Advanced Sciences and Technologies for Security Applications

Indexed by SCOPUS

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 https://link.springer.com/bookseries/5540

Adam Henschke · Alastair Reed · Scott Robbins · Seumas Miller
Editors

Counter-Terrorism, Ethics and Technology

Emerging Challenges at the Frontiers of Counter-Terrorism

Springer

Editors
Adam Henschke
Philosophy Section
University of Twente
Enschede, Netherlands

Scott Robbins
Center for Advanced Security, Strategic and Innovation Studies (CASSIS)
University of Bonn
Bonn, Germany

Alastair Reed
Cyber Threats Research Centre
Swansea University
Swansea, UK

Seumas Miller
Charles Sturt University
Canberra, Australia

TU Delft
Delft, Netherlands

University of Oxford
Oxford, England

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-030-90220-9 ISBN 978-3-030-90221-6 (eBook)
https://doi.org/10.1007/978-3-030-90221-6

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

Acknowledgments

The research was conducted under the auspices of the European Research Council's Advanced Grant program as part of the grant entitled, "Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies" (GTCMR. No. 670172) (Principal Investigator: Professor Seumas Miller; institutional partners, Delft University of Technology and the University of Oxford). The Australian Research Council Discovery Grant, entitled, "Intelligence And National Security: Ethics, Efficacy And Accountability" (DP180103439) (Principal Investigator Professor Seumas Miller; institutional partners Charles Sturt University and the Australian National University). The Australian Department of Defence Strategic Policy Grant, entitled "Countering Foreign Interference And Cyber War Challenges" (Principal Investigator Dr Adam Henschke; institutional partner, the Australian National University).

Introduction

On April 2019, the terrorist group National Thawheed Jamaath carried out a lethal terrorist attack in Sri Lanka that targeted Christians on Easter Sunday. “In all, eight men and one woman belonging to local Islamist groups detonated bombs almost simultaneously in several parts of the country, killing themselves and more than 250 others” [1]. Following the attacks, the Sri Lankan Defence Minister stated that the attacks were a response to the terrorist attack in Christchurch, New Zealand, in which the gunman killed more than 50 Muslims [2]. These attacks led the New Zealand Prime Minister Jacinta Ardern and French President Emmanuel Macron to lobby social media companies around the world to do more in the fight against terrorism. Ardern stated that “[t]his isn’t about freedom of expression; this is about preventing violent extremism and terrorism online” [3]. This shows how terrorism is now truly international—a terrorist attack conducted by an Australian in New Zealand against Muslims is said to have led to a terrorist attack in Sri Lanka conducted against Christians, driving two world leaders to seek changes from technology companies. Moreover, it shows that technology is now as much a part of terrorism and counter-terrorism as it is for all other parts of modern life. To say that we need to understand and respond to these new forms of violent extremism is obvious. The ethics of *how* we respond are complex and varied.

The 2001 al Qaeda attacks on the USA caused a seismic shift in how the world viewed terrorism. Then, in 2013 Edward Snowden released a trove of data that gave the world a glimpse of the technological power being wielded in the name of counter-terrorism. Since then we have witnessed the rise of social media being used by terrorists and counter-terrorist agencies, unprecedented hype for the use of artificial intelligence and machine learning for counter-terrorism, and the practices falling under bulk data collection ever increasing. Moreover, we are also bearing witness to a range of technologies being extended in their use as part of counter-terrorist practices—from the use of facial recognition technologies, to the ways we respond to weapons of mass destruction, to the development of social credit systems as tools for population control, justified by reference to the needs of counter-terrorism. This edited volume takes stock of the recent evolution of international terrorism, the development of modern technologies, and modernisation of more long-standing

technologies are being used to counter terrorists—and how terrorist organisations are leveraging it for their own purposes.

Getting a handle on how these technologies are actually used in the context of terrorism and counter-terrorism offers a way to start to separate the hype from the reality. For example, although there is much discussion of cyber-terrorism, there is little real-world activity that falls under this heading. This does not mean that important activities are not taking place with the aid of modern technologies. Terrorists are using drones to attack government forces, using social media for propaganda and recruitment, and encryption to evade detection. Counter-intelligence agencies are using machine learning to detect suspicious behaviour, hacking computers to gain access to encrypted data, and collecting bulk data in quantities too large to describe. The Christchurch shootings were notable as the shooter not only livestreamed his attacks, using social media to broadcast the attacks as they occurred, but also paired his attacks with an online manifesto, that has subsequently been linked to a range of nationalist terrorist efforts. Again, we see how new technologies and the social behaviours associated with them are evolving in parallel with terrorism.

Moreover, we also need to consider how terrorist use of technologies and the counter-terrorism responses impact the wider society. Social media is now a fundamental part of modern life—woven into people's personal lives, communities, and political activity. While many people might agree that social media companies ought to do more combat terrorist use of their tools, we must also confront concerns about free speech, free association, and the overreach of government. While the uses of these technologies are interesting in and of themselves, it is important to know whether or not these technologies are effective at countering terrorism. How often is a machine learning algorithm correct when it tags someone as suspicious? And how many terrorists does it miss? How does this compare to the old way of countering terrorism? Each technology and its application has its own set of difficulties when evaluating it for efficacy. This volume provides insight into either how efficacious these technologies are, or how we can go about evaluating them for efficacy. This efficacy is a key component of any ethical assessment of a counter-terrorism technology.

Ultimately, the questions here touch on deep ethical issues. What we mean here is twofold—first, when considering the adoption of a set of technologies like drones in the fight against terrorists, the use of surveillance to place individuals and groups under constant government observation, or whether encryption technologies should be used by citizens or "cracked" by counter-terrorism agencies, we are engaging with ethical content. Should drones be used at all? Is government surveillance permissible or is it a violation of individual privacy? Will the loss of encryption technology undermine the security of the internet, and should we care? Second, each of these questions requires us to engage in ethical reflection. What we mean here is that we cannot simply pass judgement on these actions by governments and individuals, deeming them right or wrong. We need to actively *reflect* upon those judgements, to look at the reasons that underpin them, to see if the actions, the judgements, and responses can be justified or not.

Finally, while some of these technologies may be effective means of counter-terrorism, we must go a step further and ensure that it is ethical to use technologies for these purposes. Much has been discussed about the ethics surrounding so-called killer robots—for counter-terrorism and warfare. Little academic discussion has been focused on other technologies. This is unfortunate as technologies like facial recognition technology, bulk data collection, and social media are actually being used today to counter terror. Each of these technologies present novel ethical issues which must be understood if we are to ensure that liberal democratic values are preserved while countering terrorism.

This book grapples with these ethical issues sitting at the frontiers of counter-terrorism, covering a range of different technologies and practices that span terrorism, counter-terrorism, and modern social practices. The threads are somewhat disparate, but weave together a story of similar challenges—how are technologies changing terrorist behaviours, driving the responses by counter-terrorism, and what are the criticisms and justifications for those behaviours and responses? The book comes in five main parts, each looking at different threads of this larger story.

The first part *Understanding Counter-Terrorism Technologies: Drones and the Ethical Risks of New Technologies* looks at how technologies shape the practice and understanding of counter-terrorism, looking at one of the most controversial sets of technologies used in efforts against terrorists: drones. Jessica Wolfendale starts by conceptualising the notion of terrorism and shows how state actions with particular technologies including drones offer significant ethical risks. Michael Robillard then looks at the relation between drone use and the narratives that develop around counter-terrorism practices. Amanda and Noel Sharkey then discuss the ways that terrorists and others can exploit particular features of drones, in service of their larger political aims.

Concepts of terrorism and technology are fundamental to any discussion of the ethics of counter-terrorism. In Technology as Terrorism: Police Control Technologies and Drone Warfare, Jessica Wolfendale presents an argument that technology, and the language we use to talk about technology, constrains and shapes our moral understanding of the nature, scope, and impact of terrorism, particularly in relation to state terrorism. This chapter offers conceptual discussions of the notion of terrorism, and the relation to state use of police control and drone technologies are combined with a narrative of precision and efficiency. This language masks the terroristic nature of the violence that these practices inflict and reinforces the moral exclusion of those against whom these technologies are deployed.

Michael Robillard also looks at drone technologies, but focusses attention on how the use of drone technologies in counter-terrorism operations bear upon the larger campaign to "win hearts and minds". He argues that an underlooked aspect of the use of drones in counter-terrorism operations is proper regard for the moral significance that the non-kinetic features of narrative, imagery, and social signalling play with respect to remote targeted killing operations. A fundamental aspect of any effective counter-terrorism operation is the narrative that goes along with that, and the use of relatively new technologies like drones must be seen with regard to that narrative.

In another approach to the ethical use of drones in counter-terrorism operations, Amanda Sharkey and Noel Sharkey look at how "deception" of these autonomous weapon systems is an increasingly important element. The basic worry here is that the absence of human control of autonomous weapon systems necessitates a changed perspective on the notion of deception that has not yet made its way into military manuals. They ask how does deception fit into the ongoing technological transformation of warfare where ever more control of weapons is being ceded to computer systems?

In the second part, *The Challenges of Technologies of Terrorism and Counter-Terrorism: Weapons of Mass Destruction, the Internet of Things, and Facial Recognition Technology* offers analysis of three different technology types to show how use of particular technology types presents challenges for counter-terrorism. Jonas Feltes begins the section looking at the notion of weapons of mass destruction (WMD), to offer an argument for a new way of considering these technologies. Adam Henschke then suggests that the Internet of Things (IoT) will usher in a new era where cyber-terrorism will present risks in the physical world, requiring us to anticipate this emergent risk and to prepare for it. Scott Robbins closes this part out by looking at Facial Recognition Technologies (FRT) to offer a set of arguments why some restrictions on the use of FRT for CT are ethically justified.

One of the deepest concerns that has driven a considerable aspect of counter-terrorism policies is what happens if a terrorist group has access to and uses a weapon of WMD. Jonas Feltes drills down into these concerns by providing a critical engagement of the concept of WMDs, showing the relations between chemical, biological, radiological, or nuclear weapons technologies the general concept of WMD. He argues that a static concept that includes or excludes certain weapon types purely on the basis of their physical impact in an attack deals with problematic threshold issues and ethical challenges. He instead offers a complex understanding of the impact of particular weapons, their availability to terrorists, such that the threat that terrorist attacks with improvised unconventional weapons can be analysed and displayed more accurately. This more nuanced approach both allows for more efficacious and precise counter-terrorism practices and policy and can reduce ethically unsustainable behaviour of first responders and the press during a terrorist incident.

Adam Henschke next looks at the IoT, the cluster of technologies that span the cyber and physical realms. In this chapter, he argues that this blurring and integration of the cyber and physical realms means that cyber-terrorism will take place. The threat of terrorism is an emergent threat, arising from the combination of five related features of the IoT: it is radically insecure, its components are in the world, that the sheer numbers of IoT devices mean potential attacks can be intense, its reliance on artificial intelligence will make aspects of it inscrutable, and that the IoT is largely invisible. As the IoT grows in scope and penetration of our physical worlds and behaviours, it means that cyber-terrorism is not a question of if, but when. This has significant ethical implications as these five features of the IoT mean that we ought to be regulating these technologies.

FRT is the third set of technologies requiring an ethical analysis. In this chapter, Scott Robbins explores the ways that FRT is used as part of counter-terrorism practices. Working from the recognition that while FRT might be justifiable, five conditions must be met for it to be ethically permissible. First, the state must create institutional constraints that only allow FRTs to be used in places where people do not (and should not) enjoy a reasonable expectation of privacy (e.g. airports, border crossings). Second, the cameras equipped with FRT must be marked to assure the public that they are not being surveilled in places that they should have a reasonable expectation of privacy. Third, FRTs should be restricted to finding serious criminals (e.g. terrorists). Fourth, the state should not use third-party companies that violate the first three conditions during the creation or use of its service. And fifth, third-party companies should not be able to access or read the sensitive data collected by the state. With these conditions satisfied, given the effectiveness of FRT, the state can harness FRT's power to counter-terrorism.

The third part, *Technologies that Extend the Reach and Power of the State: Surveillance* then moves to the development and use of surveillance technologies, and how governments seek to justify wider surveillance programs by reference to counter-terrorism efforts. In this part, the authors look at surveillance technologies to show how these technologies when used at part of wider CT programs can make the state much more powerful. John Hardy looks at the general ethical issues that arise when the state engages in surveillance that is persistent, involves pattern-of-life analysis, and activity-based surveillance. Michael Clarke then explores the way that China has used surveillance technologies as part of a "preventative" counter-terrorism campaign in the Xingjian region of China.

John Hardy's chapter "The Rise of the Modern Intelligence State" argues that the rise of the formal surveillance state in the early twenty-first century was precipitated by political impetus to empower security and intelligence organisations to perform a broad range of counter-terrorism functions. Ethical debates about the implications of the security intelligence reach of modern states have focused on balancing individual rights, liberties, and privacy against the security of the state. Meanwhile, the surveillance state has rapidly evolved into an intelligence state, capable not only of pervasive data collection, but also of analytical modelling which expands existing boundaries of surveillance. Existing concerns about the ethical collection and use of surveillance data are compounded by three emergent capabilities of the modern intelligence state: persistent data surveillance, pattern-of-life analysis, and activity-based intelligence. The ethical implications of counter-terrorism intelligence extend beyond the collection and use of data to the application of predictive modelling to dehumanised patterns of behaviour. The chapter shows that this process has the potential to redefine the boundaries of the person, particularly by blurring the distinction between thoughts and actions which threaten the state.

Moving to a particular instance of the surveillance state, Michael Clarke explores the ways that the Chinese government has actively integrated "preventative" counter-terrorism policies that uses new surveillance technologies, particular discourses of the "global war on terrorism" with the ideology of the Chinese Communist Party (CCP) in order to negate the very possibility of "terrorism". The chapter argues that

the contemporary situation in the Xinjiang Uyghur Autonomous Region (XUAR) represents not only the mass repression of an ethnic and religious minority by an authoritarian regime but also an example of the dystopian potentialities of ostensibly "neutral" technologies.

Contrasting surveillance technologies, the fourth part, *The Ethical of Technologies that Limit State Power: Encryption Technologies*, details and expands the ways that encryption technologies can be used to limit state power. In part as a counter-weight to surveillance technologies, encryption technologies offer ways for people to avoid certain state surveillance. Seumas Miller and Terry Bossomaier present a discussion of how encryption technologies work and what the ethical implications of such technologies are. Kevin Macnish then presents an ethical case in favour of encryption.

Starting with the recognition that encryption is obviously a good thing since it protects privacy, but potentially problematic as it might unreasonably impede legitimate counter-terrorism operations, Seumas Miller and Terry Bossomaier explore the technology of encryption technologies. The chapter begins with a general overview of core ethical values relating to encryption and information technologies; privacy, confidentiality, autonomy, and secrecy. It then goes on to show how encryption technologies function. This then allows the final argument of the chapter, a discussion of the privacy rights and security needs in relation to encryption in the overall context of the counter-terrorism policies of liberal democratic states.

Kevin Macnish's contribution looks at end-to-end encryption, a relatively common technology, that has become even more widespread on mobile phones operating over the Internet. This has provided tools for terrorists to plan activities that lead directly to the deaths of innocent civilians. At the same time, it has also been used by dissidents challenging totalitarian regimes and holding liberal democracies to account. The chapter argues that while terrorist use of such encryption may render that encryption unjustifiable within a liberal democracy, within an international context the protection that it provides to those seeking to establish law-abiding democracies is too great to be ignored.

The fifth part, *Responding to Terrorism in Cyberspace: Extremism Online*, closes the collection out by looking at how the online environment has changed terrorism and what can be done in the name of counter-terrorism. Alastair Reed and Adam Henschke start this part by looking at the ethical issues around who gets to decide to remove terrorists and other political extremists from online environments. Kosta Lucas and Daniel Baldino complete the collection with an examination of the ways that online manifestos can be treated.

A fundamental challenge to modern liberal democracies is how they balance the capacity for free public communication with the need to curtail terrorist use of social media, in a context where this social media dominates people's lives, public discourse, and even modern politics. Alastair Reed and Adam Henschke ask who should regulate extremist content online. Rather than questions of how this should be done, or what material is relevant, this chapter asks questions of *who* gets to make these decisions and *why*? This chapter suggests that part of the problem with answering "who should regulate extremist content online?" is that there are different aspects to how that content is being regulated. By reflecting on what sorts of institutions and services

are being provided, we can suggest a more nuanced and collaborative approach to the regulation of online content.

Finally, Kosta Lucas and Daniel Baldino take a particular element of online political extremism, to explore identity construction and the usefulness of analysing terrorist manifestos through a narrative framework, with a view to demonstrating that manifestos can be understood as a script to a violent performance (the terrorist act) in the theatre of terrorism (the digital world). The chapter unpacks the dynamic of identity fusion and a specific online terrorist manifesto that coupled with an activist extremist agenda while seeking, in part, to exploit the media in a national security context. The way that this online material is treated has further ethical importance. Media coverage of mass shooters rewards them by making them famous and delivers a clear incentive for future offenders to attack. Instead, the authors argue that if the media modifies how they cover mass shooters, such anticipated changes might be able to deny offenders the personal attention they seek in their quest for significance and help to deter some future perpetrators from normalising violent behaviour.

As with all such projects, there are no simple answers. Moreover, the contributors bring a range of different tools and approaches to these issues, and there is no common consensus on how technologies ought to be used or controlled in the fight against terrorism. This is in part a fact of debates about counter-terrorism, and about technologies, and in part a deliberate feature of the book. These areas are broad, deep, and navigating them is a complex and challenging enterprise. However, there are common threads through the debates—not only must we grapple with terrorism as it evolves, we must also recognise and wrestle with the roles that technologies are playing in the fight against violent extremism. The challenges are considerable, but together we will forge a path to push back the frontiers of counter-terrorism.

References

1. Gunasingham A (2019) Sri Lanka attacks: an analysis of the aftermath. Count Terror Trend Analys 11(6): 8–13
2. Laxman S, Kesslen B (2019) Sri Lanka bombings were retaliation for Christchurch shooting, defense minister says NBC News, April 23, 2019. https://www.nbcnews.com/news/world/sri-lanka-bombing-was-retaliation-christchurch-shooting-defense-minister-says-n997391. Accessed 27 Jul 2021
3. Ingber S (2019) Global effort begins to stop social media from spreading terrorism. NPR, April 29, 2019. https://www.npr.org/2019/04/24/716712161/global-effort-begins-to-stop-social-media-from-spreading-terrorism. Accessed 27 Jul 2021

Contents