Counter Terrorism Technologies A Critical Assessment Advanced Sciences And Technologies For Security Applications

#counter terrorism technologies #security applications advanced sciences #critical assessment anti-terror #advanced security tech review #terrorism prevention technologies

This critical assessment meticulously examines advanced sciences and cutting-edge technologies specifically developed for counter-terrorism efforts and broader security applications. It provides an in-depth evaluation of their effectiveness, ethical considerations, and strategic impact, offering crucial insights for professionals in the field.

Our collection supports both foundational studies and cutting-edge discoveries.

Welcome, and thank you for your visit.
We provide the document Advanced Security Applications Review you have been searching for.
It is available to download easily and free of charge.

This document remains one of the most requested materials in digital libraries online.
By reaching us, you have gained a rare advantage.
The full version of Advanced Security Applications Review is available here, free of charge.

Counter-Terrorism Technologies

This book critically discusses the role of technology for counter-terrorism in general, and for securing our vulnerable open societies in particular. It is set against the backdrop of the terrorist threat posed by the combined forces of Al Qaeda and ISIS/Daesh in the foreseeable future. The book commences by illuminating current and foreseeable tactics and weapons used by these implacable enemies – weapons that may well include chemical, biological, radiological and potentially even nuclear (CBRN) devices. In a second part, it introduces technologies already available or in development that promise an increase in safety and security when it comes to the dangers posed by these terrorists. This part also includes a critical discussion of advantages and disadvantages of such technologies that are, quite often, sold as a ‘silver bullet’ approach in the fight against terrorism. Controversies such as those triggered by the abuse of millimeter wave scanners deployed at several Western European airports will demonstrate that there are costs involved with regard to human rights. The third, analytical part takes the critical discussion further by arguing that the uncritical fielding of new surveillance and control technologies in parallel with the on-going outsourcing and privatization of key services of the state could well lead to dystopias as envisaged in a rather prescient way by the so-called cyperpunk novels of the 1980s. The book concludes with the question that any liberal democracy should ask itself: how far can we go with regard to hardening our societies against terrorist threats?

Science and Technology to Counter Terrorism

This volume presents the papers and summarizes the discussions of a workshop held in Goa, India, in January 2004, organized by the Indian National Institute of Advanced Science (NIAS) and the U.S. Committee on International Security and Arms Control (CISAC). During the workshop, Indian and U.S. experts examined the terrorist threat faced in both countries and elsewhere in the world, and explored opportunities for the U.S. and India to work together. Bringing together scientists and experts with common scientific and technical backgrounds from different cultures provided a unique opportunity to explore possible means of preventing or mitigating future terrorist attacks.

Security by Design

This edited book captures salient global security challenges and presents 'design' solutions in dealing with wicked problems. Through case studies and applied research this book reveals the many perspectives, tools and approaches to support security design. Security design thereby can support risk and threat analysis, risk communication, problem framing and development of interventions strategies. From the refugee crisis to economic slowdowns in emerging markets, from ever-rising numbers of terrorist and cyberattacks to global water shortages, to the proliferation of the Internet of Things and its impact on the security of our homes, cities and critical infrastructure, the current security landscape is diverse and complex. These global risks have been in the headlines in the last year (Global Risks Report) and pose significant security challenges both nationally and globally. In fact, national security is no longer just national. Non-state actors, cyber NGO, rising powers, and hybrid wars and crimes in strategic areas pose complex challenges to global security. In the words of Horst Rittel (1968):"Design is an activity, which aims at the production of a plan, which plan -if implemented- is intended to bring about a situation with specific desired characteristics without creating unforeseen and undesired side and after effects."

Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution

This book represents an interdisciplinary academic endeavour intended to provide readers with a comprehensive, balanced, and nuanced examination of critical issues at the intersection of cyberspace, cyberterrorism, and national and international security. It draws insights from a range of diverse fields, including Computer Science, Social Science, Political Science, International Relations, Criminology, and Law. Furthermore, the book investigates the field of Artificial Intelligence (AI) and related technologies, exploring their dual role in this dynamic landscape of contemporary cyberthreats, with both constructive and malicious implications. The book comprises four distinct themes, with each theme represented by a dedicated Part. Within this organisational framework, each overarching theme is systematically explored through a series of chapters, providing readers with a clear and thematic roadmap for their journey through the content. Part I, Understanding Terrorism and Counter-Terrorism Strategies, of the book explores complexities surrounding contemporary global security challenges. It serves as the foundational segment of the book, consisting of three chapters that critically analyse various dimensions of terrorism and the strategies implemented to combat it. Part II, Cyberterrorism Landscape, of the book offers an in-depth assessment of the current cyberterrorism landscape. This section comprises two critical chapters, each contributing to a comprehensive understanding of the contemporary threats posed by cyberterrorism and their implications for national security. Part III, Countering Cyberterrorism with Technology, of the book forms the core of the book's exploration into leveraging technology to mitigate the threats of cyberterrorism. This section includes four critical chapters, collectively providing an in-depth understanding of the intersection between technology and counterterrorism strategies. Part IV, Artificial Intelligence and National and International Security, of the book delves into the complex relationship between AI technology and the broader security landscape. Comprising three pivotal chapters, this section provides a detailed understanding of AI's transformative role in shaping the future of national and international security. This comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. This comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. This comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. This comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. This comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. This comprehensive resource serves as a valuable reference

for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. This comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. This comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. /divThis comprehensive resource serves as a valuable reference for law enforcement, policymakers, cybersecurity experts, researchers, academics, and technology enthusiasts interested in counter-terrorism efforts. By exploring the intricate landscape of cyberspace, this book equips readers with knowledge essential to addressing the evolving challenges posed by cyber terrorism. /div

Handbook of Security Science

This handbook offers insights into how science (physical, natural and social) and technology can support new developments to manage the complexity resident within the threat and risk landscape. The security landscape can be described as dynamic and complex stemming from the emerging threats and risks that are both persistent and transborder. Globalization, climate change, terrorism, transnational crime can have significant societal impact and forces one to re-evaluate what ‘national security’ means. Recent global events such as mass migration, terrorist acts, pandemics and cyber threats highlight the inherent vulnerabilities in our current security posture. As an interdisciplinary body of work, the Handbook of Security Science captures concepts, theories and security science applications, thereby providing a survey of current and emerging trends in security. Through an evidence-based approach, the collection of chapters in the book delivers insightful and comprehensive articulation of the problem and solution space associated with the complex security landscape. In so doing the Handbook of Security Science introduces scientific tools and methodologies to inform security management, risk and resilience decision support systems; insights supporting design of security solutions; approaches to threat, risk and vulnerability analysis; articulation of advanced cyber security solutions; and current developments with respect to integrated computational and analytical solutions that increase our understanding of security physical, social, economic, and technological interrelationships and problem space.

Making the Nation Safer

Vulnerabilities abound in U.S. society. The openness and efficiency of our key infrastructures â€" transportation, information and telecommunications systems, health systems, the electric power grid, emergency response units, food and water supplies, and others â€" make them susceptible to terrorist attacks. Making the Nation Safer discusses technical approaches to mitigating these vulnerabilities. A broad range of topics are covered in this book, including: Nuclear and radiological threats, such as improvised nuclear devices and "dirty bombs;" Bioterrorism, medical research, agricultural systems and public health; Toxic chemicals and explosive materials; Information technology, such as communications systems, data management, cyber attacks, and identification and authentication systems; Energy systems, such as the electrical power grid and oil and natural gas systems; Transportation systems; Cities and fixed infrastructures, such as buildings, emergency operations centers, and tunnels; The response of people to terrorism, such as how quality of life and morale of the population can be a target of terrorists and how people respond to terrorist attacks; and Linked infrastructures, i.e. the vulnerabilities that result from the interdependencies of key systems. In each of these areas, there are recommendations on how to immediately apply existing knowledge and technology to make the nation safer and on starting research and development programs that could produce innovations that will strengthen key systems and protect us against future threats. The book also discusses issues affecting the government's ability to carry out the necessary science and engineering programs and the important role of industry, universities, and states, counties, and cities in homeland security efforts. A long term commitment to homeland security is necessary to make the nation safer, and this book lays out a roadmap of how science and engineering can assist in countering terrorism.

Emergent Information Technologies and Enabling Policies for Counter-Terrorism

Explores both counter-terrorism and enabling policy dimensions of emerging information technologies in national security After the September 11th attacks, "connecting the dots" has become the watchword for using information and intelligence to protect the United States from future terrorist attacks. Advanced and emerging information technologies offer key assets in confronting a secretive, asymmetric, and networked enemy. Yet, in a free and open society, policies must ensure that these powerful technologies are used responsibly, and that privacy and civil liberties remain protected. Emergent Information Technologies and Enabling Policies for Counter-Terrorism provides a unique, integrated treatment of cutting-edge counter-terrorism technologies and their corresponding policy options. Featuring contributions from nationally recognized authorities and experts, this book brings together a diverse knowledge base for those charged with protecting our nation from terrorist attacks while preserving our civil liberties. Topics covered include: Counter-terrorism modeling Quantitative and computational social science Signal processing and information management techniques Semantic Web and knowledge management technologies Information and intelligence sharing technologies Text/data processing and language translation technologies Social network analysis Legal standards for data mining Potential structures for enabling policies Technical system design to support policy Countering terrorism in today's world requires innovative technologies and corresponding creative policies; the two cannot be practically and realistically addressed separately. Emergent Information Technologies and Enabling Policies for Counter-Terrorism offers a comprehensive examination of both areas, serving as an essential resource for students, practitioners, researchers, developers, and decision-makers.

Applications for Artificial Intelligence and Digital Forensics in National Security

This book delivers insights into how social science and technology might aid new advancements in managing the complexity inherent within national and international security landscape. The digital policing landscape is dynamic and intricate, emanating from crimes that are both persistent and transnational. Globalization, human and drug trafficking, cybercrime, terrorism, and other forms of transnational crime can have a significant impact on societies around the world. This necessitates a reassessment of what crime, national security, and policing mean. Recent global events such as human and drug trafficking, the COVID-19 pandemic, violent protests, cyber threats, and terrorist activities underline vulnerabilities residing in our current security and digital policing posture. As an interdisciplinary collection of studies, this book encapsulates concepts, theories, and technology applications, offering a comprehensive analysis of current and emerging trends and threats within the context of national and international security. Undertaking an evidence-based approach, this book offers an extraordinarily perceptive and detailed account of issues and solutions related to the complex national and international security landscape. To this end, the book: presents insights into emerging and potential technological and methodological solutions as well as advancements in relation to integrated computational and analytical solutions that could be deployed for the purposes of national and international security; provides a comprehensive analysis of technical, ethical, legal, privacy, and civil liberty challenges stemming from the aforementioned advancements; and, accordingly, offers detailed recommendations supporting the design and implementation of best practices including technical, ethical, and legal approaches for national and international security uses. The research contained in the book fits well into the larger body of work on various aspects of AI, cybersecurity, national security, digital forensics, cyberterrorism, ethics, human rights, cybercrime, and law. It provides a valuable reference for LEAs and security organizations, policymakers, cybersecurity experts, digital forensic practitioners, researchers, academicians, graduates and advanced undergraduates, and other stakeholders with an interest in national and global security.

Water Safety, Security and Sustainability

This book focuses on threats, especially contaminants, to drinking water and the supply system, especially in municipalities but also in industrial and even residential settings. The safety, security, and suitability landscape can be described as dynamic and complex stemming from necessity and hence culpability due to the emerging threats and risks, vis-a-vis globalization resulting in new forms of contaminants being used due to new technologies. The book provides knowledge and guidance for engineers, scientists, designers, researchers, and students who are involved in water, sustainability, and study of security issues. This book starts out with basics of water usage, current statistics, and an overview ofwater resources. The book then introduces different scenarios of safety and security and areas that researchers need to focus. Following that, the book presents different types of contaminants

– inadvertent, intentional, or incidental. The next section presents different methodologies of contamination sensing/detection and remediation strategies as per guidance and standards set globally. The book then concludes with selected chapters on water management, including critical infrastructure that is critical to maintaining safe water supplies to cities and municipalities. Each chapter includes descriptive information for professionals in their respective fields. The breadth of chapters offers insights into how science (physical, natural, and social) and technology can support new developments to manage the complexity resident within the evolving threat and risk landscape.

Cyber-Security in Critical Infrastructures

This book presents a compendium of selected game- and decision-theoretic models to achieve and assess the security of critical infrastructures. Given contemporary reports on security incidents of various kinds, we can see a paradigm shift to attacks of an increasingly heterogeneous nature, combining different techniques into what we know as an advanced persistent threat. Security precautions must match these diverse threat patterns in an equally diverse manner; in response, this book provides a wealth of techniques for protection and mitigation. Much traditional security research has a narrow focus on specific attack scenarios or applications, and strives to make an attack “practically impossible.” A more recent approach to security views it as a scenario in which the cost of an attack exceeds the potential reward. This does not rule out the possibility of an attack but minimizes its likelihood to the least possible risk. The book follows this economic definition of security, offering a management scientific view that seeks a balance between security investments and their resulting benefits. It focuses on optimization of resources in light of threats such as terrorism and advanced persistent threats. Drawing on the authors’ experience and inspired by real case studies, the book provides a systematic approach to critical infrastructure security and resilience. Presenting a mixture of theoretical work and practical success stories, the book is chiefly intended for students and practitioners seeking an introduction to game- and decision-theoretic techniques for security. The required mathematical concepts are self-contained, rigorously introduced, and illustrated by case studies. The book also provides software tools that help guide readers in the practical use of the scientific models and computational frameworks.

Contemporary Terrorism Studies

'Contemporary Terrorism Studies' is a comprehensive and accessible introduction to terrorism studies, examining key issues and debates, and featuring dedicated sections on terrorism and counter-terrorism. - When do individuals radicalise? - Can terrorism be rational? - How can we define terrorism? - What is the role of women in terrorism? - Can states be terrorist? World leading experts answer these questions in Contemporary Terrorism Studies, the first textbook to provide a multi-disciplinary, methodologically plural, and richly diverse introduction to terrorism studies. Contemporary Terrorism Studies covers the main approaches in terrorism studies, and is structured into three comprehensive sections. The first on 'The State of Terrorism Studies' maps the development and historical context of the discipline, and looks to the future of terrorism studies. Part two on 'Issues and Debates in Terrorism Studies' examines key contentious questions and debates such as the role of women, technology, and the media in terrorism. The final part, part three on 'Countering Terrorism' focuses specifically on counterterrorism: it's instruments, foreign policy, legal frameworks, and organisations. Overall, text will engage students, and establish a confident understanding of the subject. The textbook has been developed with pedagogical features to help enhance student learning. Each chapter contains case studies to highlight real world examples of political violence, questions for reflection to encourage critical thinking, and suggestions for further reading which provide useful sources for further reading, essays, and exam preparation. Furthermore, a consistent, accessible tone, and jargon-free writing style makes Contemporary Terrorism Studies the clearest guide to understanding terrorism. Digital formats and resources Contemporary Terrorism Studies is available for students and institutions to purchase in a variety of formats, and is supported by online resources. - The e-book offers a mobile experience and convenient access along with hyperlinks to question pointers, and a library of web links, helping you to broaden your knowledge and understanding terrorism studies: www.oxfordtextbooks.co.uk/ebooks - Student resources: additional case studies, guidance on accessing databases, pointers for tackling the questions for reflection, and suggested web links organised by chapter are available online. - Lecturer resources: customisable PowerPoint slides to adapt and use in teaching

Counter-Terrorism, Ethics and Technology

This open access book brings together a range of contributions that seek to explore the ethical issues arising from the overlap between counter-terrorism, ethics, and technologies. Terrorism and our responses pose some of the most significant ethical challenges to states and people. At the same time, we are becoming increasingly aware of the ethical implications of new and emerging technologies. Whether it is the use of remote weapons like drones as part of counter-terrorism strategies, the application of surveillance technologies to monitor and respond to terrorist activities, or counterintelligence agencies use of machine learning to detect suspicious behavior and hacking computers to gain access to encrypted data, technologies play a significant role in modern counter-terrorism. However, each of these technologies carries with them a range of ethical issues and challenges. How we use these technologies and the policies that govern them have broader impact beyond just the identification and response to terrorist activities. As we are seeing with China, the need to respond to domestic terrorism is one of the justifications for their rollout of the “social credit system.” Counter-terrorism technologies can easily succumb to mission creep, where a technology’s exceptional application becomes normalized and rolled out to society more generally. This collection is not just timely but an important contribution to understand the ethics of counter-terrorism and technology and has far wider implications for societies and nations around the world.

Protecting Individual Privacy in the Struggle Against Terrorists

All U.S. agencies with counterterrorism programs that collect or "mine" personal data-such as phone records or Web sites visited-should be required to evaluate the programs' effectiveness, lawfulness, and impacts on privacy. A framework is offered that agencies can use to evaluate such information-based programs, both classified and unclassified. The book urges Congress to re-examine existing privacy law to assess how privacy can be protected in current and future programs and recommends that any individuals harmed by violations of privacy be given a meaningful form of redress. Two specific technologies are examined: data mining and behavioral surveillance. Regarding data mining, the book concludes that although these methods have been useful in the private sector for spotting consumer fraud, they are less helpful for counterterrorism because so little is known about what patterns indicate terrorist activity. Regarding behavioral surveillance in a counterterrorist context, the book concludes that although research and development on certain aspects of this topic are warranted, there is no scientific consensus on whether these techniques are ready for operational use at all in counterterrorism.

Countering Bioterrorism

The attacks of September 11 and the release of anthrax spores revealed enormous vulnerabilities in the U.S. public-health infrastructure and suggested similar vulnerabilities in the agricultural infrastructure as well. The traditional public health response-surveillance (intelligence), prevention, detection, response, recovery, and attribution-is the paradigm for the national response not only to all forms of terrorism but also to emerging infectious diseases. Thus, investments in research on bioterrorism will have enormous potential for application in the detection, prevention, and treatment of emerging infectious diseases that also are unpredictable and against which we must be prepared. The deciphering of the human genome sequence and the complete elucidation of numerous pathogen genomes, our rapidly increasing understanding of the molecular mechanisms of pathogenesis and of immune responses, and new strategies for designing drugs and vaccines all offer unprecedented opportunities to use science to counter bioterrorist threats. But these same developments also allow science to be misused to create new agents of mass destruction. Hence the effort to confront bioterrorism must be a global one. Countering Bioterrorism makes the following recommendations: Recommendation 1: All agencies with responsibility for homeland security should work together to establish stronger and more meaningful working ties between the intelligence, S&T, and public health communities. Recommendation 2: Federal agencies should work cooperatively and in collaboration with industry to develop and evaluate rapid, sensitive, and specific early-detection technologies. Recommendation 3: Create a global network for detection and surveillance, making use of computerized methods for real-time reporting and analysis to rapidly detect new patterns of disease locally, nationally, and ultimately- internationally. The use of high-throughput methodologies that are being increasingly utilized in modern biological research should be an important component of this expanded and highly automated surveillance strategy. Recommendation 4: Use knowledge of complex biological patterns and high-throughput laboratory automation to classify and diagnose infections in patients in primary care settings. Recommendation 5: USDA should create an agency for control and prevention of plant disease. This agency should have the capabilities necessary to deal effectively with biothreats.

Prevent strategy

The Prevent strategy, launched in 2007 seeks to stop people becoming terrorists or supporting terrorism both in the UK and overseas. It is the preventative strand of the government's counter-terrorism strategy, CONTEST. Over the past few years Prevent has not been fully effective and it needs to change. This review evaluates work to date and sets out how Prevent will be implemented in the future. Specifically Prevent will aim to: respond to the ideological challenge of terrorism and the threat we face from those who promote it; prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support; and work with sectors and institutions where there are risks of radicalization which need to be addressed

Global Trends 2040

"The ongoing COVID-19 pandemic marks the most significant, singular global disruption since World War II, with health, economic, political, and security implications that will ripple for years to come." -Global Trends 2040 (2021) Global Trends 2040-A More Contested World (2021), released by the US National Intelligence Council, is the latest report in its series of reports starting in 1997 about megatrends and the world's future. This report, strongly influenced by the COVID-19 pandemic, paints a bleak picture of the future and describes a contested, fragmented and turbulent world. It specifically discusses the four main trends that will shape tomorrow's world: - Demographics-by 2040, 1.4 billion people will be added mostly in Africa and South Asia. - Economics-increased government debt and concentrated economic power will escalate problems for the poor and middleclass. - Climate-a hotter world will increase water, food, and health insecurity. - Technology-the emergence of new technologies could both solve and cause problems for human life. Students of trends, policymakers, entrepreneurs, academics, journalists and anyone eager for a glimpse into the next decades, will find this report, with colored graphs, essential reading.

National security through technology

This White Paper, divided into two parts, lays out the Government's policy objectives in relation to "National Security through Technology\

Equipment, support and technology for UK defence and security

This Green Paper looks at the procurement of equipment, support, and technology for UK defence and security and follows on from the Strategic Defence and Security Review (SDSR) (ISBN 9780101794824), published on the 19th October 2010. The UK today faces a different and more complex range of threats than last century. The most serious threats include international terrorism, hostile attacks upon UK cyberspace, a major natural hazard or an international military crisis. Therefore the Government needs access to critical technologies and skills to underpin the UK's national security and to achieve these by setting out clear plans covering the following areas: (i) acquiring the equipment needed; (ii) support for the equipment and its users; (iii) investing or acquiring the necessary technologies to secure these objectives both now and in the future. This consultation paper and the responses it receives will form part of a White Paper to be published in 2011.

Technology and Security in the 21st Century

The current policing landscape has seen the rise in serious and organized crime across the globe. Criminals are innovating in real-time leveraging cyber, social media, enhanced surveillance to support their activities. In so doing, the criminal landscape has become transnational whereby collaborative networks have flourished thereby creating greater complexity and novel threats for the international policing community. As new threats to local, regional, national and global security are emerging, leveraging science and technology innovations has become more important. Advances in big data analytics, cyber forensics, surveillance, modeling and simulation has led to a more data driven, hypothesis generated and model informed approach. Novel science and technology innovations are presented in this edited book to provide insights and pathways that challenges the emerging and complex criminal threat landscape by supporting policing operations.

Science Informed Policing

The confluence of the September 11, 2001 terrorist attack and the U.S. Army's historic role to support civil authorities has resulted in substantial new challenges for the Army. To help meet these challenges,

the Assistant Secretary of the Army for Research and Technology requested the National Research Council (NRC) carry out a series of studies on how science and technology could assist the Army prepare for its role in homeland security (HLS). The NRC's Board on Army Science and Technology formed the Committee on Army Science and Technology for Homeland Security to accomplish that assignment. The Committee was asked to review relevant literature and activities, determine areas of emphasis for Army S&T in support of counter terrorism and anti-terrorism, and recommend high-pay-off technologies to help the Army fulfill its mission. The Department of Defense Counter-Terrorism Technology Task Force identified four operational areas in reviewing technical proposals for HLS operations: indications and warning; denial and survivability; recovery and consequence management; and attribution and retaliation. The study sponsor asked the Committee to use these four areas as the basis for its assessment of the science and technology (S&T) that will be important for the Army's HLS role. Overall, the Committee found that: There is potential for substantial synergy between S&T work carried out by the Army for its HLS responsibilities and the development of the next generation Army, the Objective Force. The Army National Guard (ARNG) is critical to the success of the Army's HLS efforts.

Contest

This book provides international perspective for those studying or working in the security domain, from enforcement to policy. It focuses on non-traditional threats in a landscape that has been described as transnational in nature and incorporates natural disasters, gang violence, extremism and terrorism, amongst other issues. Chapters provide innovative thinking on themes including cyber security, maritime security, transnational crime, human security, globalization and economic security. Relevant theoretical frameworks are presented and readers are expertly guided through complex threats, from matters pertaining to health security which pose threats not only to humans but also have significant national security implications, to issues regarding critical infrastructure vulnerability and the complexity of understanding terrorist operations. Authors reveal how emerging uncertainties regarding global critical infrastructure and supply chain security, food security, and health security are linked to the notion of human security. Security professionals, policy makers and academics will all gain from the insights, strategies and perspectives in this book. It builds understanding of the deepening and broadening domain of security studies and provides a valuable reference text for courses on security studies and international relations.

Science and Technology for Army Homeland Security

Based on a series of regional meetings on university campuses with officials from the national security community and academic research institutions, this report identifies specific actions that should be taken to maintain a thriving scientific research environment in an era of heightened security concerns. Actions include maintaining the open exchange of scientific information, fostering a productive environment for international scholars in the U.S., reexamining federal definitions of sensitive but unclassified research, and reviewing policies on deemed export controls. The federal government should establish a standing entity, preferably a Science and Security Commission, that would review policies regarding the exchange of information and the participation of foreign-born scientists and students in research.

Exploring the Security Landscape: Non-Traditional Security Challenges

"Published in cooperation with NATO Emerging Security Challenges Division"--T.p.

Science and Security in a Post 9/11 World

This book explores how social media and its advances enables citizens to empower themselves during a crisis. The book addresses the key issues related to crises management and social media as the new platform to assist citizens and first responders dealing with multiple forms of crisis, from major terrorist attacks, larger scale public disorder, large-scale movement of people across borders, and natural disasters. The book is based on the results and knowledge gained during the European Commission ATHENA project which has been addressing critical issues in contemporary crisis management and social media and smart mobile communications. This book is authored by a mix of global contributors from across the landscape of academia, emergency response and experts in government policy and private industry. This title explores and explains that during a modern crisis, the public self-organizes into voluntary groups, adapt quickly to changing circumstances, emerge as leaders and experts and

perform life-saving actions; and that they are increasingly reliant upon the use of new communications media to do it.

A Question Of Trust

This book is about the strategic relevance of quantum technologies. It debates the military-specific aspects of this technology. Various chapters of this book cohere around two specific themes. The first theme discusses the global pattern of ongoing civilian and military research on quantum computers, quantum cryptography, quantum communications and quantum internet. The second theme explicitly identifies the relevance of these technologies in the military domain and the possible nature of quantum technology-based weapons. This thread further debates on quantum (arms) race at a global level in general, and in the context of the USA and China, in particular. The book argues that the defence utility of these technologies is increasingly becoming obvious and is likely to change the nature of warfare in the future.

Defence Against Terrorism

This book aims to uncover the root causes of natural and man-made disasters by going beyond the typical reports and case studies conducted post-disaster. It opens the black box of disasters by presenting ‘forensic analysis approaches’ to disasters, thereby revealing the complex causality that characterizes them and explaining how and why hazards do, or do not, become disasters. This yields ‘systemic’ strategies for managing disasters. Recently the global threat landscape has seen the emergence of high impact, low probability events. Events like Hurricane Katrina, the Great Japan Earthquake and tsunami, Hurricane Sandy, Super Typhoon Haiyan, global terrorist activities have become the new norm. Extreme events challenge our understanding regarding the interdependencies and complexity of the disaster aetiology and are often referred to as Black Swans. Between 2002 and 2011, there were 4130 disasters recorded that resulted from natural hazards around the world. In these, 1,117,527 people perished and a minimum of US$1,195 billion in losses were reported. In the year 2011 alone, 302 disasters claimed 29,782 lives; affected 206 million people and inflicted damages worth a minimum of estimated US$366 billion.

Application of Social Media in Crisis Management

The COVID-19 pandemic is not only a threat to our health and economy, but also has strong implications for defence and security. Indeed, defence leaders have highlighted a second fight surrounding the spread of COVID-19, namely disinformation and preparing to face adversaries willing to exploit the public health crisis for nefarious purposes. The current pandemic is a breeding ground for the propagation of disinformation, as it represents the first major global health event in which large social media platforms have become the main distributor of information. This multi-national edited volume consists of contributions from Defence Science, academia and industry, including NATO Headquarters, United States, Netherlands, Singapore, United Kingdom and Norway. The content is aimed at a diverse audience, including NATO members, researchers from defence and security organizations, academics, and militaries including analysts and practitioners, as well as policy makers. This volume focuses on various aspects of COVID-19 disinformation, including identifying global dominant disinformation narratives and the methods used to spread disinformation, examining COVID-19 disinformation within the broader context of the cognitive domain, examining the psychological effects of COVID-19 disinformation and COVID-19 disinformation on instant messaging platforms, along with examining various countermeasures to disinformation.

Quantum Technologies and Military Strategy

This book is nothing less than a complete and comprehensive survey of the state-of-the-art of terrorism informatics. It covers the application of advanced methodologies and information fusion and analysis. It also lays out techniques to acquire, integrate, process, analyze, and manage the diversity of terrorism-related information for international and homeland security-related applications. The book details three major areas of terrorism research: prevention, detection, and established governmental responses to terrorism. It systematically examines the current and ongoing research, including recent case studies and application of terrorism informatics techniques. The coverage then presents the critical and relevant social/technical areas to terrorism research including social, privacy, data confidentiality, and legal challenges.

Disaster Forensics

In 2004, the Government Accountability Office provided a report detailing approximately 200 government-based data-mining projects. While there is comfort in knowing that there are many effective systems, that comfort isn't worth much unless we can determine that these systems are being effectively and responsibly employed. Written by one of the most respected consultants in the area of data mining and security, Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies reviews the tangible results produced by these systems and evaluates their effectiveness. While CSI-type shows may depict information sharing and analysis that are accomplished with the push of a button, this sort of proficiency is more fiction than reality. Going beyond a discussion of the various technologies, the author outlines the issues of information sharing and the effective interpretation of results, which are critical to any integrated homeland security effort. Organized into three main sections, the book fully examines and outlines the future of this field with an insider's perspective and a visionary's insight. Section 1 provides a fundamental understanding of the types of data that can be used in current systems. It covers approaches to analyzing data and clearly delineates how to connect the dots among different data elements Section 2 provides real-world examples derived from actual operational systems to show how data is used, manipulated, and interpreted in domains involving human smuggling, money laundering, narcotics trafficking, and corporate fraud Section 3 provides an overview of the many information-sharing systems, organizations, and task forces as well as data interchange formats. It also discusses optimal information-sharing and analytical architectures Currently, there is very little published literature that truly defines real-world systems. Although politics and other factors all play into how much one agency is willing to support the sharing of its resources, many now embrace the wisdom of that path. This book will provide those individuals with an understanding of what approaches are currently available and how they can be most effectively employed.

COVID-19 Disinformation: A Multi-National, Whole of Society Perspective

Scores of talented and dedicated people serve the forensic science community, performing vitally important work. However, they are often constrained by lack of adequate resources, sound policies, and national support. It is clear that change and advancements, both systematic and scientific, are needed in a number of forensic science disciplines to ensure the reliability of work, establish enforceable standards, and promote best practices with consistent application. Strengthening Forensic Science in the United States: A Path Forward provides a detailed plan for addressing these needs and suggests the creation of a new government entity, the National Institute of Forensic Science, to establish and enforce standards within the forensic science community. The benefits of improving and regulating the forensic science disciplines are clear: assisting law enforcement officials, enhancing homeland security, and reducing the risk of wrongful conviction and exoneration. Strengthening Forensic Science in the United States gives a full account of what is needed to advance the forensic science disciplines, including upgrading of systems and organizational structures, better training, widespread adoption of uniform and enforceable best practices, and mandatory certification and accreditation programs. While this book provides an essential call-to-action for congress and policy makers, it also serves as a vital tool for law enforcement agencies, criminal prosecutors and attorneys, and forensic science educators.

Terrorism Informatics

As the so-called Arab Spring has slid into political uncertainty, lingering insecurity and civil conflict, European and American initial enthusiasm for anti-authoritarian protests has given way to growing concerns that revolutionary turmoil in North Africa may in fact have exposed the West to new risks. Critical in cementing this conviction has been the realisation that developments originated from Arab Mediterranean countries and spread to the Sahel have now such a potential to affect Western security and interests as to warrant even military intervention, as France’s operation in Mali attests. EU and US involvement in fighting piracy off the Horn of Africa had already laid bare the nexus between their security interests and protracted crises in sub-Saharan Africa. But the new centrality acquired by the Sahel after the Arab uprisings – particularly after Libya’s civil war – has elevated this nexus to a new, larger dimension. The centre of gravity of Europe’s security may be swinging to Africa, encompassing a wide portion of the continental landmass extending south of Mediterranean coastal states. The recrudescence of the terrorist threat from Mali to Algeria might pave the way to an American pivot to Africa, thus requiring fresh thinking on how the European Union and the United States can better collaborate with each other and with relevant regional actors.

Data Mining for Intelligence, Fraud & Criminal Detection

This book deals with two areas: Global Commons and Security: inextricably melted together and more relevant than ever in a world which is ever globalized and... with an incognita looming on the horizon: the effects of the Coronavirus pandemic upon the International Relations and globalization. Global Commons have always been relevant. It was Mahan who argued that the first and most obvious light in which the sea presents itself from the political and social point of view, is that of a great highway; or better, perhaps, of a wide common... Nowadays, this view has been further developed and, in addition to the unique legal implications that the Global Commons introduce, they are viewed, more and more intently, as a common pool of resources. Or perhaps, not that common... Resources, the key word! Which has to be always supplemented by two key words: access and security. And still, another one: data, the cyberspace contribution to the equation.

Building Resilience Against Terrorism

In the decade that followed 9/11, technologies and technology policies became central to homeland security. For example, the U.S. erected new border defenses with remote sensors and biometric scanners, and deployed new autonomous air warfare capabilities, such as the drone program. Looking at efforts to restore security after 9/11, the work examines issues such as the rise in technology spending, the various scenarios of mass terror, and America's effort to ensure that future engagements will take place far from the homeland. Operation Iraqi Freedom, Iran's emergence as nuclear threat, and North Korea's acceleration of its missile program are analyzed along with the "axis of evil" and America's effort to create a ballistic missile shield to thwart this emerging threat to its security. By focusing on the technologies of homeland security rather than on cyber warfare itself, the work offers a unique and needed survey that will appeal to anyone involved with the study and development of homeland and strategic security.

ECCWS 2019 18th European Conference on Cyber Warfare and Security

Department of Homeland Security Appropriations Bill, 2005