

| | |
|-------------------------|---|
| 1. Record Nr. | UNINA9910584481203321 |
| Autore | Oakley Jacob G. |
| Titolo | Theoretical cybersecurity : principles and advanced concepts // Jacob G. Oakley [and four others] |
| Pubbl/distr/stampa | Berkeley, California : , : Apress, , [2022] ©2022 |
| ISBN | 1-4842-8300-7 |
| Descrizione fisica | 1 online resource (224 pages) |
| Disciplina | 005.8 |
| Soggetti | Computer security - Technological innovations Computer security - Philosophy Computer security - Forecasting |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di contenuto | Chapter 1. Introduction Chapter 2. A Cyber Taxonomy Chapter 3. Cost Benefit Chapter 4. Roles and Responsibilities Chapter 5. Experimentation Chapter 6. Strategic Cybersecurity Chapter 7. Strategic Defensive Security Chapter 8. Infinite Cybersecurity Chapter 9. Cybersecurity and Game Theory Chapter 10. Game Theory Case Study: Ransomware |
| Sommario/riassunto | There is a distinct lack of theoretical innovation in the cybersecurity industry. This is not to say that innovation is lacking, as new technologies, services, and solutions (as well as buzzwords) are emerging every day. This book will be the first cybersecurity text aimed at encouraging abstract and intellectual exploration of cybersecurity from the philosophical and speculative perspective. Technological innovation is certainly necessary, as it furthers the purveying of goods and services for cybersecurity producers in addition to securing the attack surface of cybersecurity consumers where able. The issue is that the industry, sector, and even academia are largely technologically focused. There is not enough work done to further the trade--the craft of cybersecurity. This book frames the cause of this and other issues, and what can be done about them. Potential methods and directions are outlined regarding how the industry can evolve to embrace |

theoretical cybersecurity innovation as it pertains to the art, as much as to the science. To do this, a taxonomy of the cybersecurity body of work is laid out to identify how the influences of the industry's past and present constrain future innovation. Then, cost-benefit analysis and right-sizing of cybersecurity roles and responsibilities--as well as defensible experimentation concepts--are presented as the foundation for moving beyond some of those constraining factors that limit theoretical cybersecurity innovation. Lastly, examples and case studies demonstrate future-oriented topics for cybersecurity theorization such as game theory, infinite-minded methodologies, and strategic cybersecurity implementations. What you'll learn

The current state of the cybersecurity sector and how it constrains theoretical innovation
How to understand attacker and defender cost benefit
The detect, prevent, and accept paradigm
How to build your own cybersecurity box
Supporting cybersecurity innovation through defensible experimentation
How to implement strategic cybersecurity
Infinite vs finite game play in cybersecurity
Who This Book Is For
This book is for both practitioners of cybersecurity and those who are required to, or choose to, employ such services, technology, or capabilities.
