1. Record Nr. UNINA9910637731903321

Autore	Montasari Reza
Titolo	Countering Cyberterrorism : The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity / / by Reza Montasari
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	9783031219207 9783031219191
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (175 pages)
Collana	Advances in Information Security, , 2512-2193 ; ; 101
Disciplina	060 363.325
Soggetti	Computer networks - Security measures Artificial intelligence Computer crimes Mobile and Network Security Artificial Intelligence Cybercrime
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Introduction -- References -- Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom -- Abstract -- Introduction -- The Most Prevalent Cyber Threats -- The UK Cyber Landscape -- How Cyber Threats Are Identified in the UK Threats -- Types of Cyber-Attacks -- The UK Cybersecurity Policies and Practices Cybersecurity in Government Policies and Strategies -- Current Policies, Strategies, and Practices -- National Cyber Security Centre -- Active Cyber Defence Programme -- National Cyber Security Strategy 2022-2030 -- Recommendations -- Criticisms of the NCSC and Recommendations -- Criticisms of the ACD and Recommendations -- Criticisms of the NCSS 2022-2030 and Recommendations -- Recommendations for the Government’s Role -- Discussion and Conclusion- Key Findings -- Limitations of the Chapter -- Concluding Remarks -- References --

Internet of Things and Artificial Intelligence in National Security: Applications and Issues -- Abstract -- Introduction -- Background -- Definitions -- National and Domestic Security -- Definition of Artificial Intelligence -- The Internet of Things -- The Internet of Things Forensics -- AI and IoT in National and Domestic Security -- The Role of AI and IoT in Digital Security -- AI for Protecting IoT Devices against Hacking -- The Malicious Use of AI to Hack IoT Devices -- The Use of AI in the Military to Hack IoT Devices. - The Use of AI by Institutions to Safeguard Citizens -- AI and IoT in Political Security -- Deepfake and Mis- and Disinformation -- AI and the Formation of Filter Bubbles -- AI and Online Content Moderation -- AI and IoT in Physical Security -- Augmented Intelligence Analysis -- Military Weaponisation of AI and the IoT -- Privacy Implications of AI Algorithms -- Impacts of AI Algorithms on User Privacy -- Legal Frameworks for Privacy Relating AI Algorithms -- Potential Solutions for Privacy Implications -- Conclusion -- References -- Artificial Intelligence and the Internet of Things -- Forensics in a National Security Context -- Abstract -- Introduction -- AI Techniques in Automating Tasks of IoT Forensics -- A Brief Summary of IoT Forensics from Chapter 3 -- Types of AI Techniques Relevant to IoT Forensics -- Natural Language Processing -- Machine Learning -- Machine Learning and Anomaly Detection -- Machine Learning and Detection of Steganography -- Machine Learning and Detection of Steganography -- Sources and Detection of Algorithmic Bias -- Algorithmic Bias -- Sources of Algorithmic Bias -- Algorithmic Transparency and Military AI -- Recommendations -- Recommendations for Detecting Algorithmic Bias -- Recommendation for Algorithmic Transparency in Military AI Applications -- Conclusion -- References -- The Application of Big Data Predictive Analytics and Surveillance Technologies in the Field of Policing -- Abstract -- Introduction -- Key Concepts and History of AI- Predictive Policing -- History of AI -- Facial Recognition Technology -- 3D Facial Recognition -- Machine Learning -- SupervisedLearning -- Unsupervised Learning -- Reinforcement Learning -- Support Vector Machine -- Natural Language Processing -- Big Data -- RQ 1: The Use of AI by Law Enforcement I -- Big Data Predictive Analytics -- PredPol -- CompStat -- Person-Based Forecasting -- Innovative Surveillance Technology -- Hard and Soft Technology -- Closed-Circuit Television -- Facial Recognition Technology -- Body-Worn Cameras -- Social Media -- RQ 2: The Use of AI by Law Enforcement II -- ML and Data Mining in Policing -- Police Discrimination and Big Data -- DNA Databases and Big Data -- Recommendations -- Accountability and Transparency -- Bias in ML Algorithms -- Conclusion -- References -- The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights -- Abstract -- Introduction -- Background -- Big Data Predictive Analytics -- The Application of Predictive Policing -- Civil Liberties and National Security -- RQ 1: The Use of AI by Law Enforcement I -- Civil Liberties and National Security -- ChillingEffect, Privacy Rights and Freedom of Speech -- The Fourth Amendment and Stop and Search -- Striking a Smart Balance -- RQ 2: The Use of AI by Law Enforcement II -- Overpolicing of Certain Areas -- Focus on Crimes of the Poor -- System Avoidance -- Recommendations -- Conclusion -- References -- National Artificial Intelligence Strategies: A Comparison of the UK, EU and US Approaches with Those Adopted by State Adversaries -- Abstract -- Introduction -- AI Strategies of the UK, EU and US -- The UK AI Strategy -- The EU AI Strategy -- AI Strategies of Russia and China -- The Chinese AI Strategy -- The Russian AI Strategy -- Shortcomings and Recommendations -- Shortcomings of the UK AI Strategy -- Shortcomings of the EU AI

Strategy -- Shortcomings of the US AI Strategy -- Shortcomings of the Chinese AI Strategy -- Shortcomings of the Russian AI Strategy -- Conclusion -- References. .

Sommario/riassunto

This book provides a comprehensive analysis covering the confluence of Artificial Intelligence (AI), Cyber Forensics and Digital Policing in the context of the United Kingdom (UK), United States (US) and European Union (EU) national cybersecurity. More specifically, this book explores ways in which the adoption of AI algorithms (such as Machine Learning, Deep Learning, Natural Language Processing, and Big Data Predictive Analytics (BDPAs) transforms law enforcement agencies (LEAs) and intelligence service practices. It explores the roles that these technologies play in the manufacture of security, the threats to freedom and the levels of social control in the surveillance state. This book also examines the malevolent use of AI and associated technologies by state and non-state actors. Along with this analysis, it investigates the key legal, political, ethical, privacy and human rights implications of the national security uses of AI in the stated democracies. This book provides a set of policy recommendations to help to mitigate these challenges. Researchers working in the security field as well advanced level students in computer science focused on security will find this book useful as a reference. Cyber security professionals, network security analysts, police and law enforcement agencies will also want to purchase this book. .