

INDICE

EXECUTIVE SUMMARY	7		
CAPITOLO 1			
IL QUADRO EUROPEO E ITALIANO DELLA CYBERSECURITY	19		
1.1. Lo scenario europeo e nazionale degli attacchi cibernetici	21	2.3.1. L'ACN ed il nuovo modello di governance cyber. Gli obiettivi della strategia e del piano di implementazione	53
1.2. Lo stato degli investimenti in cybersicurezza in UE e in Italia	25	2.3.2. Il recepimento della direttiva NIS2 in Italia	60
		2.3.3. Il recepimento della direttiva CER in Italia	63
		2.3.4. Il Perimetro di Sicurezza Nazionale Cibernetica	64
		2.3.5. L'evoluzione della disciplina sul Golden Power	70
		2.3.5.1. <i>Esercizio dei poteri speciali e andamento delle notifiche</i>	75
		2.3.6. Gli scenari in discussione. Il disegno di legge sulla cybersicurezza	80
CAPITOLO 2			
L'ECOSISTEMA NORMATIVO SULLA CYBERSECURITY	35		
2.1. L'approccio alla cybersecurity. EU vs Cina e Stati Uniti	37	CAPITOLO 3	
2.2. L'evoluzione del framework europeo sulla cybersecurity	39	L'EVOLUZIONE DELLE CERTIFICAZIONI A LIVELLO EUROPEO	83
2.2.1. Il Cybersecurity Package ed il nuovo scenario tracciato dalla NIS 2	39	3.1. Il funzionamento e le tendenze di utilizzo dei <i>Common Criteria</i>	85
2.2.1.1. <i>I primi chiarimenti applicativi sulla direttiva NIS2</i>	45	3.2. Verso gli <i>European Common Criteria</i>	89
2.2.2. Il Cybersecurity Act e le modifiche proposte	46	CAPITOLO 4	
2.2.3. Il Cyber Resilience Act (CRA). Dalla proposta della Commissione allo stato della procedura	48	IL QUADRO REGOLATORIO EUROPEO E NAZIONALE IN CIBERSICUREZZA E LA PERCEZIONE DELLE IMPRESE	95
2.2.4. Assicurare la resilienza operativa digitale del settore finanziario: il Digital Operational Resilience Act (DORA)	51	4.1. Nota metodologica e analisi del campione	97
2.3. L'ecosistema normativo nazionale sulla cybersecurity	53	4.2. Analisi dei risultati	98
		4.3. Conclusioni dell'indagine	113

CAPITOLO 5			
LA CYBERSICUREZZA ALLA BASE DELLA COOPERAZIONE TRA PUBBLICO E PRIVATO	117		
5.1. Il partenariato pubblico-privato (PPP) applicato alla sicurezza informatica: vantaggi e criticità	119		
5.1.1. Le principali iniziative di PPP in ambito nazionale	123		
5.1.2. I Competence Center per l'orientamento e la formazione in cybersecurity	126		
5.2. Le start-up di cibernsicurezza e il <i>Cyber Innovation Network</i> dell'ACN	129		
5.3. Altre forme di collaborazione tra pubblico e privato	133		
		CAPITOLO 6	
		LE COMPETENZE IN CIBERSICUREZZA: A CHE PUNTO SIAMO E ATTIVITÀ IN CORSO	139
		6.1. La cibernsicurezza per i cittadini: lo stato dell'arte	141
		6.2. L'impegno delle imprese per la sicurezza informatica	144
		6.3. Le <i>best practices</i> per la formazione ICT & cyber	147
		6.4. L'offerta formativa nazionale in materia di cibernsicurezza	150
		6.4.1. Corsi, Master e Dottorati di ricerca	150
		6.4.2. Lo stato dell'arte e la riforma degli ITS	154
		6.4.3. La sicurezza informatica nei corsi ITS	157
		CONCLUSIONI	163