Advanced Sciences and Technologies for Security Applications

Babak Akhgar
P. Saskia Bayerl
Fraser Sampson *Editors*

Open Source Intelligence Investigation

From Strategy to Implementation

Springer

Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Babak Akhgar · P. Saskia Bayerl
Fraser Sampson
Editors

Open Source Intelligence Investigation

From Strategy to Implementation

Springer

Editors
Babak Akhgar
School of Computing and Management Sciences
Sheffield Hallam University
Sheffield
UK

P. Saskia Bayerl
Rotterdam School of Management
Erasmus University
Rotterdam
The Netherlands

Fraser Sampson
Office of the Police and Crime Commissioner for West Yorkshire
Wakefield
UK

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-319-47670-4 ISBN 978-3-319-47671-1 (eBook)
DOI 10.1007/978-3-319-47671-1

Library of Congress Control Number: 2016955064

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

It is our great privilege to welcome you to our book *Open Source Intelligence—From Strategy to Implementation*. In this collection, we offer an authoritative and accessible guide on how to conduct open-source intelligence (OSINT) investigations from data collection to analysis to the design and vetting of OSINT tools. It further highlights the broad range of challenges and complexities faced by law enforcement and other security agencies utilizing OSINT to increase our communities' security as well as to combat terrorism and organized crime.

One of the most important aspects for a successful police operation is the ability for the police to obtain timely, reliable, and actionable intelligence related to the investigation or incident at hand. OSINT provides an invaluable avenue to access and collect such information in addition to traditional investigative techniques and information sources. Examples of OSINT covered in this volume range from information posted on social media as one of the most openly available means of accessing and gathering open-source intelligence to location data, OSINT obtained from the darkweb to combinations of OSINT with real-time analytical capabilities and closed sources. And while OSINT by its nature is not generally gathered as 'evidence', it can be powerful when deployed in proceedings against criminals. The book therefore concludes with some consideration of the legal and procedural issues that will need to be addressed if OSINT is to be used in this way.

This book thus provides readers with an in-depth understanding to OSINT from a theoretical, practical, and legal perspective. It describes strategies for the design and deployment of OSINT for LEAs as well as other entities needing to capitalize on open-source data. The book offers a wide range of case examples and application scenarios from LEAs to defense and security agencies to industry, as well as hands-on guidance on the OSINT investigation process. The book outlines methods and illustrates benefits and challenges using real-life cases and (best) practices used by LEAs, security agencies, as well as industry. Another important aspect is the inclusion of legal and ethical considerations in the planning and conducting of OSINT investigations.

We would like to take the opportunity to recognize the work of our contributors to allow us to draw upon their expertise for this book—a process that has enabled us

to highlight many of the important aspects of OSINT-related needs and requirements of LEAs and other security actors within its chapters. This interdisciplinary approach has helped us to bring together a wide range of domain knowledge from law enforcement, academia and industry to present our readers with an operational focused aspect of OSINT-based investigations and related strategic narratives from planning to deployment. We hope that this book will serve as a compendium for practitioners, academics, teachers, and students for state-of-the art knowledge ranging from conceptual considerations to hands-on practical information to legal and ethical guidance.

Sheffield, UK — Babak Akhgar
Rotterdam, The Netherlands — P. Saskia Bayerl
Wakefield, UK — Fraser Sampson

Acknowledgements

The editors wish to thank the multidisciplinary team of experts who have contributed to this book, sharing their knowledge, experience, and latest research. Our gratitude is also extended to the following organizations and projects:

- CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), UK
- Rotterdam School of Management, Erasmus University, Netherland
- Information Technologies Institute, Centre for Research and Technology Hellas (CERTH-ITI), Thessaloniki, Greece
- National University of Public Service, Budapest, Hungary
- National Academy of Sciences, Institute for Computer Science and Control, Hungary
- Hungarian Competition Authority
- Police Services of Northern Ireland
- Home Office CAST, UK
- Serco Plc.
- EU-FP7 Project ATHENA (313220)
- EU-H2020 Project TENSOR (700024)
- EU-FP7 Project HOMER (312388)
- DG Home Project UNIFC2 (HOME/2013/ISEC/AG/INT/4000005215)

Contents

Editors and Contributors

About the Editors

Babak Akhgar is Professor of Informatics and Director of Center of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) at Sheffield Hallam University (UK) and Fellow of the British Computer Society. He has more than 100 refereed publications in international journals and conferences on strategic information systems with aspecific focus on knowledge management (KM) and intelligence management. He is member of editorial boards of several international journals and has acted as Chair and Program Committee Member for numerous international conferences. He has extensive and hands-on experience in the development, management, and execution of KM projects and large international security initiatives (e.g., the application of social media in crisis management, intelligence-based combating of terrorism and organized crime, gun crime, cyber-crime and cyber-terrorism, and cross cultural ideology polarization). In addition to this, he acts as technical lead in EU Security projects (e.g., "Courage" on Cyber-Crime and Cyber-Terrorism and "Athena" on the Application of Social Media and Mobile Devices in Crisis Management). Currently, he is the technical lead on EU H2020-project TENSOR on dark web. He has co-edited several books on Intelligence Management. His recent books are titled *Strategic Intelligence Management (National Security Imperatives and Information and Communications Technologies), Knowledge Driven Frameworks for Combating Terrorism and Organised Crime, Emerging Trends in ICT Security, and Application of Big Data for National Security.* Professor Akhgar is a board member of the European Organisation for Security and member of the academic advisory board of SAS UK.

P. Saskia Bayerl is Associate Dean of Diversity and Associate Professor of Technology and Organizational Behavior at Rotterdam School of Management, Erasmus University, the Netherlands. She further is Co-Director of the Centre of Excellence in Public Safety Management (CESAM, Erasmus University) and Visiting Research Fellow at CENTRIC (Center of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research, Sheffield Hallam University, UK). She is a regular speaker at police and security conferences and workshops and member of advisory boards of EU projects, as well as program committee member for international conferences. Her current research interests lie at the intersection of human–computer interaction, organizational communication, and organizational change with a special focus on the impact of technological innovations and public safety. Her research has been published in journals such as *MIS Quarterly, Communications of the ACM, New Media and Society*, and *Journal of Organizational Behavior* as well as international conferences in psychology, management, computational linguistics, and computer sciences and books. Most recently, she co-edited the book *Application of Big Data for National Security* (Elsevier).

Fraser Sampson, LL.B. (Hons), LL.M., MBA Solicitor has over 30 years experience in the criminal justice sector. A former police officer, he is the Chief Executive and Solicitor for the Office of the Police and Crime Commissioner for West Yorkshire. While practicing with national law firms, he represented police officers and the Police Federation in a number of high profile disciplinary cases and inquiries. A graduate of the Top Management Programme at the National School of Government, he is the founding author of *Blackstone's Police Manuals*, has written other key policing books published by Oxford University Press and is the editor of *Blackstone's Police Operational Handbook and the Routledge Companion to UK Counter Terrorism* (by Andrew Staniforth). Having published over 90 articles Fraser is on the editorial board of the Oxford Journal *Policing: A journal of strategy and practice*, is a member of the board of the Centre of Excellence in Terrorism, Resilience, Intelligence, and Organised Crime Research at Sheffield Hallam University and is an Associate Member of the Scottish Institute for Policing Research. Recent publications include chapters in *The Cyber Crime and Terrorism Investigators' Handbook* (Akhgar et al., Elsevier), *Big Data for National Security—A Practitioner's Guide to Emerging Technologies* (Akhgar et al., Elsevier) and *Policing in Northern Ireland—A New Beginning? It Can Be Done* (Rea & Masefield, Liverpool University Press).

Contributors

Babak Akhgar CENTRIC/Sheffield Hallam University, Sheffield, UK

András Benczúr Institute for Computer Science and Control of the Hungarian Academy of Sciences (MTA SZTAKI), Budapest, Hungary

Ben Brewster CENTRIC/Sheffield Hallam University, Sheffield, UK

Elisavet Charalambous Advanced Integrated Technology Solutions & Services Ltd, Egkomi, Cyprus

Neil Cunningham Police Service Northern Ireland, Belfast, Ireland

Tony Day CENTRIC/Sheffield Hallam University, Sheffield, UK

Géza Füzesi Hungarian Competition Authority, Budapest, Hungary

Helen Gibson CENTRIC/Sheffield Hallam University, Sheffield, UK

Eliot Higgins Bellingcat, Leicester, UK

Christos Iliou Centre for Research and Technology Hellas, Information Technologies Institute (CERTH-ITI), Thermi-Thessaloniki, Greece

George Kalpakis Centre for Research and Technology Hellas, Information Technologies Institute (CERTH-ITI), Thermi-Thessaloniki, Greece

Dimitrios Kavallieros Center for Security Studies (KEMEA), Hellenic Ministry of Interior and Administrative Reconstruction, Athens, Greece

Ioannis Kompatsiaris Centre for Research and Technology Hellas, Information Technologies Institute (CERTH-ITI), Thermi-Thessaloniki, Greece

Nikolaos Koutras Advanced Integrated Technology Solutions & Services Ltd, Egkomi, Cyprus

George Leventakis Center for Security Studies (KEMEA), Hellenic Ministry of Interior and Administrative Reconstruction, Athens, Greece

Alison Lyle Wakefield, UK

Laurence Marzell SERCO, Hook, UK

Jonathan Middleton Police Service Northern Ireland, Belfast, Ireland

Sándor Munk National University of Public Service, Budapest, Hungary

George Papalexandratos Center for Security Studies (KEMEA), Hellenic Ministry of Interior and Administrative Reconstruction, Athens, Greece

Steve Ramwell CENTRIC/Sheffield Hallam University, Sheffield, UK

Quentin Revell Centre for Applied Science and Technology, Home Office, St Albans, UK

Fraser Sampson Office of the Police and Crime Commissioner for West Yorkshire, West Yorkshire, UK

Tom Smith Centre for Applied Science and Technology, Home Office, St Albans, UK

Robert Stacey Centre for Applied Science and Technology, Home Office, St Albans, UK

Andrew Staniforth Trends Institution, Abu Dhabi, United Arab Emirates

Fahimeh Tabatabaei Mehr Alborz University, Tehran, Iran

Theodora Tsikrika Centre for Research and Technology Hellas, Information Technologies Institute (CERTH-ITI), Thermi-Thessaloniki, Greece

Pál Vadász National University of Public Service, Budapest, Hungary

Stefanos Vrochidis Centre for Research and Technology Hellas, Information Technologies Institute (CERTH-ITI), Thermi-Thessaloniki, Greece

Douglas Wells CENTRIC/Sheffield Hallam University, Sheffield, UK

B.L. William Wong Interaction Design Centre, Middlesex University, London, UK

Part I
Introduction

Chapter 1
OSINT as an Integral Part of the National Security Apparatus

Babak Akhgar

Abstract The roles of law enforcement agencies include maintaining law and order, protecting citizens and preventing, detecting and investigating crime. OSINT can provide critical capability for LEAs and security services to complement and enhance their intelligence capability, as the ability to rapidly gather and accurately process and analyze open source data can be a significant help during investigations and used for national level strategic planning to combat crime. Thus, purposeful and legal monitoring, analyzing and visualizing data from open data sources should be considered as mandatory requirement of any national security strategy. This chapter showcases the breadth of current and potential uses of OSINT based on UK's CONTEST strategy which provides the underlying basis of measures to prevent, pursue, protect and prepare against terror. It further proposes that to achieve efficient and innovative solutions, LEAs may be well advised to consider collaborations with private and public partners including academia using the successful implementation of the CENTRIC OSINT Hub is an example of how academia and LEAs can collaborate within the OSINT sphere in order to bring research into reality for the security and protection of citizens.

1.1 Introduction

A rise in the prevalence of Open Source Intelligence (OSINT) and its application by law enforcement and security agencies is set against a background of conflict, insecurity and the resurgence of violence in troubled regions across the world. For the United Kingdom, like many other nations, we remain under the constant threat of actual and potential attacks from all manner of hazards including terrorism, organized crime and cyber-related threats that—if left unchecked—can cause untold harm to citizens, communities, public services, businesses and the wider economy.

B. Akhgar (✉)
CENTRIC/Sheffield Hallam University, Sheffield, UK
e-mail: B.Akhgar@shu.ac.uk

B. Akhgar et al. (eds.), *Open Source Intelligence Investigation*,
Advanced Sciences and Technologies for Security Applications,
DOI 10.1007/978-3-319-47671-1_1

The scale and level of atrocities of recent terrorist attacks such as those in Paris, Brussels, Nice and Munich provide a cold and tangible reminder of the very real threat different nations across the world face. One of the common factors seen in the way these threats are realized is in the use of internet based communication platforms by terrorist individuals or formal groups such as the self-proclaimed Islamic State. For example, social media has increasingly become the dominant platform for projection onto overseas individuals, primarily through the dissemination of propaganda, complex indoctrination methodologies and recruitment campaigns,[1] creating a theatre of manipulation, with unprecedented ease of usage as well as access to the vulnerable. Indeed, this is reflected in both the record number of foreign nationals fighting in areas such as Iraq and Syria[2] as well as the controversial arrests and imprisonment of UK children between the ages of 14–17 for encouraging and masterminding terror attack plots.[3,4]

1.2 OSINT and Counter Terrorism Strategy

OSINT has, over the last five to ten years, been increasingly utilized by private sector organizations as a means to measure customer loyalty, track public opinion and assess product reception. Similarly, law enforcement and security agencies are acknowledging the requirement to apply similar techniques in order to enhance their investigative capability and improve their ability to identify and respond to criminal threats (see Chaps. 2, 3 and 13). The criminal entities perpetrating these threats are exploiting the internet for purposes such as recruitment (see Chap. 5), formation of illegal cartels (see Chap. 16) and the transfer of information and money to finance and co-ordinate their illicit activities.

The expansion of the internet has interwoven continents, cultures and communities, in addition to integrating with the majority of contemporary technologies. Whilst social media remains the dominant online platform for criminal and extremist psychological operations, there is an increasing potential for it to follow

[1]Helmus, T. C., York, E., Chalk, P. (2013). Promoting Online Voices for Countering Violent Extremism. (Rand Corporation, Santa Monica, California). Available at: http://www.rand.org/pubs/research_reports/RR130.html (Accessed: 03/08/2016).

[2]Bartlett, E. (2014). Record number of foreign nationals fighting in Iraq and Syria. The Independent Online. Available at: http://indy100.independent.co.uk/article/record-number-of-foreign-nationals-fighting-in-iraq-and-syria–gk2635auox (Accessed: 03/08/2016).

[3]BBC. (2015) "Anzac Day terror plot: Blackburn boy sentenced to life". Available at: http://www.bbc.co.uk/news/uk-34423984 (Accessed Online: 03/08/2016).

[4]Dodd, V. (2016). "Counter-terrorism detectives arrest east London teenager". The Guardian Online, Available at: https://www.theguardian.com/uk-news/2016/jun/16/counter-terrorism-detectives-arrest-east-london-teenager (Accessed Online: 03/08/2016).

the path of the internet, branching out, utilizing the likes of gaming consoles,[5] mobile applications,[6] cloud storage[7] and P2P services. Whilst social media and the surface web are used fundamentally for psychological, moral and emotional tactics, the dark web is used to a greater degree for the physical and tactical side of operations, focusing on arms and munitions,[8] false documents,[9] explosive making guides, crypto currency funding[10] and encrypted anonymous strategic communications.

The ubiquity of the internet has vastly increased the quantity, value and accessibility of OSINT sources. By definition, OSINT is intelligence based upon information that is freely available from public sources such as newspaper reports, journals, radio and television broadcasts, and more commonly in the current environment; social media and the internet.

When dealing with intelligence derived from the public domain, and specifically social media, there is a requirement to manage the public's privacy expectations appropriately, as although often freely available, much of the information posted to sites such as Facebook and Twitter is considered to be personal by registered users. When dealing with OSINT as opposed to more traditional closed intelligence sources, the concerns of the intelligence community turn from the availability of information to the identification of pertinent and accurate information. For these reasons it is increasingly necessary to validate intelligence derived from open sources with that from robust, closed source intelligence and the domain expertise of security professionals (see Chap. 9). Intelligence validation in this way is a particularly poignant topic when addressing social media content, as users often choose not to disclose or to falsify the personal information that they provide on these platforms (Bayerl and Akhgar 2015).

---

[5]Tassi, P. (2015). "How ISIS terrorists may have used PlayStation 4 to discuss and plan attacks". Forbes Online. Available at: http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/#39d5c755731a (Accessed Online: 03/08/2016).

[6]Billington, J. (2015). "Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators". International Business Times. Available at: http://www.ibtimes.co.uk/paris-terrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880 (Accessed: 03/08/2016).

[7]Hall, K. (2011). "Cyber terrorism set to increase after al-Qaeda calls for more cyber-attacks, says government". Computer Weekly Online. Available at: http://www.computerweekly.com/news/2240105012/Cyber-terrorism-set-to-increase-after-al-Qaeda-calls-for-more-cyber-attacks-says-government (Accessed Online: 03/08/2016).

[8]See listed Dark Web onion gun site vendors: https://www.deepdotweb.com/tag/guns/.

[9]Charlton, A. (2015). "Dark web vendors sell blank British passport and entry to database for just £2000". Available at: http://www.ibtimes.co.uk/dark-web-vendors-sell-blank-british-passports-entry-passport-database-just-2000-1509564 (Accessed Online: 03/08/2016).

[10]Smith, M. (2015). "Hacktivists claim ISIS terrorists linked to Paris attacks had bitcoin funding". Network World. Available at: http://www.networkworld.com/article/3005308/security/hacktivists-claim-isis-terrorists-linked-to-paris-attacks-had-bitcoin-funding.html (Accessed Online: 03/08/2016).

Table 1.1 Overview of the CONTEST strategy principles and their application for OSINT

	Contest components	OSINT proposition
Prevent strategy	The Prevent strategy is concerned with tackling the radicalisation of people who sustain the international terrorist and organised crime threat	Identification of terrorist narratives, influencers and propaganda over the surface web, particularly in countering attempts to turn people to terrorism by 'incitement and recruitment', thus tackling the factors or root causes which can lead to radicalisation and recruitment, in Europe and internationally More effective development of counter-extremists narratives and to encourage inter-cultural dialogue promoting good governance, democracy, education and economic prosperity Understanding of communities and areas of concern
Pursue strategy	The Pursue strategy is concerned with reducing the terrorist threat by disrupting terrorists and organised criminal groups and their operations	Gathering intelligence from the dark web (see also Chap. 8) Legal and ethical collection of evidence for securing convictions International corporation helping to pursue and investigate terrorist threats inside and outside of national borders, to impede the travel and communication of terrorists and criminals, to disrupt their support networks and to cut off funding and access to attack materials, and to bring individuals to justice
Protect strategy	The Protect strategy is concerned with reducing vulnerability to terrorist and organised crime attacks for European Member States	Proactive threat assessment of vulnerabilities (e.g., border security) and social areas of risk such as Child Sexual exploitation (CSE) (see Chap. 15) Proactive and live assessment of threats to mass gatherings Protection of National Critical Infrastructure and reduction of their vulnerability to attacks, including through increased security of borders and transport. (see Chap. 4)
Prepare strategy	The Prepare strategy is concerned with ensuring that the population and European Member States are as ready as they can be for the consequences of a terrorist attack and organised criminal event.	Building of communities' resilience (see Chap 4) Preparation for potential CBRNE (Chemical, Biological Radioactive, Nuclear and Explosive) attacks Modelling of emerging organised crime Early warning for health hazards

From the national security perspective, OSINT-based solutions should enhance the capabilities of law enforcement agencies and security services, providing access to more actionable intelligence that can support existing decision making, tasking and coordination activities. The core of any OSINT solution should focus on internet-centric data gathering and exploitation. The latter includes development of enhanced capabilities and services to gather, analyze, visualize and combine relevant data from which dynamic and real time hypothesizes can be generated.

Measures to combat crime and terrorism—online and offline—are an increasingly important element of any national security strategy. Looking at current approaches to counter terrorism in the UK, the 4 Ps of the CONTEST strategy[11] provide the underlying basis of measures to prevent, pursue, protect and prepare against terror. An overview of the four principles and how OSINT may be employed in their support can be found in Table 1.1. Later chapters in the book discuss how these examples manifest within a real operational context.

It should be noted that although the goals of terrorist and organised crime groups (OCGs) are different, the connections between terrorist and organised criminal activities appear to be growing. For example, in the recent attack in Munich (22nd July 2016) the perpetrator of the attack is believed to have procured his weapon through the dark web. Criminal activities that terrorist groups are involved in, either through affiliation with individual criminals and criminal groups or through their own operations, can include the trafficking of illegal goods and substances such as weapons and drugs, trafficking in human beings, financial fraud, money laundering and extortion (see Chap. 16)

OSINT is already being utilized as one of the key intelligence sources for national security and its importance is only increasing. And as Table 1.1 demonstrates, the breadth of current and potential uses is enormous. However, OSINT cannot be the only source that LEAs and security agencies rely on. OSINT is at its most powerful, when it is able to augment existing closed source intelligence by providing additional information and direction to where further intelligence may be required (see Chap. 9). The combined effect of OSINT and traditional intelligence sources reflect national security intelligence apparatus of a nation.

A promising approach to ensure efficient and innovative solutions and processes are collaborations between various public and private actors and organizations such as LEAs, industry and academia, amongst others. In the following we illustrate this approach by describing the setup and functioning of the OSINT Hub at CENTRIC (Centre of Excellence for Terrorism, Resilience, Intelligence and Organized Crime Research).

[11]Contest Strategy. The UK's Strategy for Countering Terrorism, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, July 2011.

1.3 The CENTRIC OSINT Hub

Since 2012, the Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research (CENTRIC) has built a strong research and development capability focused on the operational utilization of OSINT in regards to its application in relation to counter terrorism, cybercrime, crisis management and in the identification and modeling of organized crime.

At the beginning of 2016, CENTRIC launched its Open Source Intelligence Hub, or OSINT Hub, which has been gaining momentum as a physical and virtual space for the operational exploitation, dissemination and development of CENTRIC capabilities. Such capabilities are constantly being acquired, developed and improved in technical and non-technical expertise and tooling. This is happening in close collaboration with national, pan-European, and international partners in academia, public and private sectors. The OSINT Hub is ultimately the sum of CENTRIC's and its partners' experiences and is quickly setting a benchmark in research and development around:

- Counter-terrorism
- Major investigations
- Cybercrime
- Crisis management
- Public order
- Child sexual exploitation
- Identification and modeling of Organized Crime

Domain expertise has been ingrained into the Hub through direct collaboration with a number of law enforcement agencies and investigatory teams to directly influence and increase the capabilities of the hub.

The foundation of the OSINT Hub's situational awareness and data processing capabilities were born out of CENTRIC's participation in major EU projects, in collaboration with law enforcement, as a major technical partner responsible for the delivery of the projects situational awareness dashboard, web crawling, entity extraction, content categorization, social media and data aggregation functionalities—all of which are built on state-of-the-art tools offered by leading providers, open source communities and existing academic research. Harnessing these capabilities has enabled CENTRIC to more efficiently deliver data processing and command and control capabilities to its partners. To date, the OSINT Hub provided support to various live investigations ranging from child sexual exploitation to terrorism.

The secure physical environment in the OSINT Hub enables investigators to work directly with the CENTRIC team and their tools and to provide direct input into the development of future capabilities. Many of the investigatory capabilities of the OSINT Hub have been developed through such collaboration and can clearly benefit law enforcement through cost reductions in both targeted investigations and strategic situational awareness. They may also explore the potential of OSINT

making use of the Hub's tools, ensuring compatibility with existing workflows and processes and compliance with existing governance and legal requirements such as RIPA and the Data Protection Act (see Chaps. 17 and 18).

1.4 Concluding Remarks

The roles of law enforcement agencies include maintaining law and order, protecting citizens and preventing, detecting and investigating crime. In achieving these goals, LEAs will fulfill the purpose of protecting the security of society and the citizens they serve. OSINT can potentially provide critical capability for LEAs and security services to complement and enhance their intelligence capability. Purposeful and legal monitoring, analysing and visualizing public open source data source should be considered as mandatory requirements of any national security strategy. The ability to rapidly gather and accurately process and analyse open source data can be a significant help during investigations, whilst it can also be used for national level strategic planning to combat crime. However, to achieve efficient and innovative solutions, LEAs may be well advised to consider collaborations with private and public partners including academia. The successful implementation of the CENTRIC OSINT Hub is an example of how academia and LEAs can collaborate within the OSINT sphere in order to bring research into reality for the security and protection of citizens.

References

Bayerl PS, Akhgar B (2015) Surveillance and falsification implications for open source intelligence investigations. Commun ACM 58(8):62–69

Billington J (2015) Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators. International Business Times. Available at: http://www.ibtimes.co.uk/paris-terrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880 Accessed Aug 03 2016

Charlton A (2015). Dark web vendors sell blank British passport and entry to database for just £2000. Available at: http://www.ibtimes.co.uk/dark-web-vendors-sell-blank-british-passports-entry-passport-database-just-2000-1509564 Accessed Online Aug 03 2016

Contest Strategy (2011) The UK's strategy for countering terrorism, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, July 2011

Hall K (2011) Cyber terrorism set to increase after al-Qaeda calls for more cyber attacks, says government. Computer Weekly Online. Available at: http://www.computerweekly.com/news/2240105012/Cyber-terrorism-set-to-increase-after-al-Qaeda-calls-for-more-cyber-attacks-says-government Accessed Online Aug 03 2016

Tassi P (2015) How ISIS terrorists may have used PlayStation 4 to discuss and plan attacks. Forbes Online. Available at: http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/#39d5c755731a Accessed Online Aug 03 2016

Smith M (2015) Hacktivists claim ISIS terrorists linked to Paris attacks had bitcoin funding. Network world. Available at: http://www.networkworld.com/article/3005308/security/hacktivists-claim-isis-terrorists-linked-to-paris-attacks-had-bitcoin-funding.html Accessed Online 3 Aug 2016

Chapter 2
Open Source Intelligence and the Protection of National Security

Andrew Staniforth

Abstract Given the scale and complexity of the threats from international terrorism, intelligence agencies must continue to advance counter-terrorism measures to keep us all safe; and most importantly, seek new ways in which to embed progressive developments to ensure that the primary driver for change in counter-terrorism practice is not simply the next successful attack. Harnessing the power of OSINT via Big Data continues to be a game-changer for counter-terrorism policy-makers, professionals and practitioners. The purpose of this chapter is to explain the importance of OSINT within the context of national security and the role of intelligence agencies to prevent and protect citizens from the threat of international terrorism. To outline the operational requirements for intelligence agencies use of OSINT, this chapter also outlines key components of the modern terrorist threat, which includes explanations of terrorist radicalization development processes and how OSINT and the power of Big Data analytics is increasingly being used to combat terrorism and prevent violent extremism.

2.1 Introduction

The first duty of government remains the security of its citizens. The range of threats to national security is becoming increasingly complex and diverse. Terrorism, cyber-attack, unconventional attacks using chemical, nuclear, or biological weapons, as well as large-scale accidents or natural hazards—anyone could put citizen's safety in danger while inflicting grave damage to a nation's interests and economic well-being. When faced with a combination of current levels of economic uncertainly and political instability, governments must be able to act quickly and effectively to address new and evolving threats to their security. Tough security measures are needed to keep citizens, communities and commerce safe

A. Staniforth (✉)
Trends Institution, Abu Dhabi, The United Arab Emirates
e-mail: info@trendsinstitution.org

B. Akhgar et al. (eds.), *Open Source Intelligence Investigation*,
Advanced Sciences and Technologies for Security Applications,
DOI 10.1007/978-3-319-47671-1_2

from contemporary security hazards, the most pressing of which remains the enduring threat from international terrorism.

Threats from terrorism are matters of intense public and political concern but they also raise acute challenges for the security apparatus of the State. These challenges arise because terrorism can inflict significant loss of life, yet it is not the scale of the atrocities committed in its name that gives terrorism its special status; it is the threat it poses to the State, for it undermines the basis of State legitimacy—the capacity to protect its citizens. Therefore, measures known as Counter-Terrorism (CT), as a major aspect of national security, attract high-profile political and public attention and correlatively failures in CT lead to significant outcries followed by stringent scrutiny from a variety of quarters including the media, public opinion, police investigation, government inquiry, parliamentary questioning and academic study.

The purpose of this chapter is to explain the importance of OSINT within the context of national security and the role of intelligence agencies to prevent and protect citizens from the threat of international terrorism (see Chap. 1). To outline the operational requirement for intelligence agencies use of OSINT, this chapter also outlines key components of the modern terrorist threat, which includes explanations of terrorist radicalization development processes and how OSINT and the power of Big Data analytics is increasingly being used to combat terrorism and prevent violent extremism.

2.2 From Threat to Threat

To understand the importance of OSINT in protecting national security from international terrorism we must first examine the nature of the changing threat from terrorists in this post-9/11 era of global terrorism. Over recent years, following a decade of tackling the terrorist atrocities committed by Al Qaeda and their global network of affiliates and inspired lone-actors, a new global terrorist phenomenon has risen from the conflict in Syria. The rise of Daesh—the self-proclaimed 'Islamic State'—provides further evidence that many nations across the world face a continuing threat from extremists who believe they can advance their aims through acts of terrorism. This threat is both serious and enduring, being international in scope and involving a variety of groups, networks and individuals who are driven by violent and extremist beliefs (see Chap. 12).

The violent progress of Daesh through towns and villages in Iraq has been swift—aided by foreign fighters from across the Middle East and Europe. Daesh have now taken control of large swathes of Iraq leading the British Prime Minister David Cameron to warn his Cabinet that violent Daesh jihadists were planning attacks on British soil. The warning came amid growing concerns amongst senior security officials that the number of Britons leaving the UK to fight alongside extremist groups abroad was rising. The export of British born violent jihadists is nothing new but the call to arms in Iraq this time had been amplified by a slick online

recruitment campaign, urging Muslims from across the world to join their fight and to post messages of support for Daesh. In a chilling online recruitment video designed to lure jihadists to Iraq, 20 year-old Nasser Muthana, a medical student from Cardiff in Wales, and his 17 year old brother Aseel, declared their support for Daesh while sitting alongside each other holding their semi-automatic assault rifles. In the video, Nasser states: 'We understand no borders. We have participated in battles in Syria and in a few days we will go to Iraq and will fight with them.' (Dassanayake 2014). Despite Nasser attaining 12 GSCE's at grade A, studying for his A-levels and being offered places to enroll on medical degrees at four UK universities, he instead volunteered to join the ranks of Daesh. Unbeknown to his parents or authorities, the former school council member and his younger brother, who was studying A-levels at the time, travelled to Syria via Turkey to fight the Assad regime. The father of the brothers-in-arms fighting for Daesh, Mr Muthana, declared no knowledge of their intended travel plans to Syria and had reported them missing to the police during November 2013. Mr Muthana remained devastated that his sons had turned to violent extremism, stating that: 'Both my sons have been influenced by outsiders, I don't know by whom. Nasser is a calm boy, very bright and a high achiever', going on to say that: 'He loved rugby, playing football and going camping with friends. But he has been got at and has left his home and everyone who loves him' (Dassanayake 2014).

The online propaganda of Daesh has proved ruthlessly effective. On 13 June 2015, a group of Daesh suicide bombers delivered a deadly attack near the city of Baiji in the Salahuddin province of Iraq. A four-strong terrorist cell killed eleven people in two separate explosions as they detonated bombs placed in their vehicles at an oil refinery. One of the bombers was 17 year old Talha Asmal, who had travelled thousands of miles from his home town in Dewsbury, West Yorkshire in England to join and fight alongside Daesh. Talha was described by his school teacher as a "conscientious student" (BBC 2015). His family, utterly devastated and heartbroken by the loss of their son, said: "Talha was a loving, kind, caring and affable teenager", going on to suggest that he had been: "exploited by persons unknown who were hiding behind the anonymity of the World Wide Web." (Grierson 2015) In committing his act of martyrdom in support of the Daesh cause, Talha became the youngest British suicide bomber. UK security forces are rightly concerned by British citizens fighting in Syria and Iraq. The numbers reported by various research institutes are certainly shocking. The Foreign Policy Research Institute evaluates that between 6000 and 12,000 volunteers have passed through Syrian territory, arriving from 70 different countries (Helfont 2012). Among these are approximately 2000 European citizens, creating a new dimension to terror threats across Europe, which has resulted in deadly and determined Daesh-inspired attacks in Paris and Brussels, leading to heightened levels of security across European Member States (Helfont 2012). Cecilia Malmstromm, the European Commissioner of Home Affairs, raised the alarm regarding foreign fighters to her counterparts in EU Member States saying that: "Often set on the path of radicalization in Europe by extremist propaganda or by recruiters, Europeans travel abroad to train and to fight in combat zones, becoming yet more radicalized in the process.

Armed with newly acquired skills, many of these European 'foreign fighters' could pose a threat to our security on their return from a conflict zone. And as the number of European foreign fighters rises, so does the threat to our security" (European Commission 2014). Of critical concern for the security of Western nations, is the way in which their citizens are being influenced by the extreme single narratives of religious or political ideologies promoted by terrorist and extremist groups and individuals such as Daesh. This narrative, when combined with a complex malaise of social and economic factors, serves to manipulate individuals towards adopting extremist perspectives, cultivating a terrorist threat which presents a clear and present danger to the free and democratic way of life in the West. This is a threat which is propagated via open-source information on the internet and the online radicalization of citizens remains a major source of support and new recruits for the Daesh cause.

2.3 Online Radicalisation

Understanding why young men and women from our communities have travelled to take up arms in conflict overseas is the question which most troubles intelligence agencies across Europe. The obsession with finding the answer has come to dominate the whole debate over the causes of terrorism. In the post-9/11 world, understanding how people become terrorists has come to be discussed in terms of 'radicalisation', a rather exotic term which presumably describes a similarly exotic process (Silke 2014). What is called radicalisation today, in the past was referred too much more mundanely as 'joining' a terrorist group or being 'recruited'. No one talked of the individuals joining the Irish Republican Army (IRA) or Euskadi Ta Askatasuna (ETA) as being 'radicalised', though they all certainly were according to our modern understanding arising from the Al Qaeda-inspired genre of international terrorism. After 9/11 it became awkward to talk about people 'becoming' terrorists, 'joining' terrorist groups or being 'recruited'. Those terms were too banal, too ordinary for the dawn of new-era global terrorism. Ordinary terms might imply ordinary processes and worse still, ordinary solutions. So these simple terms had to make way for something more exotic, more extreme and 'radicalisation' fitted the bill nicely, especially with the rise of online radicalisation via the internet which has changed—and continues to change—the very nature of terrorism. The internet is well suited to the nature of terrorism and the psyche of the terrorist. In particular, the ability to remain anonymous makes the internet attractive to the terrorist plotter. Terrorists use the internet to propagate their ideologies, motives, grievances and most importantly communicate and execute their plan. The most powerful and alarming change for modern terrorism, however, has been its effectiveness for attracting new terrorist recruits, very often the young and most vulnerable and impressionable in our societies. Modern terrorism has rapidly evolved, becoming increasingly non-physical, with vulnerable 'home grown' citizens being recruited, radicalized, trained and tasked online in the virtual and ungoverned domain of

cyber space. With an increasing number of citizens putting more of their lives online, the interconnected and globalized world in which we now live provides an extremely large pool of potential candidates to draw into the clutches of disparate terrorists groups and networks.

The openness and freedom of the internet unfortunately supports 'self-radicalization'—the radicalization of individuals without direct input or encouragement from others. The role of the internet in both radicalization and the recruitment into terrorist organizations is a growing source of concern for security authorities. The internet allows individuals to find people with shared views and values and to access information to support their radical beliefs and ideas. The unregulated and ungoverned expanse of the internet knows no geographical boundaries, thus creating a space for radical activists to connect across the globe. This is especially problematic as the easy access to like-minded people helps to normalize radical ideas such as the use of violence to solve grievances. Yet, solving the complex issue of radicalization by simple processes—such as the suggestion to 'clean up' the internet—is impracticable and well beyond the scope of any single government (see Chap. 5).

Understanding how and why people in our communities move towards extremist perspectives, and creating an alternative to allow them to resist adopting such views, remains the key challenge in countering the contemporary threat from terrorism. The intelligence agencies have a central role to both identify those individuals and groups who are radicalising and recruiting others to their extremist cause, as well as identifying individuals who are adopting violent views and putting in place preventative mechanisms and interventions to stop and deter the development of radicalism at source. Identifying radicalised individuals is a complex task and continues to present the greatest challenge to intelligence agencies across the world. It is widely acknowledged that nobody suddenly wakes up in the morning and decides that they are going to make a bomb. Likewise no one is born a terrorist. Conceptualisations of radicalisation have increasingly recognized that becoming involved in violent extremism is a process: it does not happen all at once. Similarly, the idea that extremists adhere to a specific psychological profile has been abandoned, as has the view that there may be clear profiles to predict who will follow the entire trajectory of radicalisation development (Hubbard 2015). Instead, empirical work has identified a wide range of potential 'push' and 'pull' factors leading to (or away from) radicalisation. There are many potential factors which may influence an individual towards adopting extremist perspectives. These include not only politics, religion, race and ideology, the very core motivations of terrorism, but may also include elements of a sense of grievance or injustice. It is important to recognize that terrorist groups can fulfill important needs for an individual: they give a clear sense of identity, a strong sense of belonging to a group, the belief that the person is doing something important and meaningful, and also a sense of danger and excitement. For some individuals, and particularly young men, these are very attractive factors. Individuals deemed to be vulnerable and potentially at risk of radicalisation share a widely held sense of injustice. The exact nature of this perception of injustice varies with respect to the underlying motivation for violence,

but the effects are highly similar. Personal attitudes such as strong political views against government foreign policies regarding conflicts overseas can also play an important role in creating initial vulnerabilities.

Intelligence agencies have come to recognize that terrorism is a minority-group phenomenon, not the work of a radicalized mass of people following a twisted version of faith. People are often socialized into this activity leading to a gradual deepening of their involvement over time. Radicalization is thus a social process, which requires an environment that enables and supports a growing commitment (Silke 2014). The process of radicalization begins when these enabling environments intersect with personal 'trajectories', allowing the causes of radicalism to resonate with the individual's personal experience. Some of the key elements in the radicalization process are thus related to the social network of the individual, for example, who is the person spending time with, and who are his or her friends, whether this activity and interaction is in the physical or cyber world. Intelligence agencies also recognize that no single radicalisation 'push' or 'pull' factor predominates. The catalyst for any given individual developing extremist views will more likely be a combination of different factors, which makes prediction with any certainty a challenging task. The manifestation of individual radicalisation factors may be subtle, resulting in very weak signs and signals of radicalisation development, while other factors may be more visible. Identifying these factors remains the key to the early prevention and intervention of radicalisation, ensuring intelligence agencies and their partners can act appropriately to stop terrorism at its source (Silk et al. 2013).

2.4 Counter Measures

The contemporary phase of counter-terrorism has evolved important new preventative trends, alongside palpable moves towards expansion and localism (Masferrer and Walker 2013). Many governments now seek to ensure that mechanisms are in place to be able to draw upon the valuable information and goodwill of communities from which aberrant extremists are recruited and radicalised. This role has fallen to both intelligence agencies and Law Enforcement Agencies (LEAs) who not only find specialist their counter-terrorism units tackling the extremist threat but a requirement for police officers engaged in community policing activities and their local authority partners (Spalek 2012). The working relationship between intelligence agencies and LEAs across Europe is developing and information to counter terrorism is no longer handled on a 'need to know' basis but rather on a 'need to share' approach (Silk et al. 2013). Although the security services and police forces retain their individual roles and responsibilities, there is currently greater sharing between them and between individual police forces within the arena of counter-terrorism. This has forged not only a greater readiness for intelligence sharing but also a sharing of equipment and human assets and a more jointly co-ordinated response to counter-terrorism activities such as surveillance

operations. Collaboration in counter-terrorism, given the immediacy and severity of the terrorist threat, is now absolutely essential, being fuelled by the relentless pursuit to gather intelligence to prevent attacks and pursue terrorists.

To kerb the terrorists' use of the internet, authorities are seeking to harness the full power of new technologies to keep communities safe from terrorist threats and intelligence agencies are using OSINT to inform and provide a richer picture to their covert and clandestine operations. An important aspect of intelligence agency use of OSINT is social media, which represents an increasing and fundamental part of the online environment in which the users are authors of the content who do not passively receive information, but they create, reshape and share it (see Chaps. 6 and 9). In some cases, the interaction among users based on social media creates communities and virtual worlds providing an excellent source of information for intelligence agencies. Although there are significant differences in the nature of these outputs, two aspects are always present and are relevant to the work of intelligence agencies: large amounts of information and user generated content. The social media platforms aggregate huge amounts of data generated by users which are in many cases identified or identifiable. When combined with other online and stand-alone datasets, this contributes to create a peculiar technological landscape in which the predictive ability that is Big Data analytics, has relevant impact for the implementation of social surveillance systems by States. Big Data is nothing new, but it is currently at the final stage of a long evolution of the capability to analyze data using computer resources which for the intelligence agencies of government provides an excellent opportunity to tackle terror and keep communities safe.

Big Data represents the convergence of different existing technologies that permit enormous data centers to be built, create high-speed electronic highways and have ubiquitous and on-demand network access to computing resources, more commonly referred to as 'cloud computing'(Akhgar et al. 2015). These technologies offer substantially unlimited storage, allow the transfer of huge amounts of data from one place to another, and allow the same data to be spread in different places and re-aggregated in a matter of seconds. All these resources permit a large amount of information from different sources to be collected and the pet bytes of data generated by social media represent the ideal context in which Big Data analytics can be used. The whole dataset can be continuously monitored by analytics, in order to identify the emerging trends in the flows of data and obtaining real-time or nearly real time results in a way that is revolutionary. Within the context of counter-terrorism, the availability of these new technologies and large datasets provides a competitive advantage, representing the greatest opportunity to increase the effective delivery of counter-terrorism. Big Data can help the identification of terrorist networks and their associations using OSINT and provide valuable corroboration of other intelligence sources to support the holistic development of intelligence. It can also rapidly support the identification of radical roots within online communities providing significantly increased capabilities and opportunities not just to prevent terrorist attacks, but to identify attack planning activity and most importantly, spot the early signs and signals of radicalization and recruitment to stop violent and extremist development at source.

2.5 Conclusions

Counter-terrorism is no longer the hidden dimension of statecraft. It has over recent years moved out of the shadows due in part to the understanding of intelligence agencies that not all counter-terrorism measures need to be cloaked in secrecy in order for them to be effective. Harnessing the power of OSINT via Big Data analytics capabilities presents a unique opportunity for governments to address the increasing threats from international terrorism at relatively low cost. But the handling of such large data-sets raises acute concerns for existing storage capacity, together with the ability to share and analyze large volumes of data. The accessibility of OSINT and the introduction of Big Data capabilities will no doubt require the rigorous review and overhaul of existing intelligence models and associated processes to ensure all in authority are ready to exploit Big Data OSINT.

While OSINT and Big Data analytics present many opportunities for national security, any developments in this arena will have to be guided by the State's relationship with its citizenry and the law. Citizens remain rightly cautious and suspicious of the access to and sharing of their online data—especially by agents of the state. As citizens put more of their lives online, the safety and security of their information matters more and more. Any damage to public trust is counter-productive to contemporary national security practices and just because the state may have developed the technology and techniques to exploit OSINT and harness Big Data does not necessarily mean that it should. The legal, moral and ethical approach to OSINT via Big Data analytics must be fully explored alongside civil liberties and human rights, yet balanced with protecting the public from security threats. Big Data analytics must not be introduced by stealth, but through informed dialogue, passing though the due democratic process of governments. Citizens are more likely to support robust measures against terrorists that are necessary, appropriate and proportionate but many citizens, and politicians for that matter, will need to be convinced that extensive use and increased reliability upon publicly-available information harnessed through the power of Big Data is an essential part of keeping communities safe from terrorism and violent extremism.

All in authority must also avoid at all costs the increased use of Big Data to maximize the potential of OSINT as a knee-jerk reaction to placate the public and the press following a terrorist attack. Experience over recent years shows that in the aftermath of terrorist events political stakes are high: politicians and legislators fear being seen as lenient or indifferent and often grant the executive broader authorities without thorough debate. New special provisions intended to be temporary turn out to be permanent. Although governments may frame their new provisions in terms of a choice between security and liberty, sometimes the loss of liberty is not necessarily balanced by the gain in safety and the measures introduced become counter-productive. The application of Big Data OSINT for national security should be carefully considered and not quickly introduced as any misuse of its power may result in long term damage of relations with citizens and communities due to the overextended and inappropriate use of Big Data capabilities.