



GUARDIA DI FINANZA
SCUOLA DI POLIZIA ECONOMICO-FINANZIARIA

Annali

38

49° Corso Superiore di Polizia Economico-Finanziaria

LA SICUREZZA NELLE NUOVE TECNOLOGIE

***CYBERSECURITY E ARTIFICIAL INTELLIGENCE:
NUOVI SCENARI E PROSPETTIVE
INVESTIGATIVE NEL DIGITAL DOMAIN***



LUGLIO 2022

A CURA:

Ten. Col. Daniele LA GIOIA
Ten. Col. Giuseppe DINOI
Ten. Col. Girolamo FRANCHETTI
Ten. Col. Emilio PALERMO
Ten. Col. Diego SERRA
Ten. Col. Paolo PETTINE
Ten. Col. Marco STELLA
Ten. Col. Giuseppe EVANGELISTA

DOCENTE TITOLARE DELLA MATERIA:

Prof. Avv. Roberto DE VITA

Editing

FIN. SC. MARIA ALESSANDRA SPECIALE

Stampa

MAR. NELLO CORRITORE
AP. QS ROCCO S. RECUPERO
APS. QS GIANLUCA BERNARDINI

INDICE

PREFAZIONE	1
PREMESSA	5

CAPITOLO I

L'ESIGENZA DI AFFERMARE NUOVE FORME DI SOVRANITÀ NEL CONTESTO DELL'EMERGENZA COVID-19, ALLA LUCE DELL'ACCELERAZIONE DIGITALE E DELLE CORRELATE NUOVE MINACCE

1. Il principio di sovranità e la sua connotazione spaziale.....	1
2. La <i>governance</i> del Web fin dalle sue origini. Il modello americano e quello cinese: due approcci antitetici	2
3. Il cyberspazio e la sua dimensione "a-spaziale". Dalla <i>governance</i> tecnica alla <i>governance</i> politica di internet.....	4
3.1 Le connotazioni strutturali del cyber-spazio ed il ruolo delle Digital Companies	5
4. La rivoluzione digitale: un'opportunità per la criminalità economica e organizzata	7
4.1 La fisionomia del cybercriminale	9
4.1.1 Il cybercrime as a service.....	12
5. I riflessi dell'emergenza pandemica COVID-19 sulle condotte criminali <i>cyber-oriented</i>	15
5.1 L'analisi dimensionale del fenomeno nel contesto dell'emergenza COVID-19 .	19
6. L'aggressione alle infrastrutture critiche. Gli attacchi indirizzati verso l' <i>Healthcare Sector</i>	21

CAPITOLO II

L'ISTITUZIONE DELL'AGENZIA PER LA CYBERSICUREZZA. PERIMETRO DI OPERATIVITÀ

1. L'evoluzione della strategia nazionale in ambito <i>cyber</i>	25
2. L'Italia e la difesa cibernetica	26
3. Il quadro legislativo e istituzionale italiano	27
4. La normativa nazionale in materia di cybersicurezza	27
5. <i>Cyber defence</i> , le sfide sul campo in tempi drammatici di cronache dalla guerra ibrida....	31
6. Le peculiarità del dominio digitale	33
7. Il ruolo della guardia di finanza, quale polizia economico finanziaria, nell'ambito del piano strategico per la cybersicurezza	35

CAPITOLO III

ANALISI DI SCENARIO E LINEE EVOLUTIVE DI TENDENZA

1. Il mondo delle reti oscure: i cripto-mercati.....	37
1.1. Modelli di mercati neri della rete	39
1.2. Prodotti e servizi	42
1.2.1. Droga	43
1.2.2. Falso Documentale	44

1.2.3.	Banconote false e carte di credito.....	45
1.2.4.	Armi.....	45
1.2.5.	Malware.....	46
1.3.	Gli altri illeciti nelle darknet	46
1.4.	Opportunità criminali nel tempo della pandemia da Covid-19.....	48
1.4.1.	Produzione, traffico e uso di sostanze stupefacenti	49
1.5.	Darkweb in numeri.....	50
2.	Linee evolutive di maggiore tendenza	52
2.1.	Rafforzamento della sicurezza operativa del crimine	52
2.2.	Incremento dell'offerta di armi e di ransomware.....	53
2.3.	Polverizzazione e mobilità degli utenti	54
2.4.	Nuove criptovalute e servizi di non-cooperative swapping	55
2.5.	Infrastruttura “grigia” a protezione delle reti criminali	56

CAPITOLO IV

TIPOLOGIA DEI *BLACK MARKET*

1.	Premessa: <i>Clear Web</i> , <i>Deep Web</i> e <i>Dark Web</i>	59
1.1	TOR project.....	61
1.2	TLD: lo “speciale” dominio “.onion”	62
2.	<i>Black market</i> : caratteristiche e peculiarità	66
2.1	Beni e servizi.....	69
2.2	Multisig o Trusted market.....	71
2.3	Escrow market.....	72
2.4	“Finish early” market.....	72
2.5	Invite/Referral market.....	73
2.6	Modalità di scambio, transazioni e pagamenti.....	74
3.	Mercati e <i>Vendor</i> attivi	75
3.1	Black market e azioni degli utenti.....	75
3.1.1	Motivazione dell'evoluzione di un black market	77
3.1.2	Interesse per il Dark Web ed i black market	77
3.1.3	Effetti migratori degli utenti dei black market	79
3.2	Acquisti nei black market	81
4.	Sviluppi e tendenze future dei <i>Black market</i>	82
4.1	Mercato degli NFT e connessioni con i black market	83
4.1.1	Wash trading.....	85
4.2	Livello di maturità dei black market	86
5.	Oscuramento e rimozione dei contenuti illeciti <i>online</i>	87
5.1	Il nuovo Regolamento UE 2021/784	88
5.2	Limiti per i black market.....	88

CAPITOLO V

ANALISI DI CONTESTO DEL RICICLAGGIO DI DENARO IN AMBITO
SOVRANAZIONALE E DOMESTICO

1.	Il fenomeno del riciclaggio nel contesto internazionale ed europeo	89
----	--	----

1.1 Il contesto internazionale	89
1.2 Il contesto europeo	93
2. Il riciclaggio nel contesto domestico: Analisi delle dimensioni del fenomeno	95

CAPITOLO VI

L'ATTUALE CONTESTO TECNOLOGICO DEL SISTEMA FINANZIARIO ITALIANO

1. Le nuove tecnologie applicate al settore finanziario italiano	101
1.1 Premessa: la "Regulation Technology" (regtech) e la "Supervisory Technology" (suptech) nel settore finanziario	101
1.2 Analisi degli investimenti nelle nuove tecnologie operati nel settore finanziario italiano	105
2. Le applicazioni suptech domestiche sviluppate e utilizzate nel settore AML/CFT ..	111

CAPITOLO VII

LO SVILUPPO DI SOLUZIONI DIGITALI PER AML/CFT BASATE SULL'INTELLIGENZA ARTIFICIALE: OPPORTUNITÀ E PROBLEMATICHE CONNESSE ALL'IMPLEMENTAZIONE DEI MODELLI ATTUALI

1. I dati prodotti dal sistema AML/CFT domestico sulla base della normativa vigente	120
1.1 Le segnalazioni di operazioni sospette	121
1.2 Le segnalazioni antiriciclaggio aggregate	125
1.3 Le comunicazioni oggettive	127
2. Le sfide di carattere normativo	129
3. Le sfide di carattere operativo	130
4. Considerazioni finali: le prospettive di sviluppo del modello AML/CFT nel peculiare contesto nazionale	131

CAPITOLO VIII

DIGITAL EVIDENCE E DIGITAL FORENSICS

1. Digital evidence e digital forensics	137
2. Cybercrimes e normativa nazionale	141
3. Reati economico-finanziari che non costituiscono cybercrimes in senso stretto.	146
4. recenti proposte e novità normative sovranazionali nel contrasto alla criminalità informatica	147
5. L'antiforensics	150
5.1 Il data hiding	151
5.2 La tool's weakness	152
5.3 L'investigator's weakness	153
6. La cyber intelligence	154
7. La ricerca delle evidenze digitali	158
7.1 Mobile Forensics & Investigation	159
7.2 Cloud forensics & investigation	160
7.3 IoT Forensics & Investigation	161
7.4 Ispezioni e perquisizioni informatiche	162

7.4.1 Le perquisizioni online	166
7.5 I sequestri informatici	168
7.6 L'acquisizione dei dati del traffico: sequestro di corrispondenza o intercettazione telematica?	173
7.6.1 L'acquisizione dei dati del traffico presso ISP esteri e il nuovo concetto di cooperazione internazionale	175
7.6.2 ISP nazionali e data retention.....	178

CAPITOLO IX

LE NUOVE FRONTIERE INVESTIGATIVE

1. Le Nuove frontiere investigative	181
1.1 Audio Processing	182
1.2. Visual Processing.....	183
1.3. Resource Optimization	184
1.4. Natural Language Processing	186
2.Problematiche etiche collegate all'utilizzo dell'intelligenza artificiale nei sistemi giudiziari	187
2.1.La Carta Etica della Commissione Europea per l'efficienza della giustizia (CEPEJ)	187
2.2 Le iniziative assunte dalle Istituzioni dell'Unione Europea	191
3. Cenni sull'utilizzo dell' intelligenza artificiale in chiave predittiva delle condotte delittuose.....	193
BIBLIOGRAFIA	197
SITOGRAFIA.....	203