| | | |
|---|---|---|
| 1. | Record Nr. | UNINA9910728952403321 |
| | Autore | Huang Linan |
| | Titolo | Cognitive Security : A System-Scientific Approach / / by Linan Huang, Quanyan Zhu |
| | Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023 |
| | ISBN | 9783031307096<br>3031307097 |
| | Edizione | [1st ed. 2023.] |
| | Descrizione fisica | 1 online resource (117 pages) |
| | Collana | SpringerBriefs in Computer Science, , 2191-5776 |
| | Altri autori (Persone) | ZhuQuanyan |
| | Disciplina | 004.019 |
| | Soggetti | Data protection - Law and legislation<br>Artificial intelligence<br>Privacy<br>Artificial Intelligence<br>Protecció de dades<br>Xifratge (Informàtica)<br>Intel·ligència artificial<br>Llibres electrònics |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Nota di contenuto | Chapter. 1. Introduction -- Chapter. 2. System-Scientific Methods -- Chapter. 3. Cognitive Capacities for Designing, Operating, Supervising, and Securing Complex Systems -- Chapter. 4. Review of System-Scientific Perspectives for Analysis, Exploitation, and Mitigation of Cognitive Vulnerabilities -- Chapter. 5. ADVERT: Defending against Reactive Attention Attacks -- Chapter. 6. RADAMS: Defending against Proactive Attention Attacks -- Chapter. 7. Summary and Conclusions. |
| | Sommario/riassunto | This book presents the latest research in cognitive security, a rapidly emerging field that addresses the vulnerabilities in human behavior and cognition that can lead to Cyber-Physical Systems (CPS) compromise. This book demonstrates that as adversaries increasingly use manipulative and deceptive information to disrupt human cognitive processes, including sensation, attention, memory, and mental operations, humans are misled into fallacious reasoning and |

manipulated decisions that can lead to system-level meltdown. Cognitive security aims to protect humans from the exploitation of cognitive vulnerabilities, help them make informed decisions that are free from manipulation and undue influence, and mitigate the aggravating risk in the ensuing steps of the attacker's kill chain. This book offers solutions that work across different fields, such as psychology, neuroscience, data science, social science, and game theory, to deal with cognitive threats. It guides the reader through the core ideas with figures, real-life examples, and case studies. Moreover, it formally defines all research questions, presents the results using mathematical theorems and proofs, and obtains insights through numerical validation. This book provides a self-contained and brief overview of essential system-scientific tools for modeling, analyzing, and mitigating cognitive vulnerabilities. The concepts of human cognitive capacities and cognitive vulnerabilities are formally discussed, followed by two case studies in the scenarios of reactive and proactive attention vulnerabilities. This book provides insights and applications on this transdisciplinary topic, with the goal of motivating future research in this emerging area and pushing the frontier of human-technology convergence. This book is a valuable reference for researchers and advanced-level students studying or working in cognitive security and related fields. It is also useful for decision-makers, managers, and professionals working within these related fields.