

# Indice

Premessa	IX	
Introduzione	1	
<b>Parte 1</b>		
<b>Principi di cybersecurity e sviluppi dell'IA</b>		
1	<b>Evoluzione degli attacchi informatici nel contesto geopolitico attuale</b>	9
2	<b>L'approccio delle organizzazioni italiane ai temi della cybersicurezza</b>	19
2.1	Luci e ombre nella postura di sicurezza delle organizzazioni italiane	19
2.2	I benefici di un approccio basato sull'intelligenza artificiale per la cybersecurity	23
3	<b>Breve storia dell'intelligenza artificiale</b>	25
3.1	Evoluzione dell'intelligenza artificiale	26
4	<b>I rischi etici, geopolitici e sistemici dell'IA</b>	31
4.1	Il rischio sistemico	33
4.2	Il rischio geopolitico	34
4.3	Il rischio etico	37
5	<b>Adeguamento AI Act: cosa sapere e cosa fare</b>	41
5.1	EU AI Act: iter approvativo e applicazione	41
5.2	A chi si applica l'EU AI Act	44
5.3	Un approccio centrato sul rischio	45
5.4	La necessaria governance dell'IA	48

5.5	Principi minimi per lo sviluppo o l'utilizzo di sistemi basati su IA	50
5.6	Modelli di governance dell'IA	51

## Parte 2

### IA e GenAI, utilizzi avanzati delle tecnologie per rafforzare la cybersecurity

<b>6</b>	<b>IA per la cybersecurity: linee guida per un utilizzo strategico</b>	<b>55</b>
6.1	I pilastri di una strategia di gestione dei rischi cyber	55
6.2	Il contributo dell'IA alla strategia di gestione dei rischi cyber	56
6.3	I punti di attenzione dell'utilizzo dell'IA nella strategia di cybersecurity	58
<b>7</b>	<b>AI Ethics e cybersecurity: luci e ombre</b>	<b>61</b>
7.1	Introduzione	61
7.2	Alcune criticità	64
7.3	Ethical Assessment	67
<b>8</b>	<b>IA e cybersecurity: utilizzi attuali e previsti</b>	<b>69</b>
8.1	Migliorare la gestione delle vulnerabilità con l'IA	70
8.2	Benefici e problemi nell'utilizzo dell'IA per la gestione delle vulnerabilità	72
8.3	Altri ambiti di utilizzo dell'IA in cybersecurity	73
<b>9</b>	<b>Migliorare il rilevamento delle minacce con l'intelligenza artificiale</b>	<b>79</b>
9.1	Il valore dell'IA per il rilevamento delle minacce	79
9.2	Dall'analisi al contesto: creare un quadro completo	80
9.3	Automazione e risposta in tempo reale	81
9.4	Rafforzare la resilienza attraverso l'IA	81
9.5	Le sfide dell'adozione dell'IA in cybersecurity	82
9.6	Il Cyber Fusion Center: sinergia tra intelligenza artificiale e difesa informatica moderna	82

9.7	Conclusioni: migliorare il rilevamento delle minacce con l'IA e la gestione dei rischi associati	83
<b>10</b>	<b>IA in azienda: impatti legali e privacy</b>	<b>85</b>
10.1	L'eredità del GDPR	86
10.2	AI Act e NIS2	88
10.3	Ulteriori aspetti da considerare: contrattualistica e licenze	89

### Parte 3

#### I rischi dell'IA nelle aziende e le strategie per prevenirli, rispondere e mitigare le minacce

<b>11</b>	<b>I rischi di un utilizzo malevolo dell'IA (da parte di attaccanti)</b>	<b>93</b>
11.1	Fragilità e potenza: l'IA come vittima e arma	93
<b>12</b>	<b>I rischi di un utilizzo scorretto dell'IA all'interno delle organizzazioni</b>	<b>103</b>
12.1	Rischi derivanti dall'uso dei modelli IA	103
12.2	Rischi derivanti dal non utilizzo dei modelli IA	106
12.3	Rischi legati a minacce ai modelli IA	107
12.4	Rischi legali e normativi	108
12.5	Rischi per altre tipologie di IA al di fuori dei LLM e della GenAI	109
<b>13</b>	<b>La risposta ai rischi dell'IA: definire un modello complessivo</b>	<b>111</b>
13.1	Definizione dell'AI governance	113
13.2	Predisposizione delle linee di indirizzo	114
13.3	Mappatura delle soluzioni e mantenimento dell' <i>asset inventory</i>	114
13.4	Progettazione delle attività di <i>awareness</i> e <i>training</i>	115
13.5	Revisione dei processi operativi	116

<b>14</b>	<b>La risposta ai rischi dell'IA: le misure da predisporre</b>	<b>119</b>
14.1	Gestione del rischio e modellazione delle minacce	119
14.2	Catalogazione degli asset	120
14.3	Formazione e consapevolezza	121
14.4	Misure di sicurezza per i modelli IA	121
14.5	Soluzioni emergenti per la sicurezza di GenAI/LLM	124
<b>15</b>	<b>La risposta ai rischi dell'IA: mettere in sicurezza il ciclo di vita dell'intelligenza artificiale</b>	<b>129</b>
15.1	La sicurezza dell'IA nel suo ciclo di vita	130
15.2	Un approccio consapevole alla sicurezza dell'IA	137
	<b>Bibliografia essenziale</b>	<b>141</b>
	<b>Gli Autori</b>	<b>145</b>