



GUARDIA DI FINANZA
SCUOLA DI POLIZIA ECONOMICO-FINANZIARIA

Annali

32

*A CURA DEGLI UFFICIALI DEL 48°
CORSO SUPERIORE DI POLIZIA ECONOMICO-FINANZIARIA*

**LA SICUREZZA NELLE NUOVE
TECNOLOGIE**



FEBBRAIO 2021

PREFAZIONE

Il cambiamento determinato dalla *digital transformation* pervade ormai tutti gli ambiti della società attuale ed il governo di tale processo è la più affascinante, complessa e persistente sfida del nuovo millennio.

Il *cyberspace* costituisce il nuovo territorio di confronto tra sovranità politica, sovranità economica e tutela degli individui. Protezione delle infrastrutture critiche, salvaguardia dei principi democratici e di libertà, difesa dalle minacce cibernetiche, reazione alle nuove forme di ingerenza: questi sono solo alcuni dei punti di contatto - e di potenziale contrasto - tra un'idea di Stato (e di sovranità) ancora radicata nelle categorie del pensiero analogico e una realtà rivoluzionata dall'innovazione digitale.

La capacità di comprendere in anticipo e, conseguentemente, di saper affrontare i radicali cambi di paradigma nell'ambito dei nuovi equilibri (nazionali ed internazionali), derivanti dalla trasformazione in atto, rappresenta una delle principali competizioni evolutive per le Istituzioni nazionali. Proprio l'ambizione di rispondere in maniera proattiva a questa necessità ha portato la Guardia di Finanza a sviluppare, attraverso il suo Polo addestrativo d'eccellenza, un percorso di formazione specialistica sulla *cybersecurity*.

Con l'introduzione della materia "La sicurezza nelle nuove tecnologie", la Scuola di Polizia Economico-Finanziaria istituisce, per prima in un contesto di FF. AA. e di FF. PP., un insegnamento organico, in grado di coniugare l'analisi tecnica dei fenomeni e delle criticità del *cyberspace* con la dimensione economica, l'approfondimento giuridico e l'approccio operativo che contraddistinguono il Corpo della Guardia di Finanza.

Grazie ad una visione strategica, analitica e di proiezione, l'Istituto assicura il potenziamento di conoscenze specialistiche e di alte competenze, alle quali si aggiunge adesso anche la *cybersecurity*. Ed è proprio attraverso lo sviluppo della cultura digitale che sarà possibile perseguire, in maniera ancor più efficace, i fini di Polizia Economico-Finanziaria e tutelare la Sicurezza Nazionale nell'ecosistema delle reti.

La prima grande condivisione metodologica conseguita con il nuovo insegnamento è stata quella di superare la convinzione che la *cybersecurity* fosse materia dei (e per) soli informatici, costituente una mera declinazione e gestione pratica (grazie al progresso tecnologico) di rapporti, relazioni, istanze e dinamiche tradizionali.

Al contrario, la *cybersecurity* è materia interdisciplinare e di responsabilità collettiva che necessita di una visione integrata: tramite la consapevolezza tecnica e dei fenomeni, consente la comprensione economica degli stessi ed il relativo inquadramento normativo internazionale, sovranazionale e domestico.

Sulla base di tali premesse, il nuovo insegnamento fornisce, innanzitutto, lo strumentario concettuale per superare visioni risalenti sulla cybersicurezza: partendo dalla dicotomia rivoluzione digitale-sovranià analogica (che vede oggi nel rapporto tra *big companies* e Stati sovrani la più lampante e attuale delle criticità), si è introdotto il concetto di “*security* come contesto”, rimarcando la distinzione tra vulnerabilità sistemiche e comportamentali, da cui ogni realtà è tenuta a difendersi.

La *cybersecurity* non è, infatti, preoccupazione solo di grandi imprese ed istituzioni, ma anche degli individui, costretti a misurarsi con la propria identità e reputazione digitali, beni preziosi da salvaguardare: e ciò anche (e soprattutto) rispetto ai rischi per il naturale sviluppo dei processi democratici, messi a repentaglio dalle *fake news* e, in maniera meno evidente ma non meno pericolosa, dall’uso incontrollato di algoritmi, processi automatizzati e sempre più diffuse forme clandestine di ingerenza.

L’esistenza e la partecipazione nella rete, l’affermazione di una identità ancor più rilevante e sicuramente più fragile di quella fisica (l’identità digitale) necessitano della costruzione di diritti nuovi, o meglio definiti in ragione dell’ecosistema digitale e non per “analogia analogica”. Solo attraverso il riconoscimento di una vera e propria cittadinanza digitale (la “*netizenship*”) è possibile proteggere diritti ed attribuire responsabilità, in una società intangibile che appare essere ancora terra di nessuno.

Il cyberspazio, inoltre, non è limitato alle (più o meno) volontarie e consapevoli interazioni umane attraverso dispositivi, ma ricomprende il sempre più fitto tessuto di relazioni tra macchine, strutture ed infrastrutture interconnesse: internet delle cose (*IoT*), intelligenza artificiale, *smart cities*, etc., sono solo alcuni degli esempi concreti che la quotidianità offre. Un universo digitale sempre più in espansione, anche grazie alla tecnologia 5G, terreno di confronto non solo in materia di investimenti economici e allocazione di risorse, ma anche riguardo ai rischi nelle relazioni tra Paesi e per la Sicurezza Nazionale.

Proprio il tema dei rapporti tra Stati sovrani e nuove forme di conflittualità è al centro della sezione di approfondimento sulla *cyberwarfare*: il *cyberspace*, infatti, è a tutti gli effetti il contesto militare logico ed operativo di difesa e di attacco, ascrivibile al c.d. “*fifth operational domain*”. In questo teatro di confronto permanente e granulare (tra *State sponsored cyber attacks*, tecniche di *cyberintelligence* e *advanced persistent threats*) è difficile ricorrere al tradizionale diritto dei conflitti armati per regolare i rapporti tra gli Stati.

E se il tema citato parrebbe appartenere alla sfera patologica delle relazioni, la gestione dei *big data* (non solo nell’ottica di protezione, ma in primo luogo in termini di *data value* e *data governance*) e la loro patrimonializzazione rappresentano un elemento centrale e fisiologico nell’analisi della *digital economy* e delle sue caratteristiche. Proprio nel momento in cui la ricchezza economica del pianeta si trasferisce dal mondo fisico a quello digitale, i dati ne rappresentano il valore più grande, e la redistribuzione di questo il tema più urgente e complesso.

In una dimensione così vasta e sfaccettata come quella del *cyberspace*, numerosi sono i fenomeni criminali: la sezione di approfondimento del *cybercrime* è orientata all’analisi concreta delle principali condotte illecite, sia direttamente derivanti da crimini commessi in rete (si pensi al *ransomware*), sia legate all’agevolazione ed evoluzione di condotte delittuose tradizionali (come il riciclaggio e l’autoriciclaggio tramite criptovalute, *mixer* e *tumbler*; oppure il traffico di armi, di farmaci e stupefacenti sui *marketplaces* nelle *darknets*). Lo stesso cyberterrorismo risente di questa duplice natura: la rete è, da un lato, l’*hub* ideale in cui radicalizzare i soggetti più esposti e vulnerabili (si pensi alle *echo-chambers* dei *social network*), dall’altro lo strumento sicuro tramite cui finanziare le campagne di odio e le organizzazioni terroristiche (si pensi all’uso distorto di *crowdfunding* e *cryptocurrencies*).

In questo mondo sommerso ed entropico, le FF. PP. non solo devono sapersi orientare, ma devono essere anche in grado di ricorrere (nel rispetto di regole e principi nazionali e sovranazionali) ai mezzi di investigazione resi disponibili dall’innovazione tecnologica: captatori informatici, perquisizioni digitali, tecniche di *digital forensics*, *hacking* etico, *private enforcement collaboration* sono ormai i capisaldi di qualsiasi indagine di polizia o attività di prevenzione e di *intelligence*. Si è pertanto cercato di fornire la più seria consapevolezza rispetto all’importanza delle nuove tecniche investigative e alla rilevanza del

rispetto di standard e protocolli di sicurezza, sia in termini di garanzie dei diritti degli individui che di efficienza investigativa e di salvaguardia del materiale raccolto.

In questo appassionante viaggio nel *cyberspace*, la solida preparazione e l'importante esperienza degli Ufficiali Frequentatori del Corso Superiore, unitamente allo straordinario entusiasmo e spirito di iniziativa e ricerca, hanno reso il vasto percorso di approfondimento dinamico e, al contempo, verticale: il risultato è il presente volume, raccolta ad alto contenuto specialistico e di grande valore delle ricerche realizzate.

La lungimiranza con cui la Guardia di Finanza ha voluto dotarsi di un nuovo insegnamento non tradizionale, costruendone visione generale e complessità particolare, è un vero modello di riferimento istituzionale per il confronto con la *digital transformation*.

PROF AVV. ROBERTO DE VITA