Gian Luca Foresti,
Francesco Zucconi
(a cura di)

L'INTELLIGENCE DEL FUTURO

Tecnologie digitali e capacità predittive per i nuovi professionisti della sicurezza

FrancoAngeli

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

La versione completa dell'e-book (a pagamento) è leggibile **con Adobe Digital Editions**.

Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta **cliccando qui** le nostre F.A.Q.

Gian Luca Foresti,
Francesco Zucconi
(a cura di)

L'INTELLIGENCE DEL FUTURO

Tecnologie digitali e capacità predittive per i nuovi professionisti della sicurezza

FrancoAngeli

Il presente volume è stato realizzato grazie al contributo del Dipartimento di Scienze Matematiche, Informatiche e Fisiche dell'Università degli Studi di Udine.

Progetto grafico di copertina: Alessandro Petrini

1a edizione.

Indice

III – Social (media) intelligence

IV – ICT per la società civile

Prefazione

di *Maurizio Vallone**

Nel 1988, quando fui designato dal Capo della Polizia quale primo dirigente della neonata Sezione Criminalità Informatica del Servizio Centrale Operativo della Polizia di Stato – germoglio dalla quale fiorirà una decina di anni più tardi la Polizia Postale e delle Telecomunicazioni – il panorama dei *computer crime* nel mondo si limitava ad attacchi hacker effettuati con tecniche antesignane, quali l'invio a taluni soggetti di floppy disk che apparentemente contenevano informazioni d'interesse ma che, in realtà, inoculavano un virus che criptava i dati contenuti nel personal computer cui seguiva la richiesta di un riscatto per ottenere i codici di decrittazione.

Solo un paio di anni più tardi, con il primo embrione di rete informatica (la quale viaggiava sui doppini telefonici della SIP e che richiedeva complesse attività di sincronizzazione della velocità dei modem), cominciarono a emergere le prime forme di hackeraggio mediante l'accesso abusivo a sistemi informatici che condussero, di lì a poco, alla emanazione della normativa anti-hacker prevista dall'art. 615 ter c.p.

All'epoca, il tema sembrava riguardare pochi eletti, dotati di computer per ragioni di lavoro, e trovava sponda essenzialmente nel sistema bancario, che ambiva a dotarsi di strumenti informatici in grado di velocizzare le procedure di sportello e l'analisi dei dati per gestire i crescenti flussi finanziari.

Il primo esperimento di *social media* in Italia, invece, nasce con la realizzazione del Videotel della SIP, all'incirca nel 1992, che crea la possibilità di chattare scambiandosi messaggi di testo tra soggetti protetti da nickname; progetto tuttavia abbandonato dalla SIP nel giro di qualche anno, sia perché superato dai nuovi strumenti informatici, sia a causa dell'ingente numero di

* Direttore della Direzione Investigativa Antimafia.

truffe a cui la SIP si vide esposta a causa dell'assoluta mancanza di regole di sicurezza del sistema.

Nel corso dei successivi 30 anni, le tecnologie si sono sviluppate con una velocità che mai l'essere umano aveva visto, e oggi continuano a svilupparsi con una velocità esponenziale che non consente più di poter tracciare una linea netta tra passato, presente e futuro.

Ma la tecnologia così spinta si presta a essere utilizzata oltre che per finalità belliche anche dalle organizzazioni criminali transnazionali descritte nel presente volume. Oggi le mafie che operano al livello superiore transnazionale dei traffici e del riciclaggio utilizzano sistematicamente la tecnologia per rendere sicure le loro comunicazioni e i canali di reinvestimento e riciclaggio del denaro, spesso attraverso l'impiego di moneta elettronica, al fine di impedire il tracciamento dei flussi economici e dei carichi di stupefacente o di materie preziose.

Non solo: le Forze dell'Ordine e la magistratura devono oggi anche interrogarsi sulle implicazioni che l'Artificial Intelligence (AI) può avere sul piano della genuinità e attendibilità delle prove in un dibattimento penale o civile: basti pensare alla possibilità di creare *deep fake* assolutamente non contestabili a favore o contro un soggetto parte del giudizio, come evidenziato nel presente volume nella parte a cura di Jaime Venturini.

È dunque sul piano digitale che si combatte oggi la guerra tra le Forze dell'Ordine e le mafie, tra tecnologia al servizio del crimine e tecnologia per contrastarlo. Per farlo efficacemente, le Forze dell'Ordine hanno bisogno di conoscenza e competenze estremamente qualificate e costantemente aggiornate.

Condivido, quindi, appieno le considerazioni espresse nel presente volume da Angelo Murano circa l'importanza del progetto Professionisti inPA; a mio avviso, il progetto dovrà superare la logica dell'emergenza gestita per far fronte al PNRR e assumere una compiuta veste giuridica normativamente prevista, per assunzioni brevi o a tempo indeterminato di particolari figure specialistiche dotate di alta formazione professionale da inserire direttamente in area dirigenziale, tale da rendersi appetibile – e dunque effettivamente competitiva – per specialisti che, altrimenti, troverebbero adeguato e remunerativo sbocco professionale solo nel mondo privato.

Per formare tali specialisti, soprattutto nel campo informatico e della cybersicurezza, occorrono mirati programmi di formazione, che trovano la loro naturale e privilegiata collocazione nel mondo universitario, unico competente a svolgere il delicato compito di selezionare i migliori giovani già negli Istituti di secondo grado, offrire loro borse di studio e percorsi di specia-

lizzazione d'intesa con le Agenzie governative, avviarli a stage di formazione on the job, indirizzarli verso le stesse Agenzie o verso le aziende di riferimento del settore che collaborano con gli Enti governativi e che garantiscano loro adeguate valorizzazioni stipendiali e percorsi di upgrade.

Un grazie all'Università di Udine, al suo Magnifico Rettore il Prof. Roberto Pinton e ai Professori Gian Luca Foresti e Francesco Zucconi per la collaborazione con la Direzione Investigativa Antimafia sui temi dell'AI e della cybersicurezza.

Roma, 21 giugno 2023

Master in Intelligence & ICT: nuovi approcci per nuove professionalità

di *Gian Luca Foresti, Guglielmo Cevolin, Manuela Farinosi, Gianluigi Sechi, Carlo Tasso, Francesco Zucconi*

Il presente volume intende raccogliere una collezione di ricerche e studi nati all'interno delle prime due edizioni del Master in Intelligence & ICT del Dipartimento di Matematica Informatica e Fisica dell'Università degli studi di Udine. I contributi sono frutto di un intenso lavoro di squadra, che vede docenti e discenti protagonisti di un esperimento didattico-formativo dalle caratteristiche assai peculiari.

Prima di introdurre i singoli risultati qui raccolti, è opportuno descrivere, brevemente, le architetture che sostengono tale processo formativo; usiamo il plurale, perché, nel disegno complessivo, concorrono, mantenendo le rispettive specificità disciplinari, molte forme del sapere contemporaneo.

Il disegno complessivo è stato continuamente raffinato. Infatti, è apparso sempre più evidente, nel succedersi delle edizioni del Master, quanto i discenti, che provengono dai più svariati ambiti formativi e lavorativi, necessitino di integrare i loro strumenti cognitivi, in una visione più olistica della realtà, e che sia un poco più orientata in senso predittivo.

Abbiamo osservato che, sia i modelli intellettuali che vengono proposti nei diversi percorsi formativi di livello universitario, sia le pratiche mentali acquisite nei rispettivi ambiti lavorativi – questi ultimi anche relativi a gradi di carriera abbastanza elevati – tendono a consolidare forme settoriali di rigidità mentale e operativa, incompatibili con la poliedricità necessaria per affrontare le sfide connaturate con i rapidi cambiamenti della società odierna, prodotti, tra le altre cose, dall'uso sempre più diffuso e pervasivo delle moderne tecnologie matematico-informatiche.

Uno dei problemi che il Consiglio Scientifico del Master si è trovato di fronte è il seguente: come integrare una preparazione mirata alla gestione consapevole delle emergenti tecnologie digitali (Intelligenza Artificiale,

Machine e Deep Learning, Big Data Analysis, Cyber Security, Biometria e Gait Analysis, Web Intelligence, Text Mining, Open Source Intelligence, Crowdsource Intelligence, Augmented e Virtual Reality, ecc.), con la capacità, che un analista di intelligence deve possedere, di interpretare, a fini predittivi, la realtà?

Questa capacità interpretativa a nostro avviso non può prescindere da una formazione umanistica. Gli argomenti presentati all'interno dei moduli di storia dell'intelligence, di diritto per l'intelligence, di fondamenti di geopolitica, e di fondamenti di intelligence economica mirano, appunto, a rafforzare le basi culturali di tipo umanistico. È, infatti, per noi evidente che una capacità tecnica, ben allenata nell'attingere a un'inesauribile mole di dati, può esser valorizzata solo se si è capaci di organizzare e interpretare tali dati, sino a produrre informazioni che, nei casi più fortunati, possono fornire una conoscenza sul "come della cosa" e, in ultimo, meta spesso irraggiungibile, sul "perché della cosa".

Per favorire un'integrazione possibile tra l'ambito culturale di tipo scientifico e tecnologico, e quello umanistico, sia nella sua versione più classica che con la versione espressa nella SOCMINT (Social Media Intelligence), abbiamo costruito dei ponti didattici, basandoci, sia sui fondamenti del Ciclo dell'Intelligence, sia sul laboratorio di OSINT (Open Source Intelligence), che su specifiche attività seminariali, condotte da esperti di chiara fama, che abbiano sperimentato sul campo l'utilità, diremmo la necessità, a fini operativi, di realizzare tale integrazione.

Un altro obiettivo di forte interesse da parte del Consiglio Scientifico del Master, il cui conseguimento ha condizionato assai il disegno complessivo, è quello di trasmettere una conoscenza sufficientemente ampia per orientarsi nelle problematiche alla base della sicurezza cibernetica quali: (a) le minacce all'integrità dei sistemi informatici, molto difficili da rilevare e mitigare, basate su tecniche sempre più sofisticate di phishing, malware, ingegneria sociale e hacking; (b) le vulnerabilità dei sistemi informatici, dovute spesso a errori di programmazione, configurazioni errate, mancata applicazione di patch di sicurezza o uso di software non aggiornato; ma soprattutto (c) la mancanza di consapevolezza degli utenti delle minacce informatiche e la scarsa adozione di quelle che possono essere considerate buone pratiche di sicurezza come, per esempio, il non aprire allegati email sospetti o il non utilizzare password deboli o comunque facilmente individuabili.

Per poter conseguire tali obiettivi non è possibile né assecondare la tentazione di indebolire quella rigidità disciplinare necessaria per acquisire davvero le capacità di utilizzare in modo efficace e consapevole gli strumenti informatici

più recenti, né rinunciare a presentare, con la dovuta ampiezza e profondità, le basi di storia dell'intelligence, di diritto per l'intelligence, di fondamenti di geopolitica, di fondamenti di intelligence economica, di fondamenti della social media intelligence e di teorie della comunicazione e della ricerca sociale.

L'approfondimento di tutte le pratiche (in verità, anche dei loro presupposti teorici) relative al ciclo dell'intelligence, e lo studio assai ampio e profondo del rapporto tra intelligence e nuovi media, nella prospettiva della SOCMINT, ci hanno permesso, come sopra accennato, di plasmare un percorso disciplinare unico nel suo genere, che, senza questi due pilastri, avrebbe rischiato di favorire un ambito mentale di tipo semplicemente specialistico. Riteniamo di esser riusciti a gettare le fondamenta per poter far emergere nelle menti dei nostri corsisti un habitus mentale proattivo, capace di sopportare autoanalisi fortemente autocorrettive e di saper leggere quelle differenze, difficoltà, incongruenze, inganni, autoinganni, che l'uso di ogni modello teorico, o di qualsivoglia pratica rigidamente codificata, incontra nella sua interazione pratica con la realtà.

Per meglio collocare i contributi qui presentati è opportuno che il lettore geometrizzi i vari apporti disciplinari suddividendoli in tre gruppi. Nel gruppo I trovano posto le tecnologie emergenti e la cyber intelligence. In particolare, le nuove tecniche di machine e deep learning applicate alle operazioni cibernetiche militari, all'anomaly detection – sia nei sistemi di sicurezza tradizionali basati su sensori multipli (telecamere RGB, termiche, infrarosso, sensori radar o acustici, ecc.) sia nei sistemi di memorizzazione e trasmissione dei dati – oppure applicate alla predizione di comportamenti di gruppi terroristici basati sull'analisi in tempo reale dei contenuti diffusi attraverso social media. Trovano inoltre spazio le tecnologie basate sulla *blockchain* sia per la sicurezza delle comunicazioni e delle transazioni finanziarie sia per la prevenzione di *deep fake*. Nel gruppo II vi sono gli elementi generali di storia dell'intelligence e del rapporto di quest'ultima con l'evoluzione tecnologica, gli elementi generali del diritto per l'intelligence, i fondamenti di geopolitica, e i fondamenti di intelligence economica. Nel gruppo III abbiamo i fondamenti del ciclo dell'intelligence, quelli del rapporto tra comunicazione e intelligence e quelli tra OSINT e analisi dei fenomeni sociali.

Tutti i gruppi disciplinari, ove possibile, si appoggiano sia su tecniche laboratoriali di intelligence (OSINT, SOCMINT, HUMINT, MASINT) per l'estrazione da fonti aperte, semi-aperte, quali quelle impartite dall'ISLAB (Intelligence and Security Laboratory) dell'Università di Udine, sia su esperienze dirette maturate nei tirocini svolti presso le aziende consorziate con il Master, sia sul gran numero di lezioni seminariali impartite da figure apicali

che svolgono o hanno brillantemente realizzato nella loro pratica professionale quanto lumeggiato nelle lezioni teoriche.

Il modello pedagogico alla base del Master, affinatosi nelle successive edizioni del medesimo, prevede che le competenze informatiche, ottenute con lo studio della teoria della sicurezza cibernetica, della computer vision, della teoria dell'intelligenza artificiale (con le opportune pratiche laboratoriali) e financo con la trasmissione dei primi rudimenti della matematica binaria (gruppo I), siano mediate con la consapevolezza metodologica acquisita nel modulo di comunicazione e intelligence e nel modulo del ciclo dell'intelligence (gruppo III) per costruire conoscenze relative agli ambiti studiati dalle discipline di tutti gruppi.

L'avere il gruppo III come cornice del quadro formato dalle discipline del gruppo I e del gruppo II, rende possibile: 1) saper, consapevolmente, estrarre dati; 2) saperli organizzare in informazioni per arrivare a costruire interpretazioni significative, prodotto finale del ciclo di intelligence. Infine, tramite le discipline del gruppo III, si insegna a scrivere un report che sia utile al decisore finale. Infatti, il corsista viene guidato, da personale specializzato, a prendere piena consapevolezza del problema della trasmissione e della comunicazione del risultato di intelligence. In particolare, viene ben chiarito come il costrutto elaborato dall'analista debba rispondere a quelle ben specifiche esigenze che ne hanno sollecitano la produzione. La capacità stessa di trasferire al decisore politico, o al manager di un'azienda, utili analisi di scenario, che siano funzionali alle esigenze che hanno motivato l'attivazione del ciclo di intelligence, è anch'essa il risultato di un'autoconsapevolezza cognitiva, i cui principi generali sono trasmessi sia nel modulo di comunicazione, che in quello del ciclo di intelligence e nelle relative pratiche laboratoriali.

Naturalmente, nella pratica corrente del Master, ogni corsista privilegia nel suo percorso di tesi un ambito ben definito e persegue fini specifici.

Abbiamo suddiviso i contributi in quattro macro-aree tematiche: 1) le tecnologie dell'intelligence in ambito militare; 2) l'Intelligence Economica; 3) la Social media intelligence; e 4) l'ICT per la società civile.

Circa le tecnologie dell'intelligence in ambito militare, il contributo intitolato *Il machine learning nell'ambito delle operazioni cibernetiche militari*, di Simone Beuzer, riporta le caratteristiche che, fin dal 2016, la Nato ha individuato quali caratteristiche essenziali del dominio di guerra cibernetica. Ricordiamo, tra tutte, l'assenza di confini ben stabiliti e la sua interazione trasversale con i rimanenti quattro domini: terra, acqua, aria, spazio. Da queste peculiari caratteristiche segue l'importante conseguenza che chi in esso domina ha il controllo del campo di battaglia e può mutarne la geografia,

interdicendo l'accesso al nemico di aree considerate strategiche (Anti Access/Area Denial – A2/AD). Inoltre, attraverso il dominio cibernetico vengono amplificate le potenzialità delle Emerging Disruptive Technologies (EDT), ma soprattutto dell'IA. L'articolo fornisce una visione completa sulle operazioni cibernetiche militari di tipo difensivo, con riferimento a recenti metodologie del DoD (Department of Defense) Usa e della Nato.

Nel secondo contributo, *Anomaly detection: le prospettive dei sistemi di video-sorveglianza*, di Andrea Trovato, dopo una breve enunciazione dei principi generali alla base dell'architettura di un sistema di CVSU (Computer Vision & Scene Understanding), e una classificazione delle video-telecamere impiegate nei sistemi di video-sorveglianza, sono illustrati: il concetto di Video-Sorveglianza Attiva (AVS), sottolineandone il suo costitutivo carattere di sistema automatico, e l'importante suddivisione tra algoritmi supervisionati e algoritmi non-supervisionati. Nel lavoro viene descritto uno specifico algoritmo, che integra la struttura profonda del deep Multiple Instance Learning (MIL) con dati etichettati con recenti tecniche di Deep Learning di tipo weakly-labeled supervised. Questo approccio permette di utilizzare dataset molto vasti per la rilevazione di anomalie. Infine, il concetto di sorveglianza viene confrontato con necessità e indirizzi provenienti da esperti dell'Alleanza Atlantica.

La macro-area dedicata all'Intelligence economica si apre con un primo contributo dal titolo *La guerra ibrida: l'evoluzione del conflitto nel mondo globalizzato.* Scritto da Pierfrancesco Merlino prima della recente guerra in Ucraina, questo contributo fornisce un'indicazione circa l'evoluzione del concetto di guerra nel mondo globalizzato, con specifico riferimento all'impatto prodotto dallo sviluppo informatico-tecnologico. In questo contesto la nozione di guerra ibrida diviene centrale. Le caratteristiche della guerra ibrida, pur non andando a mutare in alcun modo la dinamica di potere sottesa a ogni conflitto, sono tali da rendere questo tipo di conflitto difficilmente inquadrabile dal punto di vista sia giuridico che militare. Appoggiandosi su parte della recente letteratura di riferimento, l'autore indica la natura profonda della guerra ibrida, nell'interconnessione delle seguenti tre caratteristiche: individuazione delle strutture e funzioni critiche di una nazione e delle rispettive vulnerabilità, sincronizzazione dei mezzi di offesa, e ricerca di effetti di non linearità. È nell'ambito della guerra economica, della competizione tra Sistemi-Paese, della difficoltà da parte dei singoli Stati di mantenere il monopolio informativo che la guerra ibrida può trovare spazi per la sua diffusione. Una volta compreso che i meccanismi economici sono essenzialmente incapaci di autoregolamentarsi, ma che, al contrario, tendono a polarizzare la forza

nella direzione di chi già possiede la forza economica e riesce a mantenere e sviluppare una superiorità tecnologica, è ben chiaro come, non la distruzione dell'avversario, ma il suo assoggettamento economico-culturale sia il vero obiettivo strategico da perseguire. A tal fine, vengono presentate alcune condizioni sotto le quali le tecnologie digitali possono svolgere un ruolo determinante per conseguire la piena vittoria strategica. Nella sua parte finale il lavoro illustra un caso tipico di guerra ibrida, dato dagli eventi del 2014, che portarono all'annessione della Crimea alla Federazione Russa.

Il secondo lavoro della macro-area sull'Intelligence economica, *Intelligence e aziende strategiche: la minaccia ibrida* di Emmanuele Pesce, accenna a una proposta decisamente innovativa: la figura dell'intelligence manager. Questa inedita figura professionale è, nei fatti, un prodotto assai compiuto, anche se, per ora, soltanto sul piano intellettuale, del Master. Per comprenderne appieno la portata bisogna leggere la componente economica della guerra in forma ibrida nel più ampio scenario dell'attuale degrado della stabilità internazionale. Nel contesto della guerra ibrida rientra, per esempio, anche la strategia multilivello attuata dalla Cina e avente come obiettivo l'acquisizione non solo di tecnologie strategiche nel comparto dell'avionica avanzata, delle infrastrutture 5G, dei semiconduttori, ma anche di competenze universitarie in ambito STEM (Science, Technology, Engineering e Mathematics). Riportando tale contesto al caso italiano, la strategia del Golden Power così come la definizione di un perimetro nazionale di sicurezza cibernetica appaiono come grandi atti strategici, che, tuttavia, per essere veramente efficaci sul terreno, debbono incarnarsi in attori aventi: 1) ben determinate conoscenze intellettuali, 2) affinate competenze nel capire i più aggiornati usi delle moderne tecnologie informatiche a base matematica, e 3) attitudini operativo-decisionali forgiate da esperienze gestionali direttamente esperimentate sulla "prima linea". In un simile contesto una figura professionale in possesso di tali caratteristiche, l'intelligence manager, può emergere solo se si effettua un cambio di paradigma, spostando il problema della sicurezza dal piano dei costi a quello degli investimenti. Per far ciò l'articolo *Intelligence e aziende strategiche: la minaccia ibrida* mostra come le funzioni di contrasto rivolte contro: a) la minaccia reputazionale, b) la minaccia cibernetica, c) la minaccia interna (*insider threat*), pur essendo attivate dalla security aziendale, per essere realmente efficaci necessitano di una profilazione e conoscenza dettagliata e strutturata di tutti i dati sensibili di un'azienda. La figura apicale e pienamente consapevole di questa conoscenza svolge, nei fatti, un ruolo di vera intelligence. Tale conoscenza contiene racchiusa in sé una parte non piccola del valore economico di un'azienda, e non solo con-

sente di prevedere potenziali situazioni di criticità, ma, se intelligentemente sfruttata, può anche trasformarsi in opportunità di business. Inoltre, la figura dell'intelligence manager potrebbe raccordarsi, condividendo i dati in modo responsabile e non lesivo degli interessi aziendali, con le strutture deputate alla sicurezza del cittadino e dello Stato. In questo modo verrebbe a instaurarsi un circolo informativo e una modalità operativa virtuosa, che andrebbe a rafforzare sia la difesa dell'azienda, che quella esercitata dallo Stato nazionale.

Il contributo *Fare intelligence in contesti sottoposti ad alta discontinuità nella loro governance* mostra un esempio, tratto da un seminario tenuto dal dottor Gabriele Martignago nella seconda edizione del master. Nel seminario i corsisti e le corsiste furono posti di fronte a interrogativi critici, quali emergono dalla vivida narrazione di chi abbia concretamente vissuto, in prima persona e in ruoli operativi strategici, situazioni attraversate da gravi discontinuità geopolitiche. In questa introduzione non possiamo che rimandare il lettore alla lettura di tale contributo che, a nostro avviso, si staglia per la profondità e la concretezza delle indicazioni in esso contenute.

La terza macro-area tematica, dedicata alla Social Media Intelligence si apre su un caso di studio che ha fatto scuola nel settore: *Social media intelligence: il caso Cambridge Analytica*. Questo contributo, di Giacomo Perrina, focalizzato sulla SOCMINT – attività conoscitiva rivolta ad acquisire e monitorare contenuti presenti sui social networking sites –, intende mostrare come l'utilizzazione di modelli interpretativi tratti dalla statistica applicata alle scienze sociali, acquisisca una forte valenza predittiva, dovuta alle possibilità di applicare le attuali tecniche di machine learning e di AI su enormi insiemi di dati, prodotti, spesso inconsapevolmente, dai fruitori dei servizi offerti dalle piattaforme informatiche. Il lavoro condotto mostra come, attraverso l'applicazione di consolidate teorie psicologiche, quali, per esempio, quelle espresse nella teoria dei *Big Five Personality traits*, sia possibile arrivare alla costruzione di modelli predittivi della personalità e dunque a una classificazione degli utenti dei social network che permetta di predire alcune tendenze ad adottare determinate forme comportamentali. Viene poi illustrato il caso di Cambridge Analytica, con particolare attenzione ai metodi utilizzati incentrati sugli studi di Michal Kosinski.

Il secondo contributo della terza macro-area tematica, dal titolo *Customer Analysis & Social Media Intelligence* di Alessandro Zuzzi, colloca l'utilizzo delle tecniche della SOCMINT nel contesto specifico dell'analisi del comportamento dei clienti di un'azienda, mostrando un concreto esempio di applicazione di metodologie apprese durante il Master, quali la "Team

Data Science Process Lifecycle". Nel lavoro vengono presentate e descritte dettagliatamente le varie fasi di una ricerca – dall'acquisizione dei dati, all'elaborazione finale di un Modello Dati, passando per la Comprensione dei dati – sui consumatori finali di prodotti dolci da forno nel periodo gennaio-agosto 2020.

L'ultimo contributo della macro-area tematica riservata alla Social Media Intelligence, *OSINT predittiva per il cyber peacekeeping* di Roberta Maisano, illustra come le tecniche di OSINT predittiva possano svolgere un ruolo importante nell'identificare potenziali attacchi terroristici o minacce alla sicurezza delle missioni di pace all'estero. In particolare, mostra come l'OSINT predittiva, attraverso l'individuazione di indicatori di situazioni potenzialmente sospette, possa essere utilizzata per monitorare attivamente i canali di comunicazione aperti, quali, per esempio, social media, forum online e altre fonti pubbliche, con l'obiettivo di rilevare segnali di possibili potenziali minacce alla sicurezza. Il presente lavoro evidenzia inoltre come grazie alle tecniche di OSINT sia possibile raccogliere informazioni su potenziali attori malevoli che potrebbero essere coinvolti in attività di cyber peacekeeping: l'analisi dei dati online, dei comportamenti passati e delle relazioni tra gli attori, consente infatti di creare profili dettagliati in grado di aiutare a identificare e mitigare minacce future.

La quarta e ultima macro-area tematica, intitolata *ICT per la Società Civile,* consta di quattro contributi. Il primo, *La tecnologia blockchain per la prevenzione dei deep fake*, chiarisce, con dovizia di informazioni, la natura algoritmica che sta dietro alla produzione dei *deep fake* e ne studia alcuni. L'autore, Jaime Venturini, parte dal paradosso che per addestrare due reti neurali in modo che una generi *deep fake*, mentre l'altra cerchi di individuare la veridicità o meno di un'immagine, si finisce per rafforzare la capacità della prima nel tentativo di migliorare le sue performance nel superare le verifiche operate dalla seconda. Alla luce quindi della sempre maggiore precisione degli algoritmi di generazione dei *deep fake*, per risolvere il problema l'autore suggerisce un approccio di contrasto più attivo, proponendo, per esempio, di certificare le immagini nel momento stesso in cui vengono create. Dato che, anche solo per ragioni artistiche, tale certificazione non dovrebbe arrivare a impedire modifiche non essenziali delle immagini, elabora un progetto, denominato Anti-DeepFake Certified, scritto in linguaggio di programmazione Python, che utilizza il modello certificatorio tipico di una *blockchain*.

Il secondo contributo dell'ultima macro-area tematica*, Convolutional neural network per il rilevamento automatico della violenza negli spazi educativi* di Erica Perseghin, presenta un nuovo prototipo di sistema integrato

a basso costo, chiamato School Violence Detection system (SVD), basato su una rete neurale convoluzionale in grado di classificare e identificare automaticamente le azioni violente negli ambienti scolastici. La rete Convolutional Neural Network (CNN) proposta è stata pre-addestrata con un modello ImageNet e un approccio di transfer learning. Per estendere le sue capacità, il dataset di addestramento della rete neurale è stato arricchito con immagini raccolte online che rappresentano studenti in ambienti scolastici. Il sistema proposto, che raggiunge un'accuratezza di riconoscimento del 95% sui dataset di test, è considerato computabilmente efficiente e a basso costo.

Nel terzo lavoro dell'ultima macro-area del libro, *Un Contributo per il change management del settore pubblico: Il progetto professionisti inPA* di Angelo Murano, la teoria della complessità fa da cornice alla costruzione di uno strumento informatico finalizzato a favorire un'allocazione e una selezione ottimale del personale della Pubblica Amministrazione (PA). Il quadro teorico di riferimento proviene dalla Teoria dei Giochi, che, con piena consapevolezza dei limiti inerenti a tale approccio, viene utilizzata per modellizzare le dinamiche conflittuali all'interno del modello organizzativo della Pubblica Amministrazione e, in particolare, per studiare il rapporto dialettico tra dinamiche istituzionali consolidate e "meccanismi emergenti" che sfidano il paradigma dominante. La risultante ottenuta da questo approccio teorico è la costruzione di uno strumento digitale, che nei fatti può diventare un vero e proprio software che PA potrebbe agevolmente utilizzare per ottimizzare il processo di reclutamento delle risorse umane e la loro collocazione nei ruoli della Pubblica Amministrazione. Alla base dello strumento digitale proposto c'è l'algoritmo di ottimizzazione multiobiettivo elaborato da David Gale e Lloyd Shapley, presentato nel corso delle lezioni del Master in Intelligence & ICT.

L'ultimo contributo, *Intelligence per il territorio: l'impatto dell'esercito italiano sul Friuli-Venezia Giulia* di Martina Cremon, presenta una importante messe di dati numerici circa le servitù militari accolte sul territorio del Friuli-Venezia Giulia (FVG). Nel lavoro è analizzata la questione degli immobili ceduti alle amministrazioni civili e le difficoltà burocratiche e legislative legate alla loro riqualificazione a uso civile. La lentezza con la quale si sta procedendo ai possibili cambi di destinazione d'uso di siti militari dismessi è, tuttavia, solo in parte collegabile sia all'onerosità della riqualificazione ambientale, che alle impattanti normative rappresentate dalla presenza di effettive servitù militari. Il lavoro classifica i corpi dell'Esercito maggiormente presenti sul territorio e i reparti che da questi dipendono e misura in maniera puntuale l'impatto economico che la presenza dell'Esercito produce sull'economia

regionale, svelando il gravissimo danno che ne potrebbe ricevere l'economia regionale stessa a seguito di un'ipotetica ulteriore diminuzione della presenza militare in FVG. Infine, è utilmente sottolineato come il turismo di tipo storico-militare e quello della guerra simulata, realizzabile in modo assai fattibile grazie all'ampiezza e numerosità di idonee strutture e a opportunamente citati esempi stranieri, possano divenire utili vettori economici, propiziati dal lunghissimo e intenso rapporto che intercorre tra il FVG e l'Esercito Italiano.

Il ruolo dell'analista di intelligence nella società civile

di *Marco Blanchini*

1. Dallo spionaggio all'analisi di intelligence

Lo studio dell'intelligence non è stato oggetto di specifici studi accademici per lungo tempo. La sua pratica, nella forma più basilare dello spionaggio, è invece di lunghissima data, tanto che quello della spia è spesso definito come il secondo lavoro più antico del mondo (Mantici, 2020). Esso ha accompagnato tutta la storia dell'umanità, sviluppandosi insieme alla conflittualità tra soggetti politici e alla pratica della guerra. La necessità di raccogliere informazioni nell'ambito bellico è stata la prima forma di intelligence ed è tuttora il significato prevalente che si associa al termine nel linguaggio comune. Nel suo celebre trattato l'*Arte della Guerra*, Sun Tzu insisteva sull'importanza dell'informazione in guerra: "se conosci il nemico e te stesso, la tua vittoria è sicura. Se conosci te stesso ma non il nemico, le tue probabilità di vincere e perdere sono uguali. Se non conosci il nemico e nemmeno te stesso, soccomberai in ogni battaglia" (Sun Tzu, VI-V secolo a.C.). Essa si configura come un'attività necessaria e inevitabile, in quanto strettamente correlata alle necessità di previsione e pianificazione. Dove c'è necessità di pianificazione politica, in tempo di guerra così come in tempo di pace, è fondamentale disporre di informazioni inserite in un quadro coerente. L'attività di raccoglierle e utilizzarle è l'attività di intelligence (Caligiuri, 2021). I due aspetti, raccogliere e utilizzare, sono strettamente correlati in un unico ciclo: il ciclo dell'intelligence appunto. Questo perché la raccolta influenza l'utilizzazione, che, a sua volta, tra i suoi obiettivi ha quello di stabilire dove e come procurarsi le prossime informazioni, in relazione ai cambiamenti di scenario percepiti. Il flusso informativo costruisce la rappresentazione dello scenario, che è inevitabilmente dinamica. La consapevolezza di come funziona questo flusso è inoltre fon-

damentale anche per sapere in che tempi e in che modalità diffondere l'informazione, divenendo un aspetto chiave anche per l'efficacia comunicativa (Clark, 2019). Le informazioni possono riguardare gli avversari, la propria stessa organizzazione, i concorrenti, partner economici e gli aspetti ambientali. L'estensione delle conoscenze necessarie dipende dalla interconnessione della comunità in questione con l'esterno. Più gli interessi della comunità si estendono nello spazio, più l'intelligence allarga il suo spazio di operatività. Quando in determinati momenti storici essa ha assunto dimensione riguardevoli ed elevata complessità, le sono stati dedicati professionisti che se ne occupassero. Per questa ragione insieme all'attività di spionaggio nel tempo vi si è aggiunta una componente di studio specifico della materia. Anche se non veniva quasi mai riconosciuta in passato come disciplina autonoma, alcuni studiosi iniziarono ad approfondire questi temi. Iniziarono a mettere assieme le informazioni utilizzando le loro competenze, tra cui quelle economiche, giuridiche e militari, per porle al servizio del decisore politico. Un esempio rilevante in questo senso lo possiamo rintracciare nella Serenissima, la Repubblica di Venezia, che già disponeva nel XVII secolo di "analisti" *ante litteram*, i quali cercavano di studiare le informazioni che potevano avere rilevanza per l'economia della Repubblica e di adeguare le decisioni alle conoscenze disponibili (Preto, 1999). La figura che si occupa di mettere assieme le diverse informazioni in un quadro coerente, utilizzabile dal decisore, è l'analista di intelligence. Oggi questa figura è quella prevalente negli apparati di intelligence più organizzati e potenti. Nella Center Intelligence Agency (CIA) americana essi rappresentano la maggioranza del personale impiegato presso l'agenzia (Steele, 2001).

L'analista ha dunque, oggi più che mai, un ruolo predominante nelle attività di intelligence. Questa evoluzione è determinata da un importante cambiamento che si è venuto a creare nel corso del XX secolo con la diffusione della così detta società dell'informazione. Con l'avvento di Internet, negli ultimi trenta anni, si è vissuto un aumento esponenziale dell'informazione disponibile, la proliferazione dei soggetti che la producono e il dissolvimento dei confini della stessa. Questa profonda mutazione riguarda il rapporto tra esseri umani e informazione. Infatti fino a pochi decenni fa le conoscenze disponibili riguardo a luoghi distanti, ma anche vicini in molti casi, erano scarse. Pochi erano i soggetti preposti all'elaborazione e/o alla distribuzione dell'informazione, dunque per gli apparati di intelligence era fondamentale disporre di persone capaci di raccogliere le informazioni sul territorio. La spia, l'informatore che viveva nel territorio, era spesso l'unico a conoscere determinate realtà e la loro evoluzione. Ora invece per moltissimi Paesi di-

sponiamo di una mole impressionante di dati e informazioni, prodotte dalle fonti più disparate, dalle quali potenzialmente possiamo conoscere moltissime cose. Il problema è che esse sono rapidamente diventate troppo numerose e disordinate per poterle utilizzare agilmente e sfruttarne il potenziale. Questo comporta che l'estrazione della conoscenza non passa più solamente dalle persone nel territorio che raccolgono gli elementi conoscitivi ancora non noti, ma passa anche dalla selezione delle informazioni utili. L'operazione richiede la formazione di una figura competente nell'analizzare le notizie, i dati e i diversi elementi conoscitivi incrociando le competenze da diversi campi del sapere: l'analista. Questa professionalità deve essere costruita con un percorso formativo *ad hoc* e il suo ruolo è destinato a crescere in ambito sia militare che civile.

Gli eventi dell'11 settembre 2001 hanno evidenziato la necessità della competenza degli analisti nell'ambito della sicurezza del Paese più potente del mondo, gli Stati Uniti d'America. Infatti fu ampiamente dimostrato, da analisi successive degli eventi, che l'intelligence americana disponeva di molte informazioni che potevano far presagire l'attacco, ma esse erano sommerse in mezzo a migliaia di altre notizie. La CIA e il Dipartimento di Stato arrivarono alla conclusione che vi fu una mancanza nella capacità di analisi nel mettere in connessione le diverse conoscenze acquisite. In particolare la carenza riguardava l'analisi delle fonti aperte, l'OSINT, da cui si sarebbero potute avere molte informazioni utili sull'attività dei terroristi e l'attualità del pericolo. Nel caso specifico di Al Qaida il problema ha riguardato la mancata considerazione di alcune informazioni confidenziali raccolte dall'intelligence dovuta a una carente attività di analisi, che avrebbe potuto permettere di dare la giusta priorità a quelle notizie (Steele, 2001).

Se da un lato la raccolta di informazioni sul campo è indispensabile per conoscere i movimenti di un gruppo o di soggetti e le loro attività, l'analisi delle fonti aperte invece permette di cogliere molti aspetti dell'evoluzione generale di una situazione politica, militare, economica o sociale. L'OSINT consente infatti di monitorare l'evoluzione del pensiero di una comunità e delle sue intenzioni, dalle quali per esempio può sorgere l'interesse di un gruppo terroristico a colpire con un attentato oppure la volontà di un leader politico di scatenare una guerra. Essa permette di avere una visione panoramica e complessiva della situazione analizzata, aspetto che è sempre più centrale nella società dell'iperinformazione, dove eventi molto distanti nello spazio possono influenzarsi vicendevolmente con estrema facilità (Benes, 2013).

Le informazioni che si possono estrarre con l'attività di OSINT sono numerosissime e saranno sempre più importanti in prospettiva con l'ampliarsi

della infosfera, termine utilizzato prima da Alvin Toffler (1988) e successivamente da Luciano Floridi (2009) per descrivere il fitto ecosistema che i mezzi di informazione vanno a creare. In questo nuovo oceano di informazioni, paradossalmente, anche i pericoli di disinformazione cresceranno (Caligiuri, 2019). Infatti vi sarà una sempre maggiore tendenza a immergersi nelle informazioni più familiari, dando meno peso a quelle che potrebbero invece essere fondamentali. Questo pericolo non riguarda solamente, né prevalentemente, il mondo dell'intelligence; invece è un pericolo reale per la società intera. La disinformazione può venire acuita dalla abnorme disponibilità di informazioni se mancano gli strumenti per comprenderla e darne la giusta collocazione nella realtà. La capacità di analisi delle informazioni è quindi un problema che va oltre gli apparati d'intelligence ma riguarda sempre di più tutti i decisori che agiscono ai vari livelli della società e in una certa misura l'intera popolazione. La realtà dell'iperinformazione è ancora più insidiosa in quanto si è evoluta, e continua a evolversi, con estrema rapidità senza lasciare il tempo alla società di comprendere le sue implicazioni (Caligiuri, 2019).

2. Oltre la sicurezza: la figura dell'analista di intelligence

Lo studio dell'intelligence diventa così un problema che va oltre la sicurezza dello Stato e i suoi apparati di raccolta delle informazioni. La capacità di maneggiare le informazioni diviene fondamentale in sempre più ambiti, in particolare nel contesto dell'imprenditoria e dell'economia, ma anche per le diverse associazioni e organizzazioni che desiderano avere un impatto sulla società. L'iperinformazione è una realtà che ci avvolge e rappresenta una nuova dimensione operativa. Possiamo sapere moltissime cose su uno sterminato numero di attori, e specularmente ogni attore ha accesso alla medesima conoscenza per raggiungere i suoi obiettivi. Dunque è inevitabile che la capacità di utilizzare l'informazione diventi fattore decisivo in svariati campi dell'agire umano, specialmente se caratterizzati dalla competizione. Per questa ragione le competenze che si apprendono nello studio dell'intelligence potrebbero e dovrebbero essere estese a settori sempre più ampi della società. Questa esigenza si pone in tutti quegli ambiti dove bisogna fare i conti con la complessità della società, dove la comprensione della realtà è necessaria al proprio agire strategico. Bisogna tenere presente che tutti, compresi i propri competitor, hanno a disposizione grandi quantità di informazioni; e se sono capaci di utilizzarle con maggiore efficienza acquisiranno un vantaggio competitivo notevole. Il vantaggio competitivo è dato dalla capacità di elaborare

strategie migliori e soprattutto di adattarle rapidamente ai cambiamenti della realtà. L'esempio più importante in questo caso è quello delle aziende che si trovano a operare sul mercato globale e dal cui andamento dipende più o meno direttamente il loro successo e la loro sopravvivenza. In questo ambito avere a fianco al decisore qualcuno capace di selezionare e interpretare le informazioni utili è un elemento che fa la differenza. Riuscire a cogliere in anticipo i cambiamenti, per rispondere prima degli altri alle esigenze del mercato, è fondamentale. L'analista di intelligence in ambito aziendale dovrebbe avere questo compito. Potremmo paragonare l'analista al consigliere del re, che prova ad avere una visione panoramica sul futuro, per dare consigli su come sviluppare la propria strategia a medio e lungo termine. Infatti se vi sono molti esperti e consulenti che aiutano un'azienda a elaborare strategie a breve termine, spesso manca qualcuno che si occupi della visione di insieme dell'azienda e ne immagini il suo futuro dopo dieci anni, mettendo assieme tutti gli elementi informativi esterni a quelli che normalmente rientrano nella quotidianità delle sue attività. Elementi informativi che riguardano l'evolvere della realtà sociale, politica ed economica, che non influenzeranno la strategia dell'azienda di lì a qualche mese, ma di lì a qualche anno. Certo queste sono le caratteristiche del bravo imprenditore lungimirante e del grande manager, ma vale la pena di formare professionisti *ad hoc* che coadiuvino il decisore nell'analisi delle informazioni di cui spesso non ha il tempo sufficiente di occuparsi in prima persona.

La figura dell'analista però trova la sua utilità anche in molti altri ambiti diversi dalle aziende, come all'interno delle associazioni e delle istituzioni che si occupano di affrontare i problemi sociali, combattere la povertà, la criminalità e l'esclusione sociale. Anche per queste organizzazioni infatti è indispensabile capire l'evoluzione della società in maniera pronta ed efficiente, mentre si trovano ad affrontare cambiamenti sempre più rapidi che solo un'attenta analisi dell'informazione può rilevare. La capacità di avere una direzione strategica a lungo termine, incide fortemente sull'efficacia delle misure sociali. Molti dei fatti che influenzeranno questa strategia vengono individuati solo se si considerano informazioni di ampio respiro, che alla lunga però rivelano profondi cambiamenti della realtà in cui l'ente in questione opera. Pensiamo per esempio a un ente che è incaricato di prendere misure contro la povertà. Deve certamente occuparsi di aiutare chi nel presente ha necessità, con aiuti alimentari e assistenza di varia natura. Nella selezione e formazione del personale, esso deve assumere persone esperte in materia assistenziale, con competenze per esempio in psicologia e con forte motivazione nell'aiutare il prossimo. Ma essere consapevoli di un'informa-

zione apparentemente esterna al proprio operare può essere decisivo nella evoluzione strategica dell'organizzazione. Per esempio conoscere l'evoluzione del mercato del lavoro e in quali settori vi saranno maggiori possibilità di collocamento nel futuro, informazioni di natura socioeconomica, reperibili da parte dell'analista consultando gli esperti. Se non risulta immediatamente utile, l'informazione potrebbe diventare importante in prospettiva strategica. Sapere dove saranno i posti di lavoro nel futuro permette all'organizzazione di affiancare al sostegno materiale ai bisognosi un aiuto aggiuntivo. Essa infatti potrebbe studiare anche strategie non per l'inserimento diretto dei lavoratori nei corsi di formazione, cosa che spetta a un'organizzazione *ad hoc*, ma orientare le persone che aiuta a percorrere la strada della formazione nella giusta direzione. Potrebbe stabilire contatti con chi si occupa di inserimento nel mondo del lavoro in pianta stabile, formando un apposito network. Questo suggerimento potrebbe arrivare dall'analista di intelligence dell'organizzazione, consultato per l'ideazione del piano strategico per gli anni a venire. La visione strategica non può essere solo una competenza degli Stati e delle grandi aziende, ma deve essere una cultura che deve estendersi anche a soggetti diversi. La figura dell'analista ne diventa una componente indispensabile.

Lo studio dell'intelligence deve dare una capacità generale all'analista di trattare l'informazione, che poi lui adatterà agli obiettivi della sua organizzazione. Per rendere l'intelligence una materia di studio è necessario delimitarne il campo individuando le esigenze a cui essa risponde. La questione riguarda il rapporto tra l'uomo e la grande quantità di informazione che per la prima volta nella storia lo immergono così copiosamente. Queste informazioni sono facilmente accessibili, il che spesso comporta un'illusione di facile conoscenza che a sua volta può portare a delle decisioni sbagliate. La comodità nel reperire informazioni in Internet e il pullulare di sedicenti esperti può far sì che si venga a creare un'errata convinzione di possedere una conoscenza riguardo a un determinato tema. All'informazione errata e approssimativa si aggiunge anche la disinformazione prodotta dolosamente e in maniera interessata. Inoltre è fondamentale considerare che i tentativi di orientare la cognizione del pubblico sono meno efficaci se basati su informazioni false o tendenziose, mentre diventano estremamente efficaci se derivati dalla selezione stessa delle informazioni fatta a monte dai diffusori. Infatti fornire delle notizie vere ma selezionate per favorire un determinato interesse è una delle tendenze più evidenti dei mass media ed è di gran lunga la forma di disinformazione più insidiosa (Lasch, 1995). Tutto ciò comporta il rischio che le decisioni vengano basate su informazioni

sbagliate, non adeguatamente interpretate oppure ignorando informazioni più utili e adatte alla situazione. Inoltre la realtà del ventunesimo secolo è soggetta a rapidi cambiamenti che richiedono frequenti aggiornamenti della propria strategia operativa. Per rispondere a queste esigenze il bagaglio tecnico degli analisti di intelligence, basato sul ciclo dell'informazione e sull'analisi delle fonti, deve essere utilizzato in sempre più ambiti. Lo studio dell'intelligence serve quindi a formare una figura professionale specifica, che deve operare non solo nel campo della sicurezza ma anche in tutti quei contesti in cui bisogna confrontarsi con la complessità delle informazioni. Nel contesto della società civile l'attività prevalente sarà quella sulle fonti aperte, anche se deve necessariamente essere integrata con le informazioni a disposizione dell'organizzazione. L'analista deve affiancare il decisore nella progettualità strategica dell'organizzazione azienda o dell'organizzazione senza scopo di lucro che sia. Affinché queste capacità possano diventare patrimonio dell'analista, esse vanno affiancate a due competenze fondamentali e trasversali: la cultura generale e la consapevolezza delle nuove tecnologie.

Sono proprio queste le due competenze che diventano base indispensabile per una corretta comprensione dell'informazione disponibile, da cui derivano un'azione e una comunicazione efficaci verso la società.

3. Il sapere orizzontale e la cultura generale: lo strumento del report

La cultura generale è la capacità di muoversi orizzontalmente tra le informazioni ovvero la capacità di affrontare campi del sapere in cui non si è esperti, riuscendo comunque a distinguere entro un certo limite le informazioni affidabili da quelle non affidabili (De Marco, 1983). Un'organizzazione che deve prendere decisioni in una realtà complessa necessita di elaborare un'adeguata strategia. Questa operazione richiede di raccogliere e interpretare rapidamente informazioni per le quali sono necessarie competenze diverse. Spesso non è possibile avere tutte queste competenze all'interno dell'organizzazione stessa, quindi è importante sviluppare la competenza di sapere dove trovare le informazioni appropriate. Non è possibile diventare esperti di ogni materia, dato che la conoscenza verticale è diventata estesissima in ogni campo. Però è possibile sviluppare la capacità di individuare le fonti competenti da cui attingere informazioni sulle tematiche di interesse. Capire dove sono gli esperti e di chi fidarsi e in quale misura non è affatto qualcosa di scontato, soprattutto per via del moltiplicarsi delle fonti da un lato e dalla sempre maggiore complessità

della società dall'altro. Questa capacità di selezionare le fonti riguarda il sapere orizzontale, ovvero quel sapere che a sua volta permette di orientarsi all'interno dei complessi e approfonditi saperi verticali, che inevitabilmente non si possono approfondire tutti esaurientemente. Per affrontare questo problema è necessario acquisire una robusta cultura generale. La cultura generale dell'analista vai intesa come presupposto necessario alla capacità di previsione, infatti chi capisce a quali fonti attingere e comprende quali sono le conoscenze di sintesi trasmesse dagli esperti, in particolare distinguendo gli elementi che essi ritengono più rilevanti, riuscirà a fare previsioni migliori sul futuro e dunque a elaborare strategie più efficaci.

All'analista viene richiesto di approfondire testi divulgativi dall'alto valore informativo, nelle discipline che possono risultare utili nelle decisioni dell'organizzazione. In particolare quelle materie delle scienze sociali come psicologia, sociologia e scienze politiche che aiutano a orientarsi nella società e nei suoi cambiamenti. In generale per l'analista è fondamentale allenare l'elasticità della mente, con un sistematico approccio all'interdisciplinarietà. Tale approccio richiede di leggere testi diversi nel corso della propria formazione per migliorare la propria visione panoramica sull'esistente e abituarsi al confronto continuo con argomenti nuovi. Inoltre all'analista è richiesto di fare un importante lavoro su se stesso, per capire quali possono essere i propri errori nell'approcciarsi all'informazione e come correggerli. In questo campo sono fondamentali le recenti scoperte della psicologia comportamentale e del funzionamento dei bias cognitivi (Taversky, 1983). Le ricerche portate avanti da psicologi come Daniel Kahneman permettono di conoscere meglio noi stessi e i nostri errori quando effettuiamo delle analisi sulla realtà. La psicologia comportamentale e cognitiva infatti hanno mostrato come spesso nelle nostre decisioni siamo ingannati da ragionamenti precostituiti, per via dei quali diamo delle risposte senza utilizzare efficientemente le nostre capacità analitiche (Kahneman, 2013). Uno dei compiti dell'analista in un'organizzazione è quello di istruire se stesso, anzitutto, ma anche gli altri su queste problematiche per migliorare l'efficienza strategica di tutti i componenti.

Nella quotidianità la figura dell'analista dentro l'organizzazione ha il compito di raccogliere sistematicamente informazioni che possano influire sulle decisioni dell'organizzazione, soprattutto quelle appartenenti a campi del sapere dove l'organizzazione non possiede esperti specifici. Per esempio all'interno di un'azienda siderurgica, l'analista di intelligence dovrebbe monitorare questioni come la geopolitica, l'evoluzione della sensibilità ambientale nella politica e le problematiche che possono influire sul prezzo dell'energia. In questi diversi campi trovare degli esperti affidabili e seguire l'evoluzione

delle informazioni, costruendo dei report che aiutino i manager a sviluppare strategie reattive nei confronti degli eventi che si profilano all'orizzonte. Certamente la cultura dell'analista varia a seconda dell'organizzazione, ma si distingue per la capacità di fare approfondimenti interdisciplinari, che si adattano all'evolversi della realtà. Una certa tematica può diventare più rilevante in un certo contesto rispetto a prima, quindi va individuato questo fatto in tempo e devono venire raccolte le relative informazioni utili. Tutte quelle necessità conoscitive che ora sono affidate per lo più alla cultura generale dei manager e alla loro sensibilità personale potrebbero essere unite nella figura dell'analista che si dedica a questa attività a tempo pieno. Il report di intelligence diventa così un documento centrale per l'azienda, in quanto ne orienta non solo le scelte, ma anche la cultura stessa dei manager, che vi trovano spunti per ampliare le proprie conoscenze. Come suggeriscono gli studi di management sulla complessità, la migliore reazione che può avere un'organizzazione all'aumentare della complessità esterna è aumentare la propria complessità interna. Infatti per fronteggiare nuove problematiche è necessario rendere più articolata la pianificazione delle proprie attività e della propria strategia. Questo si può ottenere da un lato creando nuove unità operative che siano specificatamente dedicate alle nuove sfide da affrontare, dall'altro aumentando competenze e sinergie nell'organizzazione (De Toni e De Zan, 2015). L'analista in questo senso aumenta la complessità introducendo in maniera sistematica nuove informazioni, visioni ed elementi di riflessione all'interno dell'organizzazione.

4. Le sfide della tecnologia

La conoscenza dell'evoluzione della realtà tecnologica è fondamentale in quasi ogni settore della società, salvo pochissime eccezioni. La tecnologia influenza la comunicazione, la percezione della realtà, i contesti di socializzazione e sempre di più i contesti lavorativi. La tecnologia secondo molti cambierà radicalmente i lavori del futuro (Klaus, 2019), chiedendo nuove competenze e rendendo desuete alcune di quelle che oggi sono centrali nel mercato del lavoro (Brynjolfsson e McAfee, 2016). La tecnologia e il suo utilizzo sono già oggi alla base di molte inuguaglianze economiche, tra chi ha le conoscenze e la possibilità di utilizzarla e chi ne rimane escluso. Tra chi la controlla, la genera e riesce a utilizzarne le informazioni e chi invece la subisce passivamente. I beni immateriali diventano ogni giorno più centrali nel determinare la ricchezza di una nazione o di un'azienda

(Haskel e Westlake, 2018). La capacità di produrli determina il vantaggio competitivo in economia così come in ambito militare. Il rapporto tra tecnologia e informazione è strettissimo, quasi simbiotico. La tecnologia permette di avere e produrre più informazioni. Le informazioni producono idee che a loro volto migliorano la tecnologia. In questo circolo virtuoso si modificano vari aspetti della società, sempre più velocemente. Le criticità però sono numerose, da diversi punti di vista. Questo processo crea disuguaglianze sia cognitive che economiche, inoltre la sua evoluzione è troppo rapida perché ne vengano comprese subito le implicazioni, ed è dunque estremamente difficile per la società adattarsi in tempo al cambiamento. La scomparsa di posti di lavoro, per esempio, non sempre viene prevista dai decisori politici e gli adattamenti potrebbero non essere tempestivi. In mano a regimi non democratici o a compagnie private la tecnologia può assumere aspetti decisamente inquietanti, come il sistema di credito sociale in Cina realizzato con l'applicazione su larga scala dell'intelligenza artificiale (Seehusen, 2021), o l'uso discutibile dei dati personali in campagna elettorale che è emerso nel caso Cambridge Analytica (Kaiser, 2019). Su questi e molti altri aspetti manca il tempo di riflettere ed è ancora più difficile prenderne la giusta consapevolezza. Capire il mondo della tecnologia, che non implica l'essere un esperto verticale su un determinato ambito tecnologico, ma invece conoscere a grandi linee le tendenze della tecnologia e il loro probabile impatto sul futuro della società. Questa conoscenza deve essere assolutamente acquisita dall'analista di intelligence. Il suo compito è cercare di comprendere e, per quanto possibile, prevedere come l'espansione della tecnologica dell'informazione potrà influire nell'ambito di operatività della sua organizzazione. Questa forma di conoscenza, riguardante le implicazioni sociali della tecnologica e come tenersi aggiornati su di esse, diventa sempre più preziosa. Le organizzazioni che riescono ad assimilare in fretta questo genere di informazioni possono adeguarsi con più facilità ai cambiamenti e avranno quindi più possibilità di emergere o di sopravvivere.

Inoltre va anche rilevato un altro aspetto dell'evoluzione tecnologica in cui le competenze orizzontali dell'analista di intelligence possono risultare quanto mai utili: il fenomeno della open innovation. L'*open innovation* è un nuovo approccio all'innovazione aziendale e non, sia tecnologica che organizzativa, che si basa sul principio, enunciato da Chesbrough (2003, p. 12), che "le conoscenze utili sono ora presenti in tutta la società. Nessuna impresa ha il monopolio delle grandi idee, e tutte, non importa quanto efficaci al proprio interno, hanno bisogno di collaborare intensamente ed estesamente con le reti e le comunità della conoscenza". La questione riguarda la grande