Terror On The Internet The New Arena The New Challenges

Terrorist groups with a shared enemy or ideology have ample reason to work together, even if they are primarily pursuing different causes. Although partnering with another terrorist organization has the potential to bolster operational effectiveness, efficiency, and prestige, international alliances may expose partners to infiltration, security breaches, or additional counterterrorism attention. Alliances between such organizations, which are suspicious and secretive by nature, must also overcome significant barriers to trust—the exposure to risk must be balanced by the promise of increased lethality, resiliency, and longevity. In Why Terrorist Groups Form International Alliances, Tricia Bacon argues that although it may seem natural for terrorist groups to ally, groups actually face substantial hurdles when attempting to ally and, when alliances do form, they are not evenly distributed across pairs. Instead, she demonstrates that when terrorist groups seek allies to obtain new skills, knowledge, or capacities for resource acquisition and mobilization, only a few groups have the ability to provide needed training, safe haven, infrastructure, or cachet. Consequently, these select few emerge as preferable partners and become hubs around which other groups cluster. According to Bacon, shared enemies and common ideologies do not cause alliances to form but create affinity to bind partners and guide partner selection. Bacon examines partnerships formed by the Popular Front for the Liberation of Palestine, Al-Qaida, and Egyptian jihadist groups, among others, in a series of case studies spanning the dawn of international terrorism in the 1960s to the present. Why Terrorist Groups Form International Alliances advances our understanding of the motivations of terrorist alliances and offers insights useful to counterterrorism efforts to disrupt these dangerous relationships.

The events and aftermath of September 11, 2001, profoundly changed the course of history of the nation. They also brought the phenomenon known as terrorism to the forefront of the nation's consciousness. As it became thus focused, the limits of scientific understanding of terrorism and the capacity to develop policies to deal with it became even more evident. The objective of this report is to bring behavioral and social science perspectives to bear on the nature, determinants, and domestic responses to contemporary terrorism as a way of making theoretical and practical knowledge more adequate to the task. It also identifies areas of research priorities for the behavioral and social sciences.

Terrorist use of the Internet has become a focus of media, policy, and scholarly attention in recent years. Terrorists use the Internet in a variety of ways, the most important being for propaganda purposes and operations-related content, but it is also potentially a means or target of attack.This book presents revised versions of a selection of papers delivered at the NATO Advanced Research Workshop (ARW) on 'Terrorists' Use of the Internet' held in Dublin, Ireland in June 2016. One aim of the workshop was to nurture dialogue between members of the academic, policy and practitioner communities, so the 60 delegates from 13 countries who attended the workshop included representatives from each of these. The participants encompassed a wide range of expertise (including engineering, computer science, law, criminology, political science, international relations, history, and linguistics) and the chapters contained herein reflect these diverse professional and disciplinary backgrounds. The workshop also aimed to address the convergence of threats. Following an introduction which provides an overview of the various ways in which terrorists use the Internet, the book's remaining 25 chapters are grouped into 5 sections on cyber terrorism and critical infrastructure protection; cyber-enabled terrorist financing; jihadi online propaganda; online counterterrorism; and innovative approaches and responses.The book will be of interest to all those who need to maintain an awareness of the ways in which terrorists use the Internet and require an insight into how the threats posed by this use can be countered.

As terrorist organizations such as Al-Qaeda have been transformed from hierarchical organizations to more fluid networks, countering terrorism requires an understanding of networks. These networks evolve rapidly in response to actions to thwart them, leading to an ongoing struggle of terrorist and antiterrorist networks. In this chapter, Boaz Ganor examines the evolving threat of terrorist networks and network-based responses. As he notes, “it takes a network to beat a network.” He also examines direct and indirect implications for business organizations.

Cyberterrorism and the misuse of Internet for terrorist purposes represents a serious threat, since many essential aspects of today's society are completely dependent upon the functioning of computer systems and the Internet. Further to the adoption by the Council of Europe of the Cybercrime Convention (2001) and the Convention on the Prevention of Terrorism (2005), its Committee of Experts on Terrorism (CODEXTER) has been studying this matter and surveying the situation in member states to evaluate whether existing legal instruments are sufficient to combat this emerging form of crime. This publication contains an expert report prepared by the Max Planck Institute, which evaluates the main problems that arise in the context of cyberterrorism and provides recommendations, together with reports on the situation in the member and observer states of the Council of Europe and the relevant Council of Europe conventions

This major new Handbook synthesises more than two decades of scholarly research, and provides a comprehensive overview of the field of terrorism studies. The content of the Handbook is based on the responses to a questionnaire by nearly 100 experts from more than 20 countries as well as the specific expertise and experience of the volume editor and the various contributors. Together, they guide the reader through the voluminous literature on terrorism, and propose a new consensus definition of terrorism, based on an extensive review of existing conceptualisations. The work also features a large collection of typologies and surveys a wide range of theories of terrorism. Additional chapters survey terrorist databases and provide a guide to available resources on terrorism in libraries and on the Internet. It also includes the most comprehensive World Directory of Extremist, Terrorist and other Organizations associated with Guerrilla Warfare, Political Violence, Protest and Organized- and Cyber-Crime. The Routledge Handbook of Terrorism Research will be an essential work of reference for students and researchers of terrorism and political violence, security studies, criminology, political science and international relations, and of great interest to policymakers and professionals in the field of counter-terrorism.

"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.

Paul Thompson's The Terror Timeline offers a complete and thorough history of the many roads that converged on 9/11, including the development of Islamic fundamentalism, the activities of bin Laden and al-Qaeda, and the failures of U.S. investigations and counterterrorism efforts. It traces the actions (and inactions) of every important figure in the war on terror, both before and after 9/11, bringing them together in a volume that offers a comprehensive and provocative look at this complex subject. Packed with

little-known facts and disturbing questions, The Terror Timeline is the first complete reference guide to the events of 9/11 and the war on terror -- the definitive primer on the most momentous issue of our times.

Drawing from a unique dataset compiled over a decade, this text examines why women join terrorist organizations and why groups choose to incorporate them into their structures and operations, covering both religious and ethno-nationalist-motivated terrorism and conflict.

Never have so many possessed the means to be so lethal. The diffusion of modern technology (robotics, cyber weapons, 3-D printing, autonomous systems, and artificial intelligence) to ordinary people has given them access to weapons of mass violence previously monopolized by the state. In recent years, states have attempted to stem the flow of such weapons to individuals and non-state groups, but their efforts are failing. As Audrey Kurth Cronin explains in Power to the People, what we are seeing now is an exacerbation of an age-old trend. Over the centuries, the most surprising developments in warfare have occurred because of advances in technologies combined with changes in who can use them. Indeed, accessible innovations in destructive force have long driven new patterns of political violence. When Nobel invented dynamite and Kalashnikov designed the AK-47, each inadvertently spurred terrorist and insurgent movements that killed millions and upended the international system. That history illuminates our own situation, in which emerging technologies are altering society and redistributing power. The twenty-first century "sharing economy" has already disrupted every institution, including the armed forces. New "open" technologies are transforming access to the means of violence. Just as importantly, higher-order functions that previously had been exclusively under state military control - mass mobilization, force projection, and systems integration - are being harnessed by non-state actors. Cronin closes by focusing on how to respond so that we both preserve the benefits of emerging technologies yet reduce the risks. Power, in the form of lethal technology, is flowing to the people, but the same technologies that empower can imperil global security - unless we act strategically.

Offers information on cyber-terrorism, the use of computing resources to intimidate or coerce others, provided by Don Gotterbarn, Jimmy Sproles, and Will Byars. Offers information on protection from cyber-terrorism, the importance to computing professionals and the rest of society, and ethical issues.

In the tradition of nonpartisanship and current analysis that is the hallmark of CQ Press, CQ Researcher readers investigate important and controversial policy issues. The Second Edition of Issues in Terrorism and Homeland Security covers timely issues such as Terrorism and the Internet, Homeland Security, Interrogating the CIA, and Prosecuting Terrorists. Each article is engaging and reader-friendly, and opens with a human interest story that will spark the interest of students. In addition, each article gives substantial background and analysis of a particular issue as well as useful pedagogical features to inspire critical thinking and to help students grasp and review key material. Offer your students the balanced reporting, complete overviews, and engaging writing that CQ Researcher has consistently provided for more than 80 years. This text is an ideal supplementary textbook for upper-division undergraduate and graduate courses on Terrorism, Homeland Security, and U.S. National Security. New To This Edition: Includes six new articles on the following topics: Terrorism and the Internet Hate Groups Human Rights Issues Homeland Security Interrogating the CIA Prosecuting Terrorists Key Features: Pro/con box that examines two competing sides of a single question A detailed chronologies of key dates and events An annotated bibliography and web resources Outlook sections that address possible regulation and initiatives from Capitol Hill and the White House over the next 5 to 10 years Photos, charts, graphs, and maps

Terrorist organizations might increase use of digital cryptocurrencies to support their activities. RAND researchers consider the needs of such groups and the advantages and disadvantages of the cryptocurrency technologies available to them.

This book explores the interface between terrorism and the internet and presents contemporary approaches to understanding violent extremism online. The volume focuses on four issues in particular: terrorist propaganda on the internet; radicalisation and the internet; counter campaigns and approaches to disrupting internet radicalisation; and approaches to researching and understanding the role of the internet in radicalisation. The book brings together expertise from a wide range of disciplines and geographical regions including Europe, the US, Canada and Australia. These contributions explore the various roles played by the Internet in radicalisation; the reasons why terroristic propaganda may or may not influence others to engage in violence; the role of political conflict in online radicalisation; and the future of research into terrorism and the internet. By covering this broad range of topics, the volume will make an important and timely addition to the current collections on a growing and international subject. This book will be of much interest to students and researchers of cyber-security, internet politics, terrorism studies, media and communications studies, and International Relations.

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.

Two defense experts explore the collision of war, politics, and social media, where the most important battles are now only a click away. Through the weaponization of social media, the internet is changing war and politics, just as war and politics are changing the internet. Terrorists livestream their attacks, “Twitter wars” produce real?world casualties, and viral misinformation alters not just the result of battles, but the very fate of nations. The result is that war, tech, and politics have blurred into a new kind of battlespace that plays out on our smartphones. P. W. Singer and Emerson Brooking tackle the mind?bending questions that arise when war goes online and the online world goes to war. They explore how ISIS copies the Instagram tactics of Taylor Swift, a former World of Warcraft addict foils war crimes thousands of miles away, internet trolls shape elections, and China uses a smartphone app to police the thoughts of 1.4 billion citizens. What can be kept secret in a world of networks? Does social media expose the truth or bury it? And what role do ordinary people now play in international conflicts? Delving into the web’s darkest corners, we meet the unexpected warriors of social media, such as the rapper turned jihadist PR czar and the Russian hipsters who wage unceasing infowars against the West. Finally, looking to the crucial years ahead, LikeWar outlines a radical new paradigm for understanding and defending against the unprecedented threats of our networked world.

In the world of terrorism, knowledge is a critical asset. Recent studies have revealed that, among international terrorists, there is a global sharing of ideas, tactics, strategies, and lessons learned. Teaching Terror examines this sharing of information in the terrorist world, shaping our understanding of, and response to, the global threat of terrorism. Chapters cover various aspects of individual and organizational learning, some using a general level of analysis and others presenting case studies of individual terrorist groups. These groups teach each other through a variety of means, including training camps and the Internet. Terrorist networks are also learning organizations, drawing on situational awareness, adapting their behavior, and, to give one example, improving not just their use of improvised explosive devices, but also rendering technology such as unmanned aerial vehicles and satellite phones ineffective. This book provides a wealth of insights on the transfer of knowledge in the world of terrorism, and offers policy implications for counterterrorism professionals, scholars, and policymakers.

Since the symmetrical-global East-West conflict was decided in favor of the West, numerous asymmetrical conflicts have erupted around the globe. Jihadist terrorism has spread beyond the borders of the regions in which it had its origin and has reached a global dimension. Research and analysis of the root causes and underlying conditions, motivators and enablers of terrorism including the agitation propaganda of jihadist terrorists are vital to shaping appropriate countermeasures to the threat from Islamic terrorism. This paper looks at the jihadist use of strategic communication management techniques. The mass media and especially the Internet have become the key enablers and the main strategic communication assets for terrorists and have ensured them a favorable communication asymmetry.

The Oklahoma City bombing, intentional crashing of airliners on September 11, 2001, and anthrax attacks in the fall of 2001 have made Americans acutely aware of the impacts of terrorism. These events and continued threats of terrorism have raised questions about the impact on the psychological health of the nation and how well the public health infrastructure is able to meet the psychological needs that will likely result. Preparing for the Psychological Consequences of Terrorism highlights some of the critical issues in responding to the psychological needs that result from terrorism and provides possible options for intervention. The committee offers an example for a public health strategy that may serve as a base from which plans to prevent and respond to the psychological consequences of a variety of terrorism events can be formulated. The report includes recommendations for the training and education of service providers, ensuring appropriate guidelines for the protection of service providers, and developing public health surveillance for preevent, event, and postevent factors related to psychological consequences.

An essential reference for scholars and others whose work brings them into contact with managing, policing and regulating online behaviour, the Handbook of Internet Crime emerges at a time of rapid social and technological change. Amidst much debate about the dangers presented by the Internet and intensive negotiation over its legitimate uses and regulation, this is the most comprehensive and ambitious book on cybercrime to date. The Handbook of Internet Crime gathers together the leading scholars in the field to explore issues and debates surrounding internet-related crime, deviance, policing, law and regulation in the 21st century. The Handbook reflects the range and depth of cybercrime research and scholarship, combining contributions from many of those who have established and developed cyber research over the past 25 years and who continue to shape it in its current phase, with more recent entrants to the field who are building on this tradition and breaking new ground. Contributions reflect both the global nature of cybercrime problems, and the international span of scholarship addressing its challenges.

Written by a certified Arabic linguist from the Defense Language Institute with extensive background in decoding encrypted communications, this cyber-thriller uses a fictional narrative to provide a fascinating and realistic "insider's look" into technically sophisticated covert terrorist communications over the Internet. The accompanying CD-ROM allows readers to "hack along" with the story line, by viewing the same Web sites described in the book containing encrypted, covert communications. Hacking a Terror NETWORK addresses the technical possibilities of Covert Channels in combination with a very real concern: Terrorism. The fictional story follows the planning of a terrorist plot against the United States where the terrorists use various means of Covert Channels to communicate and hide their trail. Loyal US agents must locate and decode these terrorist plots before innocent American citizens are harmed. The technology covered in the book is both real and thought provoking. Readers can realize the threat posed by these technologies by using the information included in the CD-ROM. The fictional websites, transfer logs, and other technical information are given exactly as they would be found in the real world, leaving the reader to test their own ability to decode the terrorist plot. Cyber-Thriller focusing on increasing threat of terrorism throughout the world. Provides a fascinating look at covert forms of communications used by terrorists over the Internet. Accompanying CD-ROM allows users to "hack along" with

the fictional narrative within the book to decrypyt.
Collects and analyzes seventy years of communist crimes that offer details on Kim Sung's Korea, Vietnam under "Uncle Ho," and Cuba under Castro.
Drawing on a seven-year study of the World Wide Web and a wide variety of literature, the author examines how modern terrorist organizations exploit the Internet to raise funds, recruit, and propagandize, as well as to plan and launch attacks and to publicize their chilling results.
This new edition of John Horgan's critically acclaimed book is fully revised and expanded. The book presents a critical analysis of our existing knowledge and understanding of terrorist psychology. Despite the on-going search for a terrorist pathology, the most insightful and evidence-based research to date not only illustrates the lack of any identifiable psychopathology in terrorists, but demonstrates how frighteningly 'normal' and unremarkable in psychological terms are those who engage in terrorist activity. By producing a clearer map of the processes that impinge upon the individual terrorist, a different type of terrorist psychology emerges, one which has clearer implications for efforts at countering and disrupting violent extremism in today's world. In this 2nd edition, Horgan further develops his approach to the arc of terrorism by delving deeper into his IED model of Involvement, Engagement and Disengagement – the three phases of terrorism experienced by every single terrorist. Drawing on new and exciting research from the past decade, with new details from interviews with terrorists ranging from al-Qaeda to left-wing revolutionaries, biographies and autobiographies of former terrorists, and insights from historic and contemporary terrorist attacks since 2005, Horgan presents a fully revised and expanded edition of his signature text. This new edition of The Psychology of Terrorism will be essential reading for students of terrorism and political violence, and counterterrorism studies, and recommended for forensic psychology, criminology, international security and IR in general.
This handbook introduces the reader to the field of terrorism investigation. Describing how terrorists operate and how they differ from other criminals, it provides an outline of how terrorism investigations should be conducted. By helping investigators to develop skills and knowledge, this guide helps them to prepare prosecutable cases against terrorists.
This book is devoted primarily to papers prepared by American and Russian specialists on cyber terrorism and urban terrorism. It also includes papers on biological and radiological terrorism from the American and Russian perspectives. Of particular interest are the discussions of the hostage situation at Dubrovko in Moscow, the damge inflicted in New York during the attacks on 9/11, and Russian priorities in addressing cyber terrorism.
The war on terrorism has not been won, Gabriel Weimann argues in Terrorism in Cyberspace, the successor to his seminal Terror on the Internet. Even though al-Qaeda's leadership has been largely destroyed and its organization disrupted, terrorist attacks take 12,000 lives annually worldwide, and jihadist terrorist ideology continues to spread. How? Largely by going online and adopting a new method of organization. Terrorist structures, traditionally consisting of loose-net cells, divisions, and subgroups, are ideally suited for flourishing on the Internet through websites, e-mail, chat rooms, e-groups, forums, virtual message boards, YouTube, Google Earth, and other outlets. Terrorist websites, including social media platforms, now number close to 10,000. This book addresses three major questions: why and how terrorism went online; what recent trends can be discerned—such as engaging children and women, promoting lone wolf attacks, and using social media; and what future threats can be expected, along with how they can be reduced or countered. To answer these questions, Terrorism in Cyberspace analyzes content from more than 9,800 terrorist websites, and Weimann, who has been studying terrorism online since 1998, selects the most important kinds of web activity, describes their background and history, and surveys their content in terms of kind and intensity, the groups and prominent individuals involved, and effects. He highlights cyberterrorism against financial, governmental, and engineering infrastructure; efforts to monitor, manipulate, and disrupt terrorists' online efforts; and threats to civil liberties posed by ill-directed efforts to suppress terrorists' online activities as future, worrisome trends.
In the post-September 11 world, Al Qaeda is no longer the central organizing force that aids or authorizes terrorist attacks or recruits terrorists. It is now more a source of inspiration for terrorist acts carried out by independent local groups that have branded themselves with the Al Qaeda name. Building on his previous groundbreaking work on the Al Qaeda network, forensic psychiatrist Marc Sageman has greatly expanded his research to explain how Islamic terrorism emerges and operates in the twenty-first century. In Leaderless Jihad, Sageman rejects the views that place responsibility for terrorism on society or a flawed, predisposed individual. Instead, he argues, the individual, outside influence, and group dynamics come together in a four-step process through which Muslim youth become radicalized. First, traumatic events either experienced personally or learned about indirectly spark moral outrage. Individuals interpret this outrage through a specific ideology, more felt and understood than based on doctrine. Usually in a chat room or other Internet-based venues, adherents share this moral outrage, which resonates with the personal experiences of others. The outrage is acted on by a group, either online or offline. Leaderless Jihad offers a ray of hope. Drawing on historical analogies, Sageman argues that the zeal of jihadism is self-terminating; eventually its followers will turn away from violence as a means of expressing their discontent. The book concludes with Sageman's recommendations for the application of his research to counterterrorism law enforcement efforts.
Cyber Crime and Cyber Terrorism Investigator’s Handbook is a vital tool in the arsenal of today’s computer programmers, students, and investigators. As computer networks become ubiquitous throughout the world, cyber crime, cyber terrorism, and cyber war have become some of the most concerning topics in today’s security landscape. News stories about Stuxnet and PRISM have brought these activities into the public eye, and serve to show just how effective, controversial, and worrying these tactics can become. Cyber Crime and Cyber Terrorism Investigator’s Handbook describes and analyzes many of the motivations, tools, and tactics behind cyber attacks and the defenses against them. With this book, you will learn about the technological and logistic framework of cyber crime, as well as the social and legal backgrounds of its prosecution and investigation. Whether you are a law enforcement professional, an IT specialist, a researcher, or a student, you will find valuable insight into the world of cyber crime and cyber warfare. Edited by experts in computer security, cyber investigations, and counter-terrorism, and with contributions from computer researchers, legal experts, and law enforcement professionals, Cyber Crime and Cyber Terrorism Investigator’s Handbook will serve as your best reference to the modern world of cyber crime. Written by experts in cyber crime, digital investigations, and counter-terrorism Learn the motivations, tools, and tactics used by cyber-attackers, computer security

professionals, and investigators Keep up to date on current national and international law regarding cyber crime and cyber terrorism See just how significant cyber crime has become, and how important cyber law enforcement is in the modern world
This thoughtful text demonstrates how the mass media constructs a politics of fear in the United States. Using a social interactionist perspective, the chapters examines such issues as the expansion of surveillance on the Internet, the construction of a terrorism-fighting hero to promote patriotism, the use of social media by terror groups, the fear of the other fostered by the refugee crisis and western radicalization, as well as the mass-mediated reaction to recent terrorist attacks. Also covered are the politics of fear involving disease (Ebola, Zika), social control efforts, and harsh attacks on American governmental officials for not keeping people safe from harm. All chapters in this new edition have been updated with descriptions and relevant analysis of significant events, including two Israeli-Hamas wars, terrorism attacks (e.g., Boston Marathon, Charlie Hebdo, San Bernadino, etc.), global reactions—often hostility—to refugees in the United States and especially Europe, the development of ISIS, surveillance (Wiki Leaks, Snowden, NSA), and the growing significance of social media. The text explains how the social construction of fear is used to steer public and foreign policy, arguing that security policies to protect the citizenry from violence have become control systems that most often curtail privacy and civil liberties.
Terrorism continues to evolve; altered sources of funding, changes in national governments and the ever increasing importance of the internet mean that international cooperation in the development and implementation of strategies to counteract terrorist activity remain an important priority worldwide. This book contains articles arising from the presentations by eleven experts from five countries, delivered at the NATO Centre of Excellence – Defence against Terrorism (COE-DAT) advanced training course (ATC) entitled Enhancing Cooperation in Defence against Terrorism, held in Astana, Kazakhstan, in September 2010. The aim of this ATC was to stimulate discussion and facilitate interoperability between these five countries and NATO in the fight against terrorism.The book opens with an overview of the landscape in which terrorism currently exists, and a reminder that a new approach is needed in the fight against terrorism to replace the Cold War model we have become accustomed to. The remaining articles cover a wide range of issues: countering the ideology of terrorism; legal aspects of combating terrorism and responding to terrorist use of the internet; the links between terrorism and organised crime; energy security; weapons of mass destruction; international humanitarian law; suicide terrorism; the role of the media in terrorism and counterterrorism; and dilemmas in counterterrorism strategy. In addition to the presentations from the ATC, the book includes two articles by Brigitte Nacos of Columbia University: The Importance of Strategic Communication and Public Diplomacy in Combating Terrorism, and Terrorism Media and Censorship.
The virulent new brand of Islamic extremism threatening the West In November 2015, ISIS terrorists massacred scores of people in Paris with coordinated attacks on the Bataclan concert hall, cafés and restaurants, and the national sports stadium. On Bastille Day in 2016, an ISIS sympathizer drove a truck into crowds of vacationers at the beaches of Nice, and two weeks later an elderly French priest was murdered during morning Mass by two ISIS militants. Here is Gilles Kepel's explosive account of the radicalization of a segment of Muslim youth that led to those attacks—and of the failure of governments in France and across Europe to address it. It is a book everyone in the West must read. Terror in France shows how these atrocities represent a paroxysm of violence that has long been building. The turning point was in 2005, when the worst riots in modern French history erupted in the poor, largely Muslim suburbs of Paris after the accidental deaths of two boys who had been running from the police. The unrest—or "French intifada"—crystallized a new consciousness among young French Muslims. Some have fallen prey to the allure of "war of civilizations" rhetoric in ways never imagined by their parents and grandparents. This is the highly anticipated English edition of Kepel's sensational French bestseller, first published shortly after the Paris attacks. Now fully updated to reflect the latest developments and featuring a new introduction by the author, Terror in France reveals the truth about a virulent new wave of jihadism that has Europe as its main target. Its aim is to divide European societies from within by instilling fear, provoking backlash, and achieving the ISIS dream—shared by Europe's Far Right—of separating Europe's growing Muslim minority community from the rest of its citizens.
The electric power delivery system that carries electricity from large central generators to customers could be severely damaged by a small number of well-informed attackers. The system is inherently vulnerable because transmission lines may span hundreds of miles, and many key facilities are unguarded. This vulnerability is exacerbated by the fact that the power grid, most of which was originally designed to meet the needs of individual vertically integrated utilities, is being used to move power between regions to support the needs of competitive markets for power generation. Primarily because of ambiguities introduced as a result of recent restricting the of the industry and cost pressures from consumers and regulators, investment to strengthen and upgrade the grid has lagged, with the result that many parts of the bulk high-voltage system are heavily stressed. Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. Such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction. Further well-planned and coordinated attacks by terrorists could leave the electric power system in a large region of the country at least partially disabled for a very long time. Although there are many examples of terrorist and military attacks on power systems elsewhere in the world, at the time of this study international terrorists have shown limited interest in attacking the U.S. power grid. However, that should not be a basis for complacency. Because all parts of the economy, as well as human health and welfare, depend on electricity, the results could be devastating. Terrorism and the Electric Power Delivery System focuses on measures that could make the power delivery system less vulnerable to attacks, restore power faster after an attack, and make critical services less vulnerable while the delivery of conventional electric power has been disrupted.
Online Terrorist Propaganda, Recruitment, and Radicalization is most complete treatment of the rapidly growing phenomenon of how terrorists’ online presence is utilized for terrorism funding, communication, and recruitment purposes. The book offers an in-depth coverage of the history and development of online "footprints" to target new converts, broaden their messaging, and increase their influence. Chapters present the emergence of various groups; the advancement of terrorist groups’ online presences; their utilization of video, chat room, and social media; and the current capability for propaganda, training, and recruitment. With contributions from leading experts in the field—including practitioners and terrorism researchers—the coverage moves from general factors to specific groups practices as relate to

Islamic State of Iraq and the Levant (ISIL), and numerous other groups. Chapters also examine the lone wolf phenomenon as a part of the disturbing trend of self-radicalization. A functional, real-world approach is used regarding the classification of the means and methods by which an online presence is often utilized to promote and support acts of terrorism. Online Terrorist Propaganda, Recruitment, and Radicalization examines practical solutions in identifying the threat posed by terrorist propaganda and U.S. government efforts to counter it, with a particular focus on ISIS, the Dark Web, national and international measures to identify, thwart, and prosecute terrorist activities online. As such, it will be an invaluable resources for intelligence professionals, terrorism and counterterrorism professionals, those researching terrorism funding, and policy makers looking to restrict the spread of terrorism propaganda online.

This book examines two key themes in terrorism studies, the radicalization process and counter-terrorism policies, through the lens of social networks. The book aims to show that networks should be at the forefront not only when analysing terrorists, but also when assessing the responses to their actions. The volume makes a unique contribution by addressing two relatively new themes for terrorism studies. First it puts social relations and cooperation issues at the forefront – an approach often identified as crucial to future breakthroughs in the field. Second, many contributions tackle the role of the Internet in the process of radicalization and in recruitment more generally, a highly debated topic in the field today. In addition, the book provides a valuable mix of review essays, critical essays, and original empirical studies. This balanced approach is also found in the topics covered by the authors, as well as their academic disciplines, which include sociology, computer science, geography, history, engineering, and criminology as well as political science. Many of the true advances in terrorism studies depend on the successful collaboration of multi-disciplinary teams, each with a different set of methodological and conceptual tools. This volume reflects the newfound diversity in this field and is a true product of its time. This book will be of much interest to students of terrorism studies, social networks, security studies, sociology, criminology and international relations in general.

Terrorist organizations use many technologies as they plan and stage attacks. This book explores the purpose and manner of the use of communication and computer technologies, their net effect, and security forces' possible responses. The authors conclude that, instead of developing direct counters to these technologies, exploiting their use and the information they manage to enable more direct security force operations is a more promising option.