INDICE

pag.

Introduzione XI

CAPITOLO 1
REATI INFORMATICI

1.1. I reati "necessariamente informatici" previsti dall'ordinamento giuridico italiano 1
1.2. La violazione del "domicilio informatico" 4
1.2.1. L'accesso abusivo a sistema informatico o telematico (art. 615-*ter* c.p.) 4
1.2.2. Detenzione e uso di mezzi idonei all'accesso abusivo (art. 615-*quater* c.p.) 6
1.2.3. Detenzione e uso di mezzi idonei a danneggiare un sistema informatico (art. 615-*quinquies* c.p.) 7
1.3. L'alterazione delle comunicazioni telematiche e informatiche 9
1.3.1. Intercettazione, impedimento o interruzione illecita di comunicazioni e uso dei relativi mezzi (artt. 617-*quater* e 617-*quinquies* c.p.) 9
1.3.2. Falsificazione, alterazione o soppressione di comunicazioni informatiche (art. 617-*sexies* c.p.) 10
1.4. Il danneggiamento di dati e sistemi informatici 11
1.4.1. Il danneggiamento di informazioni, dati e programmi informatici (artt. 635-*bis* e 635-*ter* c.p.) 11
1.4.2. Il danneggiamento di sistemi informatici o telematici (artt. 635-*quater* e 635-*quinquies* c.p.) 13
1.5. La frode informatica 14
1.5.1. La frode informatica (640-*ter* c.p.) 14
1.5.2. Il *phishing* 17
1.5.3. Il *pharming* 20

Riferimenti bibliografici 21

pag.

CAPITOLO 2
CYBERCRIMES

2.1. Al di là dei reati necessariamente informatici 23
2.2. Il *cyberstalking* 24
2.3. La pornografia digitale 26
2.3.1. *Sexting* e *sextortion* 26
2.3.2. Pedopornografia, adescamento di minori e pornografia virtuale 28
2.3.3. Pornografia non consensuale (*revengeporn*) 29
2.4. Il cyberbullismo 32
2.5. I discorsi d'odio online (*hate speech*) 34
2.6. Le *fake news* 35
2.7. Gli illeciti contro la *privacy* 37
2.8. *Malware-as-a-Service* e DDoS 39
2.9. I *ransomware* 41
2.10. Il *cyberlaundering* 43
Riferimenti bibliografici 46

CAPITOLO 3
GUERRA CIBERNETICA

3.1. Le trasformazioni della guerra e la *cyberwar* 49
3.2. Il problema della qualificazione giuridica della *cyberwar*: i Manuali di Tallinn 51
3.2.1. La *Web War One* 51
3.2.2. Il Manuale di Tallinn 53
3.2.3. Il Manuale di Tallinn 2.0 57
3.3. Le *cyberweapons* 58
3.4. I *cyberwarriors* 61
3.4.1. Combattenti cibernetici statali 62
3.4.2. Combattenti cibernetici parastatali 63
3.4.3. Combattenti cibernetici transnazionali 64
Riferimenti bibliografici 66

CAPITOLO 4
PIRATI E TERRORISTI NELL'ERA DIGITALE

4.1. Pirati e terroristi. Due figure dell'inimicizia assoluta 69
4.2. La pirateria informatica 71

pag.

4.2.1. Il mare di silicio 71
4.2.2. Il nemico del *copyright* 72
4.2.3. Chi ha paura del pirata informatico? 73
4.3. Cyberterrorismo e terrorismo convenzionale 76
4.4. Terrorismo e tecnologie informatiche 78
4.4.1. Terrorismo per il web. Propaganda, reclutamento, addestramento 78
4.4.2. Web per il terrorismo. Pianificazione e *dark markets* 81
Riferimenti bibliografici 82

CAPITOLO 5
INFORMATICA FORENSE

5.1. Informatica forense e *digital evidence* 85
5.1.1. Definizioni 85
5.1.2. Acquisizione dei dati per l'analisi forense 87
5.2. Convenzione di Budapest e legge 48/2008: i mezzi di ricerca della prova digitale 89
5.2.1. Ispezione 90
5.2.2. Perquisizione 91
5.2.3. Sequestro e intercettazioni 92
5.3. Un caso esemplare. Il delitto di Garlasco 94
Riferimenti bibliografici 97

CAPITOLO 6
CYBERSECURITY

6.1. La sicurezza cibernetica come problema globale 99
6.2. *Cybersecurity* e Unione Europea 100
6.2.1. Direttiva ECI e infrastrutture critiche europee 100
6.2.2. La strategia dell'Unione Europea per la sicurezza cibernetica: direttiva NIS e regolamento 2019/881 (*Cybersecurity Act*) 102
6.2.3. Una nuova strategia: verso la direttiva NIS2 104
6.3. L'approccio italiano alla *cybersecurity* 108
6.3.1. La "legge perimetro" 108
6.3.2. La difesa dello spazio cibernetico italiano 110
6.3.3. Agenzia per la cybersicurezza nazionale (ACN) 111
Riferimenti bibliografici 114