

1. Record Nr.	UNINA9910488724403321
Titolo	Technology development for security practitioners // Babak Akhgar, Dimitrios Kavallieros, Evangelos Sdongos, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-69460-7
Descrizione fisica	1 online resource (551 pages)
Collana	Security Informatics and Law Enforcement
Disciplina	355.0330581
Soggetti	Security sector - Technological innovations Security, International
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents -- Part I: Cyber Crime, Cyber Terrorism and Cyber Security -- Chapter 1: ASGARD: A Novel Approach for Collaboration in Security Research Projects -- 1.1 Introduction -- 1.2 Related Work -- 1.3 Methods -- 1.4 Results -- 1.5 Discussion and Future Research -- References -- Chapter 2: SoK: Blockchain Solutions for Forensics -- 2.1 Introduction -- 2.1.1 Blockchain as a Game Changer in Digital Forensics -- 2.1.2 Goal and Plan of the Chapter -- 2.2 Methodology -- 2.3 Classification of the Available Blockchain-Based Forensics Literature -- 2.3.1 Cloud Forensics -- 2.3.2 Data Management Forensics -- 2.3.3 Healthcare Forensics -- 2.3.4 IoT Forensics -- 2.3.5 Mobile Forensics -- 2.3.6 Multimedia Forensics -- 2.3.7 Smart Grid Forensics -- 2.3.8 Intelligent Transportation Systems Forensics -- 2.4 Discussion -- 2.4.1 Limitations in Blockchain -- 2.4.2 Challenges in Blockchain Digital Forensics -- 2.5 Conclusions -- Bibliography -- Chapter 3: Query Reformulation Based on Word Embeddings: A Comparative Study -- 3.1 Introduction -- 3.2 Related Work -- 3.3 Methods -- 3.3.1 Word Embedding -- 3.3.2 Query Expansion -- 3.4 Evaluation -- 3.4.1 Experiments on Benchmark Datasets -- 3.4.2 Experiments on a Terrorism-Related Dataset -- 3.5 Results -- 3.5.1 Benchmark Datasets -- 3.5.2 Terrorism-Related Dataset -- 3.6 Conclusions -- References -- Chapter 4: Evolving from Data to Knowledge Mining

to Uncover Hidden Relationships -- 4.1 Introduction -- 4.2 State of the Art -- 4.3 Proposed System -- 4.4 Methodology and Tools -- 4.4.1 Semantic Fusion Tools -- 4.4.2 Trend Prediction -- 4.5 Conclusions -- Bibliography -- Chapter 5: Cyber-Trust: Meeting the Needs of Information Sharing Between ISPs and LEAs -- 5.1 Introduction -- 5.2 Related Work -- 5.2.1 Industry Solutions -- 5.2.2 Research Solutions.

5.3 Towards Reshaping Cyber-Crime Investigation Procedures -- 5.3.1 Platform User Requirements -- 5.3.2 LEAs Evidence Procedures in Cyber-Trust Platform -- 5.4 Cyber-Trust for LEAs -- 5.4.1 LEAs in Cyber-Trust Platform -- 5.4.2 Blockchain for LEAs -- 5.4.3 LEAs User Interface (UI) -- 5.5 Conclusions -- References -- Chapter 6: Cyber Ranges: The New Training Era in the Cybersecurity and Digital Forensics World -- 6.1 Introduction -- 6.2 State-of-the-Art of Cyber Ranges -- 6.2.1 Government, Military, and LEAs Oriented -- 6.2.1.1 Department of Defence (DoD) Cybersecurity Range -- 6.2.1.2 Arizona Cyber Warfare Range -- 6.2.1.3 Hybrid Network Simulation (HNS) Platform -- 6.2.1.4 ManTech -- 6.2.1.5 École Navale CR -- 6.2.1.6 Airbus CR -- 6.2.2 Academic -- 6.2.2.1 KYPO Cyber Range -- 6.2.2.2 Augusta University CR -- 6.2.2.3 US Cyber Range -- 6.2.2.4 Austrian Institute of Technology Cyber Range -- 6.2.2.5 Saros Technology -- 6.2.2.6 European Space Agency (ESA) CR (by RHEA Group) -- 6.2.2.7 Virginia CR -- 6.2.2.8 THE Michigan CR -- 6.2.3 Commercial -- 6.2.3.1 IXIA Cyber Range -- 6.2.3.2 Palo Alto Networks Cyber Range -- 6.2.3.3 IBM Cyber Range -- 6.2.3.4 CybExer Cyber Range -- 6.2.3.5 Raytheon Cyber Range -- 6.2.3.6 CYBERBIT Cyber Range -- 6.2.3.7 Breaking Point -- 6.2.3.8 RGCE -- 6.2.3.9 Berkatweb -- 6.2.3.10 CYBERGYM -- 6.2.3.11 CyberCENTS -- 6.2.3.12 Silensec Cyber Range -- 6.2.3.13 Cisco Cyber Range -- 6.3 IT, OT, and Hybrid Approaches of Cyber Ranges -- 6.4 Components of Modern Cyber Ranges -- 6.4.1 Artificial Intelligence (AI) and Machine Learning -- 6.4.2 Information Gathering and Sharing -- 6.4.3 Gamification and Serious Gaming -- 6.4.4 Evaluation Module -- 6.5 Operational Impact of Cyber Range Elements -- 6.5.1 Impact of Training in Cybersecurity/Defence -- 6.5.2 Impact of Training in Digital Forensics.

6.6 FORESIGHT Paradigm -- 6.7 Conclusions -- References -- Part II: Serious and Organized Crime (SOC) -- Chapter 7: COPKIT: Technology and Knowledge for Early Warning/Early Action-Led Policing in Fighting Organised Crime and Terrorism -- 7.1 Introduction -- 7.2 Relevant Characteristics of the Techniques Used -- 7.2.1 Approaches to Incorporation of Knowledge -- 7.2.2 Interpretability of Techniques -- 7.2.3 Requirements for the Information System -- 7.3 Ethical, Data Protection and Related Aspects -- 7.3.1 Legal, Ethical and Societal Challenges -- 7.4 Conclusions -- References -- Chapter 8: Detection of Irregularities and Abnormal Behaviour in Extreme-Scale Data Streams -- 8.1 Introduction -- 8.2 State-of-the-Art Research Projects -- 8.3 Available Technologies in Crime Investigations and Future Trends -- 8.3.1 Visual Intelligence -- 8.3.2 Semantic Integration and Technologies -- 8.3.3 Data Mining and Detection of Cybercriminal Activities -- 8.4 Proposed Architecture -- 8.4.1 Visual Intelligence Modules -- 8.4.2 Data Mining Modules for Crime Prevention and Investigation -- 8.4.3 Semantic Information Representation and Fusion Modules -- 8.4.4 Trend Detection and Probability Prediction Modules for Organized Terrorism and Criminal Activities -- 8.4.5 Detection Modules of Cybercriminal Activities -- 8.4.6 Situation Awareness and HMI Modules -- 8.5 Conclusions -- References -- Chapter 9: Visual Recognition of Abnormal Activities in Video Streams

-- 9.1 Introduction -- 9.2 Related Work -- 9.3 Activity Recognition Framework -- 9.4 Experiments -- 9.4.1 Dataset -- 9.4.2 Experimental Setup -- 9.4.3 Results -- 9.5 Conclusions -- Bibliography -- Chapter 10: Threats and Attack Strategies Used in Past Events: A Review -- 10.1 Introduction -- 10.1.1 Background -- 10.1.2 Purpose and Contents of the Chapter -- 10.2 Review of Terrorist Threats. 10.2.1 Defining Terrorism -- 10.2.2 Origins and Typologies of Terrorism -- 10.2.3 Key Developments in Modern Terrorism -- 10.2.3.1 The Profile of "New Terrorism" -- 10.2.3.2 Foreign Terrorist Fighters (FTFs) -- 10.2.3.3 The Terrorist Landscape in Europe -- 10.3 Review of Terrorist Attack Strategies -- 10.3.1 Lone Actors and Organisational Structure -- 10.3.2 Rationalism and Decision-Making Model -- 10.3.3 Modern Technology and Online-Digital Environments -- 10.3.4 Explosives as Weapons of Choice -- 10.4 Emerging Threats and Attack Strategies in Terrorism -- 10.4.1 Trends and Patterns in Modern Security Environment -- 10.4.2 The Explosives Threat -- 10.4.3 Misuse of Technological Advances -- Bibliography -- Chapter 11: Syntheses of 'Hemtex' Simulants of Energetic Materials and Millimetre Wave Characterisation Using the Teraview CW400 Spectrometer: Fundamental Studies for Detection Applications -- 11.1 Introduction -- 11.2 Theory -- 11.3 Experimental -- 11.3.1 Materials -- 11.3.2 Synthesis Procedure -- 11.3.3 Characterisation -- 11.4 Results and Discussion -- 11.4.1 Liquid Characterisation Results -- 11.4.2 Simulant Characterisation Results -- 11.5 Conclusions -- References -- Chapter 12: Law Enforcement Priorities in the Era of New Digital Tools -- 12.1 Introduction -- 12.2 European Law Enforcement Networks -- 12.3 Open Source Intelligence (OSINT) -- 12.3.1 Priorities of the OSINT Community of Practitioners -- 12.3.2 Opportunities for Development Within OSINT -- 12.4 Mobility for Officers -- 12.4.1 Priorities of the Mobility for Officers Community of Practitioners -- 12.4.2 Opportunities for Development for the Mobile Police Officer -- 12.5 People Trafficking -- 12.5.1 Priorities of the People Trafficking Community of Practitioners -- 12.5.2 Opportunities for Development Within People Trafficking -- 12.6 Intelligence Analysis. 12.6.1 Priorities of the Intelligence Analysis Community of Practitioners -- 12.6.2 Opportunities for Development Within the Intelligence Analysis -- 12.7 Emerging Technologies in DNA -- 12.7.1 Priorities of the Emerging Technologies Community of Practitioners -- 12.7.2 Opportunities for Development Within DNA Technologies -- 12.8 Conclusions and Future Work -- Bibliography -- Part III: Border Security -- Chapter 13: Threats and Attack Strategies Used in Past Events: A Review -- 13.1 Introduction -- 13.2 Related Literature -- 13.2.1 Information Fusion -- 13.3 Proposed Solution -- 13.4 Conclusion -- Bibliography -- Chapter 14: Early Warning for Increased Situational Awareness: A Pre-Operational Validation Process on Developing Innovative Technologies for Land Borders -- 14.1 Introduction -- 14.2 EWISA Core System -- 14.3 EWISA Validation Methodology -- 14.3.1 Technical Verification -- 14.3.2 Operational Validation -- 14.3.2.1 Definition of Validation Concepts -- 14.4 EWISA Operational Validation Execution -- 14.5 EWISA Operational Validation Results -- 14.6 Conclusions -- Bibliography -- Chapter 15: Border Surveillance Using Computer Vision-Enabled Robotic Swarms for Semantically Enriched Situational Awareness -- 15.1 Introduction -- 15.2 Swarm Intelligence for Autonomous Navigation -- 15.3 Visual Detection Capabilities -- 15.4 Semantic Enrichment for Increased Situation Awareness -- 15.5 Conclusions -- References -- Chapter 16: FOLDOUT: A Through Foliage Surveillance System for Border Security -- 16.1 Introduction -- 16.2 FOLDOUT User Requirements -- 16.3 FOLDOUT Architecture

Design -- 16.3.1 Ground Sensors -- 16.3.2 Sensor Mounted  
on a StratobusTM -- 16.3.3 Sensor Mounted on a Satellite -- 16.3.4  
Fusion of Ground Sensors, StratobusTM and Satellite Data -- 16.4  
Scenarios Description -- 16.5 Current Results -- 16.6 Conclusion --  
Bibliography.  
Chapter 17: Identifying and Prioritising Security Capabilities  
for the Mediterranean and Black Sea Regions.

---