

1. Record Nr.	UNINA9910300049503321
Titolo	Cyber Criminology // edited by Hamid Jahankhani
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	9783319971810 3319971816 9783319971803
Descrizione fisica	1 online resource (357 pages)
Collana	Advanced Sciences and Technologies for Security Applications, , 1613-5113
Disciplina	364.168
Soggetti	Computer crimes Criminal law System safety Data protection Cybercrime Criminal Law and Criminal Procedure Law Security Science and Technology Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references
Nota di contenuto	Foreword -- Cyber Criminology and Psychology -- Crime and Social Media: Legal responses to offensive online communications and abuse -- Explaining Why Cybercrime Occurs: Criminological and Psychological Theories -- Cyberaggression and Cyberbullying: Widening the Net -- Part 2 Cyber-Threat Landscape -- Policies, Innovative Self-Adaptive Techniques and Understanding Psychology of Cybersecurity to Counter Adversarial Attacks in Network and Cyber Environments -- The Dark Web -- Tor black markets: economics characterization and investigation technique; G. Me, L. Pesticcio -- A New Scalable Botnet Detection Method in the Frequency Domain -- Part 3 Cybercrime Detection -- Predicting the Cyber Attackers; a Comparison of Different Classification Techniques -- Criminal Data Mining, Threat Analysis and Prediction -- SMERF: Social Media, Ethics & Risk Framework; I. Mitchell

et al -- Understanding the cyber-victimisation of people with long term conditions and the need for collaborative forensics-enabled Disease Management Programmes -- An Investigator's Christmas Carol - Past, Present, and Future Law Enforcement Agency Data Mining Practices -- DaPA: Deconstruct and Preserve for all: A Procedure for the Preservation of Digital Evidence on Solid State Drives and Traditional Storage Media -- Part 4 Education, Training and Awareness in Cybercrime Prevention -- An examination into the effect of early education on cyber security awareness within the U.K -- An examination into the level of training, education and awareness among frontline police officers in tackling cybercrime within the Metropolitan Police Service -- Combating Cyber Victimisation: Cybercrime Prevention -- Information security landscape in Vietnam: insights from two research surveys.

---

## Sommario/riassunto

This book provides a comprehensive overview of the current and emerging challenges of cyber criminology, victimization and profiling. It is a compilation of the outcomes of the collaboration between researchers and practitioners in the cyber criminology field, IT law and security field. As Governments, corporations, security firms, and individuals look to tomorrow's cyber security challenges, this book provides a reference point for experts and forward-thinking analysts at a time when the debate over how we plan for the cyber-security of the future has become a major concern. Many criminological perspectives define crime in terms of social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition has allowed crime to be characterised, and crime prevention, mapping and measurement methods to be tailored to specific target audiences. However, this characterisation cannot be carried over to cybercrime, because the environment in which such crime is committed cannot be pinpointed to a geographical location, or distinctive social or cultural groups. Due to the rapid changes in technology, cyber criminals' behaviour has become dynamic, making it necessary to reclassify the typology being currently used. Essentially, cyber criminals' behaviour is evolving over time as they learn from their actions and others' experiences, and enhance their skills. The offender signature, which is a repetitive ritualistic behaviour that offenders often display at the crime scene, provides law enforcement agencies an appropriate profiling tool and offers investigators the opportunity to understand the motivations that perpetrate such crimes. This has helped researchers classify the type of perpetrator being sought. This book offers readers insights into the psychology of cyber criminals, and understanding and analysing their motives and the methodologies they adopt. With an understanding of these motives, researchers, governments and practitioners can take effective measures to tackle cybercrime and reduce victimization.

---