Preface

There is, at the risk of understatement, something of a disconnect between the amount of attention that cyberterrorism commands and the clarity with which it is understood. In common with many contemporary security issues—from piracy through to global climate change—the causes of, and scale of threat posed by, cyberterrorism are hotly debated. This is not in itself unusual. Estimations of threat require assessments about the future which are always open to contestation. Estimations of the threat posed by other people—in our case cyberterrorists—are doubly challenging because they require consideration of motives as well as capabilities and vulnerabilities. Thus, the threat posed by an anonymous intruder we encounter in our house is a combination of several factors including: the intruder's determination to cause us harm, her possession of the physical and other capabilities required to bring that harm about, our ability to defend ourselves against any attack and the potential scale of the damage she is capable of inflicting. Similarly, the threat posed by cyberterrorism—to us as citizens, to governments, to corporations and so on—encapsulates both the determination and capabilities of would-be 'cyberterrorists' as much as it does the vulnerability at any of these levels to such an attack.

So far, so straightforward. What is, however, a little more peculiar of cyberterrorism specifically is the absence of any real agreement on the still more fundamental question of what, exactly, cyberterrorism is. While the precise nature and parameters of potential challenges to the security of people or communities such as war, terrorism or poverty are, of course, contested, there is, it might be argued, some level of shared agreement around that to which these refer. We might debate the merits of including the allied firebombing of Dresden within a discussion of terrorism for any number of reasons—because conducted by states, conducted during wartime, and so on—without sacrificing some broad understanding of terrorism as involving violence and causing fear. So contested is the phenomenon of cyberterrorism, however, that a recent survey of researchers around the world found that 49 % believed that we had already witnessed a cyberterrorism attack, with another 49 % arguing that we were yet to do so (Macdonald et al. 2013)! Thus, where many of those attempting to define terrorism are willing to permit some ambiguity

because—as with US Supreme Court Justice Potter Stewart's now-infamous ruling on pornography—'you know it when you see it', the same emphatically cannot be said for cyberterrorism.

The reasons for this contestability—or, less charitably, confusion—are manifold and explored in much greater detail in the chapters that follow. Part of the problem here is that many of the definitional problems associated with terrorism that will be familiar to readers have simply migrated alongside this term's application to the cyber realm. Terrorism is a word that is saturated with negative associations, rendering its neutral or objective application to 'real world' violences a less-than-straightforward task. Similarly, the meaning of terrorism has evolved throughout the 200 years since its first coinage: the term being now nearly entirely stripped of its original association with violences by the state or progressive political causes. On top of this, the sheer diversity of events and campaigns to which the term terrorism is applied—from Oklahoma to Omagh, the Earth Liberation Front to Aum Shinrikyo—means it is increasingly difficult to pinpoint precisely what is meant by those most discussed of contemporary security challenges.

As if this didn't make the task difficult of defining, understanding and analysing cyberterrorism sufficiently difficult, there are, in addition, a host of unrelated challenges that derive from the 'cyber' dimension of this concept. One aspect of this is the challenge of sourcing reliable information about what is happening—or what could happen—in a cyber domain which consists of multiple owners, technologies and actors. Many of these actors, moreover, have an interest in either exaggerating or camouflaging their activities online. This might be important, for instance, if we believe either that (cyber)terrorism involves a necessary communicative element such that its author desires identification, or if we believe that it can only be conducted by certain actors such as non-state groups. Second is the speed with which developments in cybersecurity occur, and the potential impact this has upon previously adequate security paradigms. Established ideas, doctrines and strategies such as deterrence here jostle with contemporary notions such as resilience in a world of new threats including bots, trojans, zombies and worms. While we need to beware of exaggerating cyberterrorism's novelty—let us not forget that more traditional security issues such as war continuously evolve—this pace of change certainly complicates consensus building in relation to cyberterrorism's reality and significance. A third set of challenges—linked to the second—is the seemingly relentless proliferation of new words and concepts by those seeking to capture these developments. Neologisms abound in academic and media discourse around cybersecurity—with cyberterrorism but one obvious example—many of which are characterised by hyperbole and more likely to generate heat than light. Cutting through this hyperbole, and penetrating the jargon associated with cyberterrorism, is a significant challenge for furthering understanding of this contemporary security concern.

The ten chapters that follow have all been contributed by authors with a global profile and recognised expertise in this area. Between them, the contributors have worked on a range of topics of direct relevance to cyberterrorism, stretching from the technicalities of cybersecurity, through to transformations in terrorist violences,

the formulation and politics of counter-terrorism policy and the workings of criminal law. Importantly, the authors come to this topic from a range of disciplinary backgrounds. Where some approach cyberterrorism from a technical or scientific background in Engineering or Computer Science, others ground their analysis in subjects as diverse as Law, Political Science, Criminology, Politics, International Relations and Communications Studies. Although this makes consensus-building harder still, this multidisciplinarity is, we believe, vital for a thorough and balanced conversation around what cyberterrorism is, what threat it poses and how it could or should be addressed.

Background: The Cyberterrorism Project

The immediate background to this book is in an academic conference that was held in the city of Birmingham, UK, in April 2013. Nearly 50 researchers and policy-makers attended this event, arriving from a number of UK universities as well as from other countries including the Republic of Ireland, Israel, Italy, the Netherlands, Romania, Sweden, Greece, Australia and the United States. The focus of the conference was twofold. First, to share cutting-edge research relating to understandings of, and responses to, cyberterrorism. And second, to facilitate the multidisciplinary conversations that run through this book's chapters. The conference built on a smaller workshop on these themes that had taken place in Swansea University, UK, the previous autumn at which several of this book's contributors also participated.

Each of these events—and the book you are reading—was organised under the auspices of The Cyberterrorism Project. The Cyberterrorism Project was established in 2011 by academics who were then working in the School of Law, College of Engineering and Department of Political and Cultural Studies at Swansea University. The reasons for establishing the project were fourfold, each of which continues to underpin the activities of this research team. First, was a desire to improve understanding amongst scientific and academic communities by engaging in original research on the concept of, threat posed by, and possible responses to, cyberterrorism. The project's second rationale was to facilitate global networking activities around cyberterrorism and to bring together researchers from a range of backgrounds with something important to contribute to these discussions. Third was to engage with, and have impact upon, policymakers, opinion formers, citizens and other stakeholders at all stages of the research process, from data collection to dissemination. And, fourth, to try to do all of the above within a multidisciplinary and pluralist context that draws on expertise from the physical and social sciences alike. This multidisciplinary emphasis is one that underpins all of the work undertaken by this research team, and we hope to have captured it in the chapters that follow.

In our view, the multidisciplinary approach that characterises this book adds breadth to its coverage by allowing a discussion of a wider range of topics than would be possible in a more narrowly focused collection on cyberterrorism. Public policy

and the criminal law are, arguably, as essential to the countering of cyberterrorism as more technical mechanisms such as air gaps, cryptography or digital forensics. Bringing together experts with a background in all of these areas therefore increases the comprehensiveness of the book's coverage. On top of this, our hope is that bringing authors from a range of specialisms into conversation with one another also offers an opportunity for new insights to emerge. Ideas and ways of thinking that are familiar in some academic disciplines may be far less recognisable in others. Similarly, knowledge seen as standard or common sense in some areas may be unheard of or even discredited elsewhere. Facilitating discussion between different subject areas, then, may help—amongst other things—to: identify blindspots in thinking on cyberterrorism; highlight factual or logical errors within established approaches to this topic; fill gaps in knowledge caused by disciplinary silos; and produce new questions and research areas from this cross-pollination of ideas.

Core Themes

Given the spread of contributors to this book there is—as one might expect (and perhaps even hope)—much disagreement in the pages that follow. This, in our view, is a good thing, as it enables our authors the opportunity to advance, clarify and defend different approaches to thinking about cyberterrorism and its importance. Because of this, the book has been written around a series of linked objectives rather than an effort to advance one overarching argument. These objectives are as follows:

- To trace and advance conceptual and definitional debates pertaining to cyberterrorism.
- To examine, from political and criminological perspectives, how the cyberterrorism threat has been presented or constructed within political language, legislation and other sites of discourse. Included within this is an effort to explore how these constructions vary across space and time and how they relate to other designations of threat and insecurity.
- To contextualise cyberterrorism in relation to other types of terrorism or unconventional violence. In other words, is cyberterrorism simply terrorism conducted with new types of technology? Or does the presence of cyber technologies fundamentally change the nature and rationalities of terrorism?
- To contextualise and explore the distinctiveness of cyberterrorism in relation to other cybersecurity threats. How, for example, can we separate cyberterrorism from cybercrime or cyber war, and should we attempt to do so?
- To evaluate the threat posed by cyberterrorist attacks to different referents including the state, national security architectures, corporations and individuals. And, in so doing, to explore different frameworks for assessing this threat.
- To chart and assess different attempts to counter cyberterrorism at various levels of analysis, from the local through to the national, regional and global.

- To evaluate the offences which might be used to prosecute cyberterrorists, exploring tensions between the reach of these offences and conventional principles of criminalisation. Important here are the implications of these offences for human rights concerns and other protections and safeguards for citizens.
- To understand how terrorists make use of the global communications network to advance their agendas.
- To evaluate the adequacy of practical approaches to deter, identify and respond to cyberterrorist attacks.

The book has been written in such a way that the following chapters do not have to be read in the order presented. There is a general movement from issues of definition and understanding in the earliest contributions through to matters of threat assessment and response as the book proceeds, although many explore several of these issues at once. Moreover, because contributors to this book come from a range of academic backgrounds and perspectives, the chapters have been written as accessibly as possible. While conscious of the need to avoid simplification, our authors have been assiduous in minimising the use of esoteric language that would be unfamiliar to students or researchers beyond their 'home' discipline. As such, we hope, and believe, that the interested reader with no specialist background will be able to engage with the debates in the pages that follow. To assist this further, each section of the book is followed by a collection of 'key points' summarising the preceding discussion, with each chapter specifying a list of further relevant reading.

Chapter Overview

The book begins with a chapter by Keiran Hardy and George Williams which explores the adequacy of different legal definitions of terrorism in relation to cyber attacks. Focusing on the United Kingdom, Australia, Canada and New Zealand, the chapter asks what uses of computer and Internet technology would qualify as terrorism in each of these jurisdictions. Tracing quite significant differences between them, Hardy and Williams conclude that each of these countries could do more to ensure that their laws appropriately capture the threat of cyberterrorism without criminalising less serious uses of computer and Internet technology.

Chapter 2, by Lee Jarvis, Lella Nouri and Andrew Whiting investigates the ways in which cyberterrorism has been produced—or socially constructed—as a security threat across political language, popular culture and academic debate. The chapter explores a number of very different understandings of cyberterrorism and brings into focus some of the major conceptual challenges that arise when we try to describe cyber activities of different sorts as 'terrorism'. Their response to these challenges is to argue that 'cyberterrorism' already exists as a social reality—in language, culture, academic debate and so on—and therefore avoiding the term offers an unsatisfactory response to its contested and contestable meaning.

As such, they appeal for a refocusing of attention away from the question of *what* cyberterrorism is, and toward the question of *how* cyberterrorism is constructed.

Panayotis Yannakogeorgos in Chap. 3 builds on the preceding discussion by exploring the very different types of activity that occur within the technical realities of cyberspace. The challenges of defining and understanding cyberterrorism, Yannakogeorgos argues, should be grounded in a clear understanding of the vulnerabilities, threat actors and nature of conflict within cyberspace. The chapter contributes a realistic look at the technical and operational facets of cyberterrorism focusing on how terrorists use the Internet to facilitate their operations and how the Internet enables possible attacks ranging from denial of service (DoS) to sabotage of industrial control systems (ICS). The chapter concludes by arguing that cyberspace is an increasingly important environment for state and non-state actors, although the capacity of the latter to fully exploit its potential remains currently limited.

Chapter 4, by Michael McGuire bridges these definitional questions with issues of the level of threat posed by cyberterrorism. Focusing attention on what the 'cyber' prefix does in debates around the cyberterrorism threat, McGuire advances the notion of hyperconnection to describe the contemporary condition in which potential exists to connect with anyone, anywhere and at any time. This, he argues, poses potential for moving toward a more sophisticated understanding of technology and its social importance: one that presents opportunity for a more robust evaluation of the risks that cyberterrorism poses.

Michael Stohl, in Chap. 5, identifies parallels between contemporary discussions of cyberterrorism and cyber war on the one hand, and older discussions of terrorism and state terrorism on the other. As he argues, states condemn 'cyberterrorism' while building up their own cyber capabilities, just as they condemn the 'terrorism' of their enemies rather than theirselves and their allies. This inconsistency, however, is not merely a semantic one. For, the activity of states in the cyber domain means there is a real possibility that the norms required for international cooperation will be, or are being, undermined.

Chapter 6, by Maura Conway, considers four issues that each mitigates against the likelihood of cyberterrorism occurring. These issues relate to the cost factor of cyber attacks; their complexity; their capability for destruction; and their potential for media impact. Focusing on issues of motivation and interest such as these—rather than technological possibilities—is important, for Conway, as a way of correcting the dominance of the 'IT crowd' (Singer and Friedman 2014) within discussions of the cyberterrorism threat. Weighing each of them up leads Conway to conclude that traditional low-tech 'real world' terrorist attacks such as car bombings will continue to be more effective and therefore 'attractive' than their cyber equivalents for some time to come.

Chapter 7 by Clay Wilson continues Conway's engagement with the threat posed by cyberterrorism, although from a very different angle. Wilson not only focuses his attention more closely upon the technological risks posed for critical information infrastructures by cyberterrorism; he is also far less optimistic than is Conway about the likelihood of cyberterrorism's occurrence. For Wilson, cyber attacks on critical

infrastructures are the main concern for governments at present. This is, not least, because critical infrastructures are increasingly dependent on electronically networked control. At the same time, Wilson points out that these infrastructures have numerous vulnerabilities that could be easily exploited by extremists or terrorists. His chapter therefore offers a far more sobering analysis of the potential for widespread cyberterrorism damage than Conway's which precedes it.

In Chap. 8, Tim Legrand brings a public policy perspective to this discussion that focuses specifically on the importance of governmental responses to cyberterrorism. His chapter concentrates on the UK example, and illustrates the range of institutions and actors mandated with addressing cyberterrorism and related threats. His chapter argues, first, that the UK government's conception of cyberterrorism has been limited, not least in its eliding the differences between cybersecurity challenges. And, second that the post-privatisation attempt to deal with cyberterrorism by combination of private and public sector institutions generates a tension between the profit-maximising instincts of the former, and the latter's role in protecting the public interest.

In Chap. 9 Lord Carlile QC and Stuart Macdonald continue the question of how to respond to cyberterrorism by focusing on the criminalisation of online activities which are preparatory to acts of terrorism. They examine the tension between, on the one hand, the imperative of prevention and early intervention when faced with the threat of severe harm on a large scale and, on the other hand, the impact on human rights and the rule of law of excessively broad and vague criminal offences. The chapter advocates the use of the principle of normative involvement to both justify the extension of the ordinary criminal law to encompass terrorists' preparatory activities and evaluate whether these offences overreach. It also urges the importance of extra-legal constraints on prosecutorial discretion as a means of limiting these offences' practical application.

In Chap. 10, Gil Ad Ariely brings our discussion to a close by outlining the spectrum of responses available in relation to cyberterrorism, differentiating these according to two dimensions: type and time span. He argues that learning from the past is insufficient as a way of meeting this current threat. Instead, a holistic approach that focuses on the development of adaptive and agile responses to cyberterrorism is needed. Ariely takes this further by arguing that—contra more traditional forms of security framework—deterrence will not be effective in the cyber domain. These evaluations lead Ariely to a proposal for an ecosystem supporting adaptive responses spanning intelligence sharing and education.

The conclusions attempt to bring together all the "lessons" learned from the experts. At this point, definitive answers are few and not really the goal. An ongoing dialogue to share different viewpoints and insights is healthy but it will take time to bridge the differences. A few observations are offered to continue the dialogue.

London, UK — Thomas M. Chen
Norwich, UK — Lee Jarvis
Swansea, UK — Stuart Macdonald

References

Macdonald S, Jarvis L, Chen T, Lavis S (2013) Cyberterrorism: a survey of researchers. Cyberterrorism Project Research Report (No. 1). Swansea University. www.cyberterrorism-project.org

Singer P, Friedman A (2014) Cybersecurity and cyberwar: what everybody needs to know. Oxford University Press, Oxford



http://www.springer.com/978-1-4939-0961-2

Cyberterrorism
Understanding, Assessment, and Response
Chen, T.; Jarvis, L.; Macdonald, S. (Eds.)
2014, XXIII, 215 p. 5 illus. in color., Hardcover
ISBN: 978-1-4939-0961-2