1. Record Nr. UNISA996490355803316

Autore	Montasari Reza
Titolo	Artificial intelligence and national security / / Reza Montasari
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-06709-6
Descrizione fisica	1 online resource (229 pages)
Disciplina	355.03
Soggetti	National security - Decision making Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Contents -- Artificial Intelligence and the Spread of Mis- and Disinformation -- 1 Introduction -- 2 Misinformation Versus Disinformation -- 2.1 Information and the Meaning of Truth in a Post-Truth World -- 2.2 The Differences Between Misinformation and Disinformation -- 3 AI, Bots, and the Spread of Mis- and Disinformation -- 3.1 Definitions of AI and ML -- 3.2 Types of Disinformation and Detecting Fabricated Content -- 3.2.1 GAN Images -- 3.2.2 False Videos and Deepfakes -- 3.2.3 Multimodal Content -- 3.3 Software Robots -- 3.3.1 Types of Bots -- 3.4 Social Media and the Spread of Mis- and Disinformation -- 4 The Global Impact of the Spread of Disinformation -- 5 Mitigating the Impact of Mis- and Disinformation -- 6 Conclusion -- References -- How States' Recourse to Artificial Intelligence for National Security Purposes Threatens Our Most Fundamental Rights -- 1 Introduction -- 2 Background -- 2.1 National Security Being a Vague and Ambiguous Term -- 2.2 Understanding Artificial Intelligence -- 2.2.1 The Notion of Artificial Intelligence -- 2.2.2 Threats and Opportunities of Artificial Intelligence -- 3 Legal Framework of Endangered Human Rights -- 3.1 Right to Life -- 3.2 Right to a Fair Trial -- 3.3 Right to Privacy and Data Protection -- 3.4 Right to Freedom of Expression and Opinion -- 3.5 Right to Freedom of Assembly and Association -- 3.6 Right to Equality: The Prohibition of Discrimination -- 3.7 Right to Free Elections -- 4

National Security Uses of Artificial Intelligence -- 4.1 States' Recourse to Artificial Intelligence in General -- 4.1.1 Problems of Biases, Errors, False Positives and False Negatives -- 4.1.2 Problems of Transparency and Accountability -- 4.2 Surveillance Practices -- 4.2.1 Surveillance Practices Limited Only to Legitimate National Security Purposes.
4.2.2 Surveillance Practices Deployed in Predictive Policing -- 4.2.3 Facial Recognition Combined with Surveillance Practices -- 4.3 Drones and Lethal Autonomous Weapons -- 4.4 AI-Enabled Foreign State Disinformation -- 4.5 Combating Illegal Content Online: Detection of Threats -- 5 Conclusion -- References -- The Use of AI in Managing Big Data Analysis Demands: Status and Future Directions -- 1 Introduction -- 2 Previous Work -- 2.1 Policy -- 2.1.1 People: UN Future Generations (2030) -- 2.1.2 Energy: COP 26 UN Climate Change Conference -- 2.2 Technology -- 2.2.1 Artificial Intelligence (AI) -- 2.2.2 Big Data (BD) -- 2.2.3 Blockchain (BC) -- 2.3 Application -- 2.3.1 People: Health Surveillance -- 2.3.2 Energy: UK Power -- 2.4 Summary -- 3 Research Challenges -- 3.1 Policy -- 3.1.1 People: Data Protection -- 3.1.2 Energy: Predictability -- 3.2 Technology -- 3.2.1 People: Scalability -- 3.2.2 Energy: Security -- 3.3 Applications -- 3.3.1 People: Smart Meter Connectivity -- 3.3.2 Energy: Market Supplier -- 3.4 Summary -- 4 Potential Solutions -- 4.1 Policy -- 4.2 Technology -- 4.3 Application -- 4.4 Summary -- 5 Conclusion and Recommendations -- 5.1 Conclusion -- 5.2 Recommendations -- References -- The Use of Artificial Intelligence in Content Moderation in Countering Violent Extremism on Social Media Platforms -- 1 Introduction -- 2 Definitions -- 2.1 Violent Extremism -- 2.2 CVE -- 3 AI in Content Moderation -- 3.1 Measuring the Accuracy of AI in Content Moderation -- 3.2 Infringements on the Freedom of Expression and Democracy -- 4 The Use of De-platforming Measures -- 5 Conclusion -- References -- A Critical Analysis into the Beneficial and Malicious Utilisations of Artificial Intelligence -- 1 Introduction -- 1.1 Background and Definitions -- 1.1.1 Machine Learning -- 1.1.2 Natural Language Processing -- 1.2 Research Questions.
1.3 The Structure of This Chapter -- 2 The Malicious Use of Artificial Intelligence -- 2.1 Unmanned Aerial Vehicle -- 2.2 3D Printing -- 2.3 Distributed Denial of Service (DDOS) Attacks -- 2.4 Phishing -- 3 The Beneficial Uses of Artificial Intelligence -- 3.1 Efficiency and Automation -- 3.2 Business -- 3.3 Prisons -- 3.4 Counterterrorism -- 4 The Challenges Faced by Artificial Intelligence -- 4.1 Technical Challenges -- 4.1.1 Content Moderation -- 4.1.2 Facial Recognition Bias -- 4.2 Legal Challenges -- 4.2.1 Freedom of Expression -- 4.3 Ethical Challenges -- 5 Conclusion -- References -- Countering Terrorism: Digital Policing of Open Source Intelligence and Social Media Using Artificial Intelligence -- 1 Introduction -- 2 Background -- 2.1 Cybercrime -- 2.2 Digital Policing -- 2.3 Open Source Intelligence -- 2.4 Social Media Intelligence -- 2.5 Terrorism and Radicalization -- 3 Digital Policing Methods of Countering Terrorism -- 4 Challenges and Recommendations -- 4.1 Ethical and Legal Challenges -- 4.2 Technological Challenges -- 4.3 Organizational Challenges -- 5 Discussion -- 6 Conclusion -- References -- Cyber Threat Prediction and Modelling -- 1 Introduction -- 2 Business Importance of Cyber Threat Prediction and Modelling -- 2.1 What Is an Asset? -- 2.2 What Is a Threat? -- 2.3 What Is a Vulnerability? -- 2.4 What Is the Impact? -- 3 Threat Intelligence -- 4 Developing Your Threat Prediction and Modelling Capabilities -- 4.1 Traditional Threats -- 4.2 Non-traditional Threats -- 5 Threat Modelling -- 5.1 Threat Scenarios -- 6 Using the Mitre ATT&amp -- CK (MITRE. MITRE ATT&amp -- CK®) and CAPEC (MITRE. CAPEC - Common Attack Pattern Enumeration and

Classification (CAPECTM)) for Cyber Threat Prediction and Modelling -- 7 Conclusion -- References -- A Critical Analysis of the Dark Web Challenges to Digital Policing -- 1 Introduction.
2 Background -- 3 Challenges -- 4 Solutions -- 5 Discussion -- 6 Conclusion -- References -- Insights into the Next Generation of Policing: Understanding the Impact of Technology on the Police Force in the Digital Age -- 1 Introduction -- 2 Changes in the Policing Environment in the Era of Big Data and Artificial Intelligence -- 2.1 Digitisation of Work Models -- 2.2 Expanded Field of Work -- 2.3 Increased Technical Requirements for Police Officers -- 3 Current Status of the Application of Artificial Intelligence and Big Data in Policing -- 3.1 Combating Crime -- 3.2 Serving Society -- 4 Insights Around the Challenges of Digital Policing -- 4.1 Conflict Between Public Safety and Individual Rights -- 4.2 Conflict Between Transparency of Evidence and Black Box Effect -- 4.3 Conflict Between Efficiency and Legality of Law Enforcement -- 4.4 Conflict Between Emerging Crimes and Lagging Laws -- 5 The Future of Digital Policing -- 5.1 Predictive Policing -- 5.2 Collaboration in Policing -- 5.3 Reflections on Enhanced Policing -- 6 Conclusion -- References -- The Dark Web and Digital Policing -- 1 Introduction -- 2 Background -- 3 Challenges -- 4 Recommendations -- 5 Discussion -- 6 Conclusion -- References -- Pre-emptive Policing: Can Technology be the Answer to Solving London's Knife Crime Epidemic? -- 1 Introduction -- 1.1 Statistics -- 1.1.1 Who Is Affected? -- 1.1.2 Why Knife Crime? -- 2 What Is A Knife Crime -- 3 Motivations and Risk Factors for Carrying Knives -- 3.1 Risk Factors -- 3.1.1 Gender -- 3.1.2 Ethnicity -- 3.1.3 Age -- 3.1.4 School Exclusion/Social Exclusion -- 3.1.5 Gangs -- 3.1.6 Adverse Childhood Experiences (ACEs) -- 3.1.7 Poor Relationship with the Police and Local Community Relationships with Police -- 3.1.8 Children and Young People Do Not Trust the Authorities to Protect Them -- 3.1.9 Poor Mental Health -- 3.1.10 Family Life.
3.1.11 Peer Relationships and Friends -- 3.1.12 Material Aspirations -- 3.1.13 Geographical Location -- 3.1.14 Poverty, Inequality, Deprivation and Austerity -- 3.1.15 Peer Pressure or Gang Involvement -- 3.1.16 Drug Dealing -- 3.1.17 Drug Using -- 3.1.18 Previous Arrest/Criminality -- 3.1.19 Fear and Intimidation, Protection -- 3.1.20 Social Status and Respect -- 3.1.21 Utility -- 3.1.22 Victim of Violent Crime -- 3.1.23 Bullying -- 3.1.24 Social Media -- 4 The London Metropolitan Police Force -- 4.1 Structure of MPS -- 4.1.1 The Met Comprises Four Business Groups -- 4.2 Policing Strategies in London Metropolitan Police Service (MPS) -- 4.2.1 Hot-Spot Policing -- 4.2.2 Stop and Search -- 4.2.3 Enhanced Mobility -- 5 Embracing Innovative Technology to Tackle Knife Crime -- 6 The Use of Big Data to Predict Knife-Enabled Homicides or Knife Offences in the London Metropolitan Area -- 6.1 How Can Visualisations Aid Pre-emptive Policing? -- 7 Conclusion -- References.