso fonti pubbliche è ormai quasi illimitata.

Per fare un esmpio, in tempi recenti un ricercatore ha scoperto un sito missilistico cinese, fino allora ritenuto segreto, grazie a comuni e pubblici strumenti di osservazione.

La scoperta del sito cinese è stata possibile grazie alle immagini fornite dalla *Planet*, un provider di immagini satellitari commerciali.

Lo sviluppo dell'OSINT è stato così potente da far nascere addirittura piattaforme di giornalismo partecipativo, fra cui *Bellingcat*, attiva di recente con il monitoraggio effettuato tramite le immagini satellitari del conflitto Russo-Ucraino.

Alcuni esperti recentemente hanno addirittura parlato di "democratizzazione" dell'intelligence e dell'enorme contributo che l'OSINT ha dato alla trasparenza delle informazioni ed alla possibilità aperta a tutti di conoscere verità che prima erano nascoste dai governi[2].

[2] Vedi: https://www.agendadigitale.eu/sicurezza/osint-lintelligence-del-popolo-vantaggi-e-rischi-delle-indagini-a-portata-di-clic/

3.2 UNO STRUMENTO DI INTELLIGENCE NEI SETTORI DEL PUBBLICO E DEL PRIVATO

Gli ultimi decenni sono stati caratterizzati da importanti mutamenti come la trasformazione profonda degli assetti geopolitici e strategici globali e l'abbattimento delle distanze generato dal progresso tecnologico. Nel contempo, l'accendersi del recente conflitto Russo-Ucraino, l'assenza di un ordine mondiale stabile, i conflitti etnico-religiosi ed il sempre attivo terrorismo internazionale, hanno determinato, in questo contesto, una progressiva revisione dei concetti di *Difesa* e di *Sicurezza*.

A quanto sopra si aggiunga che la diffusione dell'accesso ad internet ha mutato il mondo dell'informazione e della conoscenza contribuendo, assieme ad altri fenomeni, alla formazione sì di una *cultura globale* ma, di rimando, anche alla nascita di culture ad essa antagoniste, determinando sia nuove forme di integrazione ma anche nuove forme di conflitto tra individui e tra organizzazioni.

Con i grandi cambiamenti degli ultimi decenni e la forte accelerazione che caratterizza il nostro tempo, alcuni elementi storicamente di secondo piano vengono ora riscoperti. Soprattutto nei Paesi nordeuropei ed anglosassoni, l'*Intelligence,* che in tutte le sue forme pone particolare attenzione alle fonti aperte, è divenuta un'arma di notevole importanza.

Infatti, nell'era di Internet, la fonte di inesauribile ricchezza, è costituita dai dati che gli utenti, navigando, lasciano dietro di sé.

In media in Italia, secondo recenti indagini, una persona passa più di 6 ore al giorno al pc o a uno smartphone. Questo elevato numero di ore, spesso giustificato da esigenze lavorative, ma perlopiù dettato da scelte personali, fa sì che navigare in internet sia ormai una parte irrinunciabile della nostra vita.

Non è difficile quindi capire che ogni giorno lasciamo in rete quantità enorme di dati: elementi personali, preferenze di consumo, indirizzi e-mail, foto, abitudini, ideologia politica, orientamento sessuale o altro.

I dati degli utenti interessano quindi a tutte le aziende, istituzioni, partiti, associazioni che grazie ai dati possono venderci qualcosa o ottenere altra utilità. Gli elementi personali lasciati dagli utenti del web definiscono chi siamo, cosa facciamo e che preferenze abbiamo: informazioni preziosissime per trasformare i soggetti in clienti o, per esempio, in elettori, basti pensare allo scandalo di qualche anno fa di *Cambridge Analytica*[3].

Questo è l'aspetto pericoloso del *cyberspazio*: l'impronta digitale che lasciamo dietro di noi ogni volta che accendiamo il telefono o il computer e ci colleghiamo ad internet. Ma al contrario c'è anche un lato positivo: l'accessibilità ai medesimi dati, da parte di chi ha

[3] Vedi: https://goldenowl.medium.com/the-cambridge-analytica-scandal-unveiling-the-impact-of-osint-in-political-campaigns-b1ff6dc5ea4a

necessità di ottenere informazioni per tutelare un legittimo interesse o un diritto soggettivo. In altre parole, è vero che i dati personali che lasciamo nella rete - mentre navighiamo, ci registriamo, esprimiamo preferenze - possono essere usati "contro di noi" a discapito di privacy e libertà, ma di contro quegli stessi dati possono essere utilizzati da qualcuno che per tutelare sé stesso, in buona fede, quando legittimamente deve sapere di più su una situazione o un soggetto.

È comunque una esperienza acquisita che, sempre più negli ultimi anni, stiamo osservando lo sviluppo dell'OSINT quale strumento in evoluzione sia nel settore pubblico che in quello privato.

In particolare, nell'ultimo decennio, il settore pubblico ed il suo rapporto con il cittadino è cambiato e si è evoluto anche, e soprattutto, grazie alla rivoluzione digitale.

Questa rivoluzione digitale richiede alle amministrazioni pubbliche ed alle agenzie governative uno importante sforzo dal punto di vista normativo. La digitalizzazione ha di fatto riavvicinato lo Stato alle aziende ed ai soggetti privati.

Al fine di attivare un nuovo modello pubblico-privato integrato e interoperabile, sono stati creati ultimamente - facendo ampio ricorso anche a metodologie OSINT - progetti su larga scala, tra soggetti pubblici e privati, finalizzati a scambi informativi ed attività di ricerca su tematiche strategiche, quali l'*Industrial Security* e la *Cyber Defence*.

Tale modello di cooperazione ha consentito di sviluppare tutta una serie di progetti importanti, che hanno al loro interno una base sempre rappresentata dalle ricerche ed analisi OSINT. Uno esempio per tutti: basti pensare alle varie piattaforme tecnologiche dedicate al servizio della *Cyber Threat Intelligence* e che si possono trovare all'interno di strutture informatiche di prevenzione come i SOC (*Security Operation Centre*).

Altro esempio sono i vari tavoli che hanno l'obiettivo di favorire lo scambio informativo relativo alla crescente minaccia cibernetica portata avanti da cybergang o da paesi ostili: collaborazioni molto preziose che negli ultimi anni hanno permesso di aumentare le capacità di rilevazione delle minacce grazie alla qualità degli indicatori di compromissione scambiati.

Sia il settore pubblico che quello privato aziendale sono quindi impegnati attivamente nello scambio e nell'utilizzo di tecniche OSINT finalizzate ad accrescere, nei limiti consentiti dalla legge, la loro capacità di *intelligence*.

A scopo dimostrativo si riporta in Appendice A.[4] un esempio di Scheda Analisi Rischi Paese, gentilmente concessaci da una società specializzata nell'analisi dei rischi ed elaborata - con metodologia OSINT - ad uso di unità organizzative di Travel Security di aziende

[4] La Scheda Analisi Rischi Paese riportata in Appendice A è stata elaborata dalla società Business Intelligence Consulting Srl che ne ha gentilmente autorizzata la pubblicazione in questa tesi.

internazionali che inviano il loro personale in missione di lavoro all'estero - a volte in aree geografiche caratterizzate da condizioni di criticità o addirittura ostili - al fine di portarli a conoscenza dei possibili rischi che potrebbero trovare in quel Paese. La scheda riportata nelle pagine seguenti è stata elaborata con informazioni tratte da fonti aperte di origine istituzionale (ad esempio: i siti web dei Ministeri degli Affari Esteri e dell'Interno) e di origine privata (ad esempio: le piattaforme informative di organizzazioni private, quali L'ISPI, IAI, Transparency International, ecc.).

3.2.1 RICERCA INFORMATIVA

La ricerca per elaborare la scheda viene svolta con il metodo OSINT – *Open Source Intelligence* – per poter attingere dal bacino più ampio possibile di sorgenti informative, comprese quelle in lingua straniera.

Tale procedimento prevede di verificare anche le notizie che provengono da fonti avverse, addirittura ostili, e che contengono tracce critiche nei riguardi dell'obiettivo che viene monitorato e seguito nella molteplicità dei campi di ricerca e analisi.

La qualità delle notizie assunte consente poi di tracciare l'analisi valutativa e predittiva, al fine di garantire e preservare al meglio il conseguimento e la protezione del *business* aziendale nonché la sicurezza di coloro i quali devono svolgere le attività sul campo.

Tutte le notizie riportate sono supportate da immagini che integrano i contenuti.

3.2.2 STRUTTURA

La scheda Paese è concepita per fornire al decisore differenti punti di conoscenza e valutazione diretta, secondo un modello dinamico che viene verificato e aggiornato di norma almeno mensilmente per renderlo sempre attuale e altamente attendibile, soprattutto per quel che concerne la scala dei valori della criticità e del *trend* della stessa, entrambe raffigurate anche attraverso elementi cromatici che facilitano l'immediato approccio visivo.

Un complesso di riferimenti conoscitivi riguarda lo scenario politico del Paese-obiettivo, cioè l'insieme dei dati che raggruppano indicazioni sintetiche sull'ordinamento, il sistema legislativo l'assetto governativo, la superficie territoriale e la popolazione, la religione, le lingue parlate, la valuta locale, il fuso orario e la differenza d'orario con l'Italia, i recapiti telefonici d'emergenza, le compagnie telefoniche, le norme per l'ingresso e i codici aeroportuali.

Una seconda sezione attiene all'ambasciata italiana presente sul territorio, con indicazioni sull'ubicazione e gli indirizzi di riferimento, i recapiti telefonici, inclusi quelli d'emergenza sul posto e in Italia, e quelli telematici, la composizione della rappresentanza diplomatica.

Il *focus* è concentrato su aree tematiche integrate che compongono lo scenario di riferimento e che possono essere implementate o modificate per rispondere alle esigenze specifiche

dell'azienda committente, che in questo si è ipotizzato risponda ad una azienda operante nel settore industriale della Difesa.

L'insieme delle conoscenze comprende un esame generale che assume poi connotati più specifici e mirati in profondità, concentrando l'osservazione sugli orientamenti geopolitici, il quadro economico, i profili critici, la politica di difesa e d'armamento. In ogni voce, cioè nei singoli paragrafi, sono riportati mensilmente gli eventi di maggiore rilievo, dai quali si evince il carattere politico e strategico adottato dall'obiettivo, oppure le minacce e le criticità che sono determinate da fattori endogeni ed esogeni, così come da emergenze sanitarie o condizioni endemiche ed eventi specifici.

La sezione quadro generale raccoglie notizie che consentono d'esaminare le dinamiche di carattere nazionale e internazionale, gli assetti di governo, i cambiamenti e le iniziative, le strategie governative prevalenti e quelle delle opposizioni parlamentari, tutti aspetti che permettono di disporre costantemente d'una fotografia aggiornata e corrente sulla stabilità o meno del Paese.

Non mancano aggiornamenti sulle relazioni bilaterali con l'Italia, così come quelle in campo internazionale, così da fornire gli elementi conoscitivi per comprendere gli equilibri e la competitività sviluppata da altri Paesi nei confronti dell'Italia e delle sue aziende.

Nelle altre sezioni – quadro geopolitico, criticità, sicurezza ed economia – vengono approfondite le questioni di maggiore interesse settoriale, in modo da fornire elementi conoscitivi e d'analisi diretta circa le strategie poste in essere dai governi, e gli elementi su cui concentrare l'attenzione per assicurare la presenza del proprio personale all'estero. In merito, sono fornite indicazioni attinenti a episodi di differente livello di criticità, anche rapportate a iniziative o situazioni originate in Italia, fino a suggerire l'adozione di condotte preventive per evitare possibili inconvenienti.

La descrizione delle più importanti iniziative economiche in atto offre la possibilità di prendere conoscenza dell'affidabilità finanziaria, dell'autonomia o dipendenza del Paese da relazioni esterne vincolanti, che potrebbero riverberarsi sugli indirizzi e scelte politiche. Nella sezione "sanità" viene riportato il quadro sanitario del Paese di destinazione che include eventuali malattie a rischio, le vaccinazioni consigliate e obbligatorie, la situazione ospedaliera locale e, soprattutto a seguito della recente pandemia mondiale Covid 19, l'andamento dei contagi locali e le norme sanitarie che regolano l'ingresso nel Paese.

Le sezioni difesa e armamento completano per la specifica azienda committente il quadro di riferimento poiché illustrano le politiche di approvvigionamento militare del Paese, le sue politiche di sviluppo industriale nel settore della difesa e le alleanze con altri paesi in tema di cooperazione militare.

3.3 METODOLOGIA, VANTAGGIO COMPETITIVO E FUNZIONE STRATEGICA

In un suo ricco articolo l'esperto Michelangelo Di Stefano traccia le metodologie di ricerca OSINT / SOCMINT[5]:

Nell'ambiente internet **"**è frequente che alcuni soggetti utilizzino la c.d. *sentiment analisys*, cioè il monitoraggio e la manipolazione delle emozioni, per veicolare notizie false (*fake news*) camuffate da cornici e titoli appetibili**"**. Questo avviene spesso per esigenze di marketing, di e-commerce, di brand commerciale, ovvero per veicolare le tendenze socio-politiche o per una azione di *controinformazione* o di *disinformazione*.

Nelle attività di monitoraggio della comunicazione è, quindi, sempre più necessario procedere parallelamente all'ispezione di fonti aperte sul web, con un approccio OSINT.

Tale approccio, per una analisi completa delle fonti aperte deve necessariamente prevedere una concomitanza di diversi ambiti disciplinari quali: un uso avanzato e professionale dei motori di ricerca e di portali specializzati, ad esempio in Italia i più utilizzati sono *Cerved* e *Cribis*, dove si possono estrarre le informazioni da registro pubblico su persone fisiche e giuridiche, sulle partecipazioni societarie e cariche aziendali, proprietà immobiliari, ecc.; tutti gli strumenti definiti di *hackeraggio* al fine di frodare i dati sensibili degli utenti e le loro identità digitali. A tutto questo si deve aggiungere un attento uso delle tecniche di analisi investigative per valutare ed elaborare il materiale informativo acquisito.

L'analista OSINT dovrà procedere correlando informazioni diverse, setacciando anche nel mondo del *Deep* e *Dark Web*, cioè quella parte di una grande massa di siti non indicizzati dai motori di ricerca, raggiungibile solo attraverso software per la navigazione anonima come Tor.

Nella ricerca e nell'analisi delle fonti aperte, l'analista di intelligence trova aiuto anche attraverso l'impiego di comuni software di analisi semantica disponibili sul mercato ovvero di protocolli di analisi semantica più approfonditi, definiti *Intelligence Data Mining*, finalizzati all'individuazione di informazioni nascoste.

Le tecnologie tradizionali normalmente possono solo cercare di indovinare il senso di un testo, mentre i software di analisi semantica approfondita riescono a leggere ed interpretare le parti più potenzialmente interessanti e identificano in automatico le relazioni concettuali fra le varie informazioni, anche quelle protette da sistemi di crittografia.

Diviene evidente quanto sia importante e strategico, per gli analisti e gli esperti di intelligence, il padroneggiare le metodologie e le tecniche per il monitoraggio degli utenti del *web* dato lo sviluppo e l'imponente espansione dei *social media*.

[5] Vedi: https://www.altalex.com/documents/news/2020/02/14/ricerca-investigativa-metodologie-osint-socmint-sulle-fonti-aperte

In questo contesto la *Social Media Intelligence* o SOCMINT, una branca dell'OSINT , viene ad assumere oggigiorno una particolare importanza.

Proprio in questo specifico ambiente di *intelligence* si sta sviluppando una tecnica di monitoraggio, sia massivo che individuale, in grado di tratteggiare ed analizzare in modo profondo gli interessi e le propensioni degli utenti del *web*.

Si tratta di una tecnica nata inizialmente a fini di commercio ed avviata con l'utilizzo dei *rootkit*, installati nativamente su milioni di smartphone al fine di monitorare molteplici informazioni private relative all'utilizzo del dispositivo (applicazioni nascoste, apparentemente discrete, in grado di consentire agli operatori, ed alle stesse case produttrici, di veicolare le scelte aziendali e quelle dei consumatori; manovrare ai propri scopi, seppure in modo silente o subliminale, gli interessi degli utenti con banner pubblicitari ed altri accorgimenti commerciali).

Come detto, le tecniche di *Social Media Intelligence* consistono in avanzate procedure di monitoraggio e profilazione massiva sociale: uno strumento nato per conoscere e condizionare interessi ed orientamenti di fasce e categorie sociali, ma che ora è diventato anche lo strumento più importante ed evoluto che gli agenzie di intelligence e di sicurezza di tutto il pianeta hanno a disposizione per arginare e prevenire le nuove forme di terrorismo, le quali oggi, sempre di più, attraverso il *web*, fanno propaganda, proselitismo, favorendo l'emulazione e l'intimidazione psicologica.

SOCMINT è diventata di fatto uno strumento versatile e adattabile alla specifiche esigenze investigative di intelligence (sia essa giornalistica, commerciale, merceologica, di ricerca sociale, geopolitica, strategico militare, di investigazione giudiziaria o di informazione e sicurezza istituzionale) che, con l'adozione delle *queries* di ricerca più adatte, consente di scandagliare a fondo i profili social; rilevare le relazioni esistenti tra quelli di interesse; individuare e suddividere per tematiche ed aree geografiche i movimenti più complessi delle comunicazioni presenti sui social; effettuare ricerche fotografiche su base antropologica; effettuare ricerche e comparazioni foto/biometriche; effettuare complesse ricerche merceologiche per macro/micro area geografica, prodotto ed utenza sui motori di ricerca del *clear* e del *deep web*; ricostruire lo storico dei dominii e rintracciare vecchi siti ormai rimossi; disegnare le reti delle relazioni sociali attraverso le varie applicazioni di social network e di telefonia mobile abbinata ai profili.

Tramite la SOCMINT è possibile, tramite il monitoraggio e l'analisi dei contenuti scambiati attraverso i *Social Media*, raccogliere informazioni essenziali al lavoro di *Intelligence*.

Va poi sottolineato che l'azione della SOCMINT non si dovrà basare sui soli social network più utilizzati, come Facebook, Twitter, Instagram, Telegram, ma per una completezza di indagine, si baserà sulle informazioni acquisite tramite *tutti* i tipi di *Social Media*, anche i più desueti o inconsueti.

La SOCMINT, spiega Alessandro Burato, uno dei massimi esperti del settore, **"**si è concentrata sui processi di data mining rivolti a due principali aspetti degli ambienti social: i contenuti e le relazioni. I primi hanno dato origine a diversi studi sui cosiddetti motori semantici utili nell'analizzare e filtrare grandi stringhe di dati come sono quelle delle comunicazioni che scorrono sui social, i secondi si concentrano maggiormente sulle relazioni virtuali che intercorrono tra i diversi user avvalendosi delle moderne tecniche di visualizzazione dei dati per darne una visione più ampia ed immediata.**"** [6]

Poiché tutta la mole di dati estratti va studiata, compresa ed elaborata per cogliere profondamente la ricchezza di informazioni e significato dei dati che rappresentano, si è reso necessario nel tempo sviluppare dei sistemi di verifica dell'affidabilità e validità dei dati raccolti, anche secondo il punto di vista delle scienze sociali.

Per fini di intelligence istituzionale o di investigazione giudiziaria potrà, però, accadere che l'analista SOCMINT debba andare oltre le normali fonti aperte, ma dovrà introdursi nella rete sociale del soggetto d'interesse, anche attraverso la condivisione di una o più "amicizie", in modo da poter accedere a notizie presenti su gruppi chiusi presenti sui social media.

Prosegue sempre l'esperto OSINT Di Stefano:

"L'infiltrazione nella rete sociale del "bersaglio" avviene sempre in modo indiretto, al fine di evitare l'insospettimento del target, monitorando, accanto ai collegamenti pubblici, le sue reti (ad esempio: *Facebook*, *Linkedin*, *Twitter*, *Tinder*, *Thunder*, *Whatsapp* o qualsivoglia strumento di aggregazione e condivisione social) o, qualora possibile legalmente ed utile, attraverso richieste dirette di "amicizia" con l'utilizzo di un profilo *fake* di copertura (nel caso di attività istituzionali per fini di investigazione giudiziaria e di sicurezza nazionale, il legislatore ha previsto particolari esimenti contemplando lo status giuridico di "agente sotto copertura").

In questa fase assumono rilevante importanza i motori di ricerca semantica approfondita, attraverso cui sarà possibile analizzare, ad esempio, il profilo *Facebook* del soggetto investigato.

L'analista delle fonti aperte si troverà, inoltre, spesso a districarsi tra informazioni spesso inutili che hanno coperto un certo dominio e dovrà cercare di trovare delle connessioni logiche partendo ad esempio, dai *tools* per l'identificazione di *domine name*, fino alla riesumazione di percorsi chiusi con protocolli di *wayback* (queste ricerche sono possibili, ad esempio, attraverso il sito *archive.org*).

[6] Vedi: https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/socmint-un-nuovo-%20spazio-per-la-raccolta-di-informazioni-rilevanti.html

Una modalità di individuazione delle relazioni, che gli analisti esperti stanno usando sempre maggiormente, è quella della profilazione delle relazioni sociali attraverso l'applicativo *Facelink*, un software dedicato propriamente all'analisi dei social media ed in grado di

interfacciarsi con altri strumenti di analisi relazionale, come TETRAS HPG o SFERA, attraverso cui è possibile mettere in relazione i dati personali dei soggetti sotto osservazione, quali le utenze telefoniche, i suoi contatti, il suo identificativo seriale del telefonino (IMEI) o i codici seriali di una scheda telefonica cellulare (IMSI).

Altri strumenti di analisi più avanzati sono i *browser* forensi come AFW: essi permettono di acquisire interi siti web e riescono ad estrarre, tramite il programma *Tor* pagine web presenti sul *Dark Web*. Questo avviene tramite particolari funzioni di analisi dei contenuti di reti e databases con azioni automatizzate e in maniera metodica, al fine di rintracciare tutte le pagine *web* collegate ad una pagina principale.

Nelle versioni dedicate alle esigenze istituzionali e di indagini di pubblica sicurezza questo particolare il software consente di eseguire ricerche su pagine web anche se protette da login, come i social network, e ne permette la cattura automatica.

Ecco, allora, l'esigenza dell'analista OSINT di effettuare delle ricerche secondo *best practices* che non riguardino non solo la mera interrogazione sui motori di ricerca di una data *key word*, ma facciano ricorso a procedure complesse, in grado di filtrare, a monte, le notizie spazzatura, restringendo così il campo di ricerca alle risultanze utili e, al tempo stesso, poter riscontrare, sulla rete, se alcuni report emersi siano attendibili o "costruiti" falsamente.

Un esempio molto semplice è quello offerto dai motori di ricerca GOOGLE oppure BING i quali permettono la ricerca in rete di fotografie sempre tracciate in rete, così da individuare altre foto con la stessa estensione.[7]

Anche se l'investigazione giornalistica per prima ha usato la ricerca sulle fonti aperte, è ormai prassi consolidata per le autorità giudiziarie ricorrere alle "esplorazioni" a cura della polizia giudiziaria sulla rete per acquisire i contenuti disponibili sulla rete internet.

L'investigazione giudiziaria opera attraverso i parametri valutativi dell'attendibilità della notizia, fissati dalle consolidate prassi della comunità scientifica internazionale in materia di "fonti aperte" e a cui si è uniformata anche EUROPOL e NATO, con l'uso di protocolli di *Open Source Intelligence*,

La valutazione e la conseguente utilizzabilità delle informazioni risultanti dalle investigazioni che vengano raccolte attraverso tecniche di *Open Source Intelligence* avviene secondo un rigido protocollo che viene utilizzato al fine di stabilire l'attendibilità di una

[7] Vedi sempre: https://www.altalex.com/documents/news/2020/02/14/ricerca-investigativa-metodologie-osint-socmint-sulle-fonti-aperte

notizia spendibile in un contesto istituzionale o giudiziario e che sia rilevante per fornire agli interessati o al giudice elementi concreti di prova.

Tali metodologie operative rimandano ad una griglia di validazione di attendibilità, sia della fonte che della stessa informazione.

Di seguito sono riportati i protocolli più utilizzati:

Metodo 4X4 EUROPOL

Su una scala dei valori, sull'asse delle ascisse viene fatta una valutazione di attendibilità della fonte da 1 a 4, e stessa cosa accade sull'asse delle ordinate per la valutazione dell'informazione: laddove il risultato rientri entro il punteggio 2, l'informazione sarà da ritenersi confermata.

- I codici di attendibilità della FONTE sono cosi classificati:
  - **A**= senza dubbi di autenticità. Affidabile o competente oppure in passato sempre affidabile.
  - **B**= affidabile nella maggior parte dei casi.
  - **C**= non affidabile nella maggior parte dei casi.
  - **D**= non valutabilità dell'affidabilità (es. anonima).
- I codici di attendibilità di valutazione/accuratezza dell'INFORMAZIONE sono:
  - **1**= sicura.
  - **2**= conosciuta personalmente dalla fonte ma non dall'agente che la riferisce.
  - **3**= non conosciuta personalmente dalla fonte ma avallata da altre informazioni già registrate.
  - **4**= non conosciuta personalmente dalla fonte e non avallabile in alcun modo.

Griglia 6X6 NATO

Altra tipologia di riscontro dell'informazione trova compendio applicativo internazionale nel manuale *Admirality Code NATO System*.

- Affidabilità della FONTE:
  - **A** - affidabile: nessun dubbio sull'autenticità, sull'affidabilità o sulla competenza della fonte. History of complete reliability. Storia di completa affidabilità
  - **B** - di solito affidabile: Minori dubbi. History of mostly valid information. Storia di informazioni per lo più valide
  - **C** - abbastanza affidabile: dubbi. Provided valid information in the past. Fornito informazioni valide in passato
  - **D** - non di solito affidabile: dubbi significativi. Provided valid information in the past. Fornito informazioni valide in passato

- **E** - inaffidabile: Manca di autenticità, affidabilità e competenza. History of invalid information. Storia di informazioni non valide
- **F** - non può essere giudicato: informazioni insufficienti per valutare l'affidabilità. May or may not be reliable. Può o non può essere affidabile

- Affidabilità dell'INFORMAZIONE

  - **1 Confermato:** Logico, coerente con altre informazioni rilevanti, confermato da fonti indipendenti
  - **2 Probabilmente vero**: logico, coerente con altre informazioni pertinenti, non confermato
  - **3 Forse vero**: ragionevolmente logico, concorda con alcune informazioni rilevanti, non confermate
  - **4 Senza dubbio vero**: non logico ma possibile, nessun'altra informazione sull'argomento, non confermata
  - **5 Improbabile**: non logico, contraddetto da altre informazioni pertinenti
  - **6 Non può essere giudicato**: la validità delle informazioni non può essere determinata

4. OSINT: DA STRUMENTO DI PROTEZIONE A FATTORE VINCENTE PER IL BUSINESS

4.1 OSINT E SENTIMENT ANALYSIS PER LA SICUREZZA

La *sentiment analysis* "è un'analisi incentrata sulle opinioni e sulle interazioni che gli utenti hanno con un *brand* in un determinato contesto ed in un arco temporale specifico" [8].

I social media sono ormai dei veri e propri strumenti utilizzati a fini di marketing dalle aziende; questo presupposto ci fa capire fino in fondo il significato di *sentiment analysis.*

Rilasciando commenti, taggando o semplicemente mettendo un "like", gli utenti dei social trasmettono informazioni importanti che possono essere così descritte:

- incidenza sulla reputazione sul *web* del *brand;*
- indicazione del livello di soddisfazione del consumatore.

Elaborando i dati così raccolti, le aziende sono in grado quindi di mirare le loro strategie sia di comunicazione, sia produttive, basandosi sulle interazioni, gusti, abitudini e tendenze di gradimento degli utenti dei social media.

Tali interazioni vengono così raccolte ed analizzate, estrapolandole dai *feedback* ed dalle recensioni rilasciate, in relazione ad eventi, prodotti, servizi o, addirittura a singoli individui.

La *sentiment analysis* viene applicata in qualsiasi settore: sport, comunicazione, finanza ecc.

Inoltre, un importante uso della *sentiment analysis* è quello che se ne fa nel campo della sicurezza nazionale, laddove l'afferrare rapidamente le tendenze socio-economiche diviene sempre più importante, come ad esempio nella prevenzione e lotta delle tendenze terroristiche.

La maggior parte dei giudizi e dei commenti rilasciati sui social network sono dettati da una spinta emotiva. Gli utenti social che rilasciano giudizi sono definiti "portatori di opinioni" ; tali opinioni hanno solitamente tre orientamenti: positivo, negativo o neutro.

L'uso della *sentiment analysis* nel marketing ci pone di fronte una questione importante: come sia possibile che una macchina sia in grado di individuare "l'emozione provata da un utente in un determinato contesto e dopo una specifica esperienza?"

Negli ultimi anni sono stati ideati specifici software di *sentiment analysis* che riescono addirittura ad immedesimarsi con l'utente e capire quali emozioni ha provato quando ha

[8] Vedi: https://www.wearefiber.com/it/blog/sentiment-analysis-cose-e-come-sfruttarla-per-le-aziende

rilasciato il commento, per poi classificarlo come positivo, negativo o neutro lavorando tramite il *machine learning*, il *data mining* ed il *natural language processing*.

È sì evidente, quindi, quale sia l'importanza e l'effetto dello studio e dell'analisi dei social media per la raccolta dei *big data* fondamentali per l'azione di *sentiment analysis* svolta al fine del marketing aziendale; ma ancor più assume importanza strategica l'osservazione attenta, da parte di enti statuali, degli scenari politici e sociali, sia in tempo reale, sia per una previsione a medio e lungo termine e per il monitoraggio degli umori più o meno sotterranei di gruppi anarchici, antagonisti, terroristici, a fini di prevenzione.

A questo fine infatti estremamente attuali e correlati alla *sentiment analysis* sono i modelli predittivi, utilizzati questi all'interno di una attività di prevenzione, volta ad assicurare un livello adeguato di sicurezza di una nazione, organizzazione, ecc.

Nel caso specifico della tutela della sicurezza nazionale, coloro che utilizzeranno questi modelli predittivi dovranno sapere raccogliere le informazioni sia sui social network sia su siti già indicizzati e quindi affidabili, dopodiché analizzare, con equilibrio ed imparzialità, se potrebbe manifestarsi una situazione comprovata di rischio.

Altro fattore estremamente importante è relativo al fatto che l'analista deve sapere parlare lo stesso linguaggio con il quale ci si parla all'interno dei social media. Un esempio banale è la ricerca di una informazione utile all'interno di blog gestiti da gruppi anarchici o antimilitaristi, dove spesse volte il linguaggio, ai fini di un'analisi puntuale, deve essere interpretato correttamente.

4.2 OSINT E MARKET INTELLIGENCE ANALYSIS

La *market intelligence*[9] non è altro che una strategia sviluppata per aiutare a costruire una visione più ampia dei possibili problemi futuri, anticipando le soluzioni.

Spesso si tende a limitare la *market intelligence* alla sola analisi della concorrenza: questo tipo di analisi è denominata anche *competitive intelligence* o *business intelligence.*

Il vantaggio principale della *market intelligence* è comunque quello di conoscere la percezione del pubblico di un particolare prodotto o servizio, capire come valutano un *brand*, valutare la coerenza dei prezzi, monitorare i marchi concorrenti, identificare le tendenze del mercato.

Cosa si può fare praticamente con la *market intelligence*?

- Scoprire cosa cercano i potenziali clienti in rete: analizzando cosa essi ricercano su *Google* e tracciando come cambiano gli interessi degli stessi nel tempo.
- Scoprire cosa pensano del tuo marchio, dei tuoi prodotti e/o servizi e di quelli dei tuoi concorrenti, in tempo reale grazie al *social listening* con risultati privi di contaminazioni e senza alcun filtro esterno
- Conoscere la frequenza con cui i potenziali clienti consultano i siti dei concorrenti ed attraverso la *web intelligence*, avere una visione privilegiata per comprendere come si muovono i competitors online e quali siano i loro risultati, monitorandoli continuamente.
- Conoscere i risultati delle vendite dei concorrenti sui principali *marketplaces*.

Molteplici sono le fonti di informazioni OSINT utilizzabili per una *market intelligence analysis*:

- tendenze socio-demografiche tramite le analisi pubblicate dall' *Istat*;
- cosa piace al pubblico e il comportamento sui canali e le piattaforme web con le ricerche della società *Nielsen;*
- lo stato di salute e l'innovazione nei media, consultando riviste specializzate come *Prima comunicazione* e *Audiweb*;
- le nuove tecnologie con gli Osservatori del *Politecnico di Milano* e *Gartner*;
- le innovazioni dal mondo startup hi-tech, ad esempio con quanto pubblicato sul magazine online *TechCrunch*.

[9] Vedi: https://www.mjvinnovation.com/it/blog/market-intelligence-nell-era-digitale/

4.3 OSINT 2.0 - TRA PASSATO, PRESENTE E FUTURO

L'OSINT è uno dei più potenti strumenti utilizzabile nei conflitti contemporanei, sia essi tradizionali, come le guerre fra stati o il terrorismo, ovvero ibridi come la *cyberwar* e l'*infowar*.

Di conseguenza l'OSINT assume sempre di più importanza per il mondo dell'*intelligence*. La sua specificità operativa si innesta naturalmente e tecnologicamente nel mondo multimediale: la velocità di diffusione delle notizie, la facilità e la crescente necessità di essere informati fanno dell'OSINT una metodologia al servizio dell'intelligence di notevole interesse. La comunità che si occupa di *intelligence* analizza e raccoglie dati da tutte le fonti aperte disponibili cercando di trovare informazioni utili nell'immenso bacino di informazioni libere disponibili.

Un esempio di applicazione delle tecniche OSINT lo abbiamo avuto di recente nell'ambito del conflitto Russo-Ucraino. Già nei mesi precedenti l'invasione Russa, la comunità OSINT rivelò informazioni circa lo schieramento di truppe Russe e le sue manovre al confine con l'Ucraina, svolgendo quindi un ruolo fondamentale. In questo caso è stato utilizzato massicciamente Google Maps per la verifica delle immagini sul terreno. Dalle immagini satellitari ad alta risoluzione, molti dei servizi segreti occidentali, ivi compresi quelli degli Stati Uniti e dei Paesi della NATO, hanno attinto informazioni dalla comunità OSINT[10].

Ad esempio, l'articolo di *Buzzfeeds "How Open-Source Intelligence Is Helping Clear the Fog of War in Ukraine"* racconta che una piccola squadra di ricercatori con sede in California, comunicò che l'invasione dell'Ucraina era già iniziata diverse ore prima che Putin annunciasse, la mattina del 24 febbraio, l'inizio di "operazioni militari speciali". Infatti, guardando l'intensità di traffico - utilizzando GOOGLE MAPS - sulla strada principale da Belgorod in Russia alla seconda città dell'Ucraina, Kharkiv, i ricercatori statunitensi avevano rilevato alle prime luci dell'alba un ingorgo di mezzi blindati russi che si predisponevano ad entrare in Ucraina[11]

Anche a seguito di quanto descritto, ultimamente i grandi media internazionali hanno elogiato il lavoro della comunità OSINT definendolo uno strumento decisivo per una nuova era di comunicazione trasparente, sostenendo che le pratiche e gli strumenti dell'OSINT stanno contribuendo a far conoscere al mondo fatti ed eventi prima impossibili da rilevare.

Negli ultimi tempi già si sta parlando di OSINT del futuro, ossia una nuova frontiera informativa interconnessa e creata da individui uniti in una comunità con la finalità di promuovere studi, analisi e ricerche che siano effettivamente disponibili per tutti e possano fungere da supporto informativo per qualsiasi scopo legittimo e trasparente. Passi da gigante se consideriamo che fino ad un decennio fa nessuno conosceva la metodologia della analisi delle "fonti aperte".

[10] Vedi: https://impactskills.it/osint-la-tecnologia-open-per-documentare-la-verita-in-guerra/
[11] Vedi: https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social

5. OSINT: LA NUOVA FRONTIERA E LE SFIDE FUTURE

5.1 OSINT E CYBER SECURITY

Compito dell'OSINT nella *Cyber Security* aziendale è quello di contribuire alla protezione dei dati pubblici prima che gli *hacker* se ne impossessino per compromettere sistemi/infrastrutture informatiche o per rubare le identità degli utenti del *web*.

Un esempio concreto potrebbe essere questo: le impronte digitali lasciate online e rintracciate da estranei allo scopo di sfruttarle per propri vantaggi. Le impronte digitali possono infatti fornire ai malintenzionati dettagli molto precisi su come ci comportiamo, le nostre abitudini o le informazioni sul nostro IP o sul dispositivo che utilizziamo e molto altro.

Oggi la ricerca di informazioni avviene tramite milioni di dati raccolti su internet, indagini svolte su fonti online come i *post* dei blog, i profili dei social media o le immagini postate, si traducono in una preziosa raccolta di informazioni da strutturare, correlare e verificare. Tutte queste informazioni, unitamente all'analisi di supporti cartacei, documenti governativi, pubblicazioni accademiche e molto altro, in mano a chi sappia mettere in relazione molti punti insieme, può significare un grande potere.

La domanda di OSINT nell'ambito della *Cyber Security* sta quindi crescendo e lo sarà anche in futuro: principalmente nelle funzioni di sicurezza nazionale e sempre più nella *business intelligence*.

In questo contesto assume un ruolo fondamentale la *Cyber Threat Intelligence* - branca della *Cyber security* - che comprende l'insieme delle teorie, procedure e strumenti per la raccolta e la condivisione di informazioni sulle minacce informatiche finalizzate alla creazione di strategie, tattiche di intervento e sistemi di monitoraggio. Il fine ultimo della *Cyber Threat Intelligence* è principalmente la ricerca, l'individuazione e la selezione dati relativi a target, asset, indirizzi IP, email, dati personali[12].

La *Cyber Threat Intelligence* utilizza spesso termini specifici dello spionaggio quali ad esempio target, attacchi, tattiche. Anche se tali definizioni e un preciso frasario possono far pensare a qualcosa di particolarmente complesso, in realtà le soluzioni di *cyber intelligence* dovrebbero essere applicate anche a contesti molto piccoli come le PMI e singoli cittadini, adattandosi ottimamente alle esigenze di protezione dei dati.

Il fine ultimo risiede nell'utilizzo di informazioni accurate e rilevanti che, dopo attento esame e contestualizzazione, possano essere utilizzate tempestivamente, al fine di proteggere l'entità monitorata dall'esposizione al rischio di violazione della sua sicurezza. La valutazione preventiva dei rischi può così aiutare a mitigarli.

[12] Vedi: https://www.dssecurity.it/blog/trends/cyber-threat-intelligence-quello-che-ce-da-sapere/

Una delle principali fonti di dati di interesse sono quindi i *data breach* (violazione dei dati personali), tramite i quali è possibile ricercare dati di interesse e in particolare password.

Infatti, la pessima abitudine degli utenti di riciclare password su più servizi on line, li espone a rischi di violazioni dei dati. Pertanto, chiunque abbia accesso a *data leak* (divulgazione dei dati) può agevolmente violare sistemi che si pensa siano ben protetti.

Altra ricchissima fonte di informazioni sono i *social network*, nei quali si trovano miriadi di informazioni utili per attacchi basati su tecniche di *social engineering*.

La *Cyber Threat Intelligence* applica una metodologia ben definita, che permette di raccogliere e analizzare i dati; la procedura è organizzata seguendo principalmente i seguenti punti focali:

- la gestione della vulnerabilità: è la fase in cui si esaminano i punti deboli di un sistema informatico con il fine di eliminarli, rendendo inutili gli eventuali tentativi d'intrusione;
- l'analisi delle minacce e dei rischi: monitoraggio dell'esposizione agli attacchi informatici e dei rischi ad essi correlati e relativo rilevamento;
- la prevenzione delle frodi: creazione di sistemi che permettano di stimare la possibilità di incorrere in eventuali tentativi di truffa;
- l'individuazione di elementi di esposizione agli attacchi informatici, al fine di consentire interventi rapidi ed efficaci;
- la reazione tempestiva in caso di intrusione nel sistema informatico.

In un mondo che, come il nostro, è iper-connesso, tutte le organizzazioni e le aziende rischiano di finire nel mirino dei criminali *cyber*. Aumentando gli attacchi cyber in termini di quantità e di gravità, le difese tipiche della classica sicurezza IT possono diventare infatti insufficienti.

La sempre più dannosa e persistente minaccia informatica, ha ormai raggiunto livelli talmente sofisticati che il suo trattamento preventivo è ormai fondamentale e necessario. Infatti, piuttosto che aspettare di subire un attacco, è assolutamente necessario implementare le prassi attive di intelligence: in pratica le organizzazioni e le aziende devono adottare criteri e metodi più moderni e costruttivi verso i rischi legati alle minacce informatiche ed aumentare la propria consapevolezza e preparazione verso tali rischi.

L'utilizzo dell'intelligence sul *Dark Web* può fornire tale conoscenza e consapevolezza, attraverso lo studio e l'individuazione dei possibili avversari che si nascondono nel *Dark Web*.

Gli analisti possono raccogliere informazioni strategiche attraverso l'intelligence sul *Dark Web.* Si possono con questa via conoscere le intenzioni malevole dei *cyber* criminali, riconoscendone le tattiche attuate. Attraverso tale studio si può quindi ipotizzare e calcolare il rischio imminente o potenziale ed addirittura predirne l'eventuale accadimento[13].

Gli analisti d'intelligence usano il *Dark Web* per reperire informazioni preziose sulle minacce e sui potenziali target, informazioni che non accessibili con le normali ricerche convenzionali. Tramite il *Dark Web* è possibile reperire, oltre a tutte le informazioni sottratte nei *data breach* contenenti i dati esfiltrati ai danni di vittime inconsapevoli, vi sono anche liste di codici informatici trafugati, liste di vulnerabilità informatiche messe in vendita.

Raccogliere ed osservare tutte queste informazioni rende possibile per gli analisti individuare le modalità o i tempi con cui un attacco informatico potrebbe presentarsi verso un determinato obiettivo, azienda, organizzazione o individuo che sia.

Le aziende, quindi, possono trarre un indiscutibile vantaggio competitivo effettuando attività di intelligence sul *Dark Web* e riuscendo ad insinuarsi digitalmente nelle varie community del mercato nero digitale. Ciò permette di conoscere le intenzioni dei nemici cyber e poter anticipare le azioni di difesa agli attacchi messi in atto da questi avversari, rafforzando in modo mirato quegli ambiti dei sistemi informatici che risultano più vulnerabili.

Per un utilizzo più mirato dell'intelligence sul *Dark Web* esistono quindi strumenti e piattaforme di supporto alla *Cyber Threat Intelligence*, che possono avvisare quando siano rilevate nuove informazioni di precipuo interesse dell'azienda. Nonostante l'intelligence sul *Dark Web* abbia un grandissimo potenziale in termini di tipologia e qualità delle informazioni, è necessario tenere presente che esistono difficoltà ad essa correlate.

Le informazioni raccolte che siano insignificanti e non rilevanti ai fini propri, fanno sicuramente sprecare il tempo e le risorse dedicate loro dalle aziende. Per questo motivo la maggiore difficoltà dell'intelligence sul *Dark Web* riguarda principalmente l'essere in grado di filtrare e controllare l'enorme quantità di conversazioni delle comunità sotterranee.

È quindi essenziale saper discernere e riconoscere le community che gravitano negli ambiti di interesse dell'azienda stessa, scremando tra quelle non utili alle proprie ricerche. Inoltre, grande difficoltà presenta l'essere accettati in una community, dimostrando capacità e motivazioni, vincendo la diffidenza dei suoi componenti.

Ultima difficoltà, ma non meno importante, è quella di saper destreggiarsi nel gergo specifico parlato in certi gruppi ristretti, che può essere ad esempio, una lingua o un dialetto locale della zona geografica dove un mercato nero o un traffico illecito si svolge. La non conoscenza di un tipo di linguaggio specifico può rendere complessa sia la comprensione delle informazioni e quello a cui si riferiscono, sia delle stesse minacce.

[13] Vedi: https://blog.cerbeyra.com/threat-intelligence/come-fare-intelligence-dark-web-per-difendere-azienda/

5.2 OSINT E PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

Cosa sia una *Infrastruttura Critica* è precisato dalla Direttiva Europea 2008/114/CE: essa è **"**un elemento, un sistema o parte di questo […] che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo […] a causa dell'impossibilità di mantenere tali funzioni**"**.[14]

La Direttiva viene attuata e regolata in Italia attraverso il D. Lgs n°61 dell'11 Aprile 2011 il quale definisce le metodiche e gli strumenti per identificare le *Infrastrutture Critiche* di interesse nazionale.

Identificare quali siano i rischi e i danni potenziali di una minaccia su di un determinato settore è fondamentale nella definizione e nella gestione delle *Infrastrutture Critiche.*

Possiamo per sommi capi circoscrivere la tipologia delle minacce possibili come segue:

• minacce di natura antropica, sia volontarie come potrebbe essere un attacco terroristico, un attentato, sia minacce accidentali, come un errore umano;

oppure

• minacce di tipo naturale – prevedibili o imprevedibili – che facilmente in Italia si identificano in particolare nel rischio idrogeologico, alluvioni, terremoti, eruzioni vulcaniche ed incendi.

A definire il livello di criticità di una data infrastruttura è l'impatto stesso che tali minacce, naturali od antropiche che siano, possono avere sul settore individuato come essenziale per la nazione.

Il criterio per determinare quali siano queste le *Infrastrutture Critiche* è definito dall' Unione Europea è la valutazione dell'impatto "che una crisi potrebbe avere in termini di vittime, di effetti economici (intesi come perdite e deterioramento di prodotti e servizi) e di effetti pubblici, ossia l'impatto sulla fiducia dei cittadini, il turbamento della vita quotidiana e la salute pubblica".[15]

L'utilizzo di attacchi dello *spazio cibernetico* sta in questi ultimi anni acquistando sempre più rilevanza tra i rischi di natura antropica. La minaccia *cyber* si sta infatti evolvendo e ciò permette di individuare nuovi settori critici e aumentare la percezione della complessità e l'importanza dell'interconnessione tra di essi.

La tecnologia informatica è sempre più essenziale e indispensabile al funzionamento di tutte le infrastrutture fondamentali, le quali sono ovviamente informatizzate ed utilizzano servizi

[14] Vedi: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32008L0114
[15] Vedi: https://www.ictsecuritymagazine.com/articoli/infrastrutture-critiche/

on line. Anche i settori strategici di una nazione ne sono coinvolti: dalla stessa infrastruttura di telecomunicazioni al settore della pubblica amministrazione, dei trasporti, dell'energia, della salute pubblica, della finanza e del credito, così come al settore della difesa e della sicurezza pubblica.

L' impatto di un attacco cibernetico che porti all'interruzione ed al deterioramento di processi essenziali potrebbe risultare notevole in termini di vittime, di danni economici e di effetti sulla vita pubblica.

Per comprendere con chiarezza il rischio intrinseco dello spazio cibernetico si possono prendere come esempio i non rari eventi di incidenti, molto spesso ad opera di *cyber* criminali, che colpiscono alcuni sistemi informatici di controllo e di supervisione ed acquisizione di dati, demandati al monitoraggio e al controllo di sistemi fisici dei processi industriali come il sistema SCADA - *Supervisory Control and Data Acquisition* (per citarne uno: il sistema di produzione e logistico di Amazon è gestito da piattaforme SCADA).

Diventa quindi quanto mai importante per le *Infrastrutture Critiche* che venga attuata una programmazione di valutazione ed una gestione dei rischi investendo risorse nella loro messa in sicurezza e nel miglioramento della resilienza e robustezza dei sistemi di protezione.

Data, infatti, la potenziale gravità dell'impatto, il costo di una mancata sicurezza potrebbe risultare più alto dell'investimento in tal senso; elementi vitali di un Paese e delle sue funzioni potrebbero essere colpiti con un rischio altissimo. Il danno che potrebbe scaturire da gravi attacchi *cyber* alle *Infrastrutture Critiche* e dalla loro scarsa sicurezza potrebbe essere di potenziale perdita non solo economica o fisica, ma anche avere altre gravi ripercussioni come la mancanza di fiducia nelle istituzioni, il turbamento dell'ordine sociale e gli eventuali effetti sulla reputazione delle aziende coinvolte.

L'introduzione e l'osservazione di *best practices* e di standard di sicurezza riconosciuti a livello internazionale diviene fondamentale. Inoltre è sempre più essenziale definire politiche per la gestione ed ottimizzazione della sicurezza delle *Infrastrutture Critiche* prendendo anche in considerazione l'interdipendenza del settore pubblico e privato in tale ambito.

"Nel campo della sicurezza delle *Infrastrutture Critiche* attori pubblici e privati si trovano a cooperare proprio in ragione dell'interconnessione delle infrastrutture stesse, che diventano così realtà più complesse e reciprocamente dipendenti, e che necessitano di coordinamento per affrontare le vulnerabilità che in tale sistema reticolare potrebbero portare ad un pericoloso effetto domino"[16] .

La gestione della sicurezza nello spazio cibernetico è quindi necessariamente demandata sia alle istituzioni pubbliche, sia alle società private. Un esempio per tutti attraverso cui si capisce bene che la cooperazione fra pubblico e privato è fondamentale: il fenomeno del

[16] Vedi sempre: https://www.ictsecuritymagazine.com/articoli/infrastrutture-critiche/

terrorismo, che difficilmente sarà sconfitto totalmente nel medio e lungo periodo, è inserito negli elenchi delle minacce prioritarie per le *Infrastrutture Critiche*.

Tra le minacce prioritarie del presente e del prossimo futuro e che vedono coinvolti tutti gli stati, vanno collocati prioritariamente il *cyber crime*, il *cyber espionage* ed il terrorismo. Per poter arginare e prevenire tali pericoli la centralità dell'OSINT rimane infatti decisiva: l'uso di tecnologie di ricerca e di analisi semantica in grado di setacciare ed estrapolare le informazioni necessarie dalle innumerevoli "fonti aperte" permette di facilitare il lavoro degli analisti nelle loro ricerche e di monitorare così i rischi correlati alle *Infrastrutture Critiche*.

Nota che, da ultimo, nei primi mesi del 2023 molte infrastrutture italiane hanno subìto *cyber* aggressioni – DdoS, *Distribuited Denial of Service* – : è il caso dell'ATAC, l'azienda municipalizzata romana dei trasporti, i ministeri dei Trasporti, della Difesa e degli Esteri, l'aeroporto di Bologna, i siti del Governo e della Camera dei Deputati, la Corte Costituzionale, tutti episodi rivendicati dal gruppo di conclamata fede filorussa denominato NoName057(16), già protagonista di altre azioni simili in Italia.

In un recente messaggio di rivendicazione veicolato attraverso il canale Telegram (Foto 1 e 2), il gruppo ha dichiarato: "*20 soldati ucraini sono stati addestrati per usare Samp-T in Italia. Il primo ministro italiano Giorgia Meloni ha detto che le condizioni per l'avvio di un processo negoziale in Ucraina non sono ancora mature, ma i nostri missili DDoSS per il sistema internet russofobo italiano lo sono. Frattasi stiamo arrivando*". Tale minaccia si riferisce al prefetto Bruno Frattasi, capo dell'ACN – Agenzia per la Cybersicurezza Nazionale.

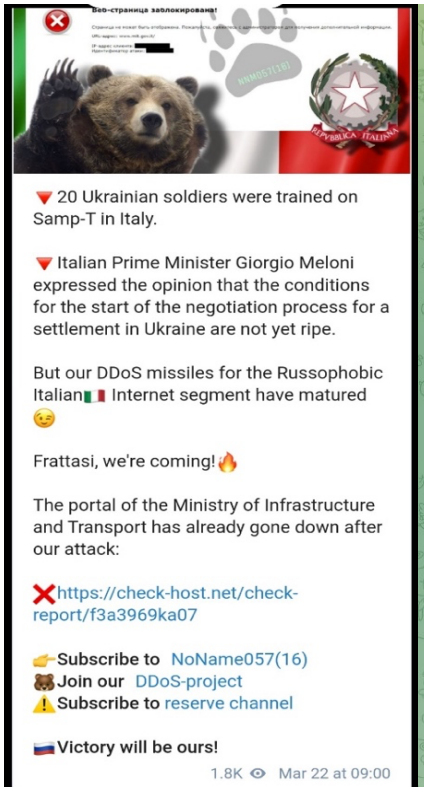


Foto 1

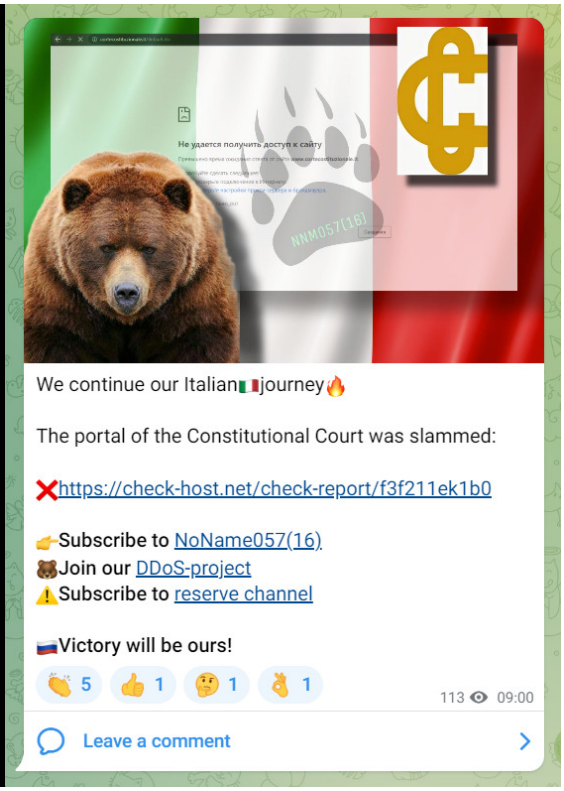


Foto 2

Fonte: Telegram

5.3 OSINT E ARTIFICIAL INTELLIGENCE

In termini tecnici, l'*Intelligenza Artificiale* è quella branca dell'informatica in cui la programmazione e progettazione di sistemi sia hardware che software consentono di fornire alle macchine determinate caratteristiche tipicamente umane quali "le percezioni visive, spazio-temporali e decisionali"[17].

Non si parla quindi di una intelligenza che abbia solo capacità di calcolo e di elaborazione di dati. L'Intelligenza Artificiale ha soprattutto tutte le diverse forme di intelligenza, come quella spaziale, l'intelligenza sociale, l'intelligenza introspettiva e l'intelligenza cinestetica, cioè quella capacità di usare il proprio corpo in molteplici modi molto articolati e con diverse abilità, per fini espressivi oltre che concreti. "La cinestesia fornisce consapevolezza dei propri muscoli e dei loro movimenti."[18]

Si può realizzare, quindi, un sistema intelligente cercando di ricreare particolari comportamenti derivanti da differenti forme di intelligenza che, anche se sono riconosciute come umane, vengono resi riproducibili da alcune macchine[19].

Parlando di *Intelligenza Artificiale*, l'immaginario collettivo si figura un mondo del futuro forse lontano, popolato da macchine intelligenti ed autonome e di robot.

Guardandoci attorno però ci si rende conto di quanto l'*Intelligenza Artificiale* e il suo utilizzo siano sempre di più attuali e vengano utilizzati in moltissimi settori della vita quotidiana, seppur in una maniera differente e meno intrusiva di quanto la fantascienza ci abbia abituati a pensare.

L'uso di sistemi intelligenti non è infatti destinato a *élite* di soli esperti informatici. Si deve invece pensare che l'*Intelligenza Artificiale* viene ampiamente utilizzata anche nel quotidiano. Utilizziamo tutti i giorni strumenti di riconoscimento vocale, dagli smartphone ai sistemi di sicurezza, alla domotica: tutti questi si fondano su algoritmi tipici dell'*Intelligenza Artificiale*, in particolare quelli relativi all'apprendimento automatico.

Rilevanti studi sull'apprendimento automatico e sull'*Intelligenza Artificiale*, hanno ad esempio sviluppato sistemi che vengono utilizzati nel settore automobilistico. I veicoli a guida autonoma, senza pilota, in grado di muoversi nel traffico sono ormai una realtà, che ha già superato la fase di sperimentazione, anche se il loro utilizzo è ancora limitato a settori limitati. Ormai molto comuni invece, installate nelle automobili più moderne a guida semi-autonoma, sono quelle particolari applicazioni che permettono di utilizzare i sistemi di cambi di velocità.

Ci sono molti settori di uso quotidiano in cui l'*Intelligenza Artificiale* viene utilizzata regolarmente, ad esempio come quello medico: l'*Intelligenza Artificiale* viene applicata

[17] Vedi: https://www.intelligenzaartificiale.it
[18] Vedi: https://www.treccani.it/enciclopedia/cinestesia_%28Dizionario-di-Medicina%29/
[19] Vedi: https://www.psycheatwork.com/intelligenza-artificiale-cose-e-a-cosa-serve/

nell'uso delle reti neurali, soprattutto nelle analisi del battito cardiaco, nel rilevamento della pressione arteriosa, nelle diagnosi di alcune forme tumorali e nella realizzazione di robot di accompagnamento.

Gli smartphone e i dispositivi mobili più recenti sono realizzati usando piattaforme basate su sistemi di *Intelligenza Artificiale*, che permettono una vera e propria interazione tra il telefono e il suo proprietario, e tale interazione è fondamentale per diverse funzioni. Alcuni cellulari di nuova generazione, ad esempio, sono forniti di sensori in grado di rendersi conto se il proprietario del telefono si stia muovendo a piedi o in auto, nel qual caso il telefono potrà impostarsi automaticamente sulla modalità adeguata a garantire la massima sicurezza nella guida. Alcuni telefoni avvertendo che ci si sta muovendo al buio sono in grado di accendere automaticamente la torcia incorporata. Tutte queste funzioni sono volte ad implementare comodità e sicurezza di quanti ne fanno uso[20].

È interessante definire anche quando l'*Intelligenza Artificiale*, in relazione all'OSINT, aiuta a sviluppare delle attività predittive come, ad esempio, il contrasto alle attività di frode. Infatti si stima che ogni anno nel mondo svariati miliardi di dollari vengono bruciati a causa di frodi cibernetiche, ma grazie all'intelligenza artificiale, oggi è possibile rendere più rapidi ed automatizzare i processi di *business intelligence*, fondamentali per supportare gli utenti che compiano online operazioni economiche e finanziarie, così che possano prendere decisioni in sicurezza, minimizzando i rischi.

Inoltre, lo sviluppo dei sistemi di *Intelligenza Artificiale* sta avendo un'ampia diffusione nel mondo investigativo. Ultimamente, ad esempio, è in fase di elaborazione un innovativo software di Intelligenza Artificiale di polizia predittiva: denominato *Giove*, esso è un nuovo progetto del Dipartimento di Pubblica Sicurezza del Ministero dell'Interno e della Polizia di Stato, volto a prevedere luoghi e tempi in cui sia possibile avvengano i reati[21].

[20] Vedi ancora: https://www.intelligenzaartificiale.it
[21] Vedi: https://www.pegasoftsrl.it/polizia-predittiva-il-software-giove-prevedra-reati-e-omicidi/

6. L'OSINT COME STRUMENTO DI PREVENZIONE NELLA SOCIETÀ MODERNA

6.1 WEB, DEEP WEB E DARK WEB. ESEMPI PRATICI

Il *Deep Web*, in italiano "web profondo o web sommerso" è l'insieme dei dati e delle informazioni presenti sul web che non sono indicizzate dagli ordinari motori di ricerca. L'attività degli utilizzatori del web sommerso è, quindi, protetta dall'anonimato e non è possibile che sia identificata né tracciata.

Secondo il ricercatore Ivan Antonozzi, per comprendere il significato di *Deep Web* (o web sommerso) è possibile ricorrere alla metafora dell'iceberg. Il grande insieme delle risorse informative presenti sul *Web* viene rappresentata come un enorme iceberg, la cui punta emersa rappresenta il *surface web*. Questa è solo una piccola parte delle risorse presenti su Internet ed è composta dall'insieme di tutte le informazioni e i dati indicizzati dai comuni motori di ricerca (come per esempio *Google*, *Bing, Yahoo*, ecc.)[22].

Come in un vero iceberg, la parte più grande è quella sommersa sotto il livello del mare. Essa è enorme e si compone da due parti: una "profonda" chiamata *Deep Web* ed una "oscura", il *Dark Web*.

Il *Deep Web*, è quella parte sommersa dell'iceberg che costituisce Internet che non viene indicizzata dai motori di ricerca, per cui non è possibile trovarla tramite i normali motori di ricerca come Google.

Determinare quale sia realmente l'effettiva dimensione del *Deep Web* è molto difficile. Recenti studi indicano che le risorse del web sommerso rappresentano il 96% dell'intero *world wide web*, per un volume 500 volte superiore a quello del *surface web*.

L'estensione del *Deep Web* è confermata anche dall'enorme mole di dati di testo e multimediali contenuti all'interno dei database e della struttura interna di pagine visitabili.

Non solo, in questo immenso contenitore dei contenuti non indicizzati dai motori di ricerca finiscono i messaggi diretti, le email, le transazioni bancarie ed incredibilmente quasi tutto ciò che del web usiamo più spesso. Ci possiamo trovare le pagine Internet il cui accesso è permesso autenticandosi o farcendo il login, come, per esempio, le pagine appena pubblicate, i siti appena nati, i siti privati di aziende ed organizzazioni, i forum universitari, indirizzari di vario genere, i contenuti dinamici.

Si può accedere a molti dei contenuti del *Deep Web*, se l'indirizzo è conosciuto, anche attraverso un ordinario browser.[23]

[22] Vedi: https://blog.osservatori.net/it_it/deep-web-dark-web-navigare
[23] Vedi: https://www.cybersecurity360.it/cultura-cyber/cose-il-deep-web-e-il-dark-web-cosa-si-trova-e-come-si-accede-tutte-le-istruzioni/

Ad esempio, è possibile trovare siti che creano cataloghi di database e pagine web non indicizzate da Google; tra i principali troviamo: *The WWW Virtual Library*, S*urfwax* e *Stumpedia*.

Il materiale documentale presente sul *Deep Web* può essere suddiviso nelle seguenti categorie:

- **"**Contenuti dinamici: si tratta di pagine web il cui contenuto viene generato sul momento dal server;
- Pagine non collegate a nessun'altra pagina web;
- Pagine ad accesso ristretto: sono siti che richiedono una registrazione o che limitano l'accesso alle loro pagine impedendo che i motori di ricerca possano accedervi;
- Script: pagine che possono essere raggiunte solo attraverso link realizzati in *JavaScript* o in *Flash*;
- Contenuti non di testo: rientrano in questa categoria i file multimediali, gli archivi *Usenet* e i documenti scritti in linguaggio non HTML, in particolare quelli non collegati a tag testuali;
- Contenuti banditi dai comuni motori di ricerca perché illegali: fanno parte di questo gruppo i siti pedo-pornografici o *snuff*, i siti di commercio e produzione illegale di droghe e armi, i siti sottoposti a censure governative, i siti di *warez* e *malware*;
- Software: come ad esempio *Tor*, che consente agli utenti di accedere anonimamente a siti che utilizzano il suffisso *.onion*, e I2P, un software libero e open source usato per la realizzazione di una rete anonima che consente lo scambio di dati coperti da diversi livelli di crittografia.**"**[24]

Il *Deep Web* appare quindi come una sorta di "mondo parallelo" rispetto al normale internet del *surface web* che conosciamo bene, le cui dimensioni sono decisamente difficili da quantificare; infatti, se è difficile quantificare la dimensione dell'internet in chiaro, quantificare la sua parte "profonda" e quella "oscura" è quasi impossibile.

Una altra parte dell'universo sommerso internet è infatti il *Dark Web,* che si caratterizza anche in questo caso per essere non indicizzato dai principali motori di ricerca.

Sul *Dark Web* troviamo solo pagine con un dominio *.onion*; ai server che le ospitano si può accedere solo attraverso un protocollo particolare chiamato *Tor*. Esso fu sviluppato in origine dal Dipartimento della Difesa Statunitense per consentire comunicazioni anonime e sicure, ma dal 2004 divenne di dominio pubblico e così fu usato da milioni di utenti per per proteggere la loro privacy. Contemporaneamente, però, con il suo supporto è cresciuto anche il mercato nero ed illegale.

[24] Vedi: https://focus.namirial.it/dark-web-e-deep-web/

Diversi sono gli utilizzi delle cosiddette “reti oscure”:

- Divulgare notizie riservate;
- Vendere prodotti e materiali illegali di ogni specie;
- Effettuare crimini informatici (ad esempio: *hacking* o frodi)
- Condividere file illegali (vietati, contraffatti, video pirata, ecc.);
- Eludere la censura di internet e dei sistemi di filtraggio dei contenuti pubblicati o superare i *firewall*.”[25]

Il *Black Market* costituisce il nucleo centrale del *Dark Web*. Questo si presenta come un mercato dove si può trovare qualsiasi prodotto illegale; armi, carte di credito clonate, droga, medicinali, documenti falsi, *malaware* e dati e segreti aziendali trafugati e tutto ciò che è inimmaginabile possa essere commercializzato normalmente.

Tra le principali minacce derivanti dalle vendite sui mercati illegali del *Dark web* troviamo gli strumenti stessi utilizzati dai criminali del web per realizzare attacchi informatici:

- *Keylogger*
- *Botnet*
- *Ransomware*
- *Phishing*

L’accesso al *Dark Web* è possibile solo tramite specifici software che consentono agli utenti la navigazione anonima, sviluppati per proteggere la propria identità, nascondendo la cronologia delle pagine visitate. Quindi risulta che i siti con il dominio *.onion* non risultano raggiungibili se digitati su un normale browser, come *Google Chrome*, *Safari* o *Firefox*.

Il software più diffuso che consente l’accesso al *Dark Web* è quindi *Tor*, che è un vero e proprio normale browser, scaricabile gratuitamente ed utilizzabile per navigare sui normali siti, tutelando la propria riservatezza.

A tutt’oggi i download di *Tor* sono milioni e tra le persone che lo usano ci sono, ad esempio, molti militanti di gruppi vari, come anarchici ecc., o chi vive in paesi sotto regimi autoritari, che così riescono ad eludere filtri e censura. Come sappiamo infatti, molti regimi autoritari, come accadde con la Turchia e l’Egitto, in passato bloccarono a più riprese *Youtube* e *Twitter*, ma l’utilizzo di *Tor* rese comunque possibile accedere ad entrambi.

Il *Dark Web* è come un enorme bidone in cui tutto quello che è illegale è acquistabile. Il maggior numero delle pagine lì caricate è gestito, ad esempio, da venditori/compratori di criptovalute. Vi si trovano

[25] Vedi sempre: https://focus.namirial.it/dark-web-e-deep-web/

anche siti che somigliano a dei forum e funzionano come le piattaforme di vendita on-line più conosciute tipo *eBay*, ma sono di compra-vendita di prodotti e servizi illegali.

Nel 2016 due ricercatrici del settore Clare Gollnick e Emily Wilson, allo scopo di comprendere quale sia la proporzione tra lecito e illecito, hanno selezionato a caso 400 url *.onion* e poi le hanno esaminate scindendole in base al loro scopo e ai loro contenuti. È emerso così che pressappoco la metà di questi siti era perfettamente legale. Della restante metà delle url *.onion* che presentavano materiale illegale, "il 45 per cento aveva a che fare con il commercio di droga, l'11,9 per cento con quello di medicinali, il 4,6 per cento erano siti di frodi e un altro 4,6 per cento concerneva operazioni di *hacking*."[26]

Uno dei più popolari siti di e-commerce illegale dopo *Silk Road*, *Alpha Bay* e *Hansa Market*, chiamato *Berlusconi Market* vendeva Armi, droga, psicofarmaci, carte di credito clonate e molto altro. Tale sito, il cui nome non aveva alcuna relazione con il politico italiano, fu chiuso nel novembre 2019. Questi siti, seppur tutti chiusi dalle forze dell'ordine, sono sempre velocemente rimpiazzati da siti simili.

Nel 2016 L'*Economist* pubblicò che fra dicembre 2013 e luglio 2015 ci furono circa 360mila vendite sui mercati del *Dark Web*. Inoltre è stato stimato che sui siti *Agora*, *Evolution* e *Silk Road 2*, si sarebbero effettuate di transazioni illegali per un valore totale di circa 50 milioni di dollari.

Uno studio specifico ha analizzato il volume del business realizzato da *Silk Road,* mercato specializzato nella vendita di droghe online, chiuso nel 2014 dall'FBI, che in otto mesi di indagine calcolò che *Silk Road* ebbe un fatturato mensile di circa 1,2 milioni di dollari fruttando per i suoi gestori commissioni per 92mila dollari al mese.

Inoltre, uno dei pericoli maggiori per l'utente che accede al *Dark Web* è connesso alla presenza di *malware*, anche se in molti casi essi vengono riconosciuti dai moderni antivirus.

Maggiore potrebbe essere il pericolo riguardante l'incorrere nel il monitoraggio delle forze dell'ordine, i quali potrebbero scambiare una semplice visita nei siti del *Dark Web* per qualcosa di differente a scopo criminale.

In aggiunta a tutte le minacce esposte, si deve considerare che molti dei servizi e dei prodotti in vendita nel *Dark Web* sono delle vere e proprie truffe.

Tra le pieghe che formano questi due strati profondi di Internet si nascondono anche i pericoli collegati al *Cyber Risk* che, secondo la definizione data dall'*Institute of Risk Management*, è "un qualsiasi rischio di perdita finanziaria, interruzione o danno alla

[26] Vedi sempre: https://www.cybersecurity360.it/cultura-cyber/cose-il-deep-web-e-il-dark-web-cosa-si-trova-e-come-si-accede-tutte-le-istruzioni/

reputazione derivante da eventi accidentali (ad esempio lo spegnimento del server) o dolosi (ad esempio il furto dei dati sensibili) ai danni del sistema informatico"[27].

Il Rapporto *Clusit 2022* sulla sicurezza ICT in Italia e nel mondo, redatto dall'*Associazione Italiana per la Sicurezza Informatica*, ha posto sotto osservazione gli eventi di *cyber-crime* che si sono verificati nel mondo nel 2021 e li ha confrontati con i dati raccolti nei quattro anni precedenti.

Dallo studio si può osservare come gli attacchi informatici rappresentino una minaccia per qualsiasi settore: solo nel periodo del primo anno della pandemia del COVID 19 sono stati tracciati 1.871 attacchi gravi di dominio pubblico, con un'influenza profonda in ogni settore della società, dalla politica, all'economia, dal settore medico alla geopolitica. Nel 2020 gli attacchi cyber sono aumentati del 12% rispetto all'anno precedente a livello globale, si evidenzia anche come negli ultimi quattro anni il trend di crescita si è mantenuto costante, facendo registrare un aumento degli attacchi gravi di più del 60% rispetto al 2017. [28]

Di particolare interesse è il fenomeno degli attacchi *Ransomware*, un tipo di malware in grado di limitare l'accesso del dispositivo infettato. Indagini specifiche hanno rilevato che sin dal 2019 i cyber criminali utilizzavano il *Dark Web* per sfruttare la cosiddetta tecnica della double extortion (doppia estorsione), in cui le aziende target subiscono "due forme simultanee di estorsione: l'estorsione che avviene con il blocco dei file che vengono crittografati e l'estorsione mediante la minaccia di pubblicazione di dati sensibili dell'organizzazione o dell'azienda *hackerati*[29].

All'interno delle reti del *Dark Web* si stanno sviluppando veri e propri marketplace creati per favorire le organizzazioni di cybercriminali: esse sono piattaforme dotate di diverse funzionalità, quali i sistemi di normale supporto clienti, di fatturazione, ecc. Si possono comprare *codici malevoli*, ingaggiare un *hacker* o addirittura sviluppare *codici malevoli* su vere e proprie piattaforme online (le *malware-as-a-service platform*).

Tra le più utilizzate troviamo *RaaSberry*, una piattaforma di *ransomware-as-a-service* che permette di:

- "creare e personalizzare un attacco ransomware;
- visualizzare informazioni relative al numero di utenti infettati:
- monitorare l'ammontare di denaro accumulato grazie al pagamento dei riscatti." [30]

Fornendo una piattaforma *as-a-service* un vero e proprio servizio con pagamento al consumo, i gestori della piattaforma stessa tengono per sé una parte dei guadagni relativi ai singoli utenti.

[27] Vedi: https://www.theirm.org
[28] Vedi: https://clusit.it/wp-content/uploads/area_stampa/2022/Rapporto_Clusit_edizione_ottobre_2022.pdf
[29] Vedi: https://www.telsy.com/it/attacchi-a-doppia-e-tripla-estorsione/
[30] Vedi sempre: https://blog.osservatori.net/it_it/deep-web-dark-web-navigare

Sono inoltre stati rilevati all'interno del *Dark Web* siti con veri e propri annunci di lavoro per attività illegali, come il furto di carte di credito o la vendita di software per attacchi hacker.

Una indagine internazionale di qualche anno addietro, che coinvolse anche l'Italia, fu condotta per sconfiggere una organizzazione informatica criminale che agiva sul *Dark Web*, acquisendo i dati di codici bancari su piattaforme di scambio, come *Liberty Reserve*.

L'indagine fece emergere un fiorente commercio di carte online, codici di accesso, ecc. Tale commercio permise agli hacker di accumulare più di 530 milioni di dollari di profitti illegali.[31]

Una delle storie più emblematiche del *Dark Web*, che rappresenta sicuramente un "case study", è quella della piattaforma *Silk Road*, la Via della seta: un sito di e-commerce illegale notissimo a cui si accedeva solo attraverso *Tor*. Una specie di supermercato in cui era possibile comprare di tutto, droga, armi, documenti falsi, farmaci, narcotici e che esibiva la merce agevolmente suddivisa in categorie.

Silk Road fu fondata nel 2011 ed è stata poi chiusa dall'FBI nel 2013. Il suo creatore, Ross Ulbricht, nel 2015 è stato condannato all'ergastolo. Egli agiva dietro lo pseudonimo di "Dread Pirate Roberts", usando il nome del personaggio immaginario di un romanzo.[32]

Egli viene descritto come sensibile, ex scout laureato in ingegneria. Nell'ottobre del 2013, Ulbricht fu "letteralmente colto con le mani sulla tastiera, mentre amministrava Silk Road".[33]

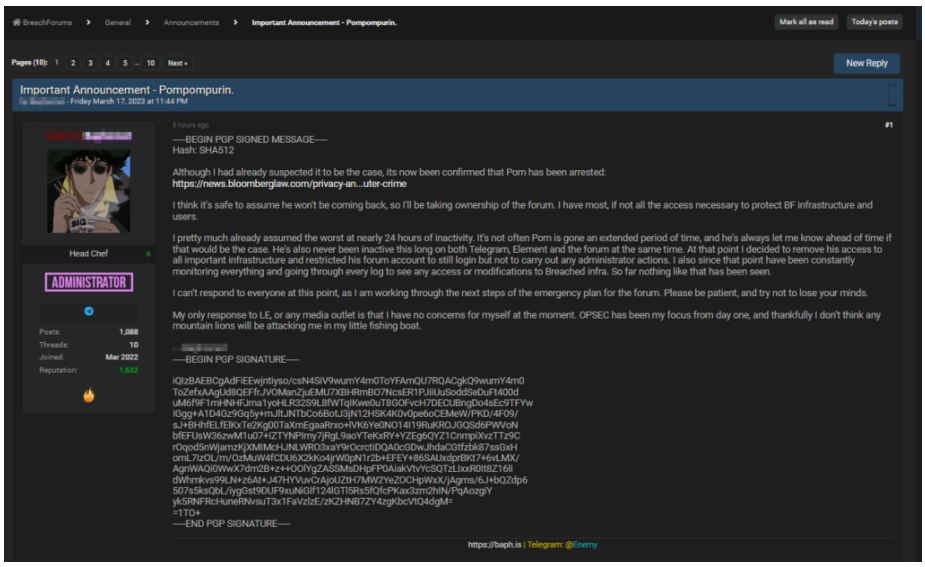
"L'arresto di Ulbricht e il sequestro di milioni di dollari in Bitcoin dovrebbero inviare un chiaro messaggio a tutti coloro che vogliono aprire una impresa illegale online", dichiarò il procuratore Preet Bahrara in una nota diffusa da un comunicato stampa ufficiale[34].

Malgrado il *Dark Web* sia sempre più vigilato dalle Autorità preposte, rimane terreno di criminali informatici sempre più agguerriti.

Per citare solo uno degli ultimi casi, nel marzo del 2023 agenti del FBI – *Federal Bureau of Investigation* – statunitense hanno proceduto all'arresto di Connor Brian Fitzpatrick, meglio noto come Pompompurin, il fondatore e amministratore di *Breach Forum*, uno degli spazi principali che si occupa di *hacking*, utilizzato come mercato nero per la compravendita del materiale sottratto attraverso la violazione di sistemi aziendali. L'accusa è di cospirazione e tentativo di frode.

A seguito di ciò è stato diffuso il seguente messaggio (Foto 3):

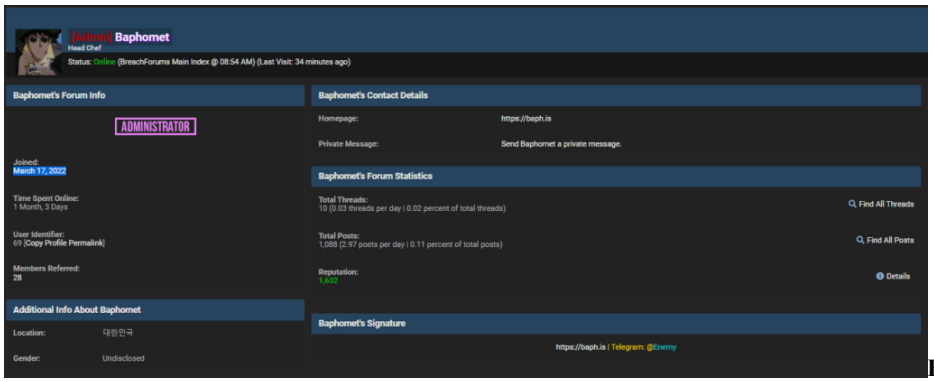
[31] Vedi: https://www.zerounoweb.it/techtarget/searchsecurity/dark-web-cose-e-come-evitarne-i-trabocchetti/
[32] Vedi: https://cyberdude.it/2020/07/27/silk-road-storia-famoso-mercato-della-droga/
[33] Vedi: https://www.repubblica.it/tecnologia/2015/02/05/news/silk_road_ross_ulbricht_il_pirata-106623740/
[34] Vedi: https://www.cybersecurity360.it/cultura-cyber/cose-il-deep-web-e-il-dark-web-cosa-si-trova-e-come-si-accede-tutte-le-istruzioni/



Fonte: Telegram

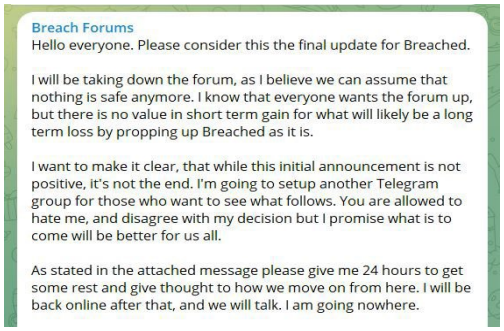
Foto 3

Il sito è stato gestito temporaneamente da un altro responsabile, Baphomet (Foto 4), il quale, però, dopo alcuni giorni, ha dovuto decretare la chiusura definitiva delle attività (Foto 5) che sono poi proseguite, prima attraverso Telegram e, poi, sotto altra forma.



Fonte: Telegram

Foto 4



Fonte: Telegram

Foto 5

Nel caso descritto, quanto verificatosi ha reso di fatto più difficoltosa l'attività degli investigatori, poiché, pur non variando la metodologia di scambio, sono stati creati nuovi spazi, funzionanti per brevi periodi e poi sostituiti da altri ambiti di confronto, in modo da eludere se non ritardare i controlli delle autorità investigative internazionali e nazionali.

6.2 OSINT, SOCMINT E DIGITAL HUMINT. LE TECNICHE DA VICINO

Ambito di indagine di recente studio, la SOCMINT, ossia la *Social Media Intelligence* (già trattata nei precedenti capitoli), pur non avendo ancora una veste di rilievo nello spettro delle discipline dei processi di intelligence, ha già trovato una collocazione importante dal punto di vista operativo, utilizzando il monitoraggio delle comunicazioni e dei materiali scambiati sui social network a fini sia di prevenzione sia di investigazione nell'ambito della lotta al terrorismo[35].

La verifica approfondita delle reti di social network fornisce:

- un tracciamento delle opinioni, dei gusti, degli orientamenti e dei comportamenti di una persona o di gruppi di persone prese ad esame nel tempo;
- l'aggiornamento in tempo reale circa gli interessi, spostamenti, vita lavorativa e vita privata delle persone stesse.

Secondo le indagini SOCMINT bisogna, però, anche tenere conto:

- della eventuale violazione della privacy dei singoli individui e delle normative ad essa collegate;
- dell'affidabilità delle informazioni pubblicate, non sempre precise o attendibili;
- della legittimità delle immagini, che potrebbero risultare manipolate[36].

La *Digital Humint* costituisce, invece, un approccio metodologico misto che basandosi sulla unione delle specifiche competenze *Human* e *Social*, quindi riguardanti l'ambito reale o virtuale, processa le informazioni provenienti dalla *Humint* e dalla *Socmint* per contribuire alla stesura di un report di *Intelligence* integrato destinato al consumo dell'utilizzatore finale.

Gli analisti della *Digital Humint* devono applicare un'attenta analisi dei gruppi sociali che popolano la piattaforma interessata, anche in considerazione della complessità che gli stessi presentano, per non ricorrere all'errore di attribuire a un individuo pensieri, valori e opinioni che sono, invece, espressione dell'identità di gruppo: la dimensione sociale legata a questi media è proprio il loro aspetto fondamentale, quindi la creazione di nuove relazioni, di stringere legami ed entrare a far parte di una comunità.

Anche se la definizione di 'comunità' in contesto social non ha una definizione pienamente condivisa, partendo dal concetto che per essere definita tale bisognerebbe che i suoi componenti fossero consapevoli di costituirne, o debbano almeno condividere gli stessi interessi.

[35] Vedi: https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/socmint-un-nuovo-spazio-per-la-raccolta-di-informazioni-rilevanti.html
[36] Vedi: https://www.resquon.com/2021/09/01/indagini-social-network/

Dunque diviene importantissimo per gli analisti della *Digital Humint*, capire a fondo il fenomeno della creazione delle comunità online, tenendo conto che presupposto comunque dato per stabilito è il fatto che, per esistere una comunità, coloro che la costituiscono devono interagire tra di loro attraverso un codice condiviso, incluso un sapere digitale comune. Infatti, conoscere a fondo i meccanismi che regolano la comunità stessa permette di capire meglio gli individui che la compongono. Arrivare ad una comprensione viscerale permetterà all'analista di raccogliere informazioni che non potrebbero essere trovate altrove. Diviene quindi fondamentale riuscire a stabilire una possibile corrispondenza di tale appartenenza alla comunità anche nel mondo reale. Ciò per riuscire a ricostruire in maniera esatta la rete di contatti di un individuo ed anche per comprendere quale sia il grado d'influenza che un tale singolo può avere sui componenti della comunità.

L'analista della *Digital Humint*, potrebbe trovarsi si fronte ad un gruppo destrutturato, a causa di temporanee situazioni o, al contrario, rilevare la presenza di comunità fortemente coese e con un alto grado di identificazione dei propri membri.

Un esempio su tutti sono gli attacchi terroristici di Parigi nel 2015 e di Bruxelles nel 2016. Le indagini successive, applicando tecniche di *Digital Humint*, riscontrarono la centralità della dimensione parentale e amicale nella costruzione dei legami che avevano caratterizzato la pianificazione e la realizzazione degli attacchi.

Alcuni degli aspetti più interessanti che emergono dall'analisi delle interazioni intercorse tra i diversi individui sono la profonda coesione delle persone e l'identificazione, agevolate dalla propaganda circolante prevalentemente online. Ne deriva quindi che un importante risultato di questa tipologia di analisi è l'attenzione specifica al motivo per cui un componente di una rete è spinto a interagire con un altro, e diventa fondamentale per capire la tipologia di relazione che li accumuna e li caratterizza.

"Sebbene diverse possano essere le motivazioni che spingono un individuo a intessere rapporti con un altro (amplificare il messaggio attraverso una sua condivisione, dimostrare la propria presenza o il proprio consenso, aumentando così la propria visibilità, oppure dimostrare amicizia e/o fedeltà nei confronti di qualcuno ecc.), la potenzialità ulteriore connessa all'applicazione della *Digital Humint* risiede proprio nel fornirne la contestualizzazione, necessaria per darne ragione in termini di valore aggiunto all'analisi complessiva."[37]

[37] Vedi: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/06/Burato_SicTerSoc_book-7.pdf

6.3 INTELLIGENCE ECONOMICA: L'OSINT A SOSTEGNO DELLA COMPETIZIONE INDUSTRIALE: CASI DI STUDIO

In un periodo storico caratterizzato da un'elevata competizione economica globale, la raccolta delle informazioni e quindi l'*intelligence economica* è intesa come risorsa sempre più strategica. Lo Stato vede trasformate le proprie funzioni: lo scopo di uno Stato moderno è oggi anche quello di favorire il proprio tessuto economico per il quale la funzione di *intelligence economica* diviene strategica.

Scopo di tale disciplina è quello di migliorare le conoscenze e le capacità decisionali che sono a supporto della complessità dell'ambiente competitivo globale, tutto ciò attraverso lo studio del ciclo dell'informazione che è sempre più necessario alle imprese e agli Stati per effettuare scelte corrette di sviluppo

Possiamo definire l'*intelligence economica* come l'insieme di tutte quelle attività di raccolta di informazioni utili e non segrete, provenienti da fonti aperte - *open sources*, che si ritengano utili ai fini dei vertici decisionali dei governi, le quali vengono utilizzate a supporto della definizione e dello sviluppo di tutte quelle strategie che siano necessarie a potenziare il sistema Paese nella competizione sui mercati internazionali.[38]

I mutamenti storici nello scenario politico ed economico degli ultimi anni hanno fatto sì che l'*intelligence economica* acquisisse una notevole importanza. Essa accresce sempre più la sua rilevanza anche a causa dell'utilizzo dell'informazione usata spesso anche al fine di cambiare l'ordine politico ed economico, in una nuova era dell'economia caratterizzata da un capitalismo che sempre più competitivo e conflittuale, e da nuove conoscenze.

Possiamo vedere nell'uso dell'*intelligence economica* una duplice utilità. Da un lato aiuta a comprendere le relazioni internazionali contemporanee; d'altro canto supporta sulla necessaria riflessione circa le metodologie e le possibilità di innovazione che uno Stato moderno debba attuare anche relativamente alle sue funzioni di pianificazione e redistribuzione delle risorse.

L'*intelligence economica* può essere strumento di collaborazione tra Stato ed imprese, in un mondo economico dove le alleanze politiche o economiche sono meno stabili anche a causa della fluidità delle relazioni internazionali e dove anche le istituzioni più compatte ed antiche rischiano di perdere la loro coesione.

Gli eventi e i modi di intendere gli aspetti della vita sono in continua evoluzione, cambia la realtà cui siamo abituati ed il mondo stesso si trasforma ogni giorno. Quindi anche gli strumenti che abbiamo per conoscerli ed affrontarli cambiano. Alcuni studiosi sostengono che la politica, ma anche l'economia, sono "guerre effettuate attraverso l'uso delle

[38] Vedi: https://sociologicamente.it/intelligence-economica-influenzare-l-ambiente-economico-globale/

informazioni". Le minacce emergenti nel mondo d'oggi sono in perenne cambiamento ed esse viaggiano in rete sul web.

Così possiamo intuire che le nuove minacce acquisiscono caratteristiche ben precise, si evolvono tempestivamente e sono rivolte contro l'intero sistema; oggetto di queste minacce non sono solo bersagli politici o militari, ma esse tendono ad aggredire anche gli interessi commerciali, industriali, scientifici e tecnologici dei Paesi e delle aziende.

La globalizzazione ha trasformato la concorrenza da locale ad una vera guerra economica. La nuova missione dell'*intelligence economica* sarà quindi quella di sostenere tutti gli anelli della filiera produttiva, anche i più deboli.

L*'intelligence economica* riguarda un insieme di attività volte a controllare tutto il mondo economico globale: oltre alla semplice raccolta ed analisi delle informazioni, essa è utilizzata per sorvegliare la concorrenza, a proteggere le informazioni strategiche. Essa si delinea quindi come un formidabile strumento di governo a disposizione delle aziende oltre che dello Stato.

Anche se gli stati e le organizzazioni internazionali, quali ad esempio l'Unione Europea, sono i principali attori dell'*intelligence economica* e restano i regolatori più influenti dello scacchiere economico, fra gli attori dell*'intelligence economica* vi sono, ovviamente, anche le imprese che per incrementare la loro competitività e tutelare la sicurezza economica e delle infrastrutture, devono utilizzare necessariamente il controllo delle informazioni ritenute strategiche.

L'*intelligence economica* risulta così un'arma che concorre ad implementare le misure necessarie a vantaggio della strategia dell'impresa, mediante l'incremento di tattiche d'influenza e di manovre di controllo e lotta della concorrenza, a sostegno della propria sicurezza o delle operazioni commerciali.

Per le aziende il ricorso all'informazione è reso necessario a causa dell'aumento di una competizione sempre più pressante, dell'instabilità dei mercati e dell'accelerazione del ritmo delle innovazioni. Ne deriva quindi che la capacità di dominare il flusso di informazioni influisce sui risultati ottenuti da un'impresa; infatti tali risultati possono essere influenzati positivamente dall'uso delle nuove tecnologie dell'informazione e della comunicazione nelle sfide della concorrenza.

La gestione dell'informazione a fini economici ha dato luogo al "concetto di «*intelligence economica*», che si può anche definire come l'insieme di comportamenti messi in atto per acquisire, arricchire, diffondere e scambiare delle informazioni e trasformarle in azione"[39].

[39] Vedi: https://cf2r.org/reflexion/intelligence-economica-una-nuova-arma-al-servizio-della-competitivita-dello-stato-delle-imprese-e-dei-territori/

L'*intelligence economica* si è quindi evoluta nel tempo per dare una risposta al bisogno degli attori economici di avere uno strumento efficiente che assicuri lo sviluppo o la sopravvivenza nel mercato globale.

Ad esempio, il mantenimento dei segreti industriali e la protezione del patrimonio tecnologico sia dello Stato che delle aziende è diventato un obiettivo strategico nell'era della internazionalizzazione delle imprese. La lotta allo spionaggio industriale e cibernetico diviene vitale e centrale nella vita di tutte le organizzazioni, che debbono avvalersi di meccanismi di difesa inimmaginabili ignorati fino a qualche anno fa.

Stati e imprese hanno la necessità sempre più impellente di custodire e proteggere le proprie informazioni strategiche, proteggendole da chi potrebbe utilizzarle in modo ostile.

A tale scopo vari paesi occidentali hanno creato nel tempo delle strutture specifiche dedicate all'*intelligence economica*.

Il Presidente degli Stati Uniti Bill Clinton avviò negli anni 90 numerose iniziative legislative volte a rafforzare la postura statunitense nel settore specifico: l'*Economic Espionage Act* (1996), il *National Economic Council* (1993), il National CounterIntelligence Policy Board e l'Office of the National CounterIntelligence Executive (NACIX). Furono creati allo scopo uffici di intelligence economica in tutti i Dipartimenti, come l*'Office of Intelligence and Analysis* del Dipartimento del Tesoro e l'*Office of Intelligence and CounterIntelligence* del Dipartimento dell'Energia.

Di grande importanza per lo sviluppo dell'*intelligence economica* è stata la creazione in Francia della *École de Guerre Economique* (EGE*)*, fondata a Parigi nel 1997. Tale istituzione è infatti attiva a supporto dello sviluppo della politica industriale francese[40].

Un caso recente di *guerra economica* condotta dai francesi riguarda il recente caso Fincantieri-STX.[41] Già dal 2017 Fincantieri manifestò l'intenzione di acquisire la maggioranza dei cantieri navali francesi di Saint Nazaire, questa operazione avrebbe posto le basi per la nascita di un "gigante navale europeo". Purtroppo però tale operazione non era gradita in alcuni ambienti decisionali francesi. Così, nel luglio 2018, il giornale economico finanziario *La Tribune* pubblicò un report "riservato" nel quale venivano mosse pesanti accuse all'azienda italiana (dal titolo molto significativo: "Fincantieri: una relazione molto, molto pericolosa per Naval Group?"). Tale report fu infatti realizzato da *ADIT* (*Agence pour la diffusion de l'information technologique* – Agenzia per la diffusione della informazione tecnologica), organizzazione francese leader nel campo dell'intelligence economica. Si noti che Adit fu creata nel 1992 su iniziativa dello Stato Francese e "le sue principali aree di competenza riguardano le strategie industriali, l'identificazione di reti di influenza e circuiti di decisione, l'analisi del panorama competitivo, i problemi di sicurezza economica e

[40] Vedi: https://www.awarethinktank.it/lintelligence-economica-che-manca-in-italia/
[41] Vedi: https://www.startmag.it/smartcity/fincantieri-stx-perche-questo-matrimonio-non-sha-da-fare/

finanziaria, nonché la comunicazione istituzionale"[42] . Una guerra dell'informazione volta a rinegoziare l'accordo tra Fincantieri e STX, che ha indebolito il player italiano al tavolo delle trattative, successivamente naufragate e ha visto l'Italia vittima purtoppo inconsapevole.

Un altro caso degno di nota è sicuramente quello relativo all'opposizione all'acquisizione della società italiana NEXT INGEGNERIA da parte del gruppo francese ALTRAN. Dopo aver acquisito "ulteriori elementi informativi e integrativi", arrivò l'opposizione del Governo Italiano all'acquisto in ragione dell'attività svolta da Next, in cui rientravano "rapporti contrattuali di natura classificata e a carattere strategico per il sistema di difesa e sicurezza nazionale". Il caso emerse in discussione nel novembre 2017, ed in particolare gli annunci dati – anche per le vie informali ma presenti sul web – fecero mettere in moto tutta una serie di verifiche (utilizzando anche tecniche OSINT) che alla fine portarono all'opposizione dell'acquisizione da parte del Governo Italiano[43]

[42] Vedi: https://formiche.net/2019/09/intelligence-economica-francia-adit-cina/
[43] Vedi: https://formiche.net/2019/04/golden-power-governo-relazione-parlamento/

7. CONCLUSIONI

In questo lavoro abbiamo voluto dimostrare il ruolo strategico che l'OSINT può e deve avere all'interno di una azienda modernamente organizzata.

L'OSINT nell'era digitale significa utilizzare un sistema di informazioni essenziale per rispondere a nuove tipologie di rischi, come quelli associati alla *Cyber Security,* piuttosto che a rischi legati a comportamenti aggressivi da parte di Paesi ostili economicamente o dediti allo spionaggio. Ma non solo.

Abbiamo anche visto che la diffusione di internet, e quindi l'abbattimento delle barriere geografiche, rappresenta un fattore che ha contribuito in maniera decisiva a rendere oggi l'OSINT uno strumento sempre più strategico per diversi attori, primi fra tutti le aziende.

In questa ottica, il presente elaborato ha voluto rappresentare una sorta di compendio all'interno del quale si è cercato di dare una rappresentazione metodologica di OSINT, per quanto possibile attendibile e aggiornata, mettendo in relazione l'attività di analisi da fonti aperte con le principali tematiche di prevenzione che ad oggi rivestono una importanza decisiva non solo per la difesa dello Stato ma anche per lo sviluppo di una azienda.

Così è stato possibile identificare l'OSINT come uno strumento strategico non solo per la prevenzione dei rischi, ma anche per aumentare il vantaggio competitivo di una azienda modernamente organizzata.

L' OSINT, unitamente all'utilizzo delle potenzialità date dallo sviluppo della Intelligenza Artificiale (AI), sono infatti le nuove armi strategiche che l'azienda ha oggi a disposizione per automatizzare buona parte dei processi, semplificarli e industrializzarli, rendendo così il suo sistema più efficiente e più sicuro.

In questo lavoro abbiamo anche cercato di sottolineare come il vantaggio competitivo di una azienda sia dato dalla sua capacità di presidiare e difendere il patrimonio aziendale dalle minacce interne ed esterne e permettere così una reazione rapida in caso di emergenze o eventi che possono alterarne le normali operazioni.

Qui per una azienda sta la portata strategica dell'OSINT: permettere al management decisioni rapide, efficaci e mirate. La capacità OSINT permette al management di acquisire informazioni utili, scartando quelle non pertinenti e prendere quindi delle decisioni corrette.

L'OSINT permette, inoltre, all'azienda di avere informazioni utili per proiettare gli scenari futuri e le linee di comportamento sul mercato di altri competitori, sviluppare nuove strategie di marketing e comunicazione, dare impulso a nuovi prodotti e servizi, sviluppare adeguate politiche di cybersecurity; in altre parole: l'OSINT ha per una azienda delle potenzialità applicative illimitate.

Abbiamo così cercato di dimostrare che il futuro di una azienda moderna è legata alla sua superiorità informativa che solo un utilizzo appropriato dell'OSINT può dare.

Compito non semplice che abbiamo cercato di affermare con la convinzione che la ricerca OSINT, tramite fonti aperte, è un qualcosa di non vincolato e di non appartenente a nessuno, e quindi rappresenta un bene comune che deve essere sempre messo al servizio della comunità.

Ora la sfida futura per ogni azienda moderna è rappresentata dal maturare la convinzione che dell'OSINT non se ne può più fare a meno e deve essere quindi considerato come parte integrante dei suoi processi organizzativi e dei suoi strumenti operativi, scorgendo, per quanto possibile, quei tratti di innovazione che potrebbero farci scoprire nuove applicazioni ancora inesplorate.

8. BIBLIOGRAFIA E SITOGRAFIA

- Carlo Centoducati - Open Source Intelligence, Cenni sulla dottrina alleata https://www.difesa.it/InformazioniDellaDifesa/periodico/IlPeriodico_AnniPrecedenti/Documents/Open_Source_Intelligence.pdf

- Jessica Bertazzo - OSINT : l'investigazione tra intelligence e fruibilità dei dati personali https://creditvision.it/focus/osint-intelligence-investigazione-dati/

- L'Open Source Intelligence e le sue declinazioni nell'investigazione privata (05 Giugno 2019) https://www.filodiritto.com/lopen-source-intelligence-e-le-sue-declinazioni-nellinvestigazione-privata

- Paolo Lecce – OSINT: STRUMENTO DI SPIONAGGIO (03/11/2020) https://www.unimpresa.it/osint-strumento-di-spionaggio/38432

- Michelangelo Di Stefano - Ricerca investigativa: le metodologie OSINT/SOCMINT sulle fonti aperte (14/02/2020) https://www.altalex.com/documents/news/2020/02/14/ricerca-investigativa-metodologie-osint-socmint-sulle-fonti-aperte

- Rodolfo Zunino: associate professor DITEN Dept. University of Genova - Intelligence open source (Osint): ecco tecniche e vantaggi (28 Feb 2018) https://www.agendadigitale.eu/sicurezza/intelligence-open-source-osint-tecniche-vantaggi/

- OSINT E CYBER INTELLIGENCE: TECNICHE DI INVESTIGAZIONE NELLA RETE di Fabio Massa (21/01/2016) https://www.sicurezzaegiustizia.com/osint-e-cyber-intelligence-tecniche-di-investigazione-nella-rete/

- Threat Intelligence: l'approccio strategico alla sicurezza delle informazioni, Pierguido Iezzi - Swascan Cybersecurity Strategy Director e Co Founder e Davide Maniscalco - Legal, Privacy Officer e Capo delle Relazioni Istituzionali di Swascan – Tinexta Group (22 Mag 2020) https://www.cybersecurity360.it/soluzioni-aziendali/threat-intelligence-lapproccio-strategico-alla-sicurezza-delle-informazioni/

- Sentiment Analysis on Social Network a cura di Ing. Vito Santarcangelo, Dott. Antonio Ruoto e Ing. Giuseppe Oddo (February 2016) https://www.orizzontiholding.it/home/wp-content/uploads/2016/07/Sentiment-Analysis-on-Social-Network.pdf

- ALGORITMI, BIG DATA E DATA SCIENCE - Se sentiment analysis e big data battono i sondaggi politici (Luglio 18, 2020) https://affaripolitici.it/sentiment-analysis-e-big-data-battono-sondaggi/

- Sentiment analysis: cos'è e come sfruttarla per le aziende (31 gennaio 2022)

https://www.wearefiber.com/it/sentiment-analysis-cose-e-come-sfruttarla-per-le-aziende/

- By MJV Team - Market Intelligence nell'era digitale: cos'è e perché investirci (29/07/2021)
  https://www.mjvinnovation.com/it/blog/market-intelligence-nell-era-digitale/

- Cosa è la Market Intelligence? Vantaggi e casi pratici
  PUBBLICATO DA CMI TEAM (29 OTTOBRE 2021)
  https://www.centralmarketingintelligence.it/cosa-e-la-market-intelligence-alcuni-casi-pratici/

- Federico Della Bella - Associated Partner P4I - Digital Customer Experience Practice. Digital Marketing Intelligence: guida pratica agli strumenti online per l'analisi del contesto e dei trend di mercato (09 Gen 2019)
  https://www.digital4.biz/marketing/big-data-e-analytics/digital-marketing-intelligence-strumenti/

- Il market intelligence a supporto del processo di internazionalizzazione della tua azienda by Michele Riderelli EQUITY PARTNER Export Advisory & Business Development
  https://www.networkadvisory.eu/il-market-intelligence-a-supporto-del-processo-di-internazionalizzazione/

- IPOTESI DI EVOLUZIONE OSINT PER CONTRASTARE IL TERRORISMO (di Francesco Bergamo)
  https://www.difesaonline.it/evidenza/approfondimenti/ipotesi-di-evoluzione-osint-contrastare-il-terrorismo

- Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise by Heather J. Williams, Ilana Blum
  https://www.rand.org/pubs/research_reports/RR1964.html

- OSINT, la tecnologia open per documentare la verità in Ucraina by Ron Salaj (10/03/2022)
  https://impactskills.it/osint-la-tecnologia-open-per-documentare-la-verita-in-guerra/

- Blog sulla sicurezza informatica e l'informazione dei sistemi - Andrea Biraghi, Cyber Security manager e direttore della divisione Security and information Systems (October 28, 2019)
  https://www.andreabiraghicybersecurity.com/open-source-intelligence-e-cyber-security/

- Come fare intelligence sul Dark Web per difendere l'azienda (10 Febbraio 2022)
  https://blog.cerbeyra.com/threat-intelligence/come-fare-intelligence-sul-dark-web-per-difendere-azienda/

- Che cos'è la cyber threat intelligence?

https://www.bit4law.com/glossario-di-informatica-forense/cyber-threat-intelligence/

- La Cyber Threat Intelligence e Data Storage Security
  https://www.dssecurity.it/blog/trends/cyber-threat-intelligence-quello-che-ce-da-sapere/

- Infrastrutture Critiche, cosa sono e come proteggerle - Luisa Franchina, Presidente AIIC (14 Dicembre 2016)
  https://www.ictsecuritymagazine.com/articoli/infrastrutture-critiche/

- Rapporto CLUSIT 2022 sulla sicurezza ICT in Italia
  https://clusit.it

- Strategia Nazionale di Cybersicurezza 2022-2026
  https://www.acn.gov.it

- ENISA Threat Landscape 2022, released by the European Union Agency for Cybersecurity (ENISA)
  Httops://www.enisa.europa.eu

- La minaccia terroristica alla sicurezza e alle infrastrutture critiche nazionali - Luisa Franchina, Presidente di AIIC – Ludovica Coletta, Dottoressa in Relazioni Internazionali presso l'Università Luiss Guido Carli (30 Maggio 2016)
  https://www.ictsecuritymagazine.com/articoli/la-minaccia-terroristica-alla-sicurezza-alle-infrastrutture-critiche-nazionali/

- Attacchi informatici alle reti elettriche: sfide e prospettive – Davide Agnello Analyst, Hermes Bay, - Rachele Cordaro Analyst, Hermes Bay (15 Apr 2022)
  https://www.cybersecurity360.it/outlook/attacchi-informatici-alle-reti-elettriche-sfide-e-prospettive/

- Il ruolo della cyber intelligence nella tutela della sicurezza nazionale By Niccolò Nalesso (8 Febbraio, 2019)
  https://www.cyberlaws.it/2019/il-ruolo-della-cyber-intelligence-nella-tutela-della-sicurezza-nazionale/

- INTELLIGENZA ARTIFICIALE: COS'È, COME FUNZIONA E A COSA SERVE?
  https://www.intelligenzaartificiale.it/

- Quando l'IA aiuta a combattere le frodi – Alessio Jacona (30 ottobre 2020)
  https://www.ansa.it/osservatorio_intelligenza_artificiale/notizie/societa/2020/10/30/quando-lia-aiuta-a-combattere-le-frodi_b836e85f-8fc2-4c08-b264-e227f894d5a4.html

- OsintItalia, l'associazione che scova le «tracce» sul web per ritrovare persone scomparse – Michela Rovelli (7 maggio 2021)

https://www.corriere.it/tecnologia/21_maggio_07/osintitalia-l-associazione-che-scova-tracce-web-ritrovare-persone-scomparse-8aa585fc-aeca-11eb-8f4e-e883921d39f5.shtml

- Cosa sono il Deep Web e il Dark Web, cosa si trova e come si accede: tutte le istruzioni – Rosita Rijtano (20 Apr 2022) https://www.cybersecurity360.it/cultura-cyber/cose-il-deep-web-e-il-dark-web-cosa-si-trova-e-come-si-accede-tutte-le-istruzioni/

- Dark web e Deep web: cosa sono, differenze e rischi potenziali (12 Luglio 2021) https://focus.namirial.it/dark-web-e-deep-web/

- Deep web e Dark web: cosa vuol dire navigare il lato oscuro della rete - IVAN ANTOZZI (17 JUNE 2021) https://blog.osservatori.net/it_it/deep-web-dark-web-navigare

- Dark web: cos'è, pericoli e come accedere al deep web - Elisabetta Bevilacqua (21 Giu 2022) https://www.zerounoweb.it/techtarget/searchsecurity/dark-web-cose-e-come-evitarne-i-trabocchetti/

- SocMInt: un nuovo spazio per la raccolta di informazioni rilevanti di Alessandro Burato (4 Luglio 2016) https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/socmint-un-nuovo-spazio-per-la-raccolta-di-informazioni-rilevanti.html

- Dalla SocMInt alla Digital HumInt di Marco Lombardi, Alessandro Burato e Marco Maiolino (7 Giugno 2016) https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/dalla-socmint-alla-digital-humint.html

- Social Media Intelligence: un nuovo spazio per la raccolta di informazioni rilevanti – by Alessandro Burato (02/12/2014) https://www.itstime.it/w/social-media-intelligence-un-nuovo-spazio-per-la-raccolta-di-informazioni-rilevanti-by-alessandro-burato/

- Ricerca investigativa: le metodologie OSINT/SOCMINT sulle fonti aperte (15.02.2020) http://www.decahr.it/ricerca-investigativa-le-metodologie-osintsocmint-sulle-fonti-aperte/

- L'intelligence economica per un nuovo ordine mondiale di Laris Gaiser (20 Luglio 2016) https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/intelligence-economica-per-un-nuovo-ordine-mondiale.html

- Intelligence economica: influenzare l'ambiente economico globale By Ferdinando Capicotto (17 Dicembre 2021)

https://sociologicamente.it/intelligence-economica-influenzare-l-ambiente-economico-globale/

- Intelligence economica a sostegno della competizione industriale di Carmine America (18 Giugno 2014) https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/intelligence-economica-a-supporto-della-competizione-industriale.html

- INTELLIGENCE ECONOMICA: UNA NUOVA ARMA AL SERVIZIO DELLA COMPETITIVITÀ DELLO STATO, DELLE IMPRESE E DEI TERRITORI by ÉRIC DENÉCÉ - Direttore del Centro Francese di Ricerca sull'Intelligence (CF2R) (NOVEMBRE 2012) https://cf2r.org/reflexion/intelligence-economica-una-nuova-arma-al-servizio-della-competitivita-dello-stato-delle-imprese-e-dei-territori/

- Geolocation and Philosopher's Stone in Kashmir. Leicester Allen, T. (04 Marzo 2019) https://www.bellingcat.com/resources/casestudies/2019/03/04/geolocation-and-a-philosophers-stone-in-kashmir/

- Open Source Intelligence Tools And Resources Handbook 2020 Bielska, A. Kurz N.R., Baumgartner, Y., Benetis, V. https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

- An Introduction To Open Source Intelligence (OSINT) Gathering. Hassan, N. (2018) https://www.secjuice.com/introduction-to-open-source- intelligence-osint/

- Open-source intelligence for risk assessment. *Business Horizons* 61(5) Hayes, D. R. and Cappa, F. (2018) https://daneshyari.com/article/preview/8948069.pdf

- Implementazione del ciclo d'intelligence tramite l'utilizzo della social media intelligence (SOCMINT) Sperini, A. (2017) https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/ricerca_Sperini.aspx

Appendice A - Esempio di Scheda Analisi Rischi Paese - Data di elaborazione: Febbraio 2023

Pubblicazione autorizzata su gentile concessione della società Business Intelligence Consulting Srl

REPUBBLICA DEMOCRATICA POPOLARE DI ALGERIA

الجمهورية الجزائرية الديمقراطية الشعبية

SCALA CRITICITÀ

- **ELEVATA**
- **INTERMEDIA**
- **MODERATA**
- **ASSENTE**

TREND CRITICITÀ

- **AUMENTO**
- **STABILE**
- **DIMINUZIONE**

CAPITALE:	**Algeri**	ORDINAMENTO:	**Repubblica Presidenziale**
PRESIDENTE:	**Abdelmadjid Tebboune**	PREMIER	**Aimene Benabderrahmane**
SISTEMA LEGISLATIVO:	**Bicamerale**	SISTEMA LEGALE:	**Diritto francese – legge islamica**
SUPERFICE:	**2.381.741 km2**	POPOLAZIONE:	**45.000.000**
RELIGIONE:	**Islam sunnita 99%, altre 1%**	LINGUE:	**Arabo, Berbero, Francese**
FUSO ORARIO:	**Uguale Italia, - 1 ora con ora legale**	MONETA:	**Dinaro - DZD** دج
PREFISSO TELEFONICO:	**00213. Per l'Italia 0039**	TELEFONIA:	**Capitalphone, Djezzy, ZS Communication, Mobilis, Ooredoo**
EMERGENZA POLIZIA	**Polizia 17 – Polizia turistica 1548**	INGRESSO:	**Passaporto con validità residua di almeno sei mesi e pagina bianca per timbro. Visto obbligatorio.**
TENSIONE :	**230 Volt/50Hz -presa elettrica Tipo C**	AEROPORTI:	**Algeri ALG**

Abdelmadjid Tebboune

Aimene Benabderrahmane

Polizia

AMBASCIATA D'ITALIA

18, Rue Mohammed Ouidir
Amellal, El Biar – Algeri 16030 Tel. 0021323051433 / 34 Fax. 0021323051409 / 20
RECAPITO EMERGENZE 00213(0)23051403 (rete fissa) 00213(0)661546410 (mobile)
Email segreteria.algeri@esteri.it connazionali.algeri@esteri.it
PEC amb.algeri@cert.esteri.it
sito web www.ambalgeri.esteri.it

AMBASCIATORE:
dott. Giovanni Pugliese

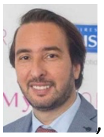
UNITÀ DI CRISI MAE – MINISTERO AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE –
+39 06 36225

ABSTRACT

Il Capo dello Stato e il Governo sono impegnati a rimuovere gli ostacoli che potrebbero ritardare l'interessamento degli investitori stranieri e anche nazionali, nel quadro della promozione di opportunità e forme di partenariato in grado di rilanciare e stabilizzare l'economia del Paese. Agli sforzi volti al miglioramento delle relazioni con l'UE – Unione Europea – e alcuni dei Paesi membri, come l'Italia e la Francia, fanno da contraltare i timori manifestati dagli Stati Uniti circa l'ingerenza che la Russia esercita sull'Algeria, soprattutto se sarà confermata la realizzazione di una base militare logistica sul Territorio algerino. Gli equilibri interni sono incerti e risentono della mancanza del rispetto delle libertà individuali, mentre sul piano internazionale rimangono alte le tensioni con il Marocco. La diplomazia è indirizzata ad affermare il ruolo del Paese nel contesto regionale e come apertura diretta all'area saheliana.

QUADRO GENERALE

1. Il prossimo 17 marzo, ad Algeri, si disputerà il Gran Premio Ciclistico internazionale per il quale sarà interdetta la viabilità nella gran parte della città. Il successivo giorno 23 marzo inizierà il periodo del *Ramadan*, le cui giornate conclusive sono previste il 21, 22 e 24 aprile. Si tratta d'una delle principali ricorrenze religiose musulmane.

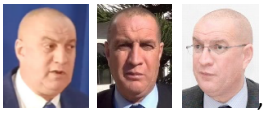
2. Gli scorsi 22 e 23 gennaio, il presidente del Consiglio dei Ministri italiano, Giorgia Meloni, s'è recato in visita ufficiale in Algeria per consolidare i rapporti strategici in materia di energia e gettare le basi per quello che è stato ridefinito il piano Mattei per l'Africa. Il *premier* è stato accompagnato, tra gli altri, dal presidente della CONFINDUSTRIA, Carlo Bonomi, e dall'amministratore delegato dell'ENI, Claudio Descalzi, e ha avuto colloqui con il Capo dello Stato e con il primo ministro, Aimene Benabderrahmane. Gli accordi non hanno riguardato esclusivamente le forniture di gas, ma hanno investito anche il settore della Difesa, sebbene l'Algeria s'approvvigioni di armi soprattutto dalla Russia e dalla Cina. Alcuni *media* italiani hanno indicato le possibili collaborazioni con il gruppo Leonardo, per gli elicotteri e il sito produttivo di Setif, inoltre le trattative per un cantiere navale con Fincantieri, mentre a MBDA sarebbe richiesto un lotto di missili[44]. Bonomi ha firmato un *memorandum* d'intesa con Kamel Moula     , il presidente del CREA – *Conseil du Renouveau Economique Algérien* –, per favorire la cooperazione industriale tra le imprese italiane e quelle algerine, mentre ENI e Sonatrach, l'azienda statale algerina che tratta le materie energetiche, hanno sottoscritto un accordo per una nuova *pipeline* che trasferisca l'idrogeno verso l'Europa e altri impegni per la valorizzazione della rete d'interconnessione energetica. Altrettanto di rilievo gli accordi tra le rispettive agenzie spaziali, la ASI – Agenzia Spaziale Italiana – e l'ASAL – *Agence Spatiale Algerienne* –, per un programma di collaborazione nel campo dell'esplorazione spaziale che comporta anche l'acquisto in Italia di satelliti, servizi tecnologici e trasferimento di *know-how*. La missione del presidente Meloni in Algeria è stata preceduta da alcune dichiarazioni rilasciate dall'ambasciatore algerino in Italia, Abdelkrim Touahria     , sull'importanza di rafforzare l'asse di cooperazione italo-algerina sul piano politico ed economico. Il successivo 25 gennaio, a Napoli, si è svolto un incontro organizzato dall'ambasciata algerina in Italia, in

---

44 https://espresso.repubblica.it/politica/2023/01/27/news/algeria_italia_armi_gas-385300638/.

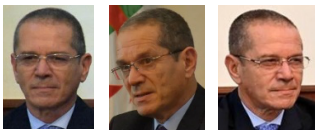
collaborazione con l'UIN – Unione Industriale di Napoli – e in *partnership* con il Club degli Imprenditori e Industriali di Mitidja, nell'ambito del rafforzamento delle relazioni di cooperazione e partenariato economico tra Algeria e Italia, al di fuori del settore degli idrocarburi.

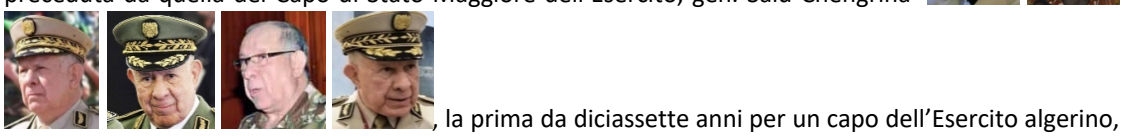
3. Gli scorsi 29 e 30 gennaio, si è svolta in Algeria la diciassettesima sessione della conferenza dell'Unione Parlamentare dei Paesi membri dell'OIC – *Organization of Islamic Cooperation* – , organizzata dal Parlamento algerino sul tema "Mondo islamico: sfide di modernizzazione e sviluppo". Uno degli scopi dell'evento è il rafforzamento del ruolo dell'Algeria nei vari *forum* parlamentari internazionali, con l'obiettivo di rendere sempre più vitale la presenza e l'attività politica diplomatica del Paese. All'evento in questione hanno preso parte diversi parlamentari dei Paesi aderenti all'OIC per confrontarsi sull'azione congiunta e gli sforzi del mondo islamico per rivestire un ruolo di primo piano nell'attuale contesto geopolitico ed economico segnato da instabilità e da quello che viene considerato un dominio feroce. Il Governo e i presidenti dei due rami del Parlamento hanno riservato molte energie per tracciare le linee di condotta che i rappresentanti nazionali hanno poi adottato e che dovranno mantenere presso l'Unione dei Consigli indicati. Il presidente dell'Assemblea Nazionale, Brahim Boughali, ha ricevuto coloro che rappresentano permanentemente l'Algeria per impartire le direttive e stabilire una linea d'intervento strategica, anche perché il Paese mira ad assicurarsi la presidenza dell'UA – Unione Africana – nel 2024, cui ambisce pure il Marocco.

4. Il Governo sta perseguendo politiche d'intervento economico e sociale con il duplice scopo da un lato di ridurre le tensioni interne e apportare significative modifiche alla qualità della vita della popolazione, dall'altra rafforzare il gradimento nei confronti del presidente Abdelmadjid Tebboune che intende aggiudicarsi un secondo mandato alle elezioni presidenziali del prossimo anno. Allo scopo di meglio monitorare la realtà sociale domestica è stato istituito l'ONSC – *Observatoire National de la Société Civile* – , con a capo Noureddine Benbraham  , che assumerà compiti consultivi. La manovra varata ha radici nella definizione di nuove strategie individuate fin dal secondo semestre dello scorso anno, mentre proprio allo scadere del 2022 Tebboune ha concordato con i ministri del Governo una serie di provvedimenti che includono aumenti dei salari, delle pensioni e dell'indennità per i disoccupati e nuovi sbocchi produttivi ed economici sono previsti con l'importazione dei veicoli stranieri, sospesa da cinque anni. Il rafforzamento generale degli emolumenti dovrebbe consentire alla popolazione d'affrontare l'inflazione con minore ansia, intervenendo su un terreno particolarmente insidioso per gli effetti destabilizzanti correlati all'antagonismo sociale. Più recentemente, è stato approvato l'aumento delle pensioni che dovrebbe essere erogato già dai prossimi mesi e avere valore retroattivo, da gennaio c.a., come confermato ufficialmente dal direttore generale della CNR – *Caisse Nationale de Retraite* – , Jaafar Abdali  , il quale ha pure reso noto che il provvedimento ammonterà a quindicimila Dinari, ovverosia l'equivalente del salario minimo. Coloro che si trovano in quiescenza beneficeranno anche di un aumento fino a ventimila Dinari. Nella prospettiva elettorale, il *leader* del Paese ha iniziato a gestire le comunicazioni ufficiali per qualificare il confronto, mentre viene esercitata una maggiore pressione sui principali *media* nazionali. Il Capo dello Stato s'è rivolto alla Nazione sottolineando la necessità di procedere con il rafforzamento dei progressi compiuti negli ultimi anni e ha fatto pure riferimento alle questioni relative al miglioramento delle condizioni di vita dei cittadini, alla promozione del servizio pubblico e alla rimozione degli ostacoli che avrebbero ritardato gli interessi degli investitori. Nell'indicare i progressi del Paese, il presidente Tebboune ha annunciato che le riserve valutarie superano i sessantamiliardi di USD, mentre la crescita economica ha registrato un tasso del 4,1% nel 2022 e dovrebbe raggiungere il 5% nell'anno in corso.

5. Le Autorità hanno negato i visti d'ingresso a una trentina di sacerdoti cattolici provenienti dall'Italia che avrebbero voluto compiere un pellegrinaggio a Tibhirine, per ricordare la memoria di sette monaci trappisti che nel 1996 furono sequestrati dal loro monastero e uccisi. Il passato si sono verificate altre situazioni in cui il visto è stato respinto a religiosi cattolici, a conferma della discriminazione in atto nel Paese nei riguardi delle comunità non di fede islamica.

6. Durante un incontro, in Algeria, con rappresentanti dell'azienda saudita Tabuk, il ministro dell'Industria farmaceutica, Ali Aoun  , ha protestato vibratamente dopo aver preso atto che nella sala della riunione allestita dagli ospiti stranieri era stata esposta una mappa geografica in cui la regione del Sahara è apparsa integrata nei confini politici del Marocco. La questione ha assunto i connotati di una crisi politica, velocemente risolta, tanto da essere riferita dal sito saudita di notizie *online* Watan che ha parlato della fermezza con cui il ministro algerino in parola ha puntualizzato la posizione del suo Paese sulla questione del Sahara occidentale.

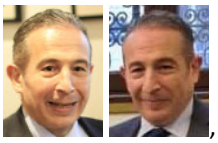
7. Nell'ambito della costante qualificazione delle relazioni politiche con la Turchia, il ministro dell'Agricoltura e dello Sviluppo Rurale, Mohamed Abdelhafid Henni  , ha incontrato l'ambasciatrice della Turchia in Algeria, Mahinur Ozdemir Goktas, con la quale ha esaminato lo stato delle relazioni bilaterali e i modi nonché i mezzi per rafforzarle nell'ambito agricolo. Il mese prossimo, si terrà un incontro tra uomini d'affari d'ambo le parti per discutere i temi della cooperazione nei settori d'interesse comune.

8. A seguito degli accordi presi tra le parti, il prossimo mese di maggio il Capo dello Stato si recherà in Francia per incontrare l'omologo Emmanuel Macron, con il quale analizzare lo stato delle relazioni bilaterali e rimuovere gli ostacoli che intralciano il percorso di riconciliazione e ricostruzione d'una memoria condivisa tra i due Paesi[45]. Il presidente Abdelmadjid Tebboune ha dichiarato d'aver "*accolto con favore il nuovo rapporto di fiducia tra l'Algeria e la Francia*", mentre il Capo di Stato francese, in un'intervista concessa allo scrittore algerino Kamel Daoud[46]  e pubblicata dal settimanale *Le Point*, ha parlato del processo di ricostruzione dei legàmi bilaterali su presupposti di rispetto e condivisione dei percorsi storici. La missione di Tebboune è stata preceduta da quella del Capo di Stato Maggiore dell'Esercito, gen. Said Chengriha  , la prima da diciassette anni per un capo dell'Esercito algerino, mentre il ministro Ali Aoun ha avuto un confronto preliminare con l'ambasciatore francese in Algeria, Francois Gouyette, con il quale ha preso in esame lo stato della cooperazione nonché le prospettive per rafforzarla nel campo dell'industria farmaceutica, temi poi approfonditi durante la riunione del gruppo di lavoro del COMEFA – *Comité Mixte Economique Franco-Algerien* –, svoltasi il 25 gennaio u.s., ad Algeri, cui hanno preso parte, tra gli altri, i ministri degli Esteri dei due Paesi. In tale contesto di distensione politica tra i due Paesi, due eventi hanno alterato gli equilibri, già fragili, laddove il secondo sembra di maggiore gravità:

---

45 Vds. aggiornamento 24 di gennaio 2023, Quadro Geopolitico punto alinea 3.
46 Direttore del *media* algerino *Le quotidien d'Oran*.

- il sito d'informazione AP – *Algerie Part* – ha sollevato uno scandalo rendendo noto che Farid Zineddine Bencheikh  , direttore della DGSN – *Direction Générale de la Sureté Nationale* – nonché capo della Polizia, finora considerato uno dei più stretti e fidati collaboratori del Capo dello Stato, tanto da far parte del Consiglio di Alta Sicurezza del Paese, sarebbe residente in Francia ove ha investito fondi in un esercizio per la ristorazione sito all'interno di un *hotel*, *L'Etoile*. Secondo risultanze in possesso di AP, l'impresa sarebbe stata portata a termine unitamente al fratello, privo di un permesso di soggiorno legale in Francia, e successivamente avrebbe costituito una società con un altro cittadino d'origine algerina, originario della regione di Bejaia, per sviluppare e incrementare le attività, cercando di tenere celata la sua posizione. Dal 2015 e per un lungo periodo di tempo, Bencheikh avrebbe vissuto nel lussuoso quartiere residenziale Vivienne – 2° *arrondissement* – di Parigi, pur mantenendo il controllo della sicurezza in Algeria. Le imprese indicate sono considerate illegali in Algeria, poiché non comunicate alle Autorità del Paese. Un altro *media*, *Maghreb Intelligence* , ha rivelato che dall'inizio dell'estate 2022 l'*intelligence* algerina sta indagando circa la presenza di un collaboratore del capo della Polizia dell'Algeria a Parigi.

- L'Algeria ha nuovamente richiamato per consultazioni il proprio ambasciatore in Francia, Said Moussi[47]  , in segno di protesta per l'estradizione di una cittadina franco-algerina, la militante Amira Bouraoui  particolarmente nota in quanto esponente di spicco del movimento denominato Barakat[48] e impegnata a richiedere un cambiamento democratico in Algeria, la quale dopo essere sfuggita al controllo della Polizia algerina è entrata clandestinamente in Territorio tunisino con l'obiettivo di fuggire in Europa. La donna è stata, però, trasferita in Francia su intervento dell'ambasciata francese a Tunisi, dopo che era stata tratta in arresto presso l'aeroporto internazionale della capitale tunisina. Secondo le notizie inizialmente fornite dal *media Algerie Part*, la predetta è stata sottoposta a fermo dalla Polizia tunisina mentre stava partendo per la Francia e poi posta in regime di libertà, in attesa di comparire difronte a una corte per accogliere i capi d'imputazione. Appena rilasciata, sarebbe stata prelevata da alcune persone e trasferita in un luogo ignoto. Le Autorità algerine hanno condannato quella che considerano "*una violazione della sovranità nazionale da parte della Francia*", aggiungendo nei commenti che si tratta d'una operazione clandestina e illegale per consentire a un cittadino algerino di fuggire all'estero. Il vice-portavoce del ministero degli Esteri francese, Francois Delmas, non ha commentato le accuse specifiche, ma ha dichiarato che Amira Bouraoui gode di protezione consolare come tutti i cittadini francesi e che la Francia continuerà i suoi sforzi per rafforzare i legàmi con l'Algeria – "*il richiamo dell'ambasciatore è una decisione algerina, ma noi intendiamo continuare a lavorare per approfondire le nostre relazioni bilaterali con una rinnovata partnership*" – .

9. Alla fine del mese di gennaio, ad Algeri, il presidente della Repubblica ha ricevuto lo sceicco Jassim Ben Hamad Al-Thani, rappresentante personale dell'emiro del Qatar, per valutare lo stato delle relazioni

---

47 Già rappresentante diplomatico in Spagna, da luglio 2022 ambasciatore in Francia.

48 Un movimento attivo nella contestazione dell'ex presidente Abdelaziz Bouteflika  .

bilaterali tra i due Paesi e alcune questioni da carattere regionale e internazionale. La rilevanza del colloquio è deducibile dall'assenza del rappresentante diplomati del Qatar in Algeria.

10. Il Consiglio esecutivo dell'UNICEF – *United Nations International Children's Emergency Fund* – ha adottato a unanimità il programma di cooperazione con l'Algeria per il periodo 2023-2027, con un *budget* complessivo proposto di settemilioni e settecentomila USD in risorse regolari e quasi novemilioni di USD in altre risorse, che contribuirà a sostenere gli sforzi del Paese per raggiungere gli SDG – *Sustainable Development Goals* – in particolari settori dell'istruzione, dello sviluppo delle capacità, del primo soccorso e della protezione. Nel suo discorso durante il dibattito, il rappresentante permanente dell'Algeria presso le Nazioni Unite, ambasciatore Nadir Larbaoui  , ha espresso la gratitudine per il sostegno fornito dall'UNICEF.

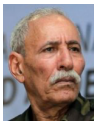
QUADRO GEOPOLITICO

1. L'ipotesi formulata dalla CIA – *Central Intelligence Agency* – statunitense circa la possibilità, considerata concreta, che l'Algeria ospiterà a breve una base militare logistica russa sul proprio Territorio ha indotto l'Amministrazione americana a esaminare con maggiore attenzione la tesi secondo cui il regime algerino sia sostenuto militarmente e politicamente dalla Russia e che ciò possa costituire un elemento d'allarme nello scacchiere africano e mediterraneo occidentale. La CIA ha fornito al presidente americano Joe Biden un rapporto dettagliato sull'espansione dell'influenza russa in Africa, con specifico riferimento allo Zimbabwe, Sudan, Repubblica Centrafricana e Algeria, oltre ai Paesi della regione saheliana e sahariana. La visita definita di cortesia dell'ambasciatore russo in Algeria, Valerian Shuvaev   , a Salah Gudjil  , presidente del CN – *Conseil de la Nation* – , è stata interpretata proprio come una conferma dell'intensità dei legàmi bilaterali, anche perché i due uomini politici citati hanno sottolineato l'impegno dei reciproci Paesi a sviluppare le "*relazioni storiche privilegiate*". Sono considerate attestazioni d'alleanza anche le dichiarazioni rilasciate da Riyad Khuveili, capo del sindacato degli editori di *media* in Algeria, all'agenzia stampa russa RIA Nosti, per stigmatizzare le sanzioni delle Autorità canadesi contro i *media* e i giornalisti russi. La via diplomatica scelta dagli Stati Uniti come misura parallela a eventuali irrigidimenti ha portato il vicesegretario di Stato, Michele Sison, responsabile delle questioni relative alle organizzazioni internazionali, a svolgere una missione in Algeria, dove s'è confrontata con il ministro degli Esteri, Ramtane Lamamra, sullo stato delle relazioni bilaterali tra i due Paesi e le prospettive di rafforzamento del dialogo strategico e la cooperazione economica, oltre che sulle notizie regionali e internazionali. Partendo dal ruolo geopolitico svolto dall'Algeria, i nuovi scenari potrebbero rivelarsi minacciosi per gli equilibri in Medioriente e, ancor più, in Cisgiordania e Palestina, atteso l'intenso richiamo antiisraeliano che il presidente e i componenti del Governo algerino svolgono da tempo. Nel contesto generale si inserisce pure la visita ufficiale che il segretario del Comitato Centrale del movimento Fatah, Jibril Rajoub, inviato speciale del presidente palestinese, Mahmoud Abbas, ha portato a termine in Algeria per incontrare Abdelmadjid Tebboune. Allo scopo di riequilibrare la situazione, gli Stati Uniti sembrano orientati a realizzare aspetti logistici in materia di Difesa in Marocco, anche come garanzia per gli alleati occidentali e per un maggiore controllo dell'accesso allo stretto di Gibilterra. L'interesse geopolitico e geostrategico dell'Algeria per le questioni continentali è stato confermato pure da due esponenti della politica in Mali, il ministro degli Esteri, Abdoulaye Diop, che ha elogiato "*il ruolo unificante svolto dall'Algeria nello stabilire la pace e la riconciliazione in Mali*", e il colonnello Assimi Goita, presidente della transizione, il quale ha apprezzato il ruolo moderatore dell'Algeria. In merito allo scenario saheliano, l'INESG – *Institut National d'Etudes*

de Stratégie Globale – Institut National d'Etudes de Stratégie Globale ha svolto, ad Algeri, un simposio per valutare le strategie più idonee per risolvere la crisi regionale. Per le necessità del caso, è stato istituito un gruppo di lavoro politicamente indipendente, presieduto dall'ex Capo di Stato del Niger, Mahamadou Issoufou e composto da diversi esperti africani, che svolgerà la prima missione proprio in Algeria per sondare le disponibilità e prendere atto delle volontà geopolitiche.

2. Le Autorità hanno istituito un gruppo parlamentare d'amicizia con il Camerun, insediato presso l'Assemblea Nazionale, al fine di sviluppare relazioni di cooperazione bilaterale attraverso la creazione di nuovi meccanismi di contatto e l'incoraggiamento di scambi parlamentari multidimensionali. Nell'occasione, il vicepresidente dell'Assemblea, Ahcene Hani   , ha affermato che l'Algeria e il Camerun sono impegnati "*a coordinare gli sforzi bilaterali nella lotta contro le sfide regionali, comprese quelle relative al contrasto al terrorismo, la criminalità organizzata transfrontaliera, l'estremismo violento e l'immigrazione illegale*". Le due parti stanno anche lavorando per promuovere il commercio e gli scambi economici ai massimi livelli.

3. Nell'ambito dello scontro in atto con il Marocco, l'Algeria ha ridotto drasticamente l'esportazione di gas verso la Spagna – riduzione del 74% – , che colpevolizza per aver approvato il piano d'autonomia del Marocco come base più attendibile per porre fine alla disputa sul Sahara occidentale. L'inasprimento del confronto tra l'Algeria e la Spagna ha comportato pure il congelamento del trattato d'amicizia bilaterale che risale a vent'anni fa, sebbene l'Associazione algerina delle banche e delle istituzioni finanziarie ha successivamente annunciato la revoca delle restrizioni, di fatto, però, non attuate. La dichiarazione di buoni propositi è sembrata rispondere alle pressioni esercitate dall'UE – Unione Europea – sull'Algeria affinché riesamini lo stato delle relazioni con la Spagna.

4. La conflittualità con il Marocco, con il quale le relazioni diplomatiche sono interrotte dall'estate del 2021[49], potrebbe trasformarsi in un fattore di criticità per tutta la regione del Maghreb, che già risente dell'instabilità in Libia e teme il possibile collasso del sistema politico e amministrativo della Tunisia. L'Algeria percepisce la vicinanza politica espressa da Israele al Marocco, sostanziata in cooperazione pure nei comparti militare e della sicurezza, come una minaccia e per tale ragione ha moltiplicato le manifestazioni di sostegno ai palestinesi, ergendosi a paladina dei diritti e delle ragioni della popolazione della Cisgiordania e della regione di Gaza. Gli aspetti del sostegno alla causa del Fronte Polisario, altro tema dirimente con il Marocco, sono stati ribaditi durante lo svolgimento del sedicesimo Congresso del Fronte Polisario[50], tenutosi a Dakhla, nei campi dei rifugiati saharawi, attraverso l'invio di un messaggio a firma delle principali Autorità di Governo e dello stesso Capo dello Stato. Al vertice del Fronte è stato confermato Brahim Ghali[51]       , particolarmente apprezzato dal presidente Tebboune per la determinazione con cui si batte per l'autodeterminazione. A livello internazionale, l'immagine del Fronte è stata, però, associata a un circuito di riciclaggio e veicolazione di denaro che si presume possa finanziare il terrorismo. Alcune indagini in Spagna e altrove hanno individuato un sistema bancario parallelo che collega l'Europa all'Africa e il Medio Oriente e si basa su tradizioni di fiducia personale che lascia spazio alle transazioni anonime, tanto da ipotizzare il controno di una cosiddetta banca *hawaladar*. Sula piano della politica diplomatica ufficiale, attraverso il CREA – *Conseil du Renouveau Economique Algérien* – è stato, invece, siglato da soggetto algerini un accordo con l'UNPM – Unione Nazionale dei Datori di lavoro Mauritani – che riveste un particolare valore geopolitico in relazione alla posizione geografica della Mauritania.

---

49 Vds. aggiornamento 08 di settembre 2021, Quadro Generale punto alinea 4.
50 Vds. aggiornamento 24 di gennaio 2023, Quadro Generale punto alinea 2.
51 *Ibidem.*

5. Per quanto riguarda lo scenario libico, il ministro degli Esteri algerino, Ramtane Lamamra, ha:

- effettuato una visita di lavoro in Libia ove ha avuto colloqui con rappresentanti locali circa lo stato delle relazioni bilaterali, ribadendo l'impegno dell'Algeria per consentire alle parti libiche di raggiungere una soluzione pacifica e duratura in grado di porre fine alla crisi attuale e garantire il ripristino del ruolo del Paese nel contesto regionale e internazionale;
- preso parte alla riunione periodica di consultazione dei ministri degli Esteri arabi che s'è tenuta a Tripoli;
- incontrato, ad Algeri, il rappresentante speciale del segretario generale delle Nazioni Unite per la Libia e capo di UNSMIL – *United Nations Support Mission in Lybia* – , Abdoulaye Bathily, col quale ha analizzato gli aspetti salienti delle prospettive di pacificazione in Libia, offrendo la disponibilità e l'esperienza dell'Algeria per supportare le iniziative delle Nazioni Unite nel contesto libico.

6. Nel corso dell'incontro con il ministro dell'Interno dei territori palestinesi, Ziad Hab Al-Riha, il primo ministro algerino, Aimene Benabderrahmane, ha ribadito la posizione filopalestinese del suo Paese e l'intenzione di sostenere costantemente la causa d'emancipazione politica in Cisgiordania e nella striscia di Gaza.

CRITICITÀ E SICUREZZA

1. Il ministero del Commercio e della Promozione delle Esportazioni ha annunciato l'organizzazione di una campagna di sensibilizzazione contro la commercializzazione di prodotti recanti i colori riconducibili alla comunità LGBT – Lesbiche Gay Bisessuali Transgender – , che "*minano i valori morali della società algerina*". Il ministro del dicastero in questione, Kamel Rezig  , ha evitato di fare riferimenti espliciti al contesto di genere, ma il comunicato che è stato emesso e l'orientamento culturale della persona e del Paese rendono impossibile equivocare. La campagna di sensibilizzazione si svolge in luoghi pubblici e ambiti mediatici, mentre SMS – *Short Message Service* – sono inviati a consumatori e operatori economici. Secondo alcuni osservatori, la presa di posizione algerina è subordinata all'aumento delle relazioni economiche con il Qatar, che esercita una pressione crescente, atteso che il Capo dello Stato dell'Algeria ha manifestato il pieno sostegno al Qatar il merito alle questioni di genere e ad altri temi – "*l'Algeria esprime il suo incrollabile sostegno al Qatar e denuncia le dubbie campagne che lo prendono di mira*" – alla vigilia dei campionati mondiali di calcio recentemente disputatisi nel Paese del Golfo Arabico.

2. La DGSN – *Direction Générale de la Sureté Nationale* – ha diffuso ulteriori dettagli circa la rete di persone che s'è infiltrata in alcune aziende economiche di rilievo e ha collaborato con finanziatori attualmente sottoposti alla misura della custodia cautelare in carcere, i quali hanno elargito consistenti somme di denaro utilizzate per rendere possibile l'attività del sito ostile *Algerie Part*[52] – che ha sede in Francia – , attorno al quale ruotava un gruppo di persone con lo scopo di destabilizzare l'Algeria e facilitare entità avverse. Samir Lounes – inizialmente identificato solamente con le iniziali – , uno dei *leader* nonché *blogger* di *Algerie Part* e noto come Amir Younes, ha ammesso le responsabilità e la stretta collaborazione con Abdou Semmar fin dal 2015, nonché la creazione di un profilo Facebook per ricevere informazioni e d'aver svolto il ruolo d'interprete per il terrorista Amir Boukhors. Negli ultimi tempi, la pagina Facebook in questione sarebbe stata gestita da Warda Nouara, seconda moglie di Semmar.

3. Nell'ambito della campagna per eradicare il fenomeno della corruzione, l'Unità Economica e Finanziaria del tribunale di Sidi M'hamed ha emesso la sentenza di condanna ad anni:

---

52 Vds. aggiornamento 18 di luglio 2022, Criticità e Sicurezza, punto alinea 6.

- sei di detenzione per Kamel Issad, ex amministratore delegato della ENTMV – *Entreprise Nationale de Transport Maritime de Voyageurs* – , riconosciuto colpevole di corruzione unitamente ad altri dirigenti della società;

- venti di detenzione, con conferma dell'ordinanza di arresto internazionale, per l'ex ministro dell'Energia e delle Miniere Chakib Khelil[53]    , giudicato unitamente ad altri ex elementi del Governo e tutti condannati a pene detentive comprese tra cinque e dieci anni di reclusione, riconsciuti colpevoli di corruzione e cattiva gestione del denaro pubblico.

Altri provvedimenti sono stati emessi per i casi che riguardano Said Bouteflika[54], nella sua veste di consigliere dell'ex presidente della Repubblica, e altri uomini d'affari coinvolti in procedimenti penali per corruzione, quali Ali Haddad[55]    , ex *leader* della principale organizzazione dei datori di lavoro, la FCE – *Forum of Business Leaders* – , e suo figlio, i quali dovranno versare un rimborso di cinquecentomilioni di Dinari per indennizzare il Tesoro pubblico.

4. Un terrorista noto come Bey Malaoui, *alias* Mokdad, che nel 2012 ha federato i gruppi islamisti armati presenti nella regione del Sahel, si è arreso alle Autorità militari di Bordj Badji Mokthar, consentendo agli elementi dei Servizi di Sicurezza dell'Esercito di recuperare il suo armamento personale e altre armi, munizioni ed esplosivo. Altre differenti operazioni condotte da militari e personale dell'*intelligence* hanno consentito la cattura di nove elementi riconducibili a gruppi terroristici che agiscono sul Territorio nazionale, con conseguente rinvenimento di armi, munizioni ed esplosivi, attrezzature per le comunicazioni.

5. Il *media* locale Le Soir d'Algerie ha riferito che il Comitato Nazionale per la Liberazione dei Detenuti ha rilasciato per motivi umanitari, concedendogli la grazia, Rachid Nekkaz[56]    , uomo d'affari e attivista imprigionato con l'accusa d'aver esortato il boicottaggio delle elezioni presidenziali del 2019, dopo aver tentato di candidarsi senza successo, e incitamento alla violenza attraverso i *social media*, dove ha grande seguito – nel 2022 è stato condannato ad anni cinque di reclusione – . Nekkaz ha dichiarato d'essersi rivolto al presidente Tebboune per informarlo della decisione d'abbandonare la vita politica e dedicarsi alla scrittura e alla famiglia. È stata, invece, confermata la misura della detenzione in carcere per Ihsane El Kadi[57], direttore e fondatore di Radio M, accusato di raccogliere fondi illegalmente e d'attaccare la sicurezza dello Stato. A favore di El Kadi si sono mobilitate organizzazioni impegnate in difesa delle libertà individuali e della stampa, oltre ai quasi venti esponenti del mondo dei *media*, tra i quali il premio Nobel per la pace Dmitry Muratov, coordinati da RSF – Reporter Senza Frontiere – per chiederne il rilascio. Nonostante le critiche rivolte alla limitazione della libertà di stampa, il presidente della PL – *Prensa Latina* –, Luis Enrique Gonzales Acosta,

---

53 *Ibidem*.
54 Vds. aggiornamento 20 di settembre 2022, nota 3 a piè di pagina
55 Vds. aggiornamento 17 di giugno 2022, Criticità e Sicurezza punto alinea 4.
56 Nato in Francia, ove ha svolto attività politica e nel 2007 s'è candidato per le elezioni presidenziali e ha poi fondato un proprio partito politico, nel 2013 ha rinunciato alla cittadinanza francese per candidarsi alle elezioni presidenziali algerine del 2014.
57 Vds. aggiornamento 24 di gennaio 2023, Criticità e Sicurezza punto alinea 1.

ha sottoscritto un accordo di cooperazione con l'APS – *Algerie Press Service* – per rafforzare i collegamenti esistenti e progettare nuovi modi per diffondere gli eventi dei rispettivi Paesi e regioni geografiche. PL sta addirittura lavorando al lancio di un servizio di notizie in lingua araba e all'istituzione di sue redazioni in nord Africa e Medio Oriente.

6. Portavoce della LADDH – *Ligue Algérienne pour la Défense des Droits de l'Homme* – hanno reso noto d'aver appreso dello scioglimento coatto dell'organizzazione dai *social media*, come esecuzione d'una sentenza processuale che risale a sei mesi fa. Said Salhi  , vicepresidente della LADDH, ha dichiarato che il ministero dell'Interno ha esercitato pressioni sulla magistratura affinché disponesse la cessazione delle attività d'*advocacy* del gruppo, colpevolizzato per la contiguità e condivisione d'ideali con il movimento popolare Hirak. La questione dei diritti umani è stata ripresa da Michele J. Sison, assistente segretario di Stato statunitense per gli Affari delle Organizzazioni Internazionali, che in missione in Algeria avrebbe dovuto incontrare proprio alcuni rappresentanti della LADDH.

7. L'accomunamento dei cittadini occidentali, comunque europei, a coloro che sono stati definiti estremisti islamofobici, ovverossia quegli svedesi che hanno bruciato copie del Corano nel corso di manifestazioni pubbliche svoltesi nelle città di Malmo (S) e Linkping (S), potrebbe costituire un fattore di pericolo nel caso di soggiorni in Algeria. Portavoce delle principali Autorità algerine hanno condannato con fermezza l'accaduto, definendolo un "*atto spregevole che potrebbe provocare odio e sentimenti religiosi dei musulmani, poiché mina profondamente i valori di libertà su cui si basano le società, compresi i valori umanitari*", ritardando, al tempo stesso, l'instaurazione d'un clima di tolleranza, rispetto e dialogo interreligioso.

SANITÀ

1. Le Autorità hanno dato notizia d'una cauta ripresa dei contagi del *virus* Covid-19, nell'ordine massimo d'una dozzina di casi al giorno, ma i decessi sarebbero azzerati o ridotti a pochissime unità. Il ministero della Salute ha confermato il mantenimento della vigilanza e il rispetto delle regole d'igiene, distanziamento fisico e ricorso alla maschera di protezione.

ECONOMIA

1. Il 24 e 25 gennaio scorsi, ad Algeri, s'è svolta la seconda edizione del *Legal Business Forum and Awards*, con la partecipazione di diverse delegazioni di esperti legali, presidenti e decisori economici provenienti da Paesi africani, inclusi i rappresentanti dell'AfDB – *African Development Bank* – . L'evento è stato patrocinato da alcuni ministeri algerini e s'è concentrato sulle principali tendenze in materia d'economia dell'anno in corso, affrontando i temi delle economie del continente e del nuovo quadro giuridico per gli investimenti in Algeria, aspetto cui il Governo attribuisce particolare rilievo per sostenere la crescita nazionale.

2. Il 26 gennaio u.s., a Bruxelles (B), l'ambasciata algerina in Belgio ha organizzato un seminario economico sul mercato algerino, in *partnership* con le agenzie regionali belghe per il commercio estero e la Camera

di Commercio Arabo-Belga-Lussemburghese, dell'ambito della cosiddetta diplomazia economica. All'evento ha preso parte l'ambasciatore dell'Algeria, Ali Mokrani    , rappresentanti del ministero algerino dell'Ambiente e delle Energie Rinnovabili, Agenzia per la Promozione degli Investimenti, del ministero dell'Energia e delle Miniere, delle aziende Sonatrach e Sonelgaz.

3. Il ministro dell'Industria, Ahmed Zeghdar       , ha avuto consultazioni con direttore della Regione Africa e Medio Oriente del gruppo Stellantis, Samir Cherfan, per fare il punto sullo stato d'avanzamento del progetto FIAT per la produzione di automobili in Algeria. Il Capo dello Stato, infatti, riversa molte attese sulla ripresa della produzione automobilistica, come volano aggiuntivo per l'economia.

4. Il presidente e amministratore delegato di Sonelgaz[58] سونلغاز SONELGAZ, Mourad Adjal     , ha avuto un incontro con alti dirigenti della GECOL – *General Electricity Company of Libya* – al fine di prendere in esame le modalità per rilanciare la cooperazione tra le due aziende menzionate, a partire dal progetto di costruzione d'una rete elettrica diretta tra i due Paesi. L'impresa necessita di fonti di finanziamento e potrà essere articolata e conclusa in un arco di tempo non ravvicinato. Il valore delle proposte formulate dall'Algeria riconduce pure alle strategie geopolitiche del Paese, a partire dalla disponibilità manifestata nel fornire i propri servizi alla parte libica in vari settori del comparto energetico, compresa la cessione di energia elettrica, manutenzione e messa in servizio di stazioni e rete elettriche, manutenzione delle infrastrutture, produzione di pezzi di ricambio e formazione del personale e dei quadri dirigenti.

5. I vertici della *Tosyali Algerie* TOSYALI ALGERIE Fer et Acier, filiale del produttore turco dell'acciaio *Tosyali Holding*, prevedono di iniziare la produzione nel complesso di Orano nel primo trimestre del 2024. Altri processi di lavorazione saranno messi in funzione l'anno successivo. L'impianto produttivo in questione ha richiesto l'investimento di un miliardo e mezzo di USD, avrà una capacità produttiva annua di due milioni di tonnellate e conta duemilacinquecento posti di lavoro. A pieno ritmo, l'azienda impiegherà un totale di seimilacinquecento persone.

6. L'aumento dell'esportazione di gas verso l'Europa ha comportato per l'Algeria un deciso aumento delle entrate, tanto da chiudere il 2022 con un introito superiore a cinquantamiliardi di USD rispetto ai trentaquattro dell'anno precedente e ai ventimiliardi del 2020. La crescita registrata è stata di trentamiliardi di USD in soli due anni, fornendo l'impulso all'economia nazionale per ulteriori *performance* positive, come rilevato dalla Banca Mondiale nel *report Algeria Economic Update*. Il *trend* positivo potrebbe, però, risentire negativamente del calo delle esportazioni registrato dall'inizio dell'anno, anche perché le dichiarazioni del presidente Tebboune di consegnare maggiori quantitativi di gas all'Italia appaiono eccessivamente ambiziose rispetto alle concrete possibilità. L'anno scorso, il produttore algerino non è riuscito a inviare tutti i quattro miliardi di metri cubi aggiuntivi previsti.

---

[58] Società pubblica responsabile della distribuzione d'energia elettrica e gas a livello nazionale.

DIFESA E ARMAMENTO

1. Il quotidiano in lingua araba *Assabah* ha riferito che l'Iran avrebbe messo a disposizione dell'Algeria attrezzature e strumenti per le attività di *hacking*, nonché addestramento degli *hacker*, nel quadro della cooperazione militare tra i due Paesi. La notizia è confermata da alcuni organismi d'*intelligence* europei per i quali "*la fornitura di armi iraniani include droni e armi tecnologiche*". Secondo fonti attendibili, gli *hacker* algerini starebbero impiegando le attrezzature ricevute per sferrare attacchi contro obiettivi del Marocco, praticando forme di spionaggio, propaganda e diffusione di notizie false, hackeraggio di siti per sottrarre dati e danneggiare i sistemi rivali. Tra i siti aggrediti vi sono quelli della Biblioteca Nazionale, del ministero dell'Istruzione Superiore e della facoltà di Scienze dell'università di Dhar El Mahraz, di Fez.

2. In differenti momenti, il segretario generale del ministero degli Esteri, Amar Belani, e il Capo di Stato Maggiore dell'Esercito, gen. Said Chengriha, hanno ricevuto, ad Algeri, il maresciallo dell'Aria Elliot Sampson, consigliere dell'Alta Difesa britannica per la regione del MENA – *Middle East North Africa* – , accompagnato da un'imponente delegazione militare. Le due parti tecniche hanno esaminato lo stato della cooperazione bilaterale anche al fine di consolidarla ulteriormente, partendo dall'addestramento delle truppe che l'Algeria potrebbe ricevere. Il giorno 8 u.s., il gen. Chengriha ha pure ricevuto il generale statunitense Michael Elliot Langley – ha incontrato anche il presidente Abdelmadjid Tebboune – , comandante dell'AFRICOM – *United States Africa Command* – , con il quale ha affrontato i temi delle sfide alla sicurezza che il continente africano deve affrontare e degli interessi comuni, compresi i modi per rafforzare la cooperazione militare tra i due Paesi.