

| | |
|-------------------------|---|
| 1. Record Nr. | UNINA9910528267103321 |
| Autore | Couretas Jerry M. <1966-> |
| Titolo | An introduction to cyber modeling and simulation / / Jerry M. Couretas |
| Pubbl/distr/stampa | Hoboken, New Jersey : , : WILEY, , [2019] ©2019 |
| ISBN | 1-119-42084-9 1-119-42081-4 |
| Edizione | [First edition] |
| Descrizione fisica | 1 online resource (190 pages) |
| Collana | Wiley series in modeling and simulation. THEi Wiley ebooks. |
| Disciplina | 005.8 |
| Soggetti | Computer security Computer simulation Cyberinfrastructure |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Brief review of cyber incidents -- Cyber security : an introduction to assessment and maturity frameworks -- Introduction to cyber modeling and simulation (M&S) -- Technical and operational scenarios -- Cyber standards for M&S -- Cyber course of action (COA) strategies -- Cyber computer assisted exercise (CAX) and situational awareness (SA) via cyber M&S -- Cyber model based evaluation background -- Cyber M&S & system risk analysis -- Cyber modeling & simulation for test and evaluation (T&E) -- Developing model based cyber M&S frameworks -- Appendix : cyber M&S supporting data, tools & techniques. |
| Sommario/riassunto | Introduces readers to the field of cyber modeling and simulation and examines current developments in the US and internationally. This book provides an overview of cyber modeling and simulation (M&S) developments. Using scenarios, courses of action (COAs), and current M&S and simulation environments, the author presents the overall information assurance process, incorporating the people, policies, processes, and technologies currently available in the field. The author ties up the various threads that currently compose cyber M&S into a coherent view of what is measurable, simulative, and usable in order to |

evaluate systems for assured operation. An Introduction to Cyber Modeling and Simulation provides the reader with examples of tools and technologies currently available for performing cyber modeling and simulation. It examines how decision-making processes may benefit from M&S in cyber defense. It also examines example emulators, simulators and their potential combination. The book also takes a look at corresponding verification and validation (V&V) processes, which provide the operational community with confidence in knowing that cyber models represent the real world. This book: Explores the role of cyber M&S in decision making Provides a method for contextualizing and understanding cyber risk Shows how concepts such the Risk Management Framework (RMF) leverage multiple processes and policies into a coherent whole Evaluates standards for pure IT operations, "cyber for cyber," and operational/mission cyber evaluations—"cyber for others" Develops a method for estimating both the vulnerability of the system (i.e., time to exploit) and provides an approach for mitigating risk via policy, training, and technology alternatives Uses a model-based approach An Introduction to Cyber Modeling and Simulation is a must read for all technical professionals and students wishing to expand their knowledge of cyber M&S for future professional work.
