



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

A CURA

TEN. COL. PIERGIORGIO VANNI
TEN. COL. FILIPPO CAPINERI
TEN. COL. GERARDO MARTINELLI
TEN. COL. CLAUDIO MOLINARI
TEN. COL. GIANLUCA FORCINA
TEN. COL. GAETANO MUCCIACCIO
TEN. COL. MICHELE VIDONI
TEN. COL. FABRIZIO MANCA

DOCENTE TITOLARE DELLA MATERIA:
PROF. AVV. ROBERTO DE VITA

EDITING
FIN. BIAGIO COLONNA

STAMPA
BRIG. C. QS EMILIO LAURIOLA
APS. QS NELLO CORRITORE
APS. QS ROCCO RECUPERO
APS. QS GIANLUCA GIOVANNETTI

INDICE

PREFAZIONE.....	I
PREMESSA.....	V

CAPITOLO I

IL 5G: IMPATTO ECONOMICO E CRITICITÀ PER LE ATTIVITÀ DELLE FORZE DI POLIZIA

1. 5G: La quinta generazione della connettività.....	1
2. L’impatto economico della rete 5G.....	6
2.1 Impatto economico dell’esclusione di soggetti extra UE nella fornitura della componentistica 5G.....	10
3. Opportunità e vulnerabilità delle reti 5G. Valutazione e gestione dei rischi.....	11
3.1 La “Road Map” Europea: dalla raccomandazione della Commissione del 26 marzo 2019 alla Comunicazione della Commissione del 29 gennaio 2020.....	13
3.1.1 <i>La raccomandazione del 26 marzo 2019</i>	13
3.1.2 <i>La relazione della valutazione dei rischi coordinata a livello UE</i>	15
3.1.3 <i>Pacchetto di strumenti UE sulla cybersicurezza del 5G</i>	17
4. Criticità del 5G connesse alle attività delle forze di polizia.....	19
4.1 Crittografia end-to-end nell’ambito dell’intercettazione legale.....	21
4.2 Identificazione e localizzazione degli utenti.....	22
4.3 L’architettura Virtuale e Frammentata.....	23
4.4 Funzione NFV	24
4.5 IoT e Genuinità della Prova.....	26
5. Conclusione.....	28

CAPITOLO II

VULNERABILITÀ DELLE RETI 5G E RESILIENZA CIBERNETICA

1. La classificazione dei rischi e delle minacce.....	29
1.1 Le vulnerabilità del 5G.....	31
1.2 Gli <i>assets</i> coinvolti nel panorama 5G.....	37
1.3 Le minacce.....	40
2. Gli autori degli attacchi: profili soggettivi e motivazioni.....	43
3. Le strategie di difesa: il quadro italiano.....	46

3.1 L'estensione al 5G del c.d. "golden power"	50
3.2 Il perimetro di sicurezza nazionale cibernetica.....	51
3.3 Il <i>Computer Security Incident Response Team (CSIRT)</i> italiano.....	53
4. Prospettive evolutive post pandemia.....	54

CAPITOLO III

BIG DATA E DECISION MAKING: IL TRASFERIMENTO DELLA SOVRANITÀ DAL PUBBLICO AL PRIVATO

1. Inquadramento generale.....	57
2. La crisi di sovranità: dalle multinazionali al ruolo degli <i>over the top</i>	58
3. Il diritto di accesso a internet, la sovranità nella rete e le finalità degli <i>over the top</i>	61
4. I big data, l'intelligenza artificiale e opportunità di sviluppo.....	64
5. L'utilizzo dei big data rispetto al problema della sovranità.....	69

CAPITOLO IV

DATA VALUE E DATA GOVERNANCE

1. Inquadramento generale.....	73
1.1 The Internet of Things.....	75
1.2 L'Intelligenza Artificiale.....	76
2. La patrimonializzazione dei dati: il nuovo mercato digitale.....	78
2.1 Data Value.....	81
2.2 L'approccio fiscale alla nuova digital economy.....	84
2.3 La tutela dell'utente: dalla protezione dei dati personali... ..	88
2.4 ...al contrasto di pratiche commerciali scorrette.....	92
3. <i>Data Governance</i> : la rilevanza della gestione del dato a livello della singola impresa.....	94
3.1 Una strategia europea per la gestione dei dati.....	95

CAPITOLO V

CYBERSPACE E CYBERCRIME

1. Il <i>cyberspace</i> : analisi di contesto.....	101
1.1 Il <i>cyberspace</i> : la quinta dimensione della conflittualità e il cybercrime.....	102

2. Il <i>cybercrime</i> : inquadramento giuridico.....	104
3. Il <i>cybercrime</i> : analisi di contesto.....	106
3.1 L'ENISA e l'elenco delle prime 15 minacce.....	107
4. L'Europol e L' <i>Internet Organized Crime Threat Assessment 2020</i>	109
5. L'Europol ed il SOCTA 2017.....	111
5.1 Il <i>cybercrime</i> come <i>cyber organized crime</i> : il modello Caas.....	111
5.2 Il riciclaggio quale “ <i>motore</i> ” della criminalità organizzata.....	112
5.3 Il riciclaggio e i <i>new payment methods</i>	113

CAPITOLO VI

CRYPTOCURRENCIES E CYBER MONEYLAUNDERING

1. Valute virtuali e Criptovalute: la direttiva 2018/843/UE e il D.Lgs. 231/07.....	115
2. Il <i>Bitcoin</i>	116
3. Il <i>Bitcoin</i> : <i>mining</i> , <i>blockchain</i> e crittografia.....	117
4. Il <i>mixing</i> e i <i>privacy-enhanced wallet services</i>	118
5. La qualificazione giuridica dei <i>crypto asset</i>	120
6. Gli usi legittimi.....	122
7. I rischi potenziali.....	124
7.1 L'EBA, l'ESMA e l'EIOPA.....	125
7.2 La Banca d'Italia.....	126
7.3 I rischi di riciclaggio e di autoriciclaggio.....	127
8. Il <i>cyber moneylaundering</i>	128
9. I <i>crypto asset</i> e i reati di riciclaggio e di autoriciclaggio	130
10. L' <i>exchanger</i> ed il <i>wallet provider</i> : possibili profili di rilevanza penale.....	135
10.1 La rilevanza penale della condotta.....	135
10.2 Il titolo di reato: riciclaggio o concorso nell'autoriciclaggio.....	137

CAPITOLO VII

RANSOMWARE: LE VULNERABILITÀ ORGANIZZATIVE E SISTEMICHE

1. Premessa.....	139
2. <i>Ransomware</i> : definizione e contesto di riferimento.....	141
3. Tipologie di <i>ransomware</i>	144
3.1 Il <i>crypto-ransomware</i>	145
3.2 Il <i>locker ransomware</i>	145

4. Esempi di <i>ransomware</i> maggiormente noti.....	145
4.1 <i>CryptoLocker</i>	145
4.2 <i>Troldesh</i>	146
4.3 <i>Locky</i>	146
4.4 <i>Jigsaw</i>	147
4.5 <i>WannaCry</i>	147
4.6 <i>Bad Rabbit</i>	148
4.7 <i>Petya</i>	148
4.8 <i>GoldenEye</i>	149
4.9 <i>Ryuk</i>	149
4.10 <i>GandCrab</i>	150
5. L' <i>Hacker</i> : profilo soggettivo del <i>cyber criminale</i>	150
6. Le fasi di un attacco informatico.....	153
6.1 Fase 1: “ <i>ricognizione e sorveglianza pre-operativa</i> ”	153
6.2 Fase 2: “ <i>analisi (scanning)</i> ”	153
6.3 Fase 3: “ <i>ottenere l’accesso</i> ”	154
6.4 Fase 4: “ <i>mantenere l’accesso</i> ”	154
6.5 Fase 5: “ <i>nascondere le tracce</i> ”	154
7. Come difendersi da un attacco <i>ransomware</i>	155
8. <i>Ransomware 2.0</i>	157
9. <i>Crime as a Service</i> e gli <i>underground forums</i>	160
9.1 <i>Ransomware as a service</i>	162
10. Inquadramento giuridico normativo.....	162
10.1 La competenza della Procura distrettuale.....	165
11. La Direttiva <i>NIS (Network and Information Security)</i>	165
12. Gli attacchi <i>ransomware</i> : <i>case studies</i>	168
12.1 Profilo tecnico operativo.....	168
12.2 Il primo caso di decesso direttamente connesso a un <i>ransomware</i>	170
12.3 I casi italiani.....	172
12.3.1 <i>Le aziende ospedaliere</i>	172
12.3.2 <i>Le società Campari, Enel, Geox e Luxottica</i>	173

CAPITOLO VIII

IL CAPATORE INFORMATICO: PROFILI TECNICO OPERATIVI E GIURIDICI

1. Le indagini digitali e il <i>trojan virus</i>	177
2. Il captatore informatico.....	178
2.1 <i>Online search</i> e <i>online surveillance</i>	181
2.2 Profilo tecnico giuridico.....	183

CAPITOLO IX

IL TROJAN: UN PROTEO DIGITALE TRA INTERCETTAZIONI E PERQUISIZIONI

1. L'acquisizione da remoto dei dati: le perquisizioni digitali.....	189
2. I principali orientamenti della giurisprudenza di legittimità.....	193
2.1 La sentenza Virruso	194
2.2 La sentenza Ryanair	195
2.3 La sentenza Grassi	196
2.4 La sentenza Scurato	198
2.5 La sentenza Romeo del 2017	200
2.6 La sentenza Occhionero del 2017	201
2.7 La sentenza Chianchiano ed altri del 2019.....	203
2.8 L'uso del captatore all'estero.....	204
3. L'indeterminatezza delle modalità di intercettazione non compromette l'utilizzo dei dati acquisiti.....	205
4. Spunti di riflessione.....	209

CAPITOLO X

L'ACQUISIZIONE DELLA PROVA DIGITALE SECONDO GLI STANDARD INTERNAZIONALI

1. Premessa.....	215
2. Le caratteristiche della prova digitale.....	217
2.1 Il documento informatico.....	219
2.2 Il sistema informatico.....	220
3. Le Linee Guida internazionali in materia di <i>Digital Forensics</i>	221
3.1 Gli standard tecnici ISO/IEC 27037 e 27042.....	223
3.2 <i>Digital Evidence First Responder (DEFRR)</i> e <i>Digital Evidence Specialist (DES)</i>	223
3.3 Le fasi di gestione delle <i>digital evidences</i>	224

4. L'acquisizione delle prove digitali per attività di polizia giudiziaria.....	226
5. L'acquisizione delle prove digitali per attività di polizia economico-finanziaria.....	227

CAPITOLO XI

L'ACQUISIZIONE DELLA PROVA DIGITALE DAI SISTEMI CLOUD

1. Premessa.....	229
2. Il <i>cloud computing</i>	229
3. La qualificazione giuridica del contratto di <i>cloud</i>	230
4. Tipologie di servizi <i>cloud</i>	230
5. Modelli di distribuzione dei servizi <i>cloud</i>	231
6. Vantaggi e vantaggi dei sistemi <i>cloud</i>	233
6.1 I "servizi nella nuvola": definizioni tecniche e normative.....	234
7. La <i>cloud forensics</i>	235
7.1 Modalità di accesso ai dati conservati nel <i>cloud</i>	235
7.2 Fasi della <i>cloud forensics</i> e relative problematiche tecniche.....	237
7.2.1 Criticità in fase di identificazione.....	238
7.2.2 Criticità in fase di acquisizione.....	239
7.2.3 Criticità in fase di conservazione.....	241
7.2.4 Criticità in fase di analisi.....	242
7.3 Profili giuridici della <i>cloud forensics</i>	244
7.3.1 Accesso al <i>cloud</i> e accesso a piattaforme social: differenze.....	244
7.3.2 Accesso al <i>cloud</i> : perquisizione informatica o intercettazione telematica?.....	245
7.3.3 Legittimità dell'acquisizione probatoria da <i>cloud</i> e profili di cooperazione internazionale.....	246
7.3.4 Esigenze di armonizzazione normativa e possibili azioni di antifoensics.....	248
Bibliografia.....	250
Sitografia.....	263