TERRORISM AND ADVANCED TECHNOLOGIES IN PSYCHOLOGICAL WARFARE

NEW RISKS, NEW OPPORTUNITIES TO COUNTER THE TERRORIST THREAT

TERRORISM, HOT SPOTS AND CONFLICT-RELATED ISSUES

Additional books and e-books in this series can be found on Nova's website under the Series tab.

TERRORISM AND ADVANCED TECHNOLOGIES IN PSYCHOLOGICAL WARFARE

NEW RISKS, NEW OPPORTUNITIES TO COUNTER THE TERRORIST THREAT

DARYA BAZARKINA

EVGENY PASHENTSEV

AND

GREG SIMONS

EDITORS

nova
science publishers
New York

We have partnered with Copyright Clearance Center to make it easy for you to obtain permissions to reuse content from this publication. Simply navigate to this publication's page on Nova's website and locate the "Get Permission" button below the title description. This button is linked directly to the title's permission page on copyright.com. Alternatively, you can visit copyright.com and search by title, ISBN, or ISSN.

For further questions about using the service on copyright.com, please contact:
Copyright Clearance Center
Phone: +1-(978) 750-8400   Fax: +1-(978) 750-4470   E-mail: info@copyright.com.

NOTICE TO THE READER

The Publisher has taken reasonable care in the preparation of this book, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained in this book. The Publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the readers' use of, or reliance upon, this material. Any parts of this book based on government reports are so indicated and copyright is claimed for those parts to the extent applicable to compilations of such works.

Independent verification should be sought for any data, advice or recommendations contained in this book. In addition, no responsibility is assumed by the Publisher for any injury and/or damage to persons or property arising from any methods, products, instructions, ideas or otherwise contained in this publication.

This publication is designed to provide accurate and authoritative information with regard to the subject matter covered herein. It is sold with the clear understanding that the Publisher is not engaged in rendering legal or any other professional services. If legal or any other expert assistance is required, the services of a competent person should be sought. FROM A DECLARATION OF PARTICIPANTS JOINTLY ADOPTED BY A COMMITTEE OF THE AMERICAN BAR ASSOCIATION AND A COMMITTEE OF PUBLISHERS.

Additional color graphics may be available in the e-book version of this book.

This book provides a valuable tool for students and practitioners by collecting different aspects of terrorism and advanced technologies into a single coherent publication. It fills in the gap in the academic literature by considering the role of emerging technologies in the hands of terrorist, as well as the use of psychological warfare. The text is engaging and well written, making it accessible for both professional, as well as non-specialists and students who need to gain a working knowledge of the problems. It is rigorous and contemporary. The publication implements international approach by presenting regulations, policies, and case studies from different jurisdictions. It also implements interdisciplinary approach, by bringing together the issues of law, politics, economy, military, cyberspace, biology, and many others.

Dr Damian M. Bielicki, Lecturer in Law, Director of the Law & Technology Research Group, Department of Law, Kingston University, London, United Kingdom. Email: D.Bielicki@kingston.ac.uk

The fact that the authors come from different countries and belong to different academic disciplines is a plus, offering a broad perspective on the means of overcoming the terrorist threat presented in the social sciences, culture, religion, media communication, Internet or computer technologies (artificial intelligence and machine learning). The book fills a gap of research of a prognostic nature that combines a consideration of the problems of new technologies and the destructive actions of aggressive actors in international relations.

Natalia Kharitonova DSc, Associate Professor, Historical Faculty, Lomonosov Moscow State University, Moscow, Russia. Email: natahari@yandex.ru

The dramatic development of AI technologies makes mankind to face new global challenges related to malicious use of AI (MUAI). The enthusiasm around recent success stories of machine learning often ignores the vulnerability of data and knowledge exchange, which may have catastrophic consequences from terrorist attacks. Even simple data distortion in neural networks and other black-box AI models may result in changing software-based decisions, not to mention autonomous intelligent agents. The book draws attention to very important issues of the current technological revolution and very timely pleas for deeper

cooperation between governmental and international decision centers with AI researchers and engineers.

Professor Sergei O. Kuznetsov, Head of International Laboratory on Intelligent Systems and Structural Analysis, National Research University Higher School of Economics, Moscow, Russia. Email: skuznetsov@hse.ru

The dynamic security environment compels us to understand the threats and risks facing our organizations environments. The edited Book by Darya Bazarkina, Evgeny Pashentsev and Greg Simons on "Terrorism and Advanced Technologies in Psychological Warfare: New Risks, New Opportunities to Counter the Terrorist Threats" allows the security professionals to comprehend the trends and motives of the perpetrators of terrorist acts which are always changing. This publication is undoubtedly a step in the right direction for a proper understanding of factors responsible for terrorism, technological development-psychological warfare in the 21st century!

Professor John M. Nomikos, Director, Research Institute for European and American Studies (RIEAS), Athens, Greece. Email: jnomikos@rieas.gr

Advanced technologies give new opportunities for the development of world terrorism. AI, for example, helps to penetrate into the deeper layers of a person's consciousness, influence his or her psyche, and evoke new emotions. Digital technologies, on the one hand, help to establish communications, and on the other, completely imperceptibly, distort the cultural code, tear friendly groups of people into pieces. The spirituality of society is falling due to the fact that natural speech is replaced by an artificial digital signal. This book, based on deep scientific research and in an accessible form, reveals dangers from different angles, helping to prevent the hazard for all humanity.

Professor Alexander Raikov, Doctor of Technical Sciences, Winner of the Russian Government award in the field of Science and Technology, Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. Email: anraikov@mail.ru

The book edited by Darya Bazarkina, Evgeny Pashentsev and Greg Simons is a useful guide to analyze in full a complex and dynamic topic as the link between terrorism, new technologies and psychological warfare. This volume contents relevant and diverse sections both in theoretical and empirical terms. Authors offer a variety of approaches working on specific scenarios and actors such the ISIS. If I had to mention the main reason to recommend the book, I would choose the attention in detail devoted to Artificial Intelligence and the impacts and challenges that derive from its growing usage by state and non-state actors.

Rubén Ruiz-Ramas, Assistant Professor at the Department of Political Science and Administration, UNED; Vice Dean for International Relations and Communication, Faculty of Political Sciences and Sociology at the UNED, Spain. Email: ruizramas@gmail.com

The book offers the great opportunity to understand the profound interrelationships between the digital revolution, the ways of diffusion and action of contemporary terrorism, the possibilities and effectiveness of prevention and contrast actions. The added value of the systemic analysis offered by the book lies in the approach followed that draws the reader's attention to the dichotomy: between what the new information and communication technologies allow a terrorist organization and what, on the contrary, allow the international community and states for an effective community protection. It is the right way in the fight against the terrorist threat that requires, of course, proper information, but above all a real understanding of the phenomenon.

Marco Ricceri, Secretary General, Eurispes Institute, Rome, Italy. Email: riccerimarco@hotmail.com

The interest and relevance of this very innovative book lies in the highlighting and the deciphering of the complex and new mechanisms which are at work with the increasing use of new technologies in the context of psychological warfare and terrorist strategies, and how they can change the geopolitical configuration. Not only are the angles of analysis varied according to the authors and the themes, but the work underlines the duality risks/opportunities inherent with new technologies, including the emergence of artificial intelligence which is addressed there in an enlightening way. In addition to the diagnosis, solutions focusing on the positive use of new technologies are also proposed to counter the terrorist threat. This book containing an excellent collection of essays is therefore essential for researchers but also professionals at the political and administrative level involved in the fight against terrorism to anticipate new threats and build a response strategy.

Pierre-Emmanuel Thomann, professor of geopolitics, France; President of Eurocontinent, Brussels, Belgium. Email: pierre-emmanuel.thomann@eurocontinent.eu

Artificial Intelligence has the potential to make radical positive changes in diverse industries from health care to science and from transportation to agriculture. However, less is known about this technology's possible malicious use. There is a concern that AI's detrimental use can be a severe threat to cybersecurity, political security, and physical security in the wrong hand. Terrorists, for example, can apply AI in cyberattacks, fake news and video generation, automated hacking, and even finding and exploiting vulnerabilities of AI systems. This book, in three parts, provides in-depth information about how terrorists use the Internet for their evil purposes. What the emergence of AI-based tools and technologies mean for both counter-terrorism agencies and the terrorists, and how it is modifying the cultural, philosophical, and political dimension in the fight against terrorism. The book is a recommended read for anybody interested in new perspectives that AI brings to the war on terror.

Dr. Mitt Nowshade Kabir
CEO,
Trouvus.com and Flerika.com
Email: nowshade@gmail.com

This edited collection provides a comprehensive assessment of the security threats that result from the abuse of advanced digital technologies such as social and mobile media, online environments, artificial intelligence, or unmanned areal vehicles by terrorist actors. The contributions mirror a wide spectrum of approaches to the emergence of terrorism, whilst convincingly demonstrating the increasingly important role of technology.

<div align="right">

Dr. Florian Zollmann, Lecturer in Journalism, Newcastle University.
Email: florian.zollmann@ncl.ac.uk

</div>

I value the main premise of the book: advanced technologies can boost the influence of terrorist organizations and, at the same time, allow these organizations to incorporate images of technological progress in their propaganda. Overall, it makes this entire edited volume a must-read book for various audiences. I highly recommend it.

<div align="right">

Dr. Jonathan Matusitz is currently a tenured associate professor in the Nicholson School of Communication and Media

</div>

Information about the contributors of endorsements

Dr Damian M. Bielicki holds a PhD in International Law. He is a director of the Law & Technology Research Group at Kingston University London. He has over 10 years of experience in the field of Space Law. He has been a Lecturer in Space Law and Cyber Law at Birkbeck, University of London. He is also a Lecturer in Law at Kingston University London and a Visiting Lecturer in Regent's University London. Damian completed International Space University's Space Studies Program at NASA Ames Research Center in California. He also worked on different projects at the European Space Agency. He was one of the founders and leads of the Space Exploration Group at Space Generation Advisory Council in support of the United Nations Programme on Space Applications. He is an author and co-author of several research outputs on space law and cyber law. He is the founder of the Space Law Centre, the world's largest database of space law and policy related issues (www.spacelawcentre.org). Email: D.Bielicki@kingston.ac.uk

Natalia Kharitonova. DSc in Politics, Associate Professor and Vice-Dean at the Historical Faculty in Lomonosov Moscow State University (MSU). Natalia is an expert on the post-Soviet space, Coordinator of the Joint Eurasian Expert Network (JEEN), Leading Expert at the Crisis Situations Research Center (Russia and Malta). In 2004 – 2009 she was a head of the special projects at the Information and Analytical Center in MSU "Russia – Ukraine", "Russia – Kazakhstan", "Energy Security In The Post-Soviet Space", since 2005 she is a Head of the Analytical Unit at the MSU Information and Analytical Center. Author of the monographs "Transdniestrian Conflict (1988-2012)" (2015), "Transdniestrian Conflict: Current Plots" (2018), "Transdniestrian Conflict: Negotiation Process within the Framework of Political Settlement (1992-2018)" (2019), more than 100 publications in academic journals and collections of articles, more than 100 newspaper publications, expert interviews and discussions on radio and television in Russia and CIS countries. Email: natahari@yandex.ru

Dr. Mitt Nowshade Kabir is a seasoned entrepreneur with broad experience in international business, technology investment, and e-commerce. CEO, Trouvus.com and Flerika.com. His present business and academic interests cover strategy, innovation, entrepreneurship, and technologies such as artificial intelligence, semantic technologies, blockchain, and knowledge management. He has served as an advisor to various governments and also consults and helps boards and businesses in areas like advanced technologies, business development, and innovation strategies. Dr. Kabir holds a Ph.D. in Information Technology, an MSc in Computer Science, an MBA, and a Doctorate in Business Administration. Author of several books, the last one is Knowledge-Based Social Entrepreneurship: Understanding Knowledge Economy, Innovation, and the Future of Social Entrepreneurship (Palgrave Studies in ... Innovation, and Entrepreneurship for Growth). Palgrave Macmillan 2019. Email: nowshade@gmail.com

Sergei O. Kuznetsov. Tenured Professor (2016) at National Research University Higher School of Economics. He graduated from Moscow Institute for Physics and Technology in 1985. After that he was a researcher at All-Russia Institute on Scientific and Technical Information (VINITI), where he defended his PhD thesis on methods of machine learning and knowledge discovery. In 1999-2005 he was a Humboldt research fellow and invited professor at TU-Dresden (Dresden Uiversity of Technology, Germany). Doctor of Sciences in Theoretical Foundations of Computer Science (2002) From 2006, he is head of Department for Data Analysis and Artificial intelligence, International Laboratory of Intelligent Systems and Structural Analysis, academic supervisor of Data Science master program at National Research University Higher School of Economics, Moscow. Since 2010: member of the Editorial Board of the International Journal of General Systems and a member of the editorial Board of the journal "Business Informatics", since 2018 a member of the Editorial Board of Information Sciences. He has about 163 publications in the field of NLP in the period from 2014 to 2019. skuznetsov@hse.ru

John M. Nomikos (PhD) is the Director at the Research Institute for European and American Studies, Chairman, European Intelligence Academy (EIA) and Founding Editor, Journal of European and American Intelligence Studies (JEAIS)- (former Mediterranean and Balkan Intelligence (JMBI). He is Assistant Professor in the Webster University (Athens Campus). He is Member of the Advisory Board for the Master Security Studies and Information Analysis (MASIS) at the American University in the United Arab Emirates (UAE) and a Fellow in the International Association for Counter-Terrorism and Security Professionals (IACSPSEA). He has done research and studied in various research institutions in USA, UK, Norway, Finland, Germany and Israel. He was awarded the "2019 Life Achievement for the Development of Intelligence Studies in Europe" by the International Association for Intelligence Education - European Chapter (IAFIE -Europe). John M. Nomikos directed the Greek team in a consortium of five countries (Northern Ireland-UK, Spain, Germany, Bulgaria, and Israel) and completed successfully a two year (2009-2011) European Union-FP7 research project titled: SAFE COMMS on "Counter-terrorism Crisis Communication Strategies for Recovery and Continuity." He is a Certified Master Antiterrorism Specialist (CMAS). He is a Member of the Editorial Advisory Board for the International Journal of Intelligence and Counterintelligence (IJIC); Editorial Advisory Board for the Spanish Journal of Intelligence Studies (Inteligencia Y Seguridad: Revista De Analisis Y Prospectiva); Editorial Board of the Journal of Intelligence Studies (JIS); International

Editorial Board of the Bulgarian Military History Journal (Voenen Zhurnal); the Advisory Board for the Police, Practice and Research Journal (PPR); Editorial Board of the European Journal of Intelligence Studies (EJIS); Editorial Board of the Journal for Intelligence, Propaganda and Security Studies (JIPSS); Editorial Board of the Journal of Military and Strategic Affairs; International Advisory Board for the World Security Network Foundation (WSN); Editorial Board of the International Journal of Intelligence Ethics (IJIE), Editorial Board of the Geopolitics, Geostrategy, International and European Policy in Civitas Gentium Journal. He is also a Member of the International Association for Intelligence Education (IAFIE), the International Association for Counterterrorism and Security Professionals (IACSP), International Association of Law Enforcement Intelligence Analysts (IALEIA), International Counter-Terrorism Academic Community (ICTAC), International Counter-Terrorism and Critical Incident Network (CTCIN) and International Counterterrorism Officers Association (ICTOA). Email: jnomikos@rieas.gr

Alexander Raikov. Professor, Doctor of Technical Sciences, State advisor of the Russian Federation of the 3rd class, Winner of the Russian government award in the field of Science and Technology, General Director of the New Strategies Agency (NSA) Ltd. Professor of the State Technological University (Russia), Leading researcher of the Institute of Control Sciences of Russian Academy of Sciences, Senior Researcher of the National Center of Excellence in the field of Digital Economy of the Lomonosov Moscow State University, Chief researcher of the Institute of Philosophy, Russian Academy of Sciences. Prior to 1993, Prof. A. Raikov developed automated control systems for the Russian Government. In 1993 – 1999, he was the head of the Information-Analytical Department of the President Administration and coordinator of the Situation Center of the Russian President. Since 1999, he and his team have completed about 60 projects for: the Administration of the President of the Russian Federation, Ministry of Education of Russia, Ministry of Economic Development of Russia, the Government of the city of Moscow, the Republic of Kazakhstan, and etc. Prof. Raikov developed strategies for improving the quality of health care and education in the regions and scientific cities of Russia. Author of more than 350 research papers, 6 monographs, 9 patents in the field of strategic management, socio-economic development, information and analytical technologies, AI, situation centers, decision support systems, and network expertise. Email: anraikov@mail.ru

Rubén Ruiz-Ramas. PhD. Assistant Professor at the National Distance Education University · Department of Political and Administration Sciences, Spain, Madrid. His field of expertise is related to the post-Soviet area where he has developed field-work in Russia, Ukraine and Kyrgyzstan. His research agenda now also includes China where he has lived for almost two years (Sun Yat-Sen University. School of International Studies. China – Guangzhou, April 2016–April 2017). Ruben's research concerns are focused on the study of State-building, political regimes, revolutionary situations, political instability, transnational organised crime, and the persistence of informal institutions. Email: ruizramas@gmail.com

Marco Ricceri. Expert, European social and labour policies, is acting as general secretary of the EURISPES, a primary Italian research institute in the economic, social, territorial development. Ricceri is also: coordinator of the Ethic Committee of the A.E.I. – European Agency of Investments, Geie, Bruxelles; enrolled in the list of "Pool of Reviewers" of the

ESF-European Science Foundation, Strasbourg, for: "European Social Policy", "Industrial Relations". Co-coordinator of the International Expert Network EURUCM. Co-founder and coordinator of the European Research Group "European Social Model" (London-Bremen-Rome). Founding member of EAVI-European Association for Viewers Interests (Brussels), dealing with the dissemination of Media Literacy and Media Education. Ricceri was awarded the Degree Honoris Causa in European Policies by the Institute of Europe of the Russian Academy of Sciences, IE-RAS. Email: riccerimarco@hotmail.com

Pierre-Emmanuel Thomann is a French researcher, lecturer and expert in Geopolitics (Doctor from the French Institute of Geopolitics, Paris 8 University, France, 2014). He teaches geopolitics (ISSEP Lyon) and is the president/founder of an international association (EUROCONTINENT) based in Brussels, Belgium, to promote geopolitical analysis and foster common interests identification between nations and states at EU with a focus on Franco-German relations, pan-European (including Russia), Eurasian (Central Asia) and Euro-Mediterranean scales. He participated in 2016 as an expert to the "EU-Russia Experts Network" organized by the EU delegation in Moscow. He was also adviser at the European Institute of International Relations (IERI-Brussels) from 2007 to 2014, a think-tank specialized in European strategic issues. Previously, he was the Director of a French region representation office towards the EU (1997–2006). He also worked in Germany (1996), in Netherlands (1993), and United Kingdom (1990-1992). Email: pierre-emmanuel.thomann@eurocontinent.eu

Florian Zollmann. Currently is the Degree Programme Director for the BA Journalism, Media and Culture at Newcastle. His research has been published in international academic journals and edited collections. With Richard Lance Keeble and John Tulloch I jointly edited Peace Journalism, War and Conflict Resolution (New York: Peter Lang 2010). His latest monograph assessing US, UK and German news media coverage of military operations in Kosovo, Iraq, Libya, Syria and Egypt is titled Media, Propaganda and the Politics of Intervention (New York: Peter Lang, 2017). Reviews of the book have been published in Peace News, European Journal of Communication, Cooperation and Conflict, E-International Relations, as well as Journal of Peace Research.

Jonathan Matusitz (Ph.D., University of Oklahoma, 2006) is currently a tenured associate professor in the Nicholson School of Communication and Media. His research focuses on the role of communication in terrorism, symbolism in terrorism, the globalization of culture, and health communication. His research methodologies include qualitative interviewing, content analysis, semiotics, and theoretical analysis. On top of having more than 140 academic publications and over 150 conference presentations, he taught at a NATO-affiliated military base in Belgium in 2010. Originally from Belgium himself, he moved to the United States in 2000.

His first book on terrorism, titled Terrorism & Communication: A Critical Introduction, was published by SAGE in 2013. His second book, Symbolism in Terrorism: Motivation, Communication, and Behavior, was published by Rowman & Littlefield in 2015. His latest book, Online Jihadist Magazines to Promote the Caliphate: Communicative Perspectives, was published by Peter Lang in 2019. Email: Jonathan.Matusitz@ucf.edu

CONTENTS

PREFACE

Eric Louw[*]

University of Queensland, Australia

Terrorism is not a new phenomenon, and neither is the work of countering terrorism. But contemporary terrorism is taking place in a context where a range of new actors, new technological possibilities and new opportunities exist – and this is impacting on how today's terrorists (and counter-terrorists) conceptualize and craft their activities in new ways. Furthermore, shifts in the global balance of power plus the emergence of social instability in many states have given rise to a plethora of new terror (and counter-terrorist) possibilities. This book seeks to open up a discussion about how terrorism is evolving and may evolve in future, plus how those seeking to counter-terrrorism will therefore need to think of new responses.

To set the scene for this book some themes will be briefly sketched out to help orientate the reader. In the first place we will look at some of the enduring features of terrorism (and counter-terrorism) – after all, although terrorism is mutating and evolving, it is also true to say that there are also some great continuities between the practices of twenty-first century terrorists and terrorists who operated in the twentieth and nineteenth centuries. So although today's terrorists are adapting to new technologies and conditions, in many ways they are still in the same business as those who in the past have tried to use political violence to:

- advertise the terrorist cause so as to recruit supporters and fighters
- undermine the legitimacy of targetted governments
- terrify those populations who support targetted governments

[*] Corresponding Author's Email: e.louw@uq.edu.au.

- spread panic, despondency, frustration and anger to destabilize targetted societies/governments
- weaken those ideologies, beliefs and value systems that the terrorists disapprove of, and
- spread their own counter-ideologies, beliefs and value systems.

Ultimately terrorists – like all politicians – are in the communication business. And, like other political players, terrorists face an increasingly mediatized political process. Hence, it should come as little surprise that terrorists (past and present) have always given serious consideration to the usefulness (or otherwise) of available media platforms, and what these platforms offer them as potential sites of struggle. This is not to say that terror wars are reducible to media struggles. Indeed terror wars necessarily involve real battles, some of which are deliberately kept out of sight of the media. However, as with other politicians, terrorists have messages to sell – and their success or failure depends in part on the terror organization's perception-management skills, plus their skills at both symbol and belief propagation. And so, as with other political players, terrorists will often try to use the media to their own advantage; and as with other politicians, will sometimes be successful, and sometimes fail. What is clear is that the development of visual media – first film; then television; and now internet-facilitated visual images – has greatly helped terrorists because visualness helps communicate emotions and so helps spread terror, shock, fear and anger.

It was Russian and French anarchists who developed the idea of deploying terrorism during the nineteenth century – Paul Brousse and Peter Kropotkin used the term 'propaganda of the deed' in 1877 to refer to how those who were politically weak (because their ambitions were being blocked by an overwhelmingly powerful political foe) needed to carry out a spectacular act that would draw attention to their cause. The idea was that if spectacular acts of political violence were well executed the media would report them. The resultant propaganda effect would then advertise the terrorist's cause, thereby enabling the recruitment of new sympathisers and fighters. The way in which the 9/11 attacks served to advertise al Qaeda's cause and recruit support and fighters for radical-Islam is a classic example of this – with a key feature of the 9/11 attack on the World Trade Centre being how the opportunities offered by global television were masterfully used to instantly globalize the al Qaeda brand. And since then the rise of the internet has enhanced even further the opportunities available to terrorists to globally advertise themselves through propaganda of the deed exercises that serve to trigger visceral emotive responses in both their supporters and opponents.

Of course, since terrorism is about political communication, successful terrorists must learn to think about how their acts will be interpreted and 'felt' by different audiences – after all well executed propaganda of the deed exercises should necessarily encode multiple messages that will simultaneously trigger different responses and feelings in different

audiences. Triggering the desired of mix responses requires skill – indeed terrorism-as-communication requires that terrorists need to design their actions so as to 'orchestrate' its likely impact(s) on eight distinct audiences:

- Existing members of terrorist organizations generally feel alienated and disempowered by the weakness of their organization/cause relative to an overwhelmingly powerful political foe. Terror attacks seek to empower these members by demonstrating a capacity to 'hit back'.
- Potential recruits are always an important target audience so attacks must encode messages inspiring to the potential supporters/constituency of terror groups.
- Attacks encode 'warnings' and provocations to enemy governments. There is often an intention to provoke government to 'lash out' against civilian populations because this helps terror groups.
- If government supporters can be made fearful and angry this can put pressure on governments to make hasty decisions, which are more likely to be poor decisions.
- Those who are neutral (neither support the terrorists nor the government) should be left untouched. Harming neutrals creates the risk of them joining the other side.
- (Sometimes) journalists are the opinion leaders being targeted by terrorist messaging in the hope they will then diffuse helpful messages to a wider audience.
- Potential allies are always sought by terror groups in the hope that they supply funds, weapons and diplomatic support (often in return for proxy actions).
- There are always specific groups or individuals who terrorists are trying to frighten into changing their behaviour. This might include foreign investors, NGOs, tourists, or those who collaborate (or might collaborate) with the enemy government. Terrorism as fear-making can be a valuable tool for driving behavioural changes.

The question to be asked is, how might new technologies help terrorists do this more effectively? To what extent might new technologies help terrorists (and counter-terrorists) understand their audiences better; or help them improve message-targeting and message-delivery; or perhaps provide new opportunities for creating both fear and polarization? The authors of this book are suggesting that is exactly what is happening because new technologies and new media platforms are creating spaces for new types of political communication (both offensive and defensive); new mechanisms of surveillance; and new weapons to attack populations and infrastructure. Effectively we see a new world of terrorism (and counter-terrorism) being born before our eyes. By way of understanding this new world let us briefly sketch out some of the key features of how terrorism looks set to be impacted by new media; new surveillance possibilities; potential new weapons; potential new targets and potential new actors.

New Media have not eliminated older media forms, but have added a number of new media platforms for terrorists to use to disseminate their messages. This means the range of possibilities for message delivery has been widened. From the point of view of terrorists the most important of these new possibilities are Facebook, Instagram, YouTube and twitter. Islamic State has already shown us how creative terrorists can be in using these new platforms to great effect – e.g., posting images of beheadings on the internet which can simultaneously serve to terrify and anger some target populations, while inspiring others to join the terrorist movement. Of course that does not mean the older media forms are abandoned. But it does mean that new communication tools are added by the new platforms. An important new tool is the ability to target niche audiences very easily because new media platforms are very good at pulling together and networking like-minded people into 'group-think bubbles' and 'echo chambers within which people can congregate in 'tribal groupings'. Such networked spaces are ideal fulcrums within which to create in-group solidarity and out-group hatreds; stir up passions; collectively build new shared identities; and share information facilitating terror acts (e.g., how to make a bomb). Clearly the building of such 'group-think bubbles' offers powerful new opportunities for both political mobilization and for triggering (individual and group) political action – including political violence against out-groups or governments. And the potential to build these 'group-think bubbles' on the dark web offers enhanced opportunities for assembling the sort of networks that can underpin the promotion of political violence. A second important feature of these new platforms is that they make it much easier to spread exaggerations, half-truths and untruths. This is because new media platforms allow anyone to post information and ideas and the sort of editorial control seen in earlier media forms falls away. Exaggeration, defamation and lying now becomes easy through phenomena like troll farms, image manipulation and deep fakes. It is now even possible to automate communication-attacks and misinformation through chat bots. The result has been the spread of fake news plus the birth of communication-operations run by both government and private-owned troll farms (which both stir up political conflicts and attack/undermine the credibility of targeted individuals). There is no reason to think terrorists will not also get into the business of fake news, trolling and using social media for agenda setting and psychological warfare. And they can also use these new media platforms to spread misinformation intended to misdirect counter-terrorist force surveillance. A third feature of these new platforms is that audiences also become producers. Because audience-producers are active their sense of group-belonging and empowerment-through-activism is enhanced. This strengthens the 'group-think bubbles'. Consequently, if terrorists learn to effectively use the opportunities offered by these new platforms they could build very powerful mechanisms to bond supporters/sympathisers with their organizations. The way in which Islamic State used social media to build a global recruitment and support/sympathiser networks shows what can be achieved if terrorist networks include people with creative flair for using available communication tools. For counter-terrorist

operatives all these new possibilities that are now available to terrorists will require the development of a whole new approach towards surveillance, as well as for conceptualizing anti-terrorist psychological warfare operations.

New surveillance possibilities are an important feature offered by new media platforms because digital media platforms are able to collect (real time) information on their users/audiences as well as store all this ongoing automated collection of information. More importantly it is now possible to process/analyse all this big data to profile each individual using these new media platforms in real time and in an automated way. What is more, machine learning now makes it potentially possible to build surveillance machinery that can improve its own abilities (i.e., learn) to watch/analyse/profile both individuals and groups. Although originally designed by those interested in marketing/advertising commercial products, big data analysis can also be used by political actors. And since a core part of counter-terrorism work is about building effective intelligence gathering, clearly counter-terrorist operatives are going to turn to big data analysis to try and identify and profile potential terrorists and terrorist sympathisers/supporters. Of course, terrorists are also in the business of intelligence gathering, but it is a moot point whether they will be able to access the big data being collected by social media platforms. No doubt, in due course terrorists will try and hack into the huge data bases being constructed by social media platforms. But even if they are not able to, the huge amounts of open source information now available on the internet makes the gathering of intelligence and planning much easier.

New weapons are another set of new possibilities for terrorists emerging from the digital revolution. Terrorism is about using terror and fear to shift behaviours, subdue populations and delegitimate governments. For Brousse and Kropotkin this meant terrorists carrying out spectacular deeds to advertise their cause – and significantly it generally meant the very real possibility that the terrorist/s would die, given that terrorists engaged in the early stages of launching their wars were usually on suicide missions. But new technologies have now created opportunities for unmanned terror attacks that can be carried out from afar. One example of this is the potential use of drones-as-bombs. Terrorists no longer have to be physically present to kill people. Indeed machine learning/Artificial intelligence means it becomes possible to create 'smart' drone-as-bombs able to seek out specific targets (e.g., gatherings of people or even individuals). Another form of terror attack from afar is using the internet to sabotage distant targets – e.g., taking over air traffic control systems to cause accidents; or shutting down electricity grids to sabotage economies; or shutting down sewerage systems to create health hazards.

But it is not only the digital revolution and new technologies that are driving innovations in terrorism. There are also *new actors* born of a shifting global balance of power plus changes in society. History has long been characterized by periods of international stability followed by periods of international instability. The stable periods occur when one, or a few great powers impose order upon the whole global system. These

stable periods are often characterized by great empires. Instabilty arises when empires break-down and/or when the balance of power between great powers changes. These periods of break-down and/or power realignments are generally chacterised by warfare, revolution and insurrection as old mechanisms to impose order dissolve; new winners emerge as lynchpin powers; and new smaller players emerge out of the turmoil. The world is currently in one of these periods of international instability – and today's instability is the outcome of two twentieth century shifts, namely the end of European imperialism and the collapse of the Soviet Union. The side-effects of these two shifts are still with us as the wash up ripples its way through the global system and through individual societies. Contempory terrorism is one of the outcomes of living through the instability caused by a shifting global balance of power because this instability gives rise to both new grievances (and new groups to institutionalize these new grievances) plus to new opportunities to act out these grievances. The fact that we are also going through a (digital) technological revolution simply means that we are witnessing not only the emergence of new terrorist actors, but also witnessing how these new actors are able to build new types of terrorism from the opportunities thrown up by simultaneous changes to both global power relationships plus technology. The challenge for counter-terrorist forces will be to keep up with the sort of terrorism emerging from this turmoil.