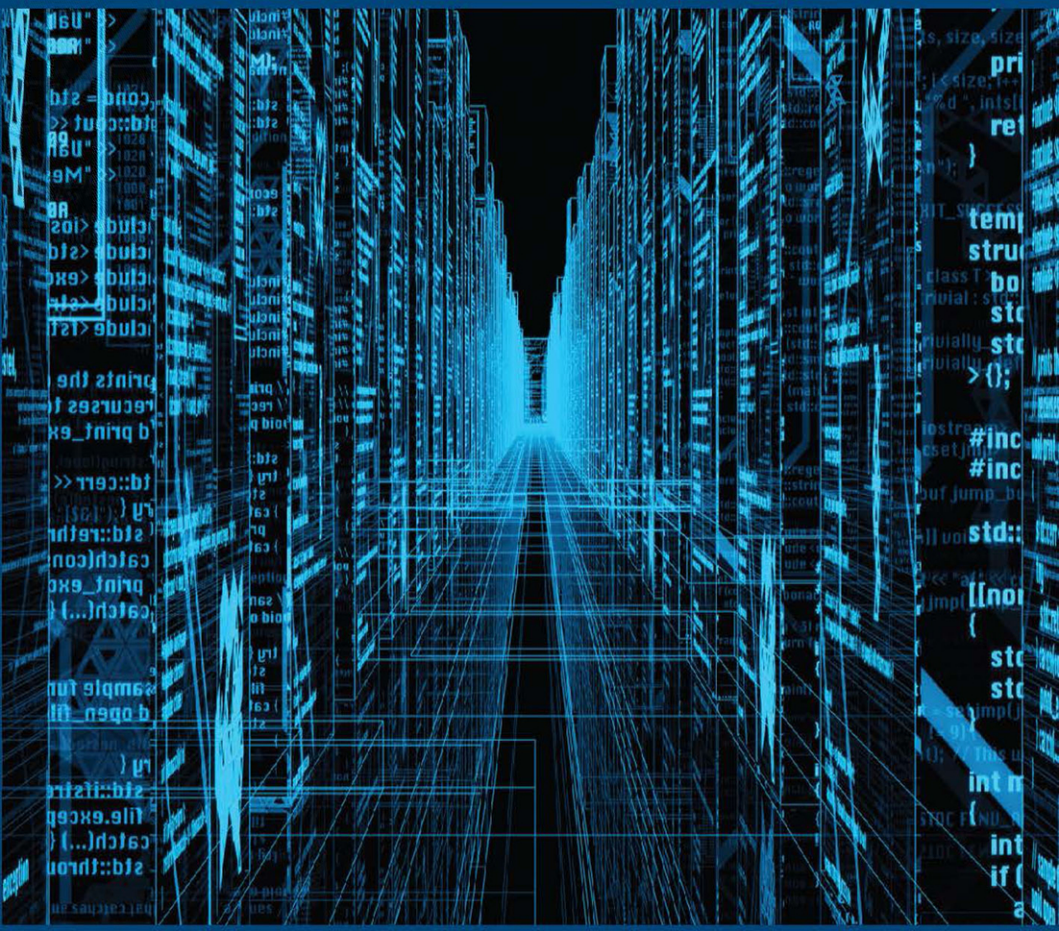
NEW SECURITY CHALLENGES

Series Editor: Stuart Croft



Open Source Intelligence in the Twenty-First Century

New Approaches and Opportunities

Edited by Christopher Hobbs, Matthew Moran and Daniel Salisbury

New Security Challenges

General Editor: **Stuart Croft**, Professor of International Security in the Department of Politics and International Studies at the University of Warwick, UK, and Director of the ESRC's New Security Challenges Programme.

The last decade demonstrated that threats to security vary greatly in their causes and manifestations, and that they invite interest and demand responses from the social sciences, civil society and a very broad policy community. In the past, the avoidance of war was the primary objective, but with the end of the Cold War the retention of military defence as the centrepiece of international security agenda became untenable. There has been, therefore, a significant shift in emphasis away from traditional approaches to security to a new agenda that talks of the softer side of security, in terms of human security, economic security and environmental security. The topical *New Security Challenges series* reflects this pressing political and research agenda.

Titles include:

Abdul Haqq Baker
EXTREMISTS IN OUR MIDST
Confronting Terror

Robin Cameron
SUBJECTS OF SECURITY
Domestic Effects of Foreign Policy in the War on Terror

Jon Coaffee, David Murakami Wood and Peter Rogers
THE EVERYDAY RESILIENCE OF THE CITY
How Cities Respond to Terrorism and Disaster

Sharyl Cross, Savo Kentera, R. Craig Nation and Radovan Vukadinovic (*editors*)
SHAPING SOUTH EAST EUROPE'S SECURITY COMMUNITY FOR THE TWENTY-FIRST CENTURY
Trust, Partnership, Integration

Tom Dyson and Theodore Konstadinides
EUROPEAN DEFENCE COOPERATION IN EU LAW AND IR THEORY

Tom Dyson
NEOCLASSICAL REALISM AND DEFENCE REFORM IN POST-COLD WAR EUROPE

Håkan Edström, Janne Haaland Matlary and Magnus Petersson (*editors*)
NATO: THE POWER OF PARTNERSHIPS

Håkan Edström and Dennis Gyllensporre
POLITICAL ASPIRATIONS AND PERILS OF SECURITY
Unpacking the Military Strategy of the United Nations

Hakan Edström and Dennis Gyllensporre (*editors*)
PURSUING STRATEGY
NATO Operations from the Gulf War to Gaddafi

Christopher Farrington (*editor*)
GLOBAL CHANGE, CIVIL SOCIETY AND THE NORTHERN IRELAND PEACE PROCESS
Implementing the Political Settlement

Adrian Gallagher
GENOCIDE AND ITS THREAT TO CONTEMPORARY INTERNATIONAL ORDER

Kevin Gillan, Jenny Pickerill and Frank Webster
ANTI-WAR ACTIVISM
New Media and Protest in the Information Age

James Gow and Ivan Zverzhanovski
SECURITY, DEMOCRACY AND WAR CRIMES
Security Sector Transformation in Serbia

Toni Haastrup
CHARTING TRANSFORMATION THROUGH SECURITY
Contemporary EU-Africa Relations

Ellen Hallams, Luca Ratti and Ben Zyla (*editors*)
NATO BEYOND 9/11
The Transformation of the Atlantic Alliance

Andrew Hill
RE-IMAGINING THE WAR ON TERROR
Seeing, Waiting, Travelling

Christopher Hobbs, Matthew Moran and Daniel Salisbury (*editors*)
OPEN SOURCE INTELLIGENCE IN THE TWENTY-FIRST CENTURY
New Approaches and Opportunities

Andrew Hoskins and Ben O'Loughlin
TELEVISION AND TERROR
Conflicting Times and the Crisis of News Discourse

Paul Jackson and Peter Albrecht
RECONSTRUCTING SECURITY AFTER CONFLICT
Security Sector Reform in Sierra Leone

Bryan Mabee
THE GLOBALIZATION OF SECURITY
State Power, Security Provision and Legitimacy

Janne Haaland Matlary
EUROPEAN UNION SECURITY DYNAMICS
In the New National Interest

Kevork Oskanian
FEAR, WEAKNESS AND POWER IN THE POST-SOVIET SOUTH CAUCASUS
A Theoretical and Empirical Analysis

Michael Pugh, Neil Cooper and Mandy Turner (*editors*)
WHOSE PEACE? CRITICAL PERSPECTIVES ON THE POLITICAL ECONOMY OF PEACEBUILDING

Brian Rappert and Chandré Gould (*editors*)
BIOSECURITY
Origins, Transformations and Practices

Nathan Roger
IMAGE WARFARE IN THE WAR ON TERROR

Aglaya Snetkov and Stephen Aris
THE REGIONAL DIMENSIONS TO SECURITY
Other Sides of Afghanistan

Ali Tekin and Paul Andrew Williams
GEO-POLITICS OF THE EURO-ASIA ENERGY NEXUS
The European Union, Russia and Turkey

Lisa Watanabe
SECURING EUROPE

Mark Webber, James Sperling and Martin A. Smith
NATO's POST-COLD WAR TRAJECTORY
Decline or Regeneration

New Security Challenges Series
Series Standing Order ISBN 978–0–230–00216–6 (hardback) and ISBN 978–0–230–00217–3 (paperback)
(*outside North America only*)

You can receive future titles in this series as they are published by placing a standing order. Please contact your bookseller or, in case of difficulty, write to us at the address below with your name and address, the title of the series and the ISBNs quoted above.

Customer Services Department, Macmillan Distribution Ltd, Houndmills, Basingstoke, Hampshire RG21 6XS, England

---

Open Source Intelligence in the Twenty-First Century

New Approaches and Opportunities

Edited by

Christopher Hobbs, Matthew Moran and Daniel Salisbury
Centre for Science and Security Studies, King's College London, UK

palgrave
macmillan

Softcover reprint of the hardcover 1st edition 2014 978-1-137-35331-3

First published 2014 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan in the US is a division of St Martin's Press LLC, 175 Fifth Avenue, New York, NY 10010.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN 978-1-349-46966-6 ISBN 978-1-137-35332-0 (eBook)
DOI 10.1057/9781137353320

This book is printed on paper suitable for recycling and made from fully managed and sustained forest sources. Logging, pulping and manufacturing processes are expected to conform to the environmental regulations of the country of origin.

A catalogue record for this book is available from the British Library.

A catalog record for this book is available from the Library of Congress.

Contents

Part IV Open Source Intelligence and Counterterrorism

Tables and Figures

Tables

Figures

Acknowledgements

This book is the product of both a longstanding interest in open source intelligence (OSINT) and a desire to build on the experience and benefits gained from applying OSINT tools and techniques in our research. Furthermore, our work has brought us into contact with a vibrant community of researchers and practitioners who deal with OSINT in various aspects of their work. We were thus presented with an opportunity to bring together the expertise and experiences of colleagues, both at King's College London and elsewhere, with a view to gaining an insight into the ways in which OSINT is understood and employed in different fields of research. By doing this, we hope to offer the reader a snapshot of what is a rapidly growing area of research and activity.

A number of colleagues and friends supported us in this work. We are grateful for the support of colleagues at the Centre for Science and Security Studies, a research centre based in the Department of War Studies at King's College London. Various discussions and exchanges about OSINT and related issues helped to develop our approach to this book. We are also very grateful to the contributors for providing us with original and diverse insights into OSINT, both in terms of its development and current uses, and in terms of its future potential. Molly Berkemeier provided valuable support in the final stages of preparing the manuscript. We would also like to thank the anonymous reviewer at Palgrave for useful comments and suggestions. Staff at Palgrave, in particular Julia Willan, Ellie Davey-Corrigan and Harriet Barker, have also been a pleasure to work with.

Christopher Hobbs, Matthew Moran and Daniel Salisbury

Contributors

John C. Amble is Managing Director of Global Torchlight LLC, a security and risk management consultancy. He has operational experience on three continents as an officer in the US Army, including deployments to both Iraq and Afghanistan. He has also served as an intelligence officer at the Defense Intelligence Agency, as part of the US military's chief counterterrorism intelligence task force. He is currently working towards a PhD at King's College London where his research focuses on regional Islamist insurgent organisations and their evolution as nodes within the transnational jihadist movement.

Jamie Bartlett is the Head of the Violence and Extremism Programme and Director of the Centre for the Analysis of Social Media at Demos. He is the co-author, with Sir David Omand and Carl Miller, of #intelligence – the first framework for the ethical and effective collection of social media intelligence.

Fred Bruls is a Royal Netherlands Air Force reserve major in the Dutch 1 CIMIC Battalion. From August 2009 to February 2010 he was deployed in Afghanistan as information manager in the intelligence branch (G2) of the Dutch-Australian Task Force Uruzgan (TFU-VII). He holds a masters' in defence studies from the Canadian Forces College, where his dissertation was based on the concept of human security intelligence.

James Chappell is co-founder of Digital Shadows and has more than a decade of experience working as a security architect advising the FTSE100 and central government. Prior to setting up Digital Shadows he was Deputy Head of Security at BAE Systems Detica and he remains a member of the CESG Listed Adviser Scheme (CLAS), GCHQ's trusted security advisers to government.

A. Walter Dorn is Professor of Defence Studies at the Royal Military College of Canada and Chair of the Department of Security and International Affairs at the Canadian Forces College. He specialises in arms control, peace/stability operations and international security. One focus is intelligence in United Nations (UN) operations where he benefits from field visits and deployments. He is author of *Keeping Watch: Monitoring Technology and Innovation in UN Peace Operations* (UN University Press, 2011).

Stevyn D. Gibson lectures on concepts of intelligence, security and risk at the UK Defence Academy and Cranfield University. His intelligence experience includes BRIXMIS, analysis for hostage rescue and intelligence briefing to war headquarters. His PhD examined how open source exploitation contributes to the national intelligence function. He is the author of *The Last Mission* (2007) and *Live and Let Spy* (2012).

Christopher Hobbs is Lecturer in Science and Security in the Department of War Studies at King's College London. A physicist by training he has more than five years of experience in applying open source intelligence (OSINT) techniques to nuclear proliferation issues and has developed training courses in this area for the European Defence Agency. His latest book, *Exploring Regional Responses to a Nuclear Iran: Nuclear Dominoes?*, was recently published by Palgrave Macmillan.

Randolph Kent directs the Humanitarian Futures Programme at King's College London. Established at the end of 2005, it is designed to enhance the adaptive and anticipatory capacities of humanitarian organisations to deal with the types of threat that need to be faced in the future. He accepted his present post after completing his assignment as UN Resident and Humanitarian Coordinator for Somalia in April 2002. Prior to his assignment in Somalia, he served as UN Humanitarian Coordinator in Kosovo (1999), UN Humanitarian Coordinator in Rwanda (1994–1995), Chief of the IASC's Inter-Agency Support Unit (1992–1994), Chief of the UN Emergency Unit in Sudan (1989–1991) and Chief of Emergency Prevention and Preparedness in Ethiopia (1987–1989).

Carl Miller is the Research Director of the Centre for the Analysis of Social Media at Demos, and a research associate at the International Centre for Security Analysis at King's College London. His interests lie in creating new ways to learn about people and society from researching social media, and to use these methods to inform policies, decisions and responses to social problems.

Matthew Moran is Lecturer in International Security in the Department of War Studies at King's College London. His research interests include nuclear non-proliferation and the methods and practice of OSINT. His latest book, *Exploring Regional Responses to a Nuclear Iran: Nuclear Dominoes?*, was recently published by Palgrave Macmillan.

Sir David Omand is a visiting professor in the Department of War Studies at King's College London, the former Director of the UK GCHQ and former Permanent Secretary at the Home Office.

Alastair Paterson is co-founder and Chief Executive Officer of Digital Shadows, an OSINT cybersecurity monitoring service. He specialises in designing 'big data' risk and intelligence systems with a particular focus on cybersecurity. Before founding Digital Shadows he was International Propositions Manager at BAE Systems Detica, working primarily with national security clients in Europe, the Gulf and Australasia.

Daniel Salisbury is a researcher at the Centre for Science and Security Studies in the Department of War studies at King's College London, where his work focuses on non-proliferation issues. Specifically, he works on Project Alpha, a UK government-sponsored project which seeks to engage the private sector in non-proliferation and export controls. Prior to his current position he worked at the International Institute for Strategic Studies in London.

Simon Wibberley is a researcher at the Text Analytics Group in the Department of Informatics at the University of Sussex. His research interests lie in statistical text analytics and he specialises in real-time text-stream analysis, event detection and entity recognition. Current projects include developing state-of-the-art event-detection and event-characterisation techniques for use on Twitter.

Abbreviations

ALNAP	Active Learning Network for Accountability and Performance
AMISOM	African Union Mission in Somalia
AOI	area of interest
AOR	area of responsibility
AP	Additional Protocol
API	application programming interface
AQIM	al-Qaeda in the Islamic Maghreb
ASCOPR	areas, structures, capabilities, organizations, people and events
ASIC	all source intelligence cell
BBC	British Broadcasting Corporation
BJP	Bharatiya Janata Party
CCRP	California Coastal Records Project
CIA	Central Intelligence Agency
CIMIC	civil-military cooperation
CISPA	Cyber Intelligence Sharing and Protection Act
COMINT	communications intelligence
COP	common operational picture
COSP	Community Open Source Program
CSA	Comprehensive Safeguards Agreement
DCI	Director of Central Intelligence
DDOS	Distributed Denial of Service Attacks
DF	document frequency
DIME	diplomatic, information, military, economic
DIMEFIL	diplomatic, information, military, economic, financial, intelligence, law enforcement
DNI	Director of National Intelligence
DNS	domain name system
EFP	explosively formed projectiles
ELINT	Electronic Intelligence
EU	European Union
EUU	End User Undertaking
FBIS	Foreign Broadcast Information Service
GIA	Armed Islamic Group
GSMA	GSM Association
GTD	Global Terrorism Database
HSI	human security intelligence
HUMINT	human intelligence

IAEA	International Atomic Energy Agency
ICRC	International Committee of the Red Cross
ICT	information and communication technology
ICU	Islamic Courts Union
IDF	inverse document frequency
IED	improvised explosive device
IFRC	International Federation of Red Cross and Red Crescent Societies
IMU	Islamic Movement of Uzbekistan
IMINT	imagery intelligence
IP	internet protocol
IRC	International Rescue Committee
ISE	Integrated Safeguards Environment
ISI	Islamic State of Iraq
IT	information technology
IVR	interactive voice response
JIC	Joint Intelligence Committee
JMAC	Joint Mission Analysis Centre
JOC	Joint Operations Centre
JTAC	Joint Terrorism Analysis Centre
KLD	Kullback–Leibler Divergence
LINKS	Livestock Information Knowledge System
MASINT	measurement and signature intelligence
MFO	Multilateral Force and Observers
MOD	UK Ministry of Defence
MONUSCO	United Nations Stabilization Mission in the Democratic Republic of the Congo
MRAP	mine-resistant ambush protected
MSF	Medecins Sans Frontieres
MTCR	Missile Technology Control Regime
MUJAO	Movement for Oneness and Jihad in West Africa
NATO	North Atlantic Treaty Organisation
NGO	non-governmental organisations
NLP	natural language processing
NNWS	non-nuclear weapons state
NPoCC	National Police Coordination Centre
NPT	Treaty on the Non-proliferation of Nuclear Weapons
NSG	Nuclear Suppliers Group
NSS	UK National Security Strategy
OPCW	Organisation for the Prohibition of Chemical Weapons
OSC	Open Source Center
OSINT	open source intelligence
OSIS	Open Source Information System
PIRs	priority intelligence requirements

PKO	peacekeeping operation
PMESII	political, military, economic, social, infrastructure and information
PMESII-PT	political, military, economic, social, infrastructure, information, physical environment and time
PO	peace operation
POC	protection of civilians
PSC	private security company
PSO	peace support operation
PTS	Procurement Tracking System
RADINT	radar intelligence
RICC	Regional Information Collection Centre
RIPA	Regulation of Investigatory Powers Act 2000
ROE	Rules of Engagement
SALI	Sustainable Agriculture Livelihoods Innovations initiative
SDSR	Strategic Defence and Security Review
SEG	State Evaluation Group
SEO	search engine optimisation
SGIM	Division of Safeguards Information Management
SGIM-ISF	State Factors Analysis Section in the Safeguards Division of Information Management
SIEL	Standard Individual Export Licence
SIGINT	signals intelligence
SLA	state-level approach
SNA	social network analysis
SOCMINT	social media intelligence
SOPA	Stop Online Piracy Act
SQL	Structured Query Language
START	Study of Terrorism and Responses to Terrorism
TEC	Tsunami Evaluation Coalition
TECHINT	technical intelligence
TF	term frequency
TTA	Trade and Technology Analysis Team
UAV	unmanned aerial vehicle
UN	United Nations
UNAMA	UN Assistance Mission in Afghanistan
UNDP	UN Development Programme
UNFICYP	UN Peacekeeping Force in Cyprus
UNSCR	United Nations Security Council resolution
USD	United States Dollars
WMD	Weapons of Mass Destruction
YHUMINT	young human intelligence

Introduction

Christopher Hobbs, Matthew Moran and Daniel Salisbury

The twenty-first century has seen a revolution in how publicly accessible, or 'open source', information is created, stored and disseminated. Driven by the rapid growth of the Internet and the World Wide Web, as well as the widespread adoption and advancement of mobile communication technology, the use of open sources has permeated the fields of intelligence, politics and business, to name but a few. This revolution has impacted significantly on how people acquire information, express ideas and interact with each other, both socially and professionally. Crucially, while traditional sources and channels of information have made great efforts to adapt to this new virtual environment and retain their presence as gatekeepers of information – many established media sources, for example, now publish large amounts of content exclusively online – the rise of user-generated content, particularly social media, has drastically transformed the information landscape. From the 500 million 'tweets' per day on Twitter, to the 98 million daily blog posts on Tumblr, we are now only a few keystrokes away from a potentially global audience.[1] Moreover, as these tools increase global connectivity, people seem increasingly willing to project their thoughts, opinions and observations into cyberspace. The process of information generation has been opened up to the masses and the sheer quantity of open source information now available online is staggering.

As in other fields, these developments have had a profound effect on the intelligence community. While open source information has long figured in the work of intelligence analysts, it has been conferred with a new status and legitimacy in recent years, moving from the periphery of intelligence efforts to become a core component of analytical products. Indeed, various high-ranking figures in the US intelligence community have for many years claimed that open sources can provide upwards of 80 per cent of intelligence needs – a claim that Stevyn D. Gibson explores in some detail in this volume (Chapter 1). This increased emphasis on open source intelligence (OSINT) – that is to say, the exploitation of open source information for intelligence purposes as part of a broader, all-source intelligence process – has served

to provide contextual detail to classified sources which are often limited in scope and fragmented. OSINT can provide background, fill gaps and create links between seemingly unrelated sources, resulting in an altogether more complete intelligence picture. Moreover, due to its open source nature, OSINT can, for the most part, be readily shared and does not present the problems normally associated with the exchange of sensitive information between governments and other organisations.

These changes in the role and perceived value of OSINT are evidenced by the changes that have taken place in the intelligence community. In the US, for example, the establishment of the national Open Source Center (OSC) under the Director of National Intelligence (DNI) in 2005 marked an important milestone.[2] The OSC is an organisation dedicated to the systematic collection and integration of media reports, user-generated online content and any other relevant types of publically available information into the US intelligence cycle. The importance of OSINT in US intelligence efforts was further cemented by the creation of a new managerial position – Assistant Deputy Director of National Intelligence for Open Source – to oversee and coordinate the OSC and, on a larger scale, the growing role played by open sources in the US intelligence enterprise.[3] Moreover, these changes in the US have been reflected to varying degrees in other intelligence communities around the world.

It is not only within the intelligence community that the use of open sources has had wide-ranging implications. The information revolution has affected all fields of research and action. Beyond the efforts of the intelligence community to better integrate OSINT into the all-source intelligence process, many other types of actor are also looking to better integrate open source analysis into their work. From non-governmental organisations (NGOs) to the business community, developments in open source methodologies and practice hold the key to new and valuable insights and analysis.

In practical terms, the current conflict in Syria provides a timely and highly relevant example of the use and value of OSINT. At the time of writing, the Organisation for the Prohibition of Chemical Weapons (OPCW) has begun the process of securing and destroying chemical weapons stockpiles and capabilities declared by the Assad regime.[4] This process is the culmination of months of political and diplomatic activity prompted by allegations of chemical weapons use, most importantly on 21 August 2013 in the suburbs of Damascus. Publically available intelligence assessments produced by the US, France and the UK, among others, claimed that there were significant grounds to believe that the Assad regime had carried out this high-casualty attack on rebel forces. The US intelligence report, for example, was a key pillar supporting the Obama administration's efforts to secure both congressional authorisation and public support for a potential military intervention in Syria, even if the subsequent Russian initiative to convince the regime in

Damascus to commit to giving up its chemical weapons capability meant that military intervention was averted.[5] Similarly, in the UK, a publically available Joint Intelligence Committee (JIC) report presented the case for action, and only defeat in parliament stopped David Cameron's plans to join a potential US-led intervention.

Crucially, these reports relied heavily on evidence gleaned from open sources. The first publicly released intelligence assessment came from the UK JIC on 29 August 2013. This report stated that there were 'no plausible alternative scenarios to regime responsibility', an assessment made with the 'highest possible level of certainty following an exhaustive review by the Joint Intelligence Organisation of intelligence reports plus diplomatic and open sources'.[6] Significantly, the assessment recognised the amount of open source information available on the attack, thus highlighting the value of OSINT in the overall assessment. The following day the White House released a more detailed assessment based on a 'significant body of open source reporting'.[7] The document gave details of the range of sources used to inform the analysis, including 'videos; witness accounts; thousands of social media reports from at least twelve different locations in the Damascus area; journalist accounts; and reports from highly credible nongovernmental organizations'.[8]

These reports and, more importantly, the value that they attributed to open sources in the intelligence process were significant in that they are among the first occasions that the role of OSINT has been so extensively credited in intelligence assessments of such high importance. Of course, this is not to suggest that the emphasis on open sources was completely free of ulterior political motives, or that the value of the open sources used was beyond question. Highlighting the role of open source in the attribution process, for example, provided the relevant governments with a means of diverting attention from the moral and analytical sensitivities associated with covert intelligence – a significant issue in an environment that continues to be overshadowed by the intelligence-related issues that surrounded the 2003 invasion of Iraq. Furthermore, the veracity of the open sources used in these assessments was questioned in the subsequent public debate. For example, commentators asked how videos of the chemical weapons attack could be verified. This question was an important one considering that clear incentives likely existed for elements of the opposition to encourage a Western intervention. On a larger scale, while open sources clearly provided important contextual information, could they provide a 'smoking gun'? Open sources clearly showed the aftermath of a chemical attack. However, could they logically and reliably lead to the conclusion that Assad was responsible?

In general terms the fact that a number of the world's most sophisticated intelligence communities publically highlighted the importance of open sources to their intelligence efforts reflects the growing importance

and utility of OSINT. However, the questions raised regarding the role and value of OSINT in the analysis of the Syrian chemical weapons attack touch on some of the enduring issues associated with this rapidly developing area of the intelligence field. On the one hand, then, OSINT presents researchers and analysts with a wealth of opportunities and potential. From the study of online terrorist recruitment to exploring how social media can be used as sources of sociopolitical analysis, OSINT can provide new and exciting data and insights. On the other hand, OSINT poses a number of challenges and obstacles – technical, political and ethical – that must be navigated with care.

In this context, this book takes a fresh look at the subject of OSINT and explores the new approaches, opportunities and challenges that this emergent field offers at the beginning of the twenty-first century. With a focus on three key areas of international security – nuclear proliferation; humanitarian crises; and terrorism – it aims to provide readers with an insight into the latest and most original research being conducted on the subject. The chapters are written by established academics, intelligence specialists, postdoctoral researchers in the early stages of their career, and postgraduate researchers in the final stages of their doctoral work. As a result, the chapters included illustrate the remarkable scope and vitality of research currently being conducted under the broad heading of 'open source intelligence'. The volume's strength lies in both the timeliness of the three security issues themselves and the novel manner in which they are addressed.

The book is presented in four parts. The first considers new methods and approaches in broad, conceptual terms, contextualising some of the new sources, approaches and methodologies which have characterised advances in OSINT in recent years. Stevyn D. Gibson (Chapter 1) begins by exploring the role of OSINT and broadly defines its value to the intelligence function. He challenges popular assumptions regarding both the capabilities and the limitations of OSINT and argues that cultural, organisational and ideological contexts exert an important influence on OSINT and must be taken into consideration in attempts to assess the value of OSINT.

David Omand, Carl Miller and Jamie Bartlett (Chapter 2) introduce the concept of social media intelligence (SOCMINT) as a branch of OSINT. They argue that the analysis of social media offers the possibility of new levels of social, political and ideological insight, and claims that the advances made in data analytics methodologies make social media analysis of immense value, both to the intelligence community and beyond. Alastair Paterson and James Chappell close Part I (Chapter 3) by exploring the impact of OSINT on cybersecurity. They describe the dangers that the availability of open source information about businesses in their digital presence poses to information assets and business activities in an increasingly web-based society. They go on to explore some innovative ways of mitigating these risks.

The three subsequent parts build on the concepts and issues raised in the more general opening section, addressing OSINT's relevance and application to three topical issues in international security: nuclear proliferation, terrorism and humanitarian crises.

In Part II on OSINT and proliferation, Christopher Hobbs and Matthew Moran (Chapter 4) begin by exploring the value of OSINT in assessing states' nuclear intentions and capabilities, focusing on the approach of the International Atomic Energy Agency (IAEA). From political statements to scientific and technical publications, open source information can provide a range of clues regarding a state's nuclear trajectory. This is followed by Daniel Salisbury (Chapter 5), who considers the opportunities and challenges that OSINT provides in understanding how states illicitly procure technologies for their nuclear and missile programmes. Using the growth in publically available information about illicit procurement as a starting point, he discusses the value of largely untapped information held by the private sector, and conversely the role that OSINT can play in informing industry about the risks posed by present-day illicit procurement attempts by states such as Iran and North Korea.

Part III explores OSINT in the context of humanitarian crises. Randolph Kent (Chapter 6) begins by exploring the growing reliance on social media as a means of dealing with humanitarian crises. While acknowledging and detailing the benefits of social media to those working to mitigate the effects of humanitarian crises, he also examines the drawbacks of this new aspect of OSINT. He argues that 'negative noise' (contradictions and inconsistencies in information) can add confusion to humanitarian operations, and he proposes systemic approaches to mitigate this problem and promote greater reliability and authenticity. Fred Bruls and A. Walter Dorn (Chapter 7) argue that a new concept, human security intelligence (HSI), holds the key to the comprehensive understanding of humanitarian crises that is essential for field operations to be a success. Based on the concept of 'human security', Dorn and Bruls argue that the idea of HSI derives, to a large extent, from the power and value of OSINT.

Part IV considers the value of OSINT in terms of understanding terrorism. It begins with Carl Miller and Simon Wibberley (Chapter 8) who build on the theme of social media set out in Part I. They explore the ways in which social media can be harnessed to detect events and improve responses to large-scale emergency situations, such as terrorist attacks. Moving the focus from the response to terrorist attacks to the groups themselves, the John C. Amble (Chapter 9) presents an analysis of jihadist groups' online presence. He argues that the notion of a global jihadist movement is both reductive and limiting, particularly in terms of counterterrorism strategy. Amble draws on the media releases of three terrorist groups – al-Qaeda in the Arabian Peninsula, Lashkar-e-Taiba and Boko Haram – with a view to illustrating the

range of identities, beliefs and ideologies that exist within the jihadist movement. Ultimately, the chapter argues that OSINT offers a means of gaining a more nuanced insight into the individual identities of terrorist groups and that this approach should form the basis of distinct, tailored approaches to mitigating the threat posed by a particular group.

In general terms, the focused and subject area-specific chapters highlighting the uses, benefits and challenges of OSINT in particular security contexts complement the more conceptual chapters set out in Part I to provide readers with a comprehensive and far-reaching analysis of an area that has grown in importance over the past two decades.

Notes

1. See Richard Holt, 'Twitter in Numbers', *The Telegraph*, 21 March 2013, http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.html; and 'Press Information', Tumblr website, http://www.tumblr.com/press.
2. 'INTellingence: Open Source Intelligence', CIA website, 23 July 2010 (updated 30 April 2013), https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open source-intelligence.html.
3. 'ODNI Announces Establishment of Open Source Center', ODNI News Release No. 6–05, 8 November 2005, https://www.fas.org/irp/news/2005/11/odni110805.html.
4. Julian Borger, 'Syria: Chemical Weapons Inspectors Begin Securing Assad Regime's Arsenal', *The Guardian*, 3 October 2013.
5. 'Obama to Seek Congress Vote on Syria Military Action', *BBC News*, 1 September 2013.
6. 'Syria: Reported Chemical Weapons Use – Letter from the Chairman of the Joint Intelligence Committee', *UK Cabinet Office*, 29 August 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/235094/Jp_115_JD_PM_Syria_Reported_Chemical_Weapon_Use_with_annex.pdf.
7. 'Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013', *Office of the Press Secretary, The White House*, 30 August 2013, http://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21.
8. Ibid.